

**SOLENT UNIVERSITY SOUTHAMPTON**  
**FACULTY OF BUSINESS, LAW AND DIGITAL TECHNOLOGY**

**MSc Cyber Security Engineering**  
**Academic Year 2021-2022**

**“Is vendor malware present in Solid State Storage Devices available  
through E-commerce.”**

**Helen Plews Q15520625**  
**September 2022**

**This project is submitted in fulfilment of the requirements of Solent  
University for the degree MSc Cyber Security Engineering.**

## Table of Contents

GLOSSARY OF TERMS .....	4
ACKNOWLEDGEMENTS .....	5
ABSTRACT .....	5
RESEARCH QUESTION AND AIM.....	5
CHAPTER 1. INTRODUCTION .....	6
CHAPTER 2. PILOT STUDY BACKGROUND.....	8
2.1 E-COMMERCE PRODUCT SAFETY .....	8
2.2 MALWARE .....	9
2.3 VENDOR MALWARE.....	11
2.4 SUPPLY CHAIN .....	13
2.5 DIGITAL BLACK & GREY MARKETS.....	13
CHAPTER 3. PILOT STUDY METHOD .....	15
CHAPTER 4. PILOT STUDY RESULTS .....	16
4.1. AUTOPSY RESULTS .....	17
4.2. BINWALK RESULTS .....	18
CHAPTER 5. PILOT STUDY DISCUSSION .....	18
5.1 PREVIOUS WORK .....	19
5.2 MALICIOUS USB DEVICES .....	19
5.2 PUBLIC AWARENESS.....	20
CHAPTER 6. PILOT STUDY RESULTS .....	21
CHAPTER 7. PILOT STUDY CONCLUSION .....	23
CHAPTER 8. RESEARCH STUDY INTRODUCTION & BACKGROUND.....	24
8.1 BACKGROUND .....	24
8.2 PREVIOUS STUDIES.....	26
8.3 MICROCODE MALWARE .....	29
8.4 OUTSOURCING AND MANUFACTURING RISKS .....	30
CHAPTER 9. RESEARCH STUDY METHOD .....	31
CHAPTER 10. PHASE 1 FORENSIC TESTING METHOD .....	33
10.1. PHASE 2 FORENSIC TESTING METHOD.....	34
10.2. PHASE 3 FORENSIC TESTING METHOD.....	35
CHAPTER 11. RESEARCH STUDY RESULTS .....	35
11.1. PHASE 1 FORENSIC TESTING: AUTOPSY & BINWALK SCAN RESULTS .....	36
11.2. PHASE 2 FORENSIC TESTING: PACKET COLLECTION & ADVANCED MONITORING TOOLS.....	39

11.3. PHASE 3 FORENSIC TESTING: ADVANCED MONITORING SOFTWARE .....	43
CHAPTER 11 WHO ARE THE VENDORS AND WHERE ARE THEY MANUFACTURED? .....	48
11.1. MADE IN CHINA.....	50
CHAPTER 12 MITIGATION .....	52
12.1. MANUFACTURING AND OUTSOURCING .....	53
12.2 THREATS TO ALLIED DEMOCRATIC VALUES.....	54
12.3. SAFE ONLINE SHOPPING SAFETY AND SECURE PACKAGING .....	56
12.4 CAN PUBLIC AWARENESS PREVENT THE PURCHASING OF SOLID-STATE STORAGE DEVICES VIA E-COMMERCE? .....	58
12.5 PUBLIC EDUCATION .....	59
12.6 PUBLIC ENGAGEMENT .....	60
12.7. UPDATING E-COMMERCE LEGISLATION.....	61
CHAPTER 13. LIMITATIONS .....	61
CHAPTER 14. FURTHER RESEARCH .....	61
CHAPTER 15. CONCLUSION .....	61
CHAPTER 16. REFERENCES .....	62
APPENDIX 1. USB PACKAGING.....	70
APPENDIX 2. UNALLOCATED BLOCK RESULTS .....	75
APPENDIX 3. DELETED FILES & MATCHING FILES .....	78
APPENDIX 4. BINWALK AND ENTROPY RESULTS .....	78
APPENDIX 5. USB DEVICES IN RESEARCH STUDY .....	81
APPENDIX 6. VENDOR CORRESPONDENCE .....	86
Appendix 7. AMAZON STORE RESEARCH .....	92
Appendix 8. KINGSTON & SANDISK CORRESPONDENCE .....	98
BIBLIOGRAPHY .....	100

## GLOSSARY OF TERMS

USB- Universal Serial Bus  
USB device- in reference to a USB device  
USB port- Host USB port  
OS- Operating System  
CPU- Central Processing Unit  
VHD- Virtual Hard Drive  
HID- Human Interface Device  
USB plug- The host connection for the USB device  
USB protocol- Protocol for the USB  
AV- Anti-Virus  
PE- Portable Executable  
DHCP- Dynamic Host Configuration Protocol  
DNS- Domain Name Server  
RAM- Random Access Memory  
JS- Java Script  
ISA- Instruction Set Architecture  
CD- Compact Disks  
NSA- National Security Administration  
US- United States of America  
GCHQ- Government Communication Head Quarters  
NATO- North Atlantic Trade Organization  
NCSC- National Cyber Security Agency  
TCP- Transmission Control Protocol  
UDP- User Datagram Protocol  
ONS- Office of National Statistics  
PPE- Personal Protection Equipment  
WSL- Windows Sub Linux

## ACKNOWLEDGEMENTS

I would firstly like to thank all those who have helped me with childcare during the long hours of work. I would like to thank my children for being as good as possible and for their support. I would like to acknowledge the wonderful support of the information security community and for the advice from the research team at Ruhr University. My cohort for the friendship and support, may it continue. Lastly, this project would not have been possible without the highly skilled and dedicated academics and support staff at Solent University in particular my supervisor Dr. Andy Farnell for all the fantastic teaching, support and for pushing me to achieve things I would not have imagined possible.

## ABSTRACT

The solid-state storage device, Universal Serial Bus (USB) was forensically examined to determine the presence of any vendor malware. Results indicated the presence of firmware malware in 63% of inspected devices, located in the machine code of the unallocated spaces of the storage device. Intel x86 Microcode was identified by forensic binary examination software as being present in the binary, which has been shown to infect a host with malware. The signatures were extracted and contained the same files and folders across several devices, with entropy scans consistent with encrypted files. Lab tests showed the infected devices performed several activities related to the presence of advanced malware, such as a modification to the Telnet client and the adding of a third-party root certificate upon connection to the internet. Vendors were contacted and registered companies researched revealing inconsistencies, suspicious trading practises with links to China in all parts of the production chain, including having 34 IP addresses associated with the SHA 1 of the third-party root certificate. The cyber-cold war with China was investigated to determine the risks associated with the findings and mitigations with education, local production, and skilled forensic product testing.

## RESEARCH QUESTION AND AIM

Is vendor malware present in solid-state storage devices available through e-commerce platforms? The aim of the research is to answer the question using digital forensic testing and dynamic malware analysis to identify the presence of malware within USB devices. The devices were purchased via e-commerce platforms where

the safety of goods is questionable, with highly accessible and convenient products governed by the e-commerce laws.

## CHAPTER 1. INTRODUCTION

E-commerce offers consumers the convenience and ease of shopping anywhere at any time for virtually all goods. This includes computer equipment such as solid-state storage devices that are readily available online from both legitimate shops that offer online services as well as e-commerce platforms such as Amazon, and eBay. Solid-state storage devices sold via such platforms are not able to guarantee the safety of the devices leading me to hypothesise that there may be preinstalled vendor malware on the devices. This study investigates if there is a possibility that vendor malware is present on such devices and public awareness of the cyber-security risks associated. This will reveal if a full research study should be undertaken to discover how large the matter is, how the malware is installed, by who and their intentions as well as a risk assessment and mitigation plan.

There is a myriad of solid-state storage devices offered through e-commerce with the leading platforms being Amazon, the first web store launched in 1995 (Rokicki 2018, p.2) and the colossal eBay, with innumerable UK transactions taking place monthly. E-commerce is the process of purchasing and selling products, services, and information through a computer network with activities such as sales carried out in internet auctions via webpages and electronic mail, which was developed in the early 1990's (Rokicki 2018, p.1). E-commerce has flourished since the early 1990s with the internet and became a part of daily life by the turn of the millennium with Amazon turning over billions in profit each year. With the development of smart phone technology, applications were built alongside the web stores improving accessibility and convenience for consumers as well as vast profits for platform-based companies. The increased pace of e-commerce was associated with shifting financial and human resources to the activity, forcing sceptical enterprises to also invest, with a rapid increase post-2005 aided by the development of mobile applications and improvements in electronic payment and distribution systems (Rokicki 2018, p.2). Global e-commerce sales reached roughly \$3.563 trillion in 2019, with the UK being in third place behind China and the US with \$137.08 billion in sales which was up 11% from 2018, by the end of 2022 the 4 top five markets will represent 85% of the worldwide e-commerce sales (Koch 2019, p.1).

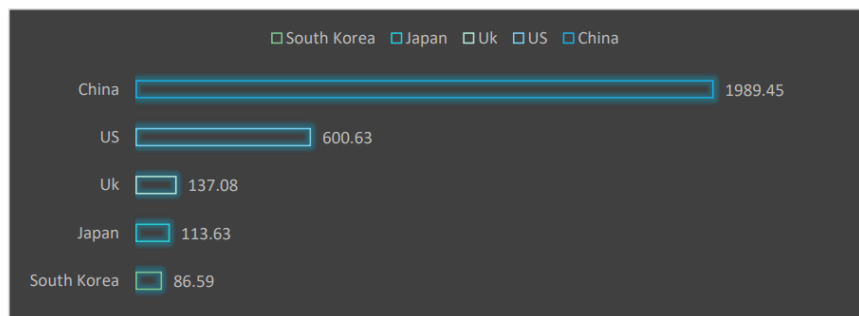


Figure 1 (Koch 2019, p.1)

The UK is the third biggest market for e-commerce with Amazon and the Amazon Prime, a subscription based fast delivery service being a key driver in its expansion and why this study will focus on their products as well as the second UK giant eBay. UK predicted e-commerce growth will come from Amazons burgeoning presence in the countries neighbouring markets benefitting consumerism in the UK with Prime being a core to their European expansion with half of internet users in the UK holding a Prime account as of 2018 (Rokicki 2018, p.3). Unfortunately, many of those signing up may have been deceived into doing so (Fingas 2019), implying the dominance Amazon has over the market may have been achieved with unethical business practises.

In the latest figures from The Office of National Statistics (ONS) (ONS 2022) the UK's online retail attributed for 26.4% of all retail with the total weekly sales being £2183.8 million for April 2022, this is around the mean average of £2161.1 million a week for 2022. The total number of computers and telecoms equipment sold in 2021 in the UK equates to 0.73% of all sales. Using the ONS (ONS 2022) figures from the year 2021 for online retail goods sold over the year it's possible to calculate that £94.4m was spent on these goods online in 2021. Some of these will be from official retailers but smaller devices are far quicker to deliver to households, with Amazon Prime offering next day delivery on many small electronic goods and with half the UK having the service as of 4 years ago, it's safe to assume there is a financially robust marketplace in the UK for e-commerce retailers offering solid-state storage devices.

The solid-state storage devices such as thumb drives, external hard drives, and SD cards are readily available for fast delivery from hundreds to thousands of sellers in both marketplaces that do indeed reflect the expected, due to the large computer sales figures. Figure 2 illustrates the results of each product from Amazon and eBay

that were found to be available to the average sized UK city of Southampton, which lies in the centre of cities in the UK by population size (City Mayors Statistics 2021).

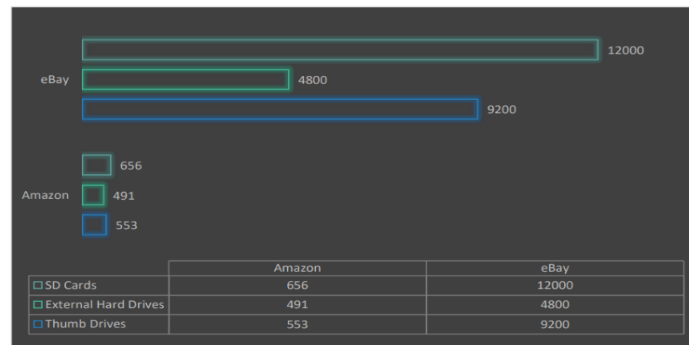


Figure 2

Both platforms show a higher rate of SD cards available for purchase with thumb drives sitting in the centre, there is also a substantial difference in the number of products available on each website as eBay focuses on allowing anyone to become a seller whereas Amazon promotes only businesses. The study will focus on thumb drives as they sit in the middle of the available solid-state storage devices, receive high sales, and offer substantial storage space of up to 2tb, to potentially hide malicious content.

## CHAPTER 2. PILOT STUDY BACKGROUND

### 2.1 E-COMMERCE PRODUCT SAFETY

Product safety concerns have increased with the rise of e-commerce platforms with regulation not updated to mitigate the complications. The rise of the power actors such as Amazon and eBay as well as their influence has created controversy with the accompaniment of demands for stronger regulation and public accountability with allegations of privacy violations, abuse of market power, unfair commercial practises, allowing electronic manipulation, facilitating copyright piracy and counterfeit sales (Ullrich 2021, p.32). Consumers trust the platform for e-commerce but there is often no support or liability for the products sold, therefore the trust is misplaced. Consumers often see the platforms as a dependable channel for purchases, online marketplaces have been criticised for lack of communication and not taking responsibility when something goes wrong (Duivenvoorde 2022).

E-commerce continues to develop, and the sale of noncompliant and unsafe products online has been identified as a growing problem impacting consumers potentially putting health and safety at risk with the sale of counterfeit goods (Ullrich 2019,



p.2). Regulation is problematic due to the globalisation of e-commerce whereby products made outside the UK are sold on a platform also based outside of the UK, and therefore outside of our laws and regulations. A further complication being, online marketplaces are exempted from liability for the products they sale under the E-commerce directive (Duivenvoorde 2022). This exempts the platforms from liability of unsafe, illegal, or counterfeit goods as they are considered the technology provider, with the responsibility placed on the seller, who are often outside of the UK and its laws. Less than a year ago the government via the Office for Product Safety and Standards issued a warning for product safety in online marketplace. They advise the platforms are often using third-party sellers, with a checklist to follow with steps including awareness of the seller's address, reputation, and contact details with advice to avoid sellers from overseas. As more shoppers use online platforms so too do unscrupulous sellers, supplying unsafe products and offering no support when things go wrong, with over 10,000 unsafe products taken down from the platforms in 2021 alone (OPSS 2021).

There is also coverage from the national press for further public awareness. Online marketplaces are a hotbed for risky electronics says a group of consumer watchdogs and safety groups, with companies such as Amazon, eBay, Wish and AliExpress held most responsible for unsafe listings which are continuing due to gaps in the law, which mean they are not held to the same standards as high street stores with no responsibility for the safety of products sold to millions due to third-party sellers which the websites facilitate (BBC 2021). The charity Electrical Safety First published an open letter to the government to warn that existing legalisation is inadequate and subsequently consumers continue to be at risk from dangerous electronic goods sold online (Electrical Safety First, 2021). Which? published its findings on online safety in 2020 which showed 66% of the 250 products brought from online marketplaces failed safety tests (Which? 2021). The background clearly shows high level of risk in the products sold from online marketplaces, particularly in electronic goods that are below current safety standards, putting the health and safety of consumers at risk.

## 2.2 MALWARE

Any software that intentionally executes malicious payloads on a victim's device on computers, smart phones, computer networks etc is considered malware, criminals have started to commit crimes online in particular using malicious software to launch

cyber-attacks to such devices (Aslan and Samet 2020, p.1). There are numerous families of malware which can lead to a cyber-attack which are explored in figure 3 and are all types of malicious software that can result in serious consequences for the victims and the world-wide economy. Each malware family is designed to affect the victims devices in different ways such as damaging the targeted system, allowing remote code execution, and stealing confidential data, the sophistication and cost of malware on the world economy is increasing with the approximate annual cost of \$6 trillion in 2021 and the creation of 1 million files per day (Aslan and Samet 2020, p.1-2).

Classification	Definition
<b>Virus</b>	Infects computers by replicating itself, it cannot exist independently so it must attach itself to other executable files and applications where it spreads across files, computers and systems through the network causing system performance degradation and denial of service attacks.
<b>Worm</b>	Malicious code that can exist independently they propagate by replicating itself through storage devices and emails creating multiple copies of itself consuming network and computer resources causing system degradation.
<b>Trojan Horse</b>	Hides malicious code inside a legitimate software application or program which is harmful which does not replicate itself instead is often downloaded by the victim and is often used to steal sensitive data, observe users, delete and modify data.
<b>Rootkit</b>	Is a malicious code that can take control of the operating system by hiding itself or by making a safe environment for other malware to trick virus scanners into masking its true behaviour and considering them normal applications.
<b>Spyware</b>	Spyware is used to watch users and to steal personal or company information, it is installed secretly to collect vast amounts of data and send it back to the creator, sometimes big companies such as Google make use of spyware to monitor consumers.
<b>Adware</b>	Adware installs advertisement software without the permission of users interrupting current activities for the benefit of financial gains leading the degradation of the systems as with the other forms of malware.
<b>Cookies</b>	A text file that contains stored information by the web browser on the users and systems they interact with for future use these are leaving footprints of machines and users as well as becoming dangerous alongside spyware.
<b>Sniffers</b>	These will monitor and record network traffic they analyse different fields of packets and collect information in preparation for a malware attack.
<b>Botnet</b>	Malicious software that allows an attacker to take control of the infected computer with a network of controlled computers controlled by hackers will be used for malicious activities without the knowledge of the user and often used for denial of service attacks, spamming and stealing information.
<b>Keylogger</b>	A type of spyware used to record keystrokes on the devices such as login credentials and personal information.
<b>Spam</b>	Or junk emails, a form of nuisance emails that cause system degradation.
<b>Ransomware</b>	Among the highest threat for industry where a malicious software will take control of the device encrypting the data, stop applications and can stop the OS until their demands are fulfilled usually in the form of a crypto-currency payment.

Figure 3(Tahir 2018, p.4-5)

To counter malicious attacks there is a need to detect malware as early as possible to prevent execution and while it is usually straightforward to detect known malware, the main problem is handling unknown code (Ori Or-Meir, et al 2019, p.2). Virus scanners and anti-spyware applications can detect most infections and mitigate

known viruses by their signature; the code they contain, but when it comes to unknown signatures or advanced malware that can obscure or change the signature then it becomes significantly trickier to detect, figure 4 explores ways that malware can avoid detection.

Method	Definition
<b>Encryption</b>	Camouflaging the code by using encryption with a different key each time which enables the concealment of the malicious files as the data will remain in hidden files until the decryption process takes place on the entire file, this can avoid antivirus detections and static code analyses as well as delaying investigation.
<b>Oligomorphic</b>	Akin to the encryption technique but it uses a unique decryptor with each infection and is also known as semi polymorphic.
<b>Polymorphic</b>	These viruses are a combination of the both the Encrypted and Oligomorphic variants in the sense they change the encryption key and use a unique decryptor with each infection. These means they change their appearance with each new infection making detection particularly challenging.
<b>Metamorphism</b>	This is where the content of the malware itself is altered to remain undetected, they do this by changing their syntax on each new copy while semantics remain the same.
<b>Instruction Replacement</b>	This is where instructions are replaced with other instructions that's have the same meaning much like synonyms in language which obscures their detection.
<b>Register Reassignment</b>	This technique will help malicious code obscure itself by reassigning the register with every copy without changing the semantics of the virus.
<b>Subroutine Reordering</b>	This is where the code itself changes its order thereby its appearance without altering its behaviour. //Subroutine: mov eax, 0A push ecx //reordering :0A push ecx ,mov eax,
<b>Code Transposition</b>	This technique changes the flow of the instructions of the original code, rearranging such that the sematic does not change, one method is to reorder by random recovering the original at the other end and more effective method is using instructions that are independent and have no impact on other instructions chosen and reordered.
<b>Code Integration</b>	This obfuscation technique is used to integrate or embed itself into a program so it can remain hidden inside its files to remain undetected.
<b>Dead Code Insertion</b>	Garbage code or statements are inserted into the code to avoid detection and they will not affect the semantics of the code.

Figure 4 (Tahir 2018, p.4-5)

There is a chance that advanced malware may be found on the devices to avoid anti-virus scanners on solid-state storage devices, it is mostly likely to be tailored to the solid-state storage device and to the dominating operating systems such as Windows.

### 2.3 VENDOR MALWARE

There are historic instances of vendor malware one such account was a scandal concerning Sony-BMG in which a contractor placed a digital rights management (DRM) rootkit on their Compact Disks (CDs) to inhibit piracy, resulting in damaged devices and offences under the computer misuse act. In 2005 two million computer users learned that software installed on their machines effectively ceded control of their computers to any hackers because of a rootkit which enabled a host of attacks, the

viruses named and XCP were distributed by Sony BMG via CDs brought by their customers (Mulligan and Perzanowski 2007, p.5). This software did far more than prevent piracy and caused public uproar because of the damages, the breaking of trust and the collection of data therefore aptly named spyware. Each time a user played a CD containing the software data was collected including the users IP address, and the title of the CD which was transmitted back to the vendor (Mulligan and Perzanowski 2007, p.9). It is likely that the vendor of the products has a higher incentive to install security software than the label itself, incentive difference made the vendor more likely than the label to accept security risks and push DRM software onto more computers (Halderman and Felten 2006, p.3). It caused an enormous public uproar for two main reasons: Users did not expect to find CDs containing software so were less willing to except it and the harmful aspects of the DRM and it was installed deliberately by the vendor and by extension Sony-BMG putting customer security and privacy at risk (Halderman and Felten 2006, p.25).

Two controversies from the US have contributed in raising awareness of malware introduced by vendors: speculation that there is malicious functionality in telecommunications equipment placed there by the Chinese government to eavesdrop of western networks which could potentially control operations and Edward Snowden's evidence that the National Security Agency (NSA) worked with leading communications companies to facilitate mass surveillance (O. Lysne et al. 2016, p.1). Vendor malware is often hidden in the complier of the source code or in further software updates that add inactive malware (O. Lysne et al. 2016). Vendor malware poses an acute problem in its detection and mitigation. Protecting software solutions from malware attacks initiated by vendors is a daunting task as detecting malicious functionality by reading source code is futile and full reverse engineering of the code is incredibly time-consuming (O. Lysne et al. 2016, p.7). Malware is also present in second-hand devices with the NSCS proving guidance on how to wipe data correctly as well as buying guides aimed at reducing the risks of purchasing (NCSC 2020). This does not go far enough with no mention of cyber security a privacy risks, especially as the UK's official civil cyber-security protection body as this study will look at further. However, there is comprehensive advice from private organisations such as we live security who state that there is no reasonable way of knowing if the seller installed malicious code on second-hand devices in an effort to defraud you with such things as keyloggers or a form of data stealing malware (Owaida 2020).

## 2.4 SUPPLY CHAIN

A cyber supply chain is a network of IT infrastructure and technology used to connect, build, and share data in virtual networks which have enabled new forms of risk un-connected to physical products or their location (Ghadge et al. 2018, p.3). There are examples of cyber-security risks found in the physical supply chain of computing devices as well as risks in the cyber-supply chain in the form of software. There are risks associated with the presence of counterfeit products, assemblies, and software in the supply chain; Dell accidentally shipped malware infected components in 2010, HP shipped malware infected switches in 2011 and Microsoft found pre-installed malware on new computers in 2012 which illustrate the need for stronger procurement, manufacturing and distribution of products containing software (Pandey et al. 2020, p.12). Four critical challenges for the management of supply chain cyber risks are: inter-organisational collaboration; employee knowledge, continuous improvement, and the need for government involvement (Ghadge et al. 2018, p.32).

## 2.5 DIGITAL BLACK & GREY MARKETS

There is a robust digital black market that supports criminal activity including the buying and selling of data and all manner of illegal materials, products, and services. Dark web marketplaces are commercial websites trading in illicit goods accessible via darknet browsers, they trade in drugs, weapons, fake ID, and stolen credit cards as well as scam sales and hacks (ElBahrawy et al. 2020, p.1). Dark markets operate like eBay, Gumtree or Craigslist on which they offer their products, service and prices with customers requesting shipping and leaving reviews which operate outside the reach of the law (ElBahrawy et al. 2020, p.2). Almost a quarter of all dark market products are hacking associated on average as seen in figure 5. The most common and severe malwares are zero-day threats, DDos services and exploits (Cherqi et al. 2018, p.81).

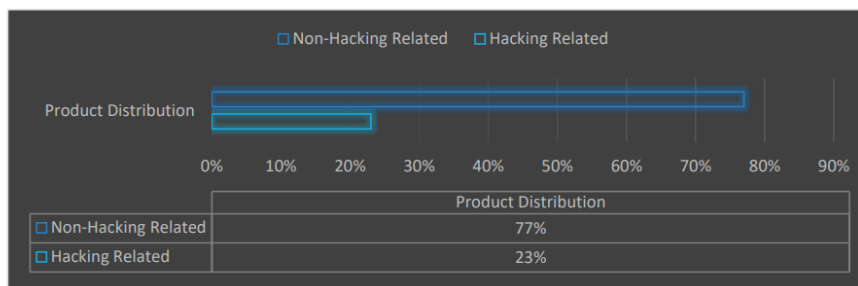


Figure 5 (Cherqi et al. 2018, p.82 )

Figures 6-8 show examples of dark web marketplaces.

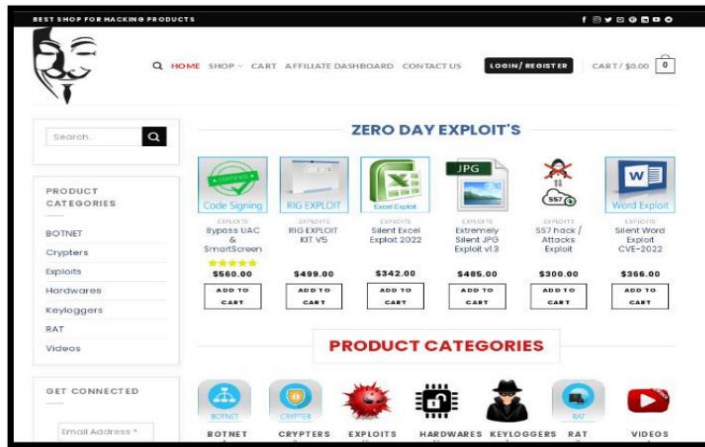


Figure 6 (Anon 2022)

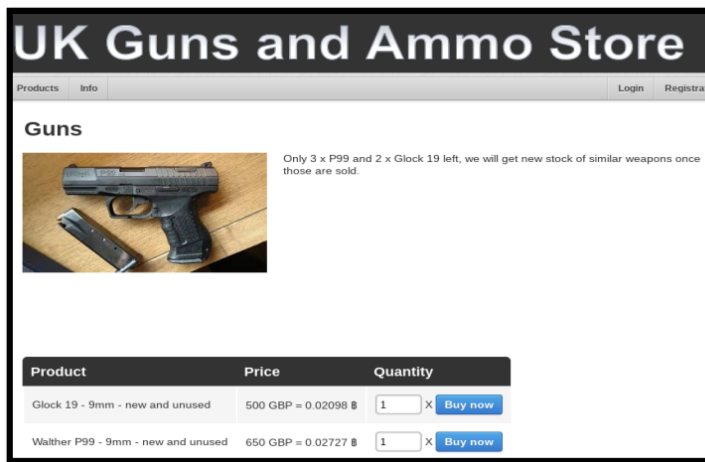


Figure 7 (Anon 2022, UK Guns and Ammo)



Figure 8 (Anon 2022, UK Passports)

The grey market was touched on earlier when examining e-commerce laws, in that each country has differing laws that regulate the sale of goods, including those that may be illegal in some and not others, making regulation on the internet extremely problematic due to its globalisation. A grey-market good is one sold lawfully in state A but imported into state B without the consent of the owner of the intellectual property, they are akin to internet packets as offshore products that are illegal within the regulating country (Goldsmith 2000, p.3).

### CHAPTER 3. PILOT STUDY METHOD

A systematic method was used to find the background research using PRISMA; unless discussing historical events, all sources are no older than 5 years in age for relevancy. The Pilot study will look at existing evidence, including an infected Windows device to examine if there is existing evidence of malware in the USB device. Recovery of previous or existing data, timeline analysis, unallocated storage block inspection, binary firmware analysis, random data testing and entropy scans were carried out with the use of write-blocking technology to limit contamination of results.

This will determine if further forensic analysis of solid-state USB devices is necessary in a full research project to further test the hypothesis of the existence of malware. Confirmatory research with a quantitative method was implemented. Firstly, a write blocker was applied so any software on the USB device could not interfere with the host computer system, which could have caused inaccurate results due to possible contamination. The write-blocker is an intermediary device that will allow the user to read, write and edit the data on the connected device but is purely a one-way connection and the device itself cannot read, write or edit any files on the host computer, meaning any infected devices would not be able to infect the host.

Secondly, the USB devices were copied to a virtual hard drive (VHD) and scanned with forensic software Autopsy, to examine the internal file system and history of the device to determine any hidden data or activity.

Lastly, if the drives were under the size of 1TB, they were inspected for any signatures of images, encrypted or embedded data hidden in the binary or machine code to look for encrypted or suspicious files that may contain malware. Signatures were then statistically analysed to omit false results with the use of entropy scans.

Following this method for my results for each device lowered the risk of contamination from the host system and used Bayesian statistical analysis to calculate the false positive rate for result confidence.

#### CHAPTER 4. PILOT STUDY RESULTS

Firstly, an infected computer was analysed leading to the hypothesis that USB drives from online marketplaces contain vendor malware. I suspected a problem with the computer due to side-channel sound of excessive CPU usage which is not related to usual activities. Figure 9 illustrates the Windows device manager where a second disk drive had been located on the device with an almost identical name.



Figure 9

Figure 10 illustrates the date in which the drive changes were made and the events that took place in the log, which matches to around the time the USB stick was used in the laptop. No further changes, new software or external links were detected as the device has full parental spyware and locks.

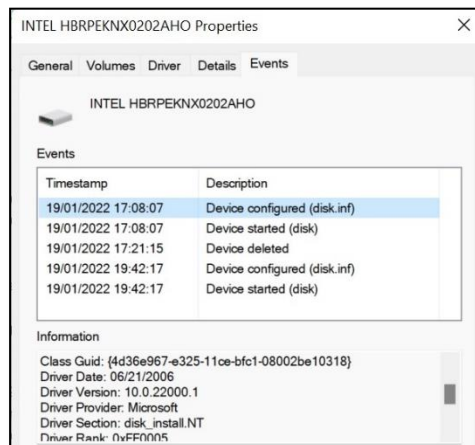


Figure 10

Windows OS was reinstalled deleting all data and restoring from a clean image as well as deep virus scans. It showed no viruses present in the system, but the hardware changes remained after reinstalling the operating system, disabling, and later deleting the drive was the solution. After a full review of the device's



activities, it was intriguing that the only outside element seemingly introduced was the USB device, although this could have happened another way, it was worth an investigation into solid-state storage devices to test the theory.

#### 4.1. AUTOPSY RESULTS

The pilot study was tested on 4 USB devices of varying sizes ranging from 8GB to 1TB, 2 from eBay and 2 from Amazon were inspected firstly with the software Autopsy, a forensic tool to inspect the device internally for any hidden or deleted data. The 4 USB devices are shown with their packaging and purchase details in Appendix 1 and all featured in the top search results on the platforms. The Netac device (USB 1) that was previously purchased was purchased again from the same store from Amazon as well as a new SanDisk USB (USB 2). Two USB devices were also purchased from eBay, a Ceramere USB (USB 3) and an unbranded USB (USB 4). The autopsy results showed that USB 3 contained expected results for an empty USB drive as it contained only unallocated blocks equating to 100% of the device, the blocks were all either fully off or on in the HEX as expected and there was no sign of the drives being accessed after their creation or any deleted data USB 1, USB 2 and USB 4 all contained data as shown in figure 11.

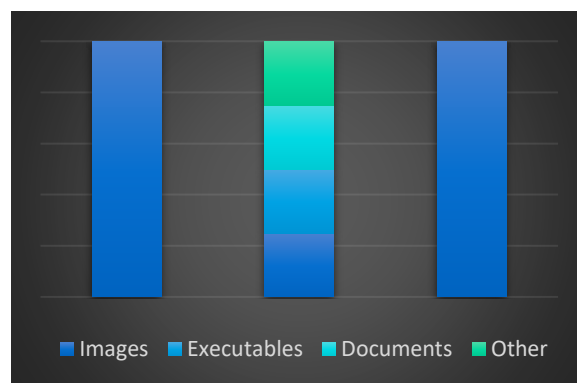


Figure 11

The 3 USB drives internal CPU showed they had all been accessed after they were created with data transfer taking place between 2018- 2021, often sometime before purchase with multiple entries.

USB 2 unallocated blocks were set to off, as seen in appendix 2 but did contain an image, a PDF image and a installSanDisk.exe all of which were checked with the extensive anti-virus Clam as well as researched to reveal that they are safe.

USB 1 had either data or random binary present in the unallocated blocks as seen in the HEX of those blocks in appendix 1. It also contained 2 deleted files an empty volume label and WPSettings as well as one deleted unallocated space in a separate partition.

USB 4 contained evidence of three deleted video files as shown in appendix 3, showing the USB had been previously used to store data and had multiple entries in the timeline of the internal CPU. USB 1 and USB 4 contained the same image file and MD5 hash as shown in Appendix 3 for the table, this file type was not located in the other devices and did not contain malware.

#### 4.2. BINWALK RESULTS

To investigate the code for any hidden, compressed, encrypted data in the unallocated blocks, inspecting the devices at the binary level was necessary to determine if any suspicious signatures could be detected using the Linux firmware analysis tool, Binwalk.

USB 3 contained no signature matches, showing the same results as Autopsy, USB 2 found only false-positives due to the included software and PDF. USB 4 was not inspected for the pilot study using Binwalk as the extraction process of the 1TB drive was too large to process on current lab equipment and will need further investigation. USB 1 had many signatures with 100% accuracy rate for the firmware signatures and 93.7% rate for the encryption.

Entropy scans were carried out on the sets of random data revealing only one rising edge and on USB 1 there were two with a peak at a slightly lower level as shown in appendix 4. A HEX dump was also carried out to reveal where the HEX has been edited, the beginning of the blocks starts in 0 as expected, then the data is clearly seen in the HEX. There were no raw strings to extract from the binary.

## CHAPTER 5. PILOT STUDY DISCUSSION

The US government has, for years claimed that Chinese companies are building surveillance devices into technology exported to the US, the NSA has also been intercepting and tampering with technical devices in transit since at least 2010, meaning it is likely such attacks are taking place in other states as well against individuals or even on a larger scale (dys2p 2022). Looking at the background

research it is clear there are private and government examples of using spyware in products which are being discovered after circulation such as the U2 and Sony BGM spyware. The Huawei news of the company spying on Pakistan (Britton 2021) and a US intelligence warning to allies is another example of how a company in a foreign country can use technology goods for spying with the inclusion of back doors, a form of malware. The US accused Huawei in 2020 of spying through technology back doors for use by law enforcement, the US shared the knowledge due to Huawei's bid to equip the UK's 5G network stating that the company is a conduit for government spying (Hamilton 2020).

## 5.1 PREVIOUS WORK

Good research has been carried out in this area but mostly focused on files recovered on the device to check if they contained malware. Similar research on the subject showed no results of malware but were limited in their forensic technique. 122 drives were inspected physically and then were tested using Autopsy piece that produced results showing that 68 drives did contain partial or fully recoverable data showing a risk for previous owners as well as buyers but none of these contained malware (Conacher, Renaud and Ophoff 2020, p.7-8). There were limitations to the study in the fact that anti-malware will not scan unallocated spaces on the drives, Autopsy will report how the HEX of the binary appears but that was not investigated further to find signatures in the blocks, leaving a gap to be explored.

## 5.2 MALICIOUS USB DEVICES

Malicious USB devices appeared in 2010 simulating a human interface device (HID) to avoid detection with continued advancement since, a 2017 study reported that 44% of the analysed USB drives contained at least one file that threatened security with malware that could cause irreparable damage to the system and that 11% of protection methods failed to detect them (Kondratev, Gamova and Gurov 2020).

There is also the news that the new Raspberry Robin has been spotted in the wild being spread by USB drives from as early as September 2021. The malware is a Windows malware with worm-like capabilities propagated by the removable USB devices in which it uses the Windows installer to reach out to QNAP-associated domains and downloads malicious DLL with the earliest signs as far back as September 2021, the USB device houses the worm payload posing as a legitimate

folder and then executes a malicious stored file which will allow command-and-control access for external network communication (Lakshmanan 2022).

## 5.2 PUBLIC AWARENESS

I looked to public awareness to see if there are tech experts and hobbyists who have investigated USB devices. *I Bought a \$3 2TB USB Drive and Got More Than Just Malware* (Jays Tech Vault 2020) was one such source. The investigator copied files to a USB bought from eBay to ascertain if the space allocation was correct but returns to find all of the data from the host computer missing. This led him to conclude many times, that he was attacked with malware from the USB device. Although this is in no way a conclusive it is indictive that he may have suffered a form of malware attack, in particular a Ransomware attack like MongoLock (Camacho 2019).

Bad USBs are SCARY!! (NetworkChuck 2021) is a guide on bad USB flash drives, explaining they are the most dangerous device, as an unknown USB can hack you in a multitude of ways directly (NetworkChuck 2021). He explains a large number are Rubber Ducky USB devices which convince the host they are a keyboard to avoid detection, they run a Rubber Ducky script, of which there are many some indeed are very dangerous (Kitchen 2022). By convincing the host machine that it is a HID device it can perform a multitude of dangerous tasks using the scripts that are easily added to the device, whilst remaining undetected by disguising itself as an ordinary HID. There is a strong market and manufacturing process already in place for infected USB devices. The design of the Rubber Ducky USB is the same as USB 1, and many others sold online as shown in figure 12, this make determining a Rubber Ducky USB by sight difficult.



Figure 12 (Mudiyanto 2022)

There seems to be public awareness among the technical community and a suspicion USB device sold online contain malware. However, it seems from the daily sale figures of the USB devices in the study that the larger public may be unaware of the assumed danger that the technical community openly discuss. The problem is, there is no general public awareness of the risks (Conacher, Renaud and Ophoff 2020, p.7-8).

## CHAPTER 6. PILOT STUDY RESULTS

USB 4 showed it had been used to store video data and is not a new device, it was sent via the eBay seller in a zip bag with a serial number sticker on it. It is unlikely to have come directly from a factory and is instead being sold after being used by the seller as there were deleted video file evidence discovered. People are advised not to plug someone's used drive onto their own computers as due to past attacks such as Stuxnet which was installed via a USB, cases of drives being left deliberately to entice users showing this is a likely actor vector and the fact that seller might also sell a drive with malware on it (Conacher, Renaud and Ophoff 2020, p.2). The 1 TB drive with the deleted files was too large to be investigated during the pilot study and would need a full study to look further at this possibility.

Unallocated blocks are significant because they are the storage spaces used to store the data on all storage devices. The unallocated space on a hard drive can contain valuable evidence, looking at the file headers and footers can lead to signatures that can be used to identify the file (Sammons 2012, p.65). USB1 had HEX values in the unallocated blocks which were randomised and may have contained data, so a binary scan was performed with Binwalk, which identifies the header of each block of data comparing it to a vast library of headers.

There were a total of 129 identical algorithmic signatures of the same algorithm of encryption in the binary and 2652 blocks of firmware updates in large blocks. There were also many false positives so using statistical analysis to omit false positives was required. A set of random data of varying sizes was created to run simulation tests on for comparison data, so the accuracy rate could be calculated with the results shown here compared to USB 1.

### ENCRYPTED SIGNATURES

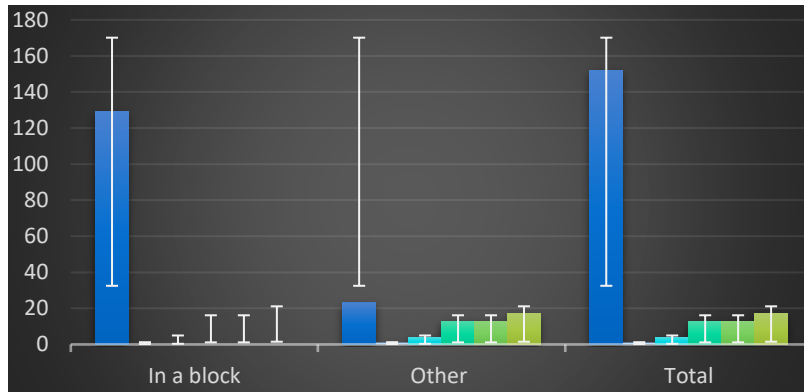


Figure 13

The results show that encryption signatures are not featured in a large block in the binary and that the results exceed the standard deviation, with a 93.7% accuracy rate.

### FIRMWARE SIGNATURES

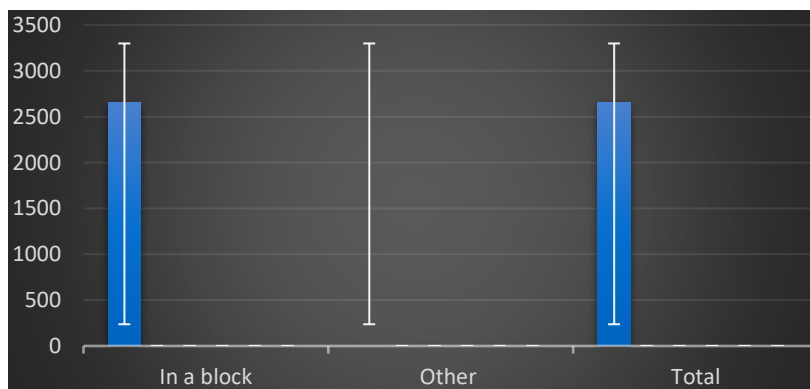


Figure 14

The firmware updates are not produced in random data sets showing 100% accuracy rate for the signatures proving that USB1 contains firmware signatures. There was a 93.7% accuracy rate on average for the encrypted signatures, in fact using prediction data on the random sets a total of approximately 900 GB of random data that would be required to produce the same number of randomly created encryption signatures which would not be found with the same encryption algorithm and far exceed the storage capabilities.

Entropy scans results in appendix 4 show that the data in the unallocated spaces is not random as a second rising and falling edge was detected on USB1 but was not present for any random data sets.

It is highly suspicious if there are visible drivers, firmware, unusable space, partition schemes or explained changes to the disks free space and must be hidden in such a way that the encapsulating file system and OS are unaware of the hidden file systems, even with forensic analysis (Barker et al. 2020, p.1). This was seen in the results above for USB 1 with visible Intel firmware, unusable space of 4GB, and explained changes to the disks space at the binary level. Rendering hidden information indistinguishable from free space is something that deniable storage devices rely by on (Barker et al. 2020, p.2). Hiding firmware and encrypted files inside unallocated blocks is exactly the type of technique deniable storage devices would adopt to hide their file systems from the OS with the use of random data on the disk accompanying the file system as a form of obscurity. Most deniable storage systems attempt to disguise access to the hidden volume by hiding data within other random information (Barker et al. 2020, p.3). The firmware found, the Intel microcode itself can be used to hack the CPU as seen here.

## CHAPTER 7. PILOT STUDY CONCLUSION

Limitations to the study were in lab equipment required to look at the higher sized USB drives, a total of 2 TB of free space would be required and a large amount of time to perform signature and entropy scans which could be included in a full study. Another limitation was the small sample size of the USB drives, although it has found possible signs of malware, it does not look at enough drives to determine the scale of the problem. Looking at multiple drives from the vendor of USB1 would be required in a full study to determine if it is linked to the vendor at the manufacturing end or within the supply chain. Lastly, to determine if malware is present a lab test must be performed on an end device letting the hidden file system of USB 1 run to analyse it as well as any communication.

A full study would be needed to look at the supply chain of the USBs in e-commerce to assess their safety, public awareness and trust to evaluate a solution to the safety issues raised. It could also look at the risks, mitigation and try to determine who is behind the possible malware.

It is clear from the results 50% were found to be safe, 25% were previously used and therefore unsafe, and 25% had an indication of firmware and likely encrypted file systems in the unallocated blocks. Due to the encryption, it has not been possible to

fully determine if the data is malware so further investigation would be required. To determine the presence of malware, dynamic malware analysis at the time the USB devices are in use is required in a sandboxed environment to avoid contamination of results.

## CHAPTER 8. RESEARCH STUDY INTRODUCTION & BACKGROUND

The results of the pilot study concluded on the need for a larger research study to determine if vendor malware is present in solid-state storage devices available through e-commerce by increasing the number of USB devices inspected and increasing the forensic testing methods. The pilot study revealed that one device contained possible data in the binary, the binary was forensically inspected using entropy to determine that it was highly likely that the signatures detected were positive results. The results indicating microcode in the form of central processing unit (CPU) updates were present, as well as encrypted data. A larger study was required to inspect more devices to determine the scale of the problem with the top two e-commerce platforms Amazon and eBay. Dynamic malware analysis was carried out to determine if the possible data in the binary contained malware.

### 8.1 BACKGROUND

The USB device has become vital to consumers for data storage due to the ease of access, relatively low cost, and speeds. Universal serial bus (USB's) has successfully replaced serial and parallel ports due to its high speeds, flexibility and convenience becoming a necessary interface for data interaction between hardware devices but one with risks as the security cases on the USB interface increased also (Sun, Lu and Liu 2021, p.1). There are well known attacks such as The Pod slurping attack, any portable storage device can be used to slurp data from a host such as iPhones, Blackberries, cameras, flash drives, and mobile phones can be altered to elicit desired information (Anderson and Anderson 2010, p.153). The term *pod slurping* was coined to describe how sensitive data was stolen via music players and other USB storage devices, "pod" being any device with its roots in the Apple iPod (Anderson and Anderson 2010, p.155). This was due to Abe Ushers work using an iPod to search local and networked computers to slurp critical data onto an iPod, with the programme situated in the iPod so that when a connection is made to a computer it can be automatically or manually executed to copy data at a rapid speed (Anderson and Anderson 2010, p.155).



the design of the bad USB; discussed in the pilot study, the development of the USB as a simulated keyboard device with wi-fi transmission, the USBee attack obtaining data through electromagnetic radiation channels (Sun, Lu and Liu 2021, p.1). More recently in 2020 Direct Memory Access (DMA) attacks (Sun, Lu and Liu 2021, p.1).

DMA attacks can use peripherals to gain complete access to the state of a computer leading to reading and writing to system memory, Thunderbolt 3 over USB provide opportunities for attacks to be performed with minimal physical access to the computer (Markettos et al. 2019). The external and ubiquity of USB accessibility result in a large attack surface that can be considered in the following categories: exhaustive privileges such as an autorun feature, electrical attacks exploiting physical design flaws by the USB in the host operating system (OS) and software vulnerabilities, all of which have a high security implication and are hard to find (Peng and Payer 2020, p.1). The USB device is read by drivers from the connected USB port using the trusted platform model making them vulnerable for exploit which is highly insecure given their privileged access to the CPU, OS and Kernel. Device drivers run directly from the kernel and are security critical, developers unaware of the risks due to the assumed difficulty of modification, developed host side software with implicit trust in the USB devices (Peng and Payer 2020, p.1). There are few defence mechanisms as a result of the assumption that hardware drivers should be implicitly trusted. Defence mechanisms for protection of vulnerable drivers from malicious USB devices are limited, packet filtering-based mechanism can miss unknown attacks, using Cinch to run the vulnerable device drivers in an isolated environment are not deployed due to complexities and hardware dependencies with fuzzing being viable, if not time and energy consuming (Peng and Payer 2020, p.1).

Alongside driver vulnerabilities there are multiple attack opportunities with USB devices remaining today, although the autorun vulnerability has now been solved via OS updates, electromagnetic radiation is a serious threat to secret-related computers as the USB plug can steal data in network-isolation, buffer overflow vulnerabilities can overwrite the memory of an application, replacing executable code with arbitrary code (Sun, Lu and Liu 2021, p.1-2). There is also the malicious programming of chips where an attacker programs the main control chip supporting the USB protocol specification to emulate as an ordinary device but with malicious

functionality, often emulating as HID, audio devices and ethernet adapters (Sun, Lu and Liu 2021, p.

The USB device is vulnerable to several attack vectors, all with significant implications due to the trusted platform model, giving it direct access to all aspects of the system. The pilot study revealed evidence of firmware signatures and encryption at the binary level in the unallocated blocks of the storage device. The attack surface for the USB device is vast so this study focused on identification using dynamic malware analysis in a sandboxed environment.

## 8.2 PREVIOUS STUDIES

A recent study into USB devices being used to attack air-gapped systems revealed frequent attacks on critical systems and networks. Attacks often use 0-day exploits, social engineering, and logical exploits to bypass all security measures in the most secure networks including bypassing anti-virus (AV), this includes air-gapped networks, in 2008 the Agent. BTZ worm was found to have compromised the US Central Command, Conflicker was next exploiting removable devices allowing it to propagate on hosts with no network access including a nuclear power plant in Korea (Guri 2021, p.1). Stuxnet is a well-researched attack that occurred in an Iranian nuclear plant via a worm in 2010 that was propagated by USB storage devices through secure networks and in 2017 the Copperfield malware infected critical national infrastructure in the middle east (Guri 2021, p.1). USBCulprit found by Kerpersky in 2020 is of particular interest with the runtime structure in figure 15.

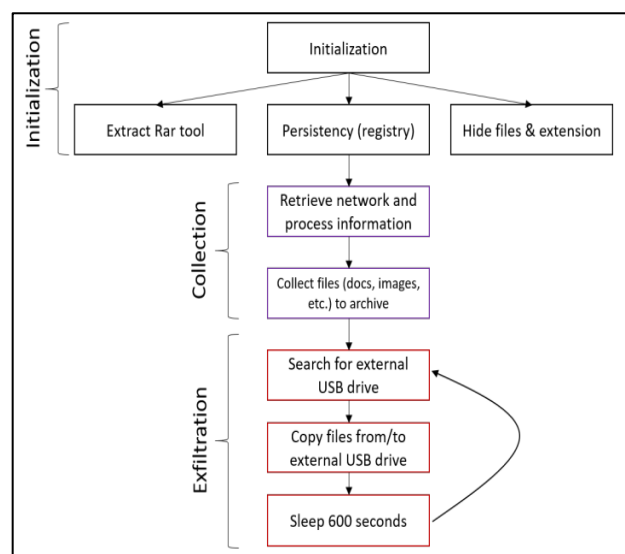


Figure 15, (Guri 2021, p.5)

The BlueCore and Redcore variants of USB-Culprit were examined further revealing advanced malware and strong obfuscation techniques using the DLL attack vector to hide itself within digitally signed processes. The BlueCore payload is delivered via an RTF document that uses vulnerabilities in the RTF such as CVE-2018-0802, when opened it caused execution of a dropper shellcode followed by a digitally signed executable 'QcConcol.exe' which then loads a malicious DLL (Guri 2021, p.1). 'QcLite.dll' follows a further extraction path which eventually leads to the 'stdole.tlb' file which contains the encrypted BlueCore binary and a custom PE loader shellcode, with the Redcore variant following a similar path using droppers and DLL exploits (Guri 2021, p.1).

Mahboubi, Camtepe and Morarji (2018) investigated the air-gapping capabilities of the USB device as well as proposing one solution using a new protocol based on radio frequency identification (RFID) to combat USB devices with malicious firmware. Manipulation of the USB devices firmware is an effective method for infection as the device can be turned into a different device and reconfiguring to load another device driver (Mahboubi, Camtepe and Morarji 2018, p.2). Proof of concept carried out by the Security Research Lab, who had intercepted the firmware update processes, reverse engineered the USB firmware then injected code to change its function, making a 'Bad USB' hard to detect, allowing it to stay obfuscated (Mahboubi, Camtepe and Morarji 2018, p.2).

USB-Based Attacks (Nissim, Yahalom and Elovici 2017) discusses the entire attack landscape of USB attacks and categorised them into 5 categories and 29 different types as of 2017. Data exfiltration via USB devices represents one of the major malicious operations, which can happen both ways in which an infected host can leak data from a USB device and secondly the device can leak information from the host without knowledge and without the ability for most forensic tools to detect it (Nissim, Yahalom and Elovici 2017, p.1). Stealing network traffic is another technique whereby the USB device emulates as an ethernet adapter enabling it to act as a DHCP server which directs traffic through a malicious DNS via modified firmware on the device, it can also supply the host with a malicious default gateway (Nissim, Yahalom and Elovici 2017, p.2). There are the keystroke/mouse click injection attacks such as the 'Rubber Ducky' and malicious firmware updates such as the 'Bad USB' where a microcontroller is placed in the device to fulfil the attackers needs (Nissim, Yahalom

and Elovici 2017, p.2). The final type of attack is the driver related attack in which the attacker enables the device to download a specific malicious driver crafted to execute malicious code on the host or to exploit a buffer overflow vulnerability (Nissim, Yahalom and Elovici 2017, p.2). The USB protocol itself can be exploited for gain, with the typical configuration consisting of a single host which can have multiple USB devices interconnected to it, the PC host has an embedded root hub in which contains the USB ports in which the device will add capabilities to the host or hub devices (Nissim, Yahalom and Elovici 2017, p.2). USB devices are controlled by a microcontroller chip responsible for the interaction with the host controller, it includes a CPU which executes firmware informing the device about how to respond it also often includes a bootloader which will allow the loading of firmware from the device for updates post-production (Nissim, Yahalom and Elovici 2017, p.2). The USB device cannot transfer data without an explicit request from the host controller which detects the connected device, determines the speed, the descriptors, and loading drivers which is done according to the class and vendor ID, however a USB device can come with custom device drivers (Nissim, Yahalom and Elovici 2017, p.3). Figure 16 variations of malicious USB devices with the red coloured attacks representing programmable microcontrollers, orange and blue are typical peripheral household devices with purple being crafted devices from electrical hardware (Nissim, Yahalom and Elovici 2017, p.3).

There are many attack vectors and the landscape for USB attacks is vast and often complex with great efforts undertaken to remain undetected via obfuscation methods.

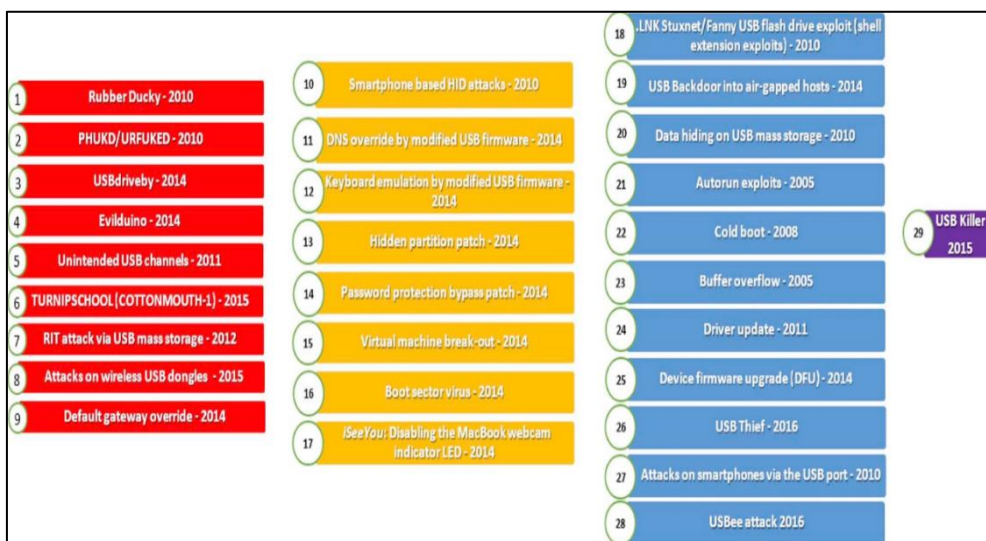


Figure 16, (Nissim, Yahalom and Elovici 2017, p.3).

### 8.3 MICROCODE MALWARE

The results of the pilot study indicated the possibility of Intel microcode present in the binary of the unallocated blocks. To determine further if the results were valid, it was necessary to investigate previous work undertaken into malicious microcode. A research team from Ruhr University in Germany have shown it is indeed possible to insert malware and malicious code into Intel and AMD microcode used to update CPU, often for security reasons. Bugs in the CPU can have severe consequences on system security so the processors list incorrect behaviour to safe-guard program execution, but they are not suited for complex design errors, which require hardware modifications (Koppe *et al.* 2017, p.1). Since the 1970s microcode has been used to decode complex instructions into a series of simplified microinstructions, originally it was read-only memory, but the update mechanism was introduced utilising Random Access Memory (RAM) (Koppe *et al.* 2017, p.1). When erroneous behaviour is detected manufactures publish microcode updates loaded via the BIOS/UEFI or OS during the boot process, they are not persistent requiring reloading after each processor rest, these updates are implemented by both AMD and Intel (Koppe *et al.* 2017, p.1). Koppe and team worked to reverse engineer the K8 and K10 AMD microcode to explore if it could be used to maliciously. They successfully proved that microcode could be used maliciously by reprogramming existing triggers in the code for malicious purposes. They executed microcode Trojans due to a dormant microcode injected hook within a vector path, such as *div* which is triggered as soon as the specific condition is met. It was possible due to the just-in-time and Ahead-of-time compilers embedded in modern web browsers allowing specific machine code instruction solely in Javascript (JS), meaning legitimate machine instructions may be misused to hide and execute arbitrary code. They also demonstrated how such Trojans facilitate implementation attacks on cryptographic algorithms, malware can be implemented in microcode and malicious microcode updates can be applied to unmodified AMD CPUs (Koppe *et al.* 2017, p.14). Microcode malware does have limitations from existing security measures however, as remote execution would require bypassing application and OS isolation to apply the microcode update (Koppe *et al.* 2017, p.13). With that level of access another vector would be suitable in terms of stealth and persistence however, they do provide post-manufacturing modifications and versatility for OS and applications running on general-purpose CPUs (Koppe *et al.* 2017, p.13).

Microcode Trojan's overcome the usual limitations of hardware Trojans as they are not static and have post manufacturing versatility, they combine low-level hardware access with software-flexibility therefore are dynamically programmable and injectable (Albartus *et al.*2021, p.1). Microcode has unique traits that can be leveraged maliciously as it gives fine-granular control of the CPU data path, registers and memory meaning once a malicious update is deployed the adversary can replace any of the original ISA instruction with their arbitrary instructions (Albartus *et al.*2021, p.3-4). The paper explores how effective and complex a microcode update can be by using stateful trigger conditions in the malicious microcode update. Targeted Trojans can be created which will not be triggered by mistake, there are many design opportunities for a payload given the access and ability of the microcode updates leading to major security violations (Albartus *et al.*2021, p.15).

Speaking to a member of the team has revealed it is theoretically possible to add malicious microcode to the USB device with legitimate microcode found on SSD cards, another form of solid-state storage devices as software updates. Discussions with USB manufacturers as seen in Appendix 8, state it is unusual for microcode to be present in USB devices and if located on a device, it would be indicative of malicious intent. One of the USB devices from the pilot study did contain manufacturer software updates but they were visible, AV scannable and optional.

#### 8.4 OUTSOURCING AND MANUFACTURING RISKS

Most solid-storage devices are manufactured outside of allied countries with the vast majority of those being manufactured in China, alongside many electronic devices. The pilot study looked at historic hardware attacks from manufacturing such as the Dell computer incident as well as vendor malware placed in CDs. Outsourcing and manufacturing of technology comes with many risks such as how the devices are packaged as well as state-sponsored interference in manufacturing, leading to information security risks.

The US government has for years claimed that Chinese companies are building surveillance technology into devices exported to the US yet it was also revealed that the National Security Agency (NSA) has been intercepting and tampering with technical devices in transit since 2010. It is claimed to be common practise to add eavesdropping technology to servers, routers, and network equipment before

exporting them with the equipment repackaged and shipped as planned (dys2p , 2022). Due to the outsourcing of manufacturing from all industries to cut costs, it led to many manufacturing risks including malware or spyware being added to electronic and computing devices which have been well documented. Outsourcing manufacturing and chip-fabrication requires the revealing of the design to external entities, creating opportunities for design infringements, counterfeiting, piracy, and insertions of malicious alterations such as hardware Trojans (Desai et al. 2013, p.1).

The US have warned of eavesdropping equipment in telecommunications equipment manufactured in China giving access to the Chinese government and the Edward Snowden evidence that NSA and Government Communications Headquarters (GCHQ) were found to have worked with information and communications technology companies to facilitate mass surveillance (Lysne et al. 2016, p.1). A report by NATO cyber defence centre discusses the threat 5G technology from the Chinese company Huawei poses, if implemented. US, Australia, New Zealand and Japan have imposed restrictions on Huawei 5G solutions due to company ties with intelligence services reinforced by the political and legal environment, requiring business cooperation (Kaska, Beckvard and Minárik 2019, p.5). There has been no public evidence of vulnerabilities in the technology (Kaska, Beckvard and Minárik 2019, p.5), however they have been accused of industrial espionage, with governmental, intelligence and military ties it raises the security threat when it comes to the reliance on 5G technology and its access to critical and private data. The company has been blamed for industrial espionage by both Cisco in 2003 and T-Mobile in 2004, continued violations of international economic sanctions, several fraud and intellectual property thefts in the US, staff members in Australia who were linked to espionage allegations, Canada and Poland detained personal (Kaska, Beckvard and Minárik 2019, p.7-8). Chinese intelligence services working within communications and manufacturing companies certainly have the motive, ability and cases of interference in the production chain of critical electronic and computing products.

## CHAPTER 9. RESEARCH STUDY METHOD

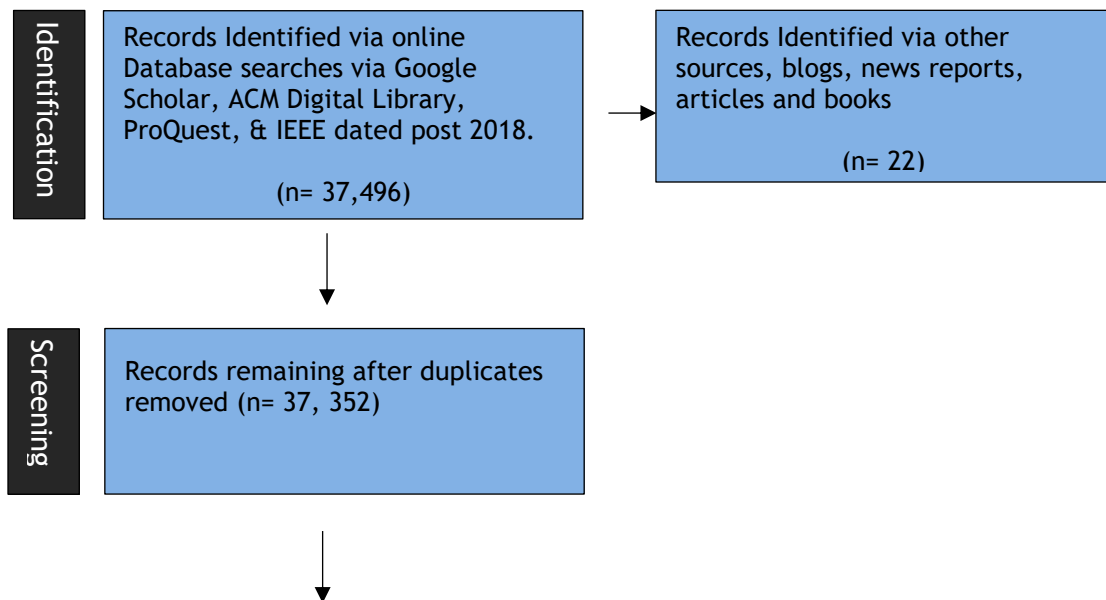
To conclude on the hypothesis confirmatory quantitative research was combined with qualitative research methods. Three phases of forensic testing was applied, firstly the forensic examination of the unallocated storage blocks, any data and binary of the drives, with extraction applied to any data located. Second sandboxed tests on a

lab machine using Win SCP and PowerShell as well as a comprehensive network test using the software Wireshark to examine network traffic. Thirdly the forensic examination to examine all hidden processes, registry changes with Process Monitor and start-up processes with Autoruns.

A public survey was carried out via social media so it would target civilians who were digitally confident and therefore more likely to use e-commerce platforms. It was more likely that participants would also be in the UK as it was shared between UK citizens, 100% of the participants were from the UK and not answering for a business.

The sellers of suspect devices were contacted using the message feature by the e-commerce platforms and rules on engagement with sellers upon receipt of goods they have provided. The platforms monitor email exchanges between customer and seller, intervening if necessary or asked to in the case of unsatisfactory goods or service.

Secondary research referenced in this study are not dated past 2018, unless it is the most recent source available. The PRISMA method was used to find the relevant sources, with the flow chart shown in figure 17.





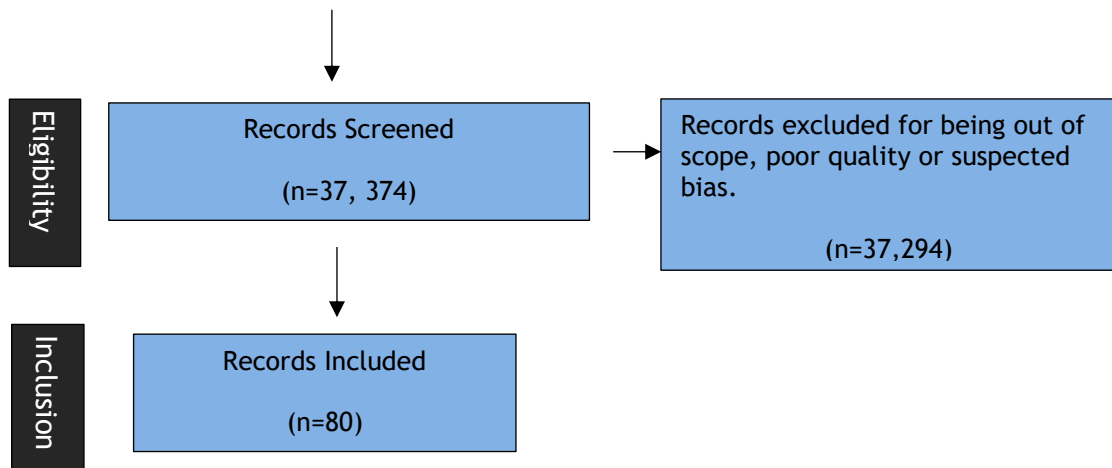


Figure 17, PRISMA flow chart

## CHAPTER 10. PHASE 1 FORENSIC TESTING METHOD

The first phase of testing carried out was the continuation of the pilot study on a larger set of devices. Appendix 5 details the drives and packaging that were examined with a total of 22 new devices were examined in this phase, adding to the 4 examined in the pilot study.

WeibeTech write blocking hardware was implemented to prevent infection of the testing computer, it allows a one-way only connection between acting as a safe go between from the host machine and the device. It will allow the host machine to read, write and execute files and commands on the host machine but will not allow any connected device to do the same effectively containing any virus, Trojan, Worm, Firmware or any other type of malicious or otherwise file from contaminating the host. This was to guarantee that results from the examination of the first phase of testing remains uncontaminated from one device to the next, creating a sterile environment.

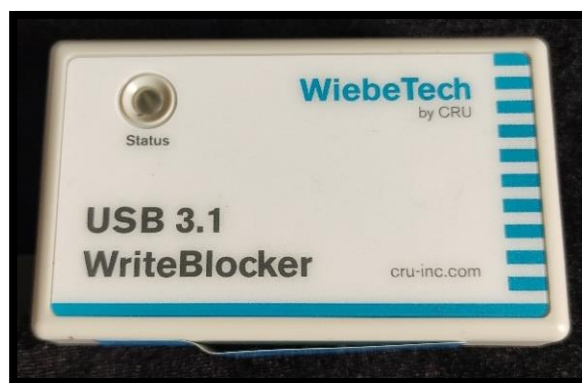


Figure 18. WeibeTech WriteBlocker

Implementing the write blocker the devices were scanned by the Autopsy digital forensic software application which looks at the previous uses of a device, current and deleted files, timeline stamps for all activity, all unallocated blocks and their binary. When anomalies were detected that match those of the pilot study the same process was carried out using the Binwalk application in an Ubuntu to examine the binary for signatures. A VHD copy of the drive is created with the application Rufus which is the windows equivalent of a dd in Ubuntu, the VHD is then examined on an Ubuntu machine with entropy scans carried out on any suspected encrypted data. The final step carried out was the extraction of any files or data from the binary using the extraction method in Binwalk so it could be possible examined and compared.

### 10.1. PHASE 2 FORENSIC TESTING METHOD

The second stage of testing was carried out on a Windows To Go Pro edition officially created by Windows, installed onto a new and safely purchased external hard drive each time a device was being tested. The external drive enabled the testing of each device without the BIOS or registry of the testing machine being altered which would have contaminated any further test results, by booting the OS on the external drive via the boot from USB function and bypassing the Lenovo laptops OS. It was also vital for guaranteeing all tests carried out were done so it ensured the same testing environment each time a test was carried out.

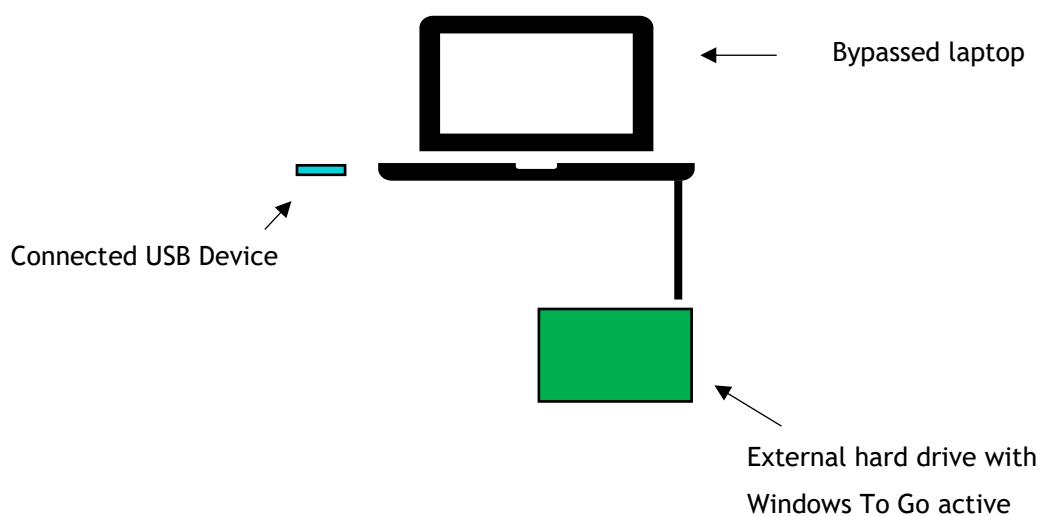


Figure 19, Lab Test 2 Set Up

This phase of testing made use of the advanced system monitoring tools, resource monitor, task manager, event viewer, device manager, as common commands via PowerShell. The applications WinSCP to view any file changes and Wireshark for detailed packet examination. Each device was tested on the same new install of the OS on the external hard drive and was plugged into a 2011 Lenovo laptop which had been fully updated. PowerShell command `>tasklist` was used before the insertion of the USB, event logs were cleared, and the network card switched off manually. The devices were connected firstly, offline for 10 minutes with `>tasklist` reading saved to a text file for future examination at 1-minute intervals. The event logs were reviewed with any notable events saved. WinSCP was used post device to determine if there were any modifications to existing files or new files had been added. The previous steps were then repeated after a reboot and then again with network access with the wi-fi turned manually back on with Wireshark readings taken to log all network traffic and events for 20 mins. Device manager was examined to see if any new devices had been connected and `>diskpart` PowerShell commands were implemented to examine if any new or hidden partitions were visible.

## 10.2. PHASE 3 FORENSIC TESTING METHOD

The final phase was implemented to examine hidden processes, registry changes and changes to the start-up processes. The application Autoruns was implemented to take a reading of the start-up processes at the start and end of each test. The application Process Monitor was implemented to capture all events hidden and otherwise in the 10 mins the device was plugged in and networked. The results were filtered for advanced malware and monitored live with all results saved for later examination. The test was repeated once the machine was rebooted and for each device. Deduction was used to determine unusual or significant process from the normal running processes, both with a safe USB and at rest with a new OS with the same testing conditions. Any processes flagged were cross checked across all devices for similarities.

## CHAPTER 11. RESEARCH STUDY RESULTS

To discuss the impact of any malware found on the devices, a public survey was carried out to assess the use of the e-commerce platforms, the suspicion of the devices and the public's civil-cyber security in relation to solid-state storage devices.

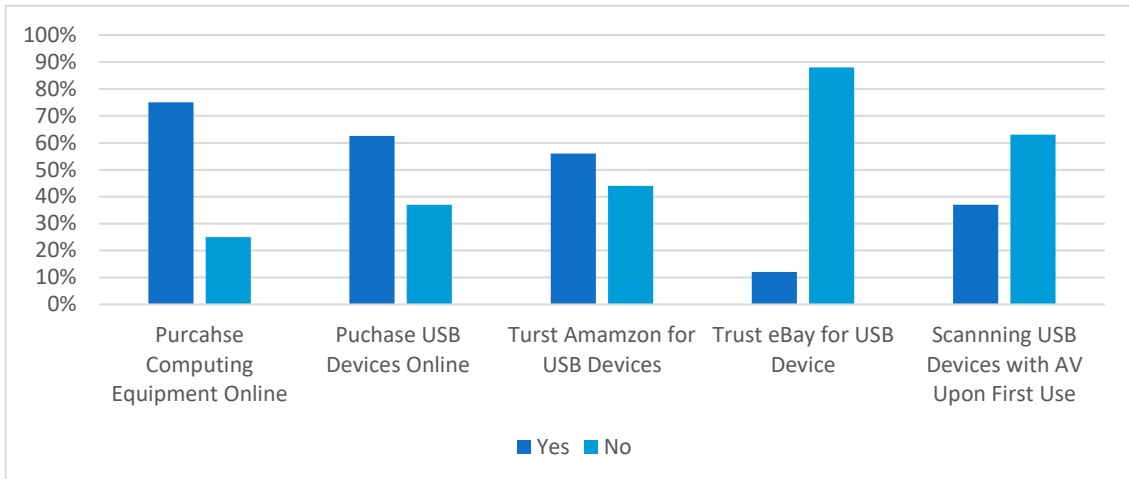


Figure 20 , Survey Results

The public survey results show 63% are the public are buying USB devices online with only 63% of the public using Anti-Virus to scan the devices upon first use leading to a significant civil cyber-security risk despite efforts over the past 15 years to educate the public of the dangers. The results also indicate that the public trust Amazon significantly more than eBay for the USB devices, this was due to the fact Amazon deal with stores directly, not via third-party sellers and reputation.

#### 11.1. PHASE 1 FORENSIC TESTING: AUTOPSY & BINWALK SCAN RESULTS

A total of 21 USB storage devices were scanned using Autopsy the open-source software and were categorised into three categories, safe devices which contained no previous files, timestamps, and no data in the binary, used devices where devices that had present or deleted files and suspicious devices which contained no files but had possible data in the binary of the unallocated spaces.

A total of 8 out of 21 devices were found to contain no previous use, data or anything suspicious in the binary of the unallocated spaces, in which all the blocks were switched fully on or off as expected due to their manufacturing properties discussed in the pilot study. Timeline evidence showed the devices were accessed when created. Safe devices were the Emtec USB, Integral USB, Kingston USB, Sandisk Refurb 1 USB, Sandisk Refurb 2 USB, Pink 2, Transend USB and Waysta USB.

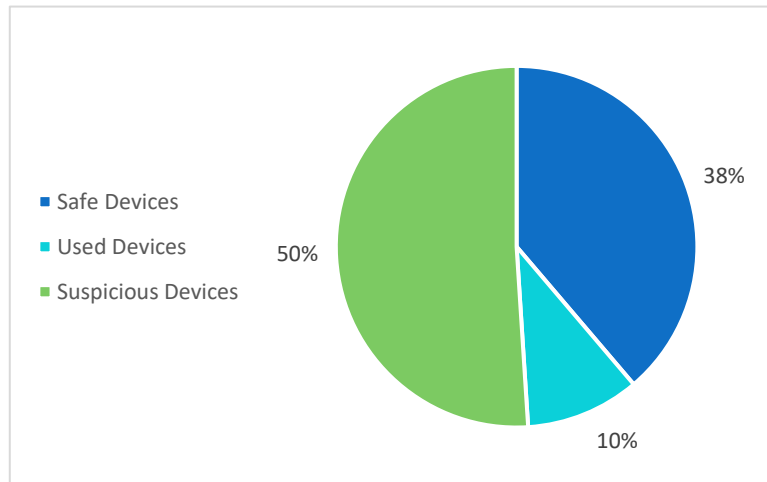


Figure 21, USB Categorized Results

2 devices contained evidence of containing previous data, the White Netac device contained 570 deleted Orphan files. The device named Pink 1 contained 256 deleted application/octet-stream stream files with symbolic names such as ‘□^’ with an unknown MD5:d41d8cd98f00b204e9800998ecf8427e hash. A total of 41 active files were found in the unallocated spaces of the device, all of which were application/octet stream data in the unallocated space with the similar naming convention and unknown MD5 hash values such as ‘□^^^’ with MD5:6be8796d51e23e4f275230680f8f18c. One file in particular stood out as it was flagged as being likely encrypted due to the high entropy score of 7.8 given by Autopsy, it followed the same file format as the other with the unknown MD5: 627fe5b0d54aa5d7315da93e684e0639. All drives were set aside to inspect the binary to see if matching Intel or encryption signatures as found in the pilot study were present, or any others that needed investigation.

The remaining 11 devices contained no deleted or present files but did contain possible data in unallocated space in the binary, further testing using Binwalk was carried out on those 11 devices, as well as the 2 used devices.

There were multiple timeline entries over periods of time between 2018-2021 on 12 out of 13 devices that contained possible binary data, deleted and present data.

A VHD copy of each of the 13 devices required binary examination to determine if valid signatures, especially those found in the pilot study, could be detected. The Unbranded Swivel USB, Qumox USB and White Netac USB contained no signatures and

so were categorized as used devices. 10 devices contained the same signatures matches as the Netac device from the pilot study, the Qumox USB did not contain signatures, was removed from further testing and categorised as a used device. Of the remaining 10 devices, 100% contained Intel signatures, with 5 different quantities of them spotted ranging from 12 to 2982 which corresponds to small storage space as the device found with only 12 was the Pink 1 USB, which contained 41 active files and was only 1GB in size, the others range from 8GB - 64GB. Figure 7 shows the number of Intel signatures detected.

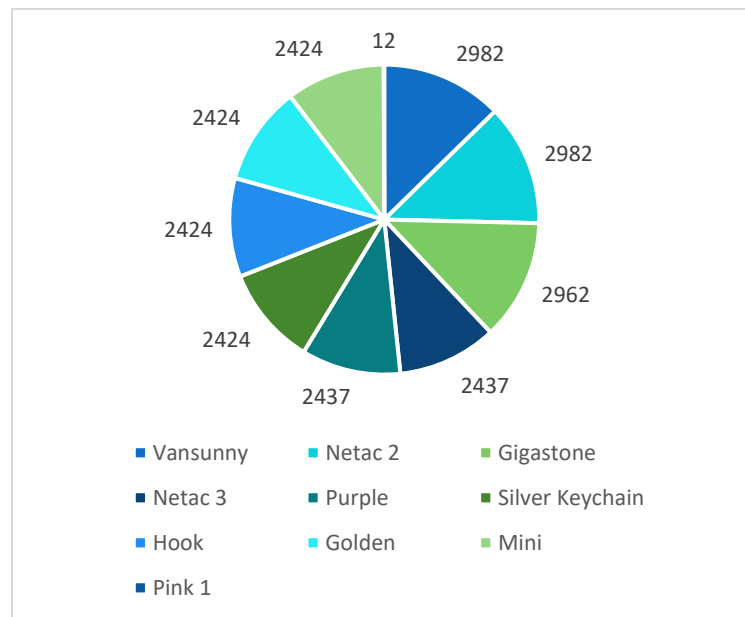


Figure 22, Intel Signatures

3 devices also contained the same encryption signatures as the Netac 1 device from the pilot study, with the same algorithm in a block formation with a total of 128 found in each USB, the Vansunny USB, Gigastone USB and Netac 2 USB. Entropy scans were carried out on each of the 10 devices revealing the same results as the pilot study in all cases, showing that a second rising and falling edge is detected showing the presence of data.

For the next stage the Netac 1 USB device from the pilot study was added back into the testing for further research to be carried out. 11 USB devices had VHD copies extracted by Binwalk to see if any data from the binary could be recovered. Out of the 11 devices 8 were found to contain extractable data in the form of .sit file and .gz files, all zipped files and folders. The files share a characteristic in their naming convention as the files found on Pink 1 USB by autopsy. They all range in sizes but

total a significant amount, often reaching over 100GB when extracted from the binary. The sit files are valid but error when extraction is attempted. The .gz files will allow the software 7zip to open the archive revealing a file or a folder containing a same named file, 8 USB shared the same file:

Ð°ÑörAjAòlvœ=à1Uî{j÷\*1ìyö"oÔrðÖàx=op±!~,Š[wP

A second file was also present in the Hook, Vansunny and Gigastone USB devices.

´q´nEÅ<...@´´|

When extraction of these files was attempted, a data error occurred resolving in the file extraction of 0 bytes and a sign of locking down the extraction method. This is the same for 3 USB's where the data extraction resulted in nothing, which is often a sign of data encryption.

If the unallocated blocks contained random data, it is impossible that 8 differently branded devices, purchased from two platforms and many vendors, would contain the same file. The test results credibly proves that the signatures in the binary of the unallocated blocks are valid results, therefore the next stage of testing was necessary to determine if the files were malicious. A total of 11 USB devices were tested in phase 2 of forensic testing, Netac 1 from the pilot study and the 10 devices from this study.

## 11.2. PHASE 2 FORENSIC TESTING: PACKET COLLECTION & ADVANCED MONITORING TOOLS

All 11 tests carried out showed only Windows processes when using the command line `>tasklist` at 1 min intervals. The WUDFhost.exe was the only new addition as this is the process associated with the USB device itself. Phase 3 testing was required to take a deeper look at the hidden processes and registry changes on the system. There were no devices added when the USB was inserted, there were also no partitions created, hidden or otherwise. There were no modifications detected using WinSCP and network tests showed that no detectable network activity.

Event viewer did find suspicious activity from 4 devices, with 83% occurring after the device was used alongside internet access. All events featured in figure 8 were present when the USB stick was in use and not at rest either after restart, networked or whilst using a safe USB stick.

<p><b>Silver Keychain USB</b></p> <p>Defrag performed after 4 minutes of internet access.</p>	<pre>boot optimisation CENA_X86FREE_EN-GB_DV9 (C) 000000026040000FD030000000000022B630DF6479C7F6E26C1C0000000000000000</pre> <hr/> <p><b>Binary data:</b></p> <p>In Words</p> <pre>0000: 00000000 00000426 000003FD 00000000 0010: DF30B622 F6C77964 001C6CE2 00000000 0020: 00000000</pre> <p>In Bytes</p> <pre>0000: 00 00 00 00 26 04 00 00  ....6... 0008: FD 03 00 00 00 00 00 00  y..... 0010: 22 B6 30 DF 64 79 C7 F6  *%0BdyC0 0018: E2 6C 1C 00 00 00 00 00  a1..... 0020: 00 00 00 00  ....</pre>
<p><b>Silver Keychain USB</b></p> <p>Third-party root certificate added after 10 minutes of internet access.</p>	<pre>CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3 D69B561148F01C77C54578C10926DF5B856976AD</pre>
<p><b>Mini Silver USB</b></p> <p>Within 1 min of internet access a telnet client file located in Temp casues an encoding error.</p>	<pre>INVALID_REQUEST 0 WindowsServicingFailureInfo Not available 0 10.0.19041.1852.1 0x800F0984 0x800F0984 Matching binary: telnet.exe missing for component: x86_microsoft-windows-telnet-client_31bf3856ad364e35_10.0.19041.1741_none_d0a12b1f2208285b 糞敬,理枯泣崇哦□灣;坤些滔灭湯浹却瀉敲瑞刺睡球粘製紫玻攪製摹備整稜敬鑑運襪枯康擲溜劑癩仿敢致區獨A疊q庫雲→T \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WERADD3.tmp\WERInternalMetadata.xml \\?\C:\ProgramData\Microsoft\Windows\WER\ReportArchive\Critical_10.0.19041.1852_3fb1b22fc63acc44ce30c6478cbb652fd82853_00000000_f66392d8-3979-4211-9705-b5ba1e42c180 0 f66392d8-3979-4211-9705-b5ba1e42c180 268435462 0</pre>




<p><b>Pink 1 USB</b></p> <p>Within 1 min of internet access problematic signatures were detected on files located in the Temp folder, involving an error on the USB port.</p>	<pre>LiveKernelEvent Not available 0 144 3003 c91e7a08 40010000 0 10_0_19044 0_0 256_1 \\?\C:\Windows\LiveKernelReports\USBHUB3\USBHUB3-20220821-1451.dmp \\?\C:\Windows\TEMP\WER-3352812-0.sysdata.xml \\? \C:\ProgramData\Microsoft\Windows\WER\Temp\WER5962.tmp.WERInternalMetadata.xml \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER5983.tmp.xml \\? \C:\ProgramData\Microsoft\Windows\WER\Temp\WER5984.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER5994.tmp.txt \\?\C:\ProgramData\Microsoft\Windows\WER\ReportArchive\Kernel_144_635993f4e435b8ab3c8e27c03ce6d4e38ba7bd_00000000_cab_bc19439c-7f31-497a-8d43- aa22ff5df784</pre>
<p><b>Purple USB</b></p> <p>Within 1 min of USB being inserted without network access the Volume Shadow Copy service has performed a background task and closed.</p>	 <p>The VSS service is shutting down due to idle timeout.</p> <p>Log Name: Application  Source: VSS  Event ID: 8224  Level: Information  User: N/A  OpCode: Info  More Information: <a href="#">Event Log Online Help</a></p> <p>Logged: 19/08/2022 16:43:13  Task Category: None  Keywords: Classic  Computer: DESKTOP-7OV2ELB</p>
<p><b>Purple USB</b></p> <p>Defrag performed after 8 minutes of internet access.</p>	<pre>boot optimisation C:\C:\WINDOWS\FREE_EN_GB_DV9 (C:) 0000000026040000FD030000000000000000022B630DF6479C7F6E26C1C00000000000000000</pre> <hr/> <p><b>Binary data:</b></p> <p>In Words</p> <pre>0000: 00000000 00000426 000003FD 00000000 0010: DF30B622 F6C77964 001C6CE2 00000000 0020: 00000000</pre> <p>In Bytes</p> <pre>0000: 00 00 00 00 26 04 00 00   ....S... 0008: FD 03 00 00 00 00 00 00   y..... 0010: 22 B6 30 DF 64 79 C7 F6   **q0Bdyçö 0018: E2 6C 1C 00 00 00 00 00   ä1..... 0020: 00 00 00 00   ....</pre>

Figure 23, Events

The added third-party root certificate added to the system by the Silver Keychain was researched using the SHA1 from the event using the website ThreatMiner (ThreatMiner ThreatMiner 2022). There were no threat reports currently on the SHA1, however related host IP addressed with the root certificate were inspected totalling 12 thousand with 34 resolving in China, including major ISP's and communication companies, the relevance of which will be discussed in a further chapter. The adding

of a third-party root certificate is a clear sign of malicious activity as it will allow applications, including malware to become digitally signed avoiding detection by AV. If a malicious party inserts a self-issued public key into the list of root public keys stored on the host device, then the party could do considerable damage to the system (Alsaid and Mitchell 2005, p.1). The IP addresses feature in figure 24 and colour coded by organisation.

117.145.179.201	China Mobile Communications
175.6.12.148	ChinaNet Hunan Province
116.211.96.146	ChinaNet Hubei Province
183.61.156.197	ChinaNet Guangdong Province
42.81.5.185	ChinaNet Tianjin Province
42.81.5.205	ChinaNet Tianjin Province
14.18.203.223	ChinaNet Guangdong Province
14.18.203.238	ChinaNet Guangdong Province
101.251.98.15	Shanghai Chenyi Network
36.250.87.224	China Unicom Fujian Province
36.250.87.204	China Unicom Fujian Province
211.90.30.182	China United Telecommunications
36.250.87.244	China Unicom Fujian Province
218.24.17.217	China Unicom Liaoning Province
113.5.253.19	China Unicom Heilongjiang Province
221.7.112.150	China Unicom Chongqing Province
61.54.31.73	China Unicom Henan Province
222.161.225.146	China Unicom Jilin Province
220.194.200.122	China United Network Communications
220.194.200.81	China United Network Communications
101.226.255.93	ChinaNet Shanghai Province
222.88.91.70	ChinaNet Henan Province
60.165.56.186	ChinaNet Gansu Province
218.66.170.76	ChinaNet Fujian Province
223.244.227.252	ChinaNet Anhui Province
222.182.202.21	ChinaNet Chongqing Province
222.214.86.29	ChinaNet Sichuan Province
120.41.1.107	ChinaNet Fujian Province
122.13.18.69	China Unicom Guangdong Province
112.90.148.83	China Unicom Guangdong Province
163.177.134.216	China Unicom Guangdong Province
210.52.220.178	Shanghai Lekai IDC of China Netcom
182.247.233.162	ChinaNet Yunnan Province
59.63.197.98	ChinaNet Jiangxi Province

Figure 24, SHA1 Related Hosts from China

The Chinese characters in the event viewer is an example of an encoding error from a new Telnet client file which was suspiciously located in the Temp folder, indicative of malicious activity. More details on the encoding error can be found from the Plain Text NDC conference in Oslo 2021 (Beattie 2022).

2 USB devices resulted in defragmentation between 4-8 mins of internet access, this event is only present on two devices when networked and not a rest, indicative it has been caused by the devices.

The Volume Shadow Copy, which can make backup copies of the system files in use, was running and the event was flagged when this service stopped within 1 minute of the Pink 1 USB device being used without internet access, this is incredibly suspicious activity as it only occurred once, was a background task with very little detail, which is often the case with the Windows OS.

### 11.3. PHASE 3 FORENSIC TESTING: ADVANCED MONITORING SOFTWARE

The final phase of testing implemented the applications Autoruns and Process Monitor for a detailed look at start up changes and a detailed look at all processes, including those hidden and changes made to the registry. Autorun testing on all 11 USB devices revealed no changes were made. Using filtering for advanced malware to look specifically for the following processes:

- create a file
- write a file
- rename a file
- creating registry keys
- set registry values
- load imag
- create process
- create pipe
- TCP and UDP

Process monitor revealed thousands of Windows processes only take place alongside the use of a suspicious device. A number of Windows processes were seen across more than one device performing the same tasks. Figure 10 features the most common set of hidden processes that featured across 80% of devices, the process is not present at all in 10 minutes taken at rest and with two safe USB devices in use. All tests were carried out with internet access. The `vssvc.exe` can be seen creating thousands of files to the `Windows\System32` file, often featuring the `.dll` extension. It was clearly seen in the results of Purple USB device, which corresponds with the

Windows Event seen in the previous test, corroborating the VSS is running and creating files. The process was present with the netac 1, 2 & 3 USB's, Pink 1 USB, Purple USB, Silver Keychain USB, Hook USB, and Golden USB.

vssvc.exe	4988	CreateFile	C:\Windows\Prefetch\VSSVC.EXE-04D079CC.pf
vssvc.exe	4988	CreateFile	C:\Windows\System32
vssvc.exe	4988	CreateFile	C:\Windows\System32\devobj.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\vssapi.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\vssapi.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\devobj.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\vsstrace.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\vsstrace.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\authz.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\virtdisk.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\authz.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\bcd.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\virtdisk.dll
vssvc.exe	4988	CreateFile	C:\Windows\System32\bcd.dll

Figure 25, Process Monitor results

The next two processes are present heavily on several devices also creating files often with a .dll extension. These were not present at rest or when using the safe devices with file creation at the same constant rate leading to thousands more files being created than ordinary when the Netac 1 & 3 USB's, Silver Keychain USB and Hook USB were inserted into the host.

NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll
NGenTask.exe	3184	CreateFile	C:\Windows\System32\MSCOREE.DLL.local
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorlib.dll
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorlib.dll
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
NGenTask.exe	3184	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\NGenTask.exe.config

Figure 26, Process Monitor results

ngen.exe	6904	CreateFile	C:\Windows\System32\mscorlib.dll.local
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll
ngen.exe	6904	CreateFile	C:\Windows\System32\mscorlib.dll.local
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorlib.dll
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorlib.dll
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
ngen.exe	6904	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe.config

Figure 27, Process Monitor results

Netac 3 USB, Hook USB and Silver Keychain USB all contained the **devicecensus.exe** which was not present on the test at rest or with the safe USB devices in use. It also has the same pattern of thousands of entries over a small period of time with the same files created across the devices.

devicecensus.e...	6784	CreateFile	C:\Windows\System32\policymanager.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\policymanager.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\msvcpl110_win.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\msvcpl110_win.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\OneSettingsClient.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\OneSettingsClient.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\wtsapi32.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\wtsapi32.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\winsta.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\winsta.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\policymanager.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\policymanager.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\msvcpl110_win.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\msvcpl110_win.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\OnDemandConnRouteHelper.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\OnDemandConnRouteHelper.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\mswsock.dll
devicecensus.e...	6784	CreateFile	C:\Windows\System32\mswsock.dll

Figure 28, Process Monitor results

Netac1 USB contained thousands of **HxTsr.exe** in a similar pattern, only a few entries of this process with the filters in place are present at rest or safe USB tests. Less entries were also observed on the Hook USB, Golden USB and Purple USB but still with hundreds more entries than when the devices are not in use.

HxTsr.exe	7400	CreateFile	C:\Windows\System32\cryptsp.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\ucrtbase.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\rpcrt4.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\combase.dll
HxTsr.exe	7400	CreateFile	C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.27323.0_x86
HxTsr.exe	7400	CreateFile	C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.27323.0_x86
HxTsr.exe	7400	CreateFile	C:\Windows\System32\msvc_p_win.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\oleaut32.dll
HxTsr.exe	7400	CreateFile	C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.27323.0_x86
HxTsr.exe	7400	CreateFile	C:\Windows\System32\win32u.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\user32.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\gdi32full.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\gdi32.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\ole32.dll
HxTsr.exe	7400	CreateFile	C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_1
HxTsr.exe	7400	CreateFile	C:\Windows\System32\sechost.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\cryptsp.dll
HxTsr.exe	7400	CreateFile	C:\Windows\System32\msvcr.dll

Figure 29, Process Monitor results

The Gigastone USB contained thousands of **DrvInst.exe** which were only present at all when the device is in use. It follows the same patterns as observed in the previous results.

DrvInst.exe	3168	CreateFile	C:\Windows\System32
DrvInst.exe	3168	CreateFile	C:\Windows\System32\ntmarta.dll
DrvInst.exe	3168	CreateFile	C:\Windows\System32\ntmarta.dll
DrvInst.exe	3168	CreateFile	C:\Windows\System32\devrtl.dll
DrvInst.exe	3168	CreateFile	C:\Windows\System32\devrtl.dll
DrvInst.exe	3168	CreateFile	C:\Windows\System32\drvstore.dll
DrvInst.exe	3168	CreateFile	C:\Windows\System32\drvstore.dll
DrvInst.exe	3168	CreateFile	C:\Windows\System32\DriverStore
DrvInst.exe	3168	CreateFile	C:\Windows
DrvInst.exe	3168	CreateFile	C:\Windows
DrvInst.exe	3168	CreateFile	C:\Windows\INF
DrvInst.exe	3168	CreateFile	C:\Windows\INF\setupapi.dev.log
DrvInst.exe	3168	CreateFile	C:\Windows\Globalization\Sorting\SortDefault.nls
DrvInst.exe	3168	CreateFile	C:\Windows\INF\setupapi.dev.log
DrvInst.exe	3168	CreateFile	C:\Windows\INF\setupapi.dev.log
DrvInst.exe	3168	CreateFile	C:\Windows\INF\setupapi.dev.log

Figure 30, Process Monitor results

The final finding was made on the Pink 1 USB device, the Windows process **WerFault.exe** which followed the same pattern as the previous results and was only present when the device was in use. This process both created and wrote files to the system and the Temp folder, in fact the same file where the encoding error was logged in the previous tests that showed the file had been erroneously modified was seen to be created and written alongside many others with the pathway of the file shown in figure 16. This result corresponds directly with the results seen in the previous testing and Windows event logs.

WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	CreateFile	C:\Windows\System32\drivers\ntfs.sys
WerFault.exe	6636	CreateFile	C:\Windows\System32\drivers\ntfs.sys
WerFault.exe	6636	CreateFile	C:\Windows\System32\drivers\ntfs.sys
WerFault.exe	6636	CreateFile	C:\Windows\System32\drivers\ntfs.sys
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml
WerFault.exe	6636	WriteFile	C:\Windows\Temp\WER-889234-0.sysdata.xml

Figure 31, Process Monitor results

The results of phase 3 testing show several Windows processes creating and writing thousands of files only when certain suspicious USB devices are in use. This is clear evidence of obscuring malicious activity by working from a hidden system Windows application to avoid detection. It shares characteristics of the USBCulprit attack featured in the background research and is clear evidence of advanced malware in action, with the same processes and files being created in a number of incidences it is incredibly likely that the same advanced malware is being used.

Further research may determine exactly what advanced malware is on the USB devices, how it impacts the system long term and the damage it can do to the BIOS which was not featured in the study. The results of all the tests over both the pilot and main study have proven that the binary of the unallocated spaces of 63% of inspected devices contained advanced firmware malware. Firmware Binwalk identifies as x86 Intel Microcode, which in theory can be used to infect a system with almost any malware. The advanced malware infects systems quickly via the trusted platform model and will employ advanced DLL methods to obscure and hide the malware within ordinary hidden Windows processes. Making it incredibly challenging and time consuming to find, similar to the notorious 'Bad USB'. The results also show that the oldest infected device was created in December 2018, meaning almost 4 years of infection possibly occurred, coupled with the sales figures posted by eBay and the number of devices for sale, the impact of this malware may be far reaching and devastating. It is often possible to remove firmware malware by rolling back all drivers to their original state, with updates applied (Guri 2021). However, if this is

indeed Intel x86 Microcode then this may prove ineffective as it applies the firmware directly at the CPU level giving it unprecedented access to all parts of the operating system, including the registry and BIOS. Rolling back the drivers and even installing the OS may not be an effective solution, it would require further investigation to determine the exact delivery method and differencing malware. Because the malware uses digitally signed applications to create and write the malware to the system it is not detectable by AV. It is highly likely that computers that have been infected with the advanced malware found on the devices would remain unsafe at this time until further research is carried out.

## CHAPTER 11 WHO ARE THE VENDORS AND WHERE ARE THEY MANUFACTURED?

Learning who was behind the firmware malware was easier than expected as the platforms had strict rules on communication with customers for goods of substandard quality. Amazon provide stores on their website rather than sellers and as a result there are far less products on the platform than on eBay as the pilot study examined. The results from the public survey show that the public trust Amazon far more than eBay because of this seemingly checked process, indeed all the companies were officially registered in their countries of operation. The largest corporation being Netac who are a highly valued and profitable with head offices in Beijing and a manufacturing plant in Shenzhen China, appendix 7 features the pictures taken from the Netac store on amazon (Amazon 2022, Netac Store) and the pictures from the official Netac website (Netac 2022). However, upon investigation of the stores there were concerning discrepancies such as business addresses in residential homes, named owners of companies regularly changed, all owners and employees originating from the same country of origin when checked with Companies House (gov.UK, 2022) and North Data (North Data 2022), which feature in Appendix 7. 3 products came with stickers belonging to the EU and UK distributors with addresses and company names making tracing them via Companies House, google maps and tax records which can be seen in Appendix 7. It was difficult to locate the company owners as they appear many times as owners of previous companies or other companies and no further information about them or about the company outside of registration and tax, which is incredibly unusual.

Sellers were contacted often resulting in no response, however a number across both platforms did communicate. There were email exchanges between the Vansunny



customer services intermediary to discuss the discrepancies and issues with the product that are featured in Appendix 6 in the Amazon correspondence table. The Amazon account was used only for research on this project which used a pseudonym and only contacted them directly using the account. The account was hacked despite the strong password and was an isolated incident, the email from Amazon about the hacking feature in Appendix 6.

Locating vendors via eBay can be difficult due to the anonymity of the sellers in their auction platform model. The vendors have profile names that do not relate to their business names or registered business owners so the only way to track these vendors was to communicate directly using the platforms, the messages in full are in Appendix 6. It seemed vendors were more than happy to tell me which country they purchased the goods from, two companies immediately dropped the supplier and one stopped the sale of goods, which has been verified. One vendor was not happy to discuss the situation further claiming all their products are certified by their vendor who they would not reveal. One company gave far more away stating they have 23 stores on eBay, 10 warehouses, in the UK, US, Germany, Australia and China, when they accessed the [securedevices.com](https://www.securedevices.com) website they did not pertain that their goods did not include malware or request evidence. Instead, they insisted they would drop the supplier and move into other electronic goods. This was also the company that sent 4 devices in total, the company failed to answer in two instances and in two failed to give me their company name at any time. I find it highly likely that if they were unaware of the findings they would have had far more to say and would have required evidence. They may be aware of it, placed it there, have found issues with the supplier before, or were suspicious of the supplier.

Discussion and investigation into the vendors from both platforms revealed that all the products tracked and discussed were manufactured, stored and exported from China, mostly in Guangdong. It seems unlikely that individual criminal gangs or hackers would use the same method of delivery of firmware malware unless the same entity placed it there themselves. The entity seems highly likely to have the same country of origin, the stores distributing them on Amazon as far as the research could ascertain, have company owners, manufacturers, and all employees from China as well as manufacturers. All the manufacturers of the infected devices from eBay were also from China. The sellers seem to be part of the malware process in some cases

and others they seem unaware with changes made showing that a number of sellers are likely being used as legitimate tools for malware delivery, possibly taking advantage of their existing reputation. It does seem that Chinese manufacturers and vendors are heavily involved throughout the production chain. It is especially concerning that it would be an unfriendly nation and one that has a history of cyber-attacks on NATO allies, with ongoing tensions and a political landscape that mixes business and state.

### 11.1. MADE IN CHINA

Governments have a range of tools for both surveillance of networks and active attacks on computer systems, with hundreds of products available for wiretapping, radio interception, and vulnerabilities in our networks and computer systems (Anderson 2020, p.35). As discussed, there are historical instances of vendor malware being added to devices at the manufacturing plant and entities such as the NSA. It is clear from the previous work that vendor malware is a serious issue and one that crosses over into espionage both corporate and national, which can have lasting implications on a country's economy and national security. This is poignant when the country the vendor malware is exported from is considered unfriendly and highly capable. China is considered the leading competitor to the USA with both its GDP and its technology progress, it demands unrestricted access to all local data including western companies who have been infiltrated such as Yahoo, Skype and Google (Anderson 2020, p.46- 47). It will work to fulfil that demand despite the organisations ethics and policy, it has also blocking outside social media platforms Facebook, Twitter and YouTube (Anderson 2020, p.46- 47).

In China the lines between state and corporations are interwoven including ISP's and the internet, it is an authoritarian country with far greater control over business and society than democratic nations. In part, it is due to the heavy influence of those democratic ideas that spread from the west with the arrival of the internet and social media. From 2002 there have been numerous hacking attacks on the US and UK defence agencies, the Chinese military sees the country in a state of cold war with the West with the preferred attack method of exporting subversive ideas to squash communistic ideas (Anderson 2020, p.47). With well researched attacks such as the 'Snooping Dragon' attack, the Open Net Initiative finding the same group had targeted 103 countries, the CIA was hacked leading to the deaths of 30 agents in

2011, hacked knowledge on the F35 fighter and other military secrets in 2013 (Anderson 2020, p.48-49). In 2015 the Chinese had hacked into the Office of Personal Management gaining personal data of federal employees, and in 2007 the UK Police and security services warned firms of the dangers posed by Chinese state sponsored attacks (Anderson 2020, p.48-49). With such attacks becoming far more sophisticated over time with 2020 seeing a series of advanced persistent threats (APT's) (Anderson 2020, p.48-49). The Huawei revelations of cellular and internet network hardware being used for international mass surveillance was further evidence of a Chinese state lead espionage plot, this time using the very equipment the West relies on, which is made in China. It is clear for the past 20 years the Chinese State have been a formidable threat to cyber-security.

As recently as July 2022 headlines for all major outlets reported fresh warnings from a collection of Western security services and advice for extra vigilance to the cyber-security threat emanating from China. Ken McCallum M15 director general and Chris Wray FBI director have put out fresh warnings on the threats posed by the Chinese Government to UK and US interests in an unprecedented joint address on the 6<sup>th</sup> July (Scroxtton 2022). They stating they have been sent the clearest signal possible on the increasing cyber aggression from China, describing it as planned, professional, strategic geopolitical contest over decades across the globe with the largest risks seen as covert theft, warnings of legitimate intellectual property transfer via acquisitions, exploitation of academic researchers, flattery towards persons of interest, and the use of APT's including targeting Microsoft in 2021 (Scroxtton 2022).

This follows on from the joint report featured in the background research, showing there is an inflating risk year on year. It was for this reason, that when confronted with the SHA 1 of the third-party root certificate and all other roads leading to China, that the IP addresses were picked out, because China are one of, if not the most, formidable threat to cyber-security and they produce a significant amount of electronic and computer hardware for us. China is one of the UK's biggest trading partners and our largest importer with £93 billion, 7.3 % of the UK total trade (ONS 2022).

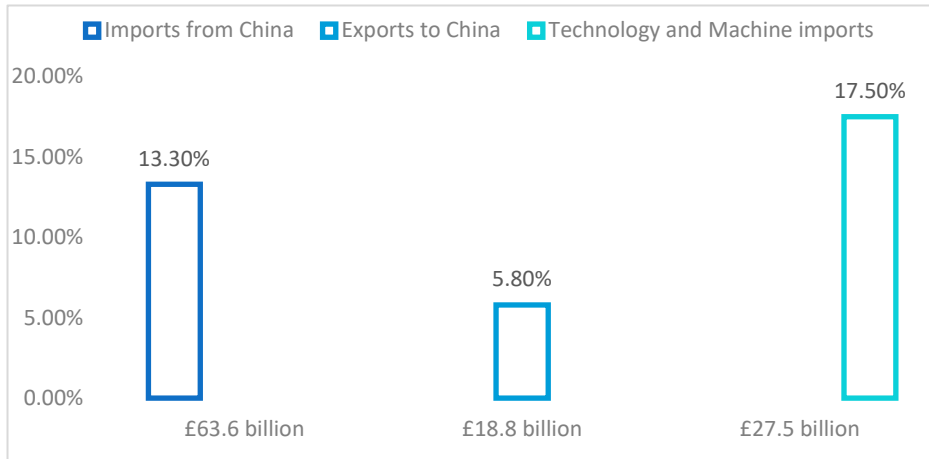


Figure 32 (ONS 2022)

The cyber-security risk of importing 17.5% of computer and office machinery from such an unfriendly state is too high to ignore, especially in line with the findings of this paper in terms of the cyber-security threat China poses combined with the test results. The malware found on the USB devices poses a threat to just all levels of society due to the rise in home working, bring-your-own-device, and mobile phone usage in workplaces as well as a lack of education in cyber-security defence, nationwide from citizens to small businesses. This type of firmware malware has the potential to cause commercial, and industry losses as, like the ‘Bad USB’ it could potentially jump air gapped environments travelling via corporate networks, it is not necessarily citizens alone that are being targeted in this way and poses a significant risk to the UK economy, intellectual property, national security, and academic research. It is clearly targeting the public with the use of e-commerce as a delivery method, which is an enormous risk for every computer user in the country who purchases such devices imported from China, which as the study found was 100% of those tracked. It is not wise to continue importing such goods from a very significant and formidable nation in which we are engaged in cyber-cold war with, there have been decades of abuses with importing such equipment, with more advanced attacks on the imported hardware discovered each year.

## CHAPTER 12 MITIGATION

### 12.1. MANUFACTURING AND OUTSOURCING

Using statistics from the ONS it is possible to calculate that £6.7 million in electronic and computer goods are imported from China and sold online per year (ONS 2022). As commercial businesses implement quality management frameworks such as the ISO 9001 (BSI, 2015) so most of the sales will be to the British public for private use. Cutting imports of computing and electronic goods from China would negatively impact the supply and demand for such devices, with demand outstripping supply causing a shortfall for ordinary users which is likely to increase overall costs.

If we stopped importing electronic and computing devices from China, it would leave us with a 17.5% shortfall of vital goods, impacting corporate and civil acquisition. It would however, mitigate the threat that vendor malware in USB devices poses as 100% of devices that were investigated were made in China. The shortfall in production has the potential to impact cyber-security as it may lead to less efficient backups and loss of data. To counter this increasing local production is necessary, but it would take several years to train the necessary highly skilled manufacturers and make factories available requiring government and private investments to achieve. This was noticeable during the COVID-19 pandemic of 2020 where PPE was required to be locally manufactured due to a decline in available imports. Many national bodies identified repurposing of manufacturing to meet increasing demand for medical equipment and PPE which includes adapting production plans, lines, and capabilities to meet to meet the new goals, which was a leading contributor to mitigating the production disruption (Okorie et al. 2020, p.2-9).

Further benefits would include the economic boost from exporting safe and secure devices to allied countries currently imported from China. It would increase jobs, improve the economy via exports of highly valued secure goods, and train an entire new generation as highly skilled electrical engineers. We have a generation of highly skilled electrical engineers who were heavily educated by the national curriculum with many going on to study electrical engineering and working in the industry for many years before it was outsourced late 21<sup>st</sup> century. We have a generation well within working age that are very capable of training a new generation in colleges, engineering schools, universities and in apprenticeships.

Although increasing production rapidly will mitigate the threat, it may take many years before production was able to completely replace the 17.5% of goods currently imported from China. To prevent a large shortfall, increasing imports from trusted allies is necessary with EU and Japanese suppliers able to cover a significant portion of the shortfall due to also being large manufacturers. Figure 33 shows the country's leading in manufacturing with some of the largest producers of computing goods such as Japan, Germany, and the US.

Country	Manufacturing Output (USD in billions)	Percent of National Output	Percent of Global Manufacturing
China	\$2,010	27%	20%
United States	1,867	12	18
Japan	1,063	19	10
Germany	700	23	7
South Korea	372	29	4
India	298	16	3
France	274	11	3
Italy	264	16	3
United Kingdom	244	10	2
Taiwan	185	31	2

Figure 33 (West and Lansang 2018)

## 12.2 THREATS TO ALLIED DEMOCRATIC VALUES

Relying solely on the US to cover the manufacturing shortfall at this time is risky, given the political and policy issues it is currently facing, echoed world-wide. US and global policy uncertainty have been highly elevated in recent years which resulted in the past dozen years seeing the highest levels of US economic uncertainty in the past 60 years, which harms macroeconomic performance (Davis 2019, p.16).

The political situation in the US is incredibly unstable, with the very democratic fabric of the nation under threat, with Republican seats acquired by those who openly do not agree with democratic values, supporting an ex-president that attempted to take power in the violent Capitol Hill riots in 2021 (BBC 2022). The threat to democracy featured heavily in President Biden's September 2022 speech celebrating the US constitution.

“Equality and democracy are under assault. Donald Trump and the MAGA Republicans represent an extremism that threatens the very foundations of our republic. MAGA Republicans do not respect the Constitution. They do not believe in the rule of law. They do not recognize the will of the people. They refuse to accept the results of a free election. And they’re working right now, as I speak, in state after state to give power to decide elections in America to partisans and cronies, empowering election deniers to undermine democracy itself (Biden 2022).”

With very recent and ongoing news that former president, Donald Trump was holding highly confidential and Top-Secret data at his address, some of which was found in use on his desk which included data on US nuclear capabilities (Barret and Leonning 2022). The US could potentially become a deeply divided and authoritarian country under the rule of the “extremists” (Biden 2022) as early as the 2024 election. Despite the upcoming election, the political tensions and uncertainty would make relying on the US solely to cover the shortfall of computing equipment unsuitable for the foreseeable future, relaying on other imports should be more stable over the period of at least 5 years increasing local production.

The new Cabinet Office report on cyber security for 2022-2030 discusses the risks posed by supply chains to government facilities and critical-national infrastructure. Their aim is to improve procurement of supplies in government facilities. As supply chains become increasingly expansive and interconnected supplier’s vulnerabilities in their systems, products and services present an increasingly attractive opportunity for adversaries (Cabinet Office 2022). The report continues to discuss how to improve their own procurement process to minimise the risks. Alignment between commercial and security functions will ensure cyber security is part of every procurement process by clearly articulating the requirements based of an understanding of risk (Cabinet Office 2022).

If the UK can produce a large computing manufacturing industry once more, it can cut those risks discussed in the report significantly by having direct control over the products that carry the highest risk. The previous report included more civil-cyber resilience via education in a joint effort with businesses and government bodies, this seems to be muted in the new report, I fear that rising international political

tensions have taken focus away from this area. This would be a shame because the public are just as at risk especially in their employment and those who have access to secure system, company secrets, data, and government systems. There is also the threat to small businesses as they cannot keep updated with training, skilled workforce, and equipment, this will eventually lead to a loss of businesses and tax income. To significantly reduce costly risk to small businesses, of disruption and loss from cyber-attacks, it is imperative to improve the cyber-security posture to overcome their limited ability to mitigate threats (Eilts 2020, p. 180).

Mobilisation and investment are key to mitigating the threats posed by manufacturing a large portion of critical computing and storage equipment in an unfriendly state. The UK has a generation who can mobilise and educate and increase the workforce needed to produce the goods that are currently a significant cyber-security threat, rendering them secure. Goods can be regularly tested, and securely packaged to ensure safety on any exports to friendly nations.

### 12.3. SAFE ONLINE SHOPPING SAFETY AND SECURE PACKAGING

The advice from the trusted manufacturers to the public on purchasing such devices indicated that high-street stores both on premises and online are the safest option for purchase due to high quality management. In fact, their knowledge of malware in e-commerce storage devices indicate it is something they are aware of and therefore something they would look for in safety checks as the biggest suppliers rely on their reputation. Some companies use secure or tamper proof packaging to ensure safety, although this was not answered in their response, Kingston recently launched a new USB device with packaging as a feature. Kingston Digital has revealed a new USB with military-grade security with XTS-AES-256-bit encryption, rechargeable battery, a PIN keypad, and the devices circuitry is coated with tamper-evident, tough epoxy to prevent access to its internal components (McCurdy 2022).

It is certainly something the UK's computer retailers should insist on in all cases to reduce the threat of goods being tampered with during transit as well as regular and on-going forensic cyber-security testing for all their devices. Secure or tamper proof packaging is providing goods that are guaranteed to remain unmodified during their transportation from factory to vendor to consumer. They are often used on screws for secure network equipment such as routers, mobile phones, storage-devices and



other highly sensitive computing and electronic equipment (dys2p, 2022). It ensures the goods have not been tampered with since their creation or at any time during transportation with several tested methods having great success such as vacuum sealing patterns of beads, coloured rice and lentils so that consumers can compare the pattern received to those sent in photos by the vendor or manufacturer (dys2p, 2022).



Figure 34 (dys2p, 2022)

Various glitter nail polishes and epoxy resin were found to be the most secure, easy to apply and cost-effective method of secure packaging in the study (dys2p, 2022). It is also one of the main tamper proof methods in the extremely securely packaged mobile phone, the Librem 5. It uses anti-interdiction techniques with glitter nail polish, a plastic sleeve covering each side with tamper-evident tape with photos sent only when the customer notifies the company, they received the package (Desai et al. 2013). The use of anti-interdiction packaging from trusted suppliers is essential to prevent tampering, even from trusted suppliers.



Figure 35 - 36 (Desai et al. 2013)

One of the reasons this has gone unnoticed for a sustained period is the lack of testing in the UK for such devices in the marketplace that lead to cyber-security

risks. We do have two world-leading organisations and government bodies the General Communications Head Quarters (GCHQ) and National Cyber Security Centre (NCSC) which, being government based would not want to involve themselves in commercial matters with national security and police matters to attend to. Trading standards oversee commercial products and services, investigating and prosecuting against commercial crimes such as counterfeit goods, tax avoidance, improper importation, custom regulations, fraud. They provide legal protection including the right return and the right to satisfactory and safe products (CTSI 2022).

Unfortunately, the shortage of skills required, cost and the time taken to examine the devices, limits the ability of trading standards to investigate with the scale of the problem too large for the organisation to handle alone. A solution to this would be to set up a permanent academic research group dedicated to continuous digital forensic analysis on existing and future high-risk imports. To begin this process a research website was created (Plews 2022) found at:

**<https://seecuredevices.com>**

The website contains a homepage with instructions on how to complete the first step of the Autopsy process for USB devices, this is aimed at hobbyists and professionals who were identified as having a clear interest in the pilot study. The public are encouraged to share their findings to the research group which will contribute to data collection on the problem, shining a light on devices that need attention and cutting testing times. It will also raise awareness of the danger to cyber-security in purchasing USB devices online on the research page and provide world-wide data collection on the USB devices which require forensic testing.

#### **12.4 CAN PUBLIC AWARENESS PREVENT THE PURCHASING OF SOLID-STATE STORAGE DEVICES VIA E-COMMERCE?**

The public survey revealed the public are not taking their cyber-security seriously enough with 63% not taking the vital step to scan external devices with anti-virus upon first use. This was asked as it is a basic in civil-cyber security resilience, although in this case it wouldn't have helped to identify the malware, as in all cases the anti-virus was unable to detect any wrongdoing due to the advanced methods. It is however, revealing of how civil-cyber security has stagnated despite growing

public awareness over the past decade when the first USB malware hit headlines and was present in pop culture. If we can improve our nation's civil-cyber security, it will keep us all safe by improving the basic security resilience of the 63% found to lack basic-cyber security skills or approximately 42.3 million UK citizens.

## 12.5 PUBLIC EDUCATION

The UK has the NCSC who do have a website dedicated to educating the public, but the results from the public survey show it is not reaching far enough (NCSC 2022). There is a section for individuals and for small businesses with highly technical information that's accessible to all, but the US counterpart goes a step further by providing a dedicated civil-cyber security education organisation and website that provides open access education and training for all (NIST 2022). We should follow suit and have a government body, connected to NCSC who can focus all their efforts and budget on civil-cyber resilience and providing education information and training for all.

We also need to include more in the national curriculum there is only a small section in the computing GCSE as follows:

“Cyber security: forms of attack (based on technical weaknesses and behaviour), methods of identifying vulnerabilities, and ways to protect software systems (during design, creation, testing, and use) (Department of Education 2015)”

Although it is in the national curriculum it has not been updated for 7 years which in cyber security terms is an age, entire systems can change in that time. It is also not enough, there is far more focus on secure software development, which although incredibly beneficial to those going into computing in further education settings, will not help every citizen to protect themselves. If we can improve the cyber-security education at this level it will stand a high chance of reaching all children and engaging public interest, which may lead to higher attention being paid to other organisations in adulthood such as NCSC.

National advertisement has always had a great impact on the public if far reaching and high quality, like the public information adverts of the previous decades and WW2 posters appealing to patriotism. In the lead up to WW2 to combat rising concern on the 'morale' of the public, the Ministry of Information was established to

produce propaganda to boost morale with most of the work undertaken in how best to communicate with the public (Bennett 2019, p.5). The language was shaped by two opposing ideologies seeking to linguistically bridge the ‘gulf’ between government and the citizens, on one hand it was authoritative, distant, and formal; and on the other colloquial, and informal (Bennett 2019, p.5). A famous example features in figure 37.

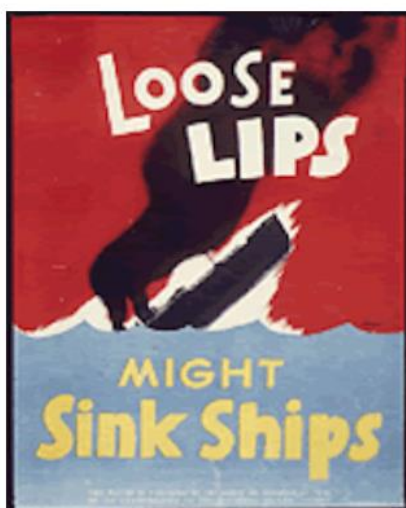


Figure 37 (*The Phrase Finder* 2022)

Investing in multi-media and advertising at a national level can draw attention to the NCSC to gain more national interest, to reach more people. Social media does play a big role in society, NCSC having a bigger presence across the platforms will be beneficial however, current posts are undisguisable from the other government bodies and may be ignored in such spaces due to their lack of entertainment.

## 12.6 PUBLIC ENGAGEMENT

Entertainment and pop culture has always been key to public information and awareness. The British Film Council and the BBC could put more focus on creation of broadcasts that engage the public with the risks of cyber-security. There are several examples recently aired, *The Undeclared War* (Channel4 2022) and *The Capture* (BBC 2022) were high budget, well written examples that really resonated with the public (Hogan 2022) causing the public to openly discuss the content, cyber-security and its relation to real world cyber-security risks (Katwala 2019).

## 12.7. UPDATING E-COMMERCE LEGISLATION

The pilot study touched on the issues raised by the current legislation for e-commerce products which were proven to be delivering unsafe and counterfeit products that put lives at risk. The current laws benefit the platform but not the public, for years public safety has been a priority in products with organisations and policy such as the EC mark for safe goods. It is undermined with current e-commerce laws and in drastic need of updating. There needs to be more liability placed on the platforms for unsafe and dangerous products, including in terms of cyber-security. It would put the platforms more in line with high-street stores, where unsafe products damage reputation and share value, leading to quality management procedures, updated policy and product testing.

## CHAPTER 13. LIMITATIONS

The study was too big for one academic in the time set aside for it. Further research would be needed for a more detailed look at the malware to determine the effects on the host system and to examine the binary manually to substantiate the Binwalk findings. It was limited by the number of devices examined relative to the number available.

## CHAPTER 14. FURTHER RESEARCH

It is clear there is vendor malware in USB devices via e-commerce but there are many more vendors both online and off to investigate and several other solid-storage devices to investigate. There is a requirement for continuous academic research to investigate cyber-security threats in retail settings on and off online. There is also further work on the use of the Intel x86 Microcode as an attack vector, the mitigations and scale of the implications. There is further interdisciplinary research in law, and business in the findings of the suspicious practices, and the future risks with manufacturing, outsourcing and importation. Finally, there is further research in civil-cyber security education for the public.

## CHAPTER 15. CONCLUSION

Advanced vendor malware has been detected using digital forensic testing on USB solid-state storage devices from e-commerce platforms. The deployment was firmware malware identified by digital forensic tools as Intel x86 Microcode, although

not conclusively proven to be the microcode it is indicative of firmware malware with 100% accuracy rate for the firmware signatures and 93.7% rate for the encryption signatures. The devices contained highly compressed files, often containing identical files indicative they are connected to the same adversary.

Evidence of differing malware being added during the attack chain when the USB devices received network access for minimum of 4 mins. Windows processes were seen rapidly creating and writing 1000's of files, indicative of a DLL attack with events showing concerning malware activities. The malware and vendors were tracked down and contacted leading to the revelation that China were the manufacturer of 100% of tracked goods and they were often involved throughout the entire supply chain. This led to the recommendation of local production and fulfilling the inevitable shortfall by increasing training in electrical engineering and repurposing existing production lines.

Mitigations for the type of malware deployment was investigated showing a weakness in UK civil-cyber security resilience to such attacks on the public and a need to update packaging. There is a clear need for a body of continuing research to look at vendor malware in all areas of retail, as it seems likely based on the timeline findings, that the attack has remained undetected for 4 years and has reached 63% of tested products, giving it a wide attack surface mostly aimed at the public, also putting their privacy and data at risk.

The e-commerce law itself allows attack vectors like these to continue unperturbed as it removes the responsibility from the platform, who often appear as an immoral logistics and marketing company. The UK needs to take action to replace and locally produce 17.5% of computing equipment it receives from China, with mounting evidence each year demonstrating it is unsafe for our national security. The findings of the research project add more evidence of large-scale malware attacks by China, in this case aimed predominately at the ordinary user.

## CHAPTER 16. REFERENCES

ALBARTUS, N. *et al.*, 2021. On the design and misuse of microcoded (embedded) processors— A cautionary note. *Usenix*, 267-284 from:

<https://www.usenix.org/conference/usenixsecurity21/presentation/albartus>

ALSAID, A. and C.J. MITCHELL, 2005. Installing Fake Root Keys in a PC from:

<https://pure.royalholloway.ac.uk/portal/files/4617217/ifrkia2.pdf>

AMAZON, 2022. Netac Amazon Store [viewed 08/09/ 2022]. Available

from: [https://www.amazon.co.uk/stores/Netac/page/4679EB13-5201-4F95-BE5D-6549FB654EF2?ref\\_=ast\\_bln](https://www.amazon.co.uk/stores/Netac/page/4679EB13-5201-4F95-BE5D-6549FB654EF2?ref_=ast_bln)

ANDERSON, B. and B. ANDERSON, 2010. Seven deadliest USB attacks. Syngress from:

<https://books.google.co.uk/books?id=T6jzJkqNonkC&printse>

ANDERSON, R., 2020. Security engineering: a guide to building dependable distributed systems. John Wiley & Sons from:

[https://www.google.co.uk/books/edition/Security\\_Engineering/GNIHEAAAQBAJ](https://www.google.co.uk/books/edition/Security_Engineering/GNIHEAAAQBAJ)

anonymousexploit 2022a. [viewed 07/06/ 2022]. Available

from: <https://www.anonymousexploit.com>

ASLAN, ÖA. and R. SAMET, 2020. A comprehensive review on malware detection approaches. *IEEE Access*, 8, 6249-6271 from:

<https://ieeexplore.ieee.org/abstract/document/8949524>

BARKER, A. *et al.*, 2020. Artifice: Data in disguise from: <https://par.nsf.gov/biblio/10282235>

BARRET and LEONNING, 2022. Material on foreign nation's nuclear capabilities seized at Trump's Mar-a-Lago. *washingtonpost.com*, 06/09/ from:

<https://www.washingtonpost.com/national-security/2022/09/06/trump-nuclear-documents/>

BBC, 2021. Online sellers 'hotbed' for dangerous items experts warn. BBC from:

<https://www.bbc.co.uk/news/technology-59432079>

BBC, 2022a. Capitol riots timeline: What happened on 6 January 2021?[viewed 12/09/ 2022].

Available from: <https://www.bbc.co.uk/news/world-us-canada-56004916>

BBC, 2022b. The Capture [viewed 13/09/ 2022]. Available

from: <https://www.bbc.co.uk/programmes/m00085sx>

BEATTIE, 2022. Plain Text. NDC Conferences&nbsp; YouTube: NDC Conferences from:

[https://www.youtube.com/watch?v=\\_mZBa3sqTrI](https://www.youtube.com/watch?v=_mZBa3sqTrI)

BENNETT, J, 2019. The Ministry of Information and the linguistic design of Britain's World War II propaganda from: <https://core.ac.uk/download/pdf/267198955.pdf>

BIDEN JOE, 2022. Remarks by President Biden on the Continued Battle for the Soul of the Nation [viewed 12/09/ 2022]. Available from: <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/01/remarks-by-president-bidenon-the-continued-battle-for-the-soul-of-the-nation/>

<https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/01/remarks-by-president-bidenon-the-continued-battle-for-the-soul-of-the-nation/>

BRITTON, 2021. Huawei accused of stealing trade secrets, spying in Pakistan [viewed 20/09/2022] from: <https://www.reuters.com/legal/transactional/huawei-accused-stealing-trade-secrets-spying-pakistan-2021-08-12/>

BSI, 2015. ISO 9001:2015. bsi. [viewed 21/03/2022].  
from: <https://bsol.bsigroup.com/Search/Search?searchKey=ISO9001&OriginPage>

CABINET OFFICE, 2022. Government Cyber Security Strategy: 2022 to 2030. gov.co.uk: Cabinet Office Available from: <https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030>

CAMACHO, P., 2019. Ransomware MongoLock Immediately Deletes Files, Formats Backup Drives. *trendmicro*, Jan from: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-mongolock-immediately-deletes-files-formats-backup-drives>

CHAKKARAVARTHY, S.S., D. SANGEETHA and V. VAIDEHI, 2019. A survey on malware analysis and mitigation techniques. *Computer Science Review*, 32, 1-23 from: <https://www.sciencedirect.com/science/article/abs/pii/S1574013718301114>

CHANNEL, 4., 2022. The Undeclared War [viewed 13/09/ 2022]. Available from: <https://www.channel4.com/programmes/the-undeclared-war>

Check Company 2022b. [viewed 25/07/ 2022]. Available from: <http://www.checkcompany.co.uk/company/11797032/KOVA-ASSOCIATES-LTD>

CHERQI, O. et al., 2018. Analysis of hacking related trade in the darkweb. 2018 IEEE international conference on intelligence and security informatics (ISI). IEEE, pp.79-84 from: <https://ieeexplore.ieee.org/abstract/document/8587311>

CITY MAYORS STATISTICS, 2021. The UK's 200 largest towns, cities and districts [viewed 25/05/ 2022]. Available from: [http://www.citymayors.com/gratis/uk\\_topcities.html](http://www.citymayors.com/gratis/uk_topcities.html)

COMPANYDIRECTORCHECK, 2022. Company Director Check [viewed 25/07/ 2022]. Available from: <https://www.companydirectorcheck.com/yun-gao-8>

CONACHER, J., K. RENAUD and J. OPHOFF, 2020. Caveat Venditor, used USB drive owner. *Used USB Drive Owner (June 19, 2020)* from: <https://arxiv.org/abs/2006.11354>

CRENSHAW, A., 2011. Plug and prey: Malicious USB devices. Proceedings of ShmooCon, from: <http://www.irongeek.com/i.php?page=security/plug-and-prey-malicious-usb-devices>

CTSI, 2022. *Looking for Consumer Help and Advice?*[viewed 19/09/ 2022]. from: [Consumer Help and Advice | CTSI - Chartered Trading Standards Institute UK](https://www.ctsi.org.uk/consumer-help-and-advice)

DAVIS, S.J., 2019. RISING POLICY UNCERTAINTY. Rising policy uncertainty from: <https://www.nber.org/papers/w26243>

DEPARTMENT OF EDUCATION, 2015. Computer science GCSE subject content [viewed 13/09/ 2022]. Available from: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/397550/GCSE\\_subject\\_content\\_for\\_computer\\_science.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/397550/GCSE_subject_content_for_computer_science.pdf)



- DESAI, A.R. et al., 2013. Interlocking obfuscation for anti-tamper hardware. ACM, 1-4 from <https://dl.acm.org/doi/abs/10.1145/2459976.2459985>
- DUIVENVOORDE, B., 2022. The Liability of Online Marketplaces under the Unfair Commercial Practices Directive, the E-commerce Directive and the Digital Services Act. Journal of European Consumer and Market Law, 11(2) from: <https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/11.2/EuCML2022009>
- DYS2P, 2022. Random Mosaic - Detecting unauthorized physical access with beans, lentils and colored rice [viewed 29/08/ 2022]. Available from: <https://dys2p.com/en/2021-12-tamper-evident-protection.html>
- eBay, 2022 from: <https://www.ebay.co.uk/>
- EILTS, D., 2020. An empirical assessment of cybersecurity readiness and resilience in small businesses from: <https://core.ac.uk/download/pdf/304334147.pdf>
- ELBAHRAWY, A. et al., 2020. Collective dynamics of dark web marketplaces from: <https://www.nature.com/articles/s41598-020-74416-y>
- ELECTRICAL SAFETY FIRST, 2021. Online Marketplaces A Hotbed For Dangerous Goods Coalition Of Industry Bodies Warns [viewed 31/05. 2022]. Available from: <https://www.electricalsafetyfirst.org.uk/media-centre/press-releases/2021/11/online-marketplaces-a-hotbed-for-dangerous-goods-coalition-of-industry-bodies-warns/>
- ENDOLE, 2022. Key Data [viewed 25/07/ 2022]. Available from: <https://suite.endole.co.uk/insight/company/11797032-kova-associates-ltd>
- FINGAS, 2019. Amazon told to stop tricking UK users into signing up for Prime from: <https://www.engadget.com/2019-10-30-amazon-prime-uk-promo-found-deceptive.html>
- GHADGE, A. et al., 2018. Managing cyber risk in supply chains: A review and research agenda from: <https://www.emerald.com/insight/content/doi/10.1108/SCM-10-2018-0357/full/html>
- GOLDSMITH, J., 2000. Unilateral Regulation of the Internet: A Modest Defence. EJIL, 11(1), 135-148 from: <https://academic.oup.com/ejil/article/11/1/135/383107>
- GOOGLE, 2022. Google Maps [viewed 25/07/ 2022]. Available from: <https://www.google.com/maps/place/21+Ellesmere+Ave,+Worsley>
- GOV.UK, 2022. Companies House [viewed 25/07/ 2022]. Available from: <https://find-and-update.company-information.service.gov.uk/>
- GURI, M., 2021. USBculprit: USB-borne Air-Gap Malware. ACM, , 7-13 from: <https://dl.acm.org/doi/abs/10.1145/3487405.3487412>
- HALDERMAN, J.A. and E.W. FELTEN, 2006. Lessons from the Sony CD DRM Episode. USENIX Security Symposium. pp.77-92 from: [https://www.usenix.org/legacy/event/sec06/tech/full\\_papers/halderman/halderman\\_html/](https://www.usenix.org/legacy/event/sec06/tech/full_papers/halderman/halderman_html/)
- HAMILTON, 2020. The US says Huawei has been spying through 'back doors' designed for law enforcement – which is what the US has been pressuring tech companies to do for

years. *businessinsider.com* from: <https://www.businessinsider.com/us-accuses-huawei-of-spying-through-law-enforcement-backdoors-2020-2?r=US&IR=T>

HOGAN, 2022. 'Spooks meets Black Mirror': how The Capture became the year's most wildly compelling TV show. *The Guardian*, 12/09/2022 from: <https://www.theguardian.com/tv-and-radio/2022/sep/12/how-the-capture-became-the-years-most-wildly-compelling-tv-show>

JAYS TECH VAULT, 2020. I Bought a \$3 2TB USB Drive and Got More Than Just Malware Available from: <https://www.youtube.com/watch?v=q2mDGIFlODI>

KASKA, K., H. BECKVARD and T. MINÁRIK, 2019. Huawei, 5G and China as a security threat. NATO Cooperative Cyber Defence Center for Excellence (CCDCOE) from: <http://195.222.11.251/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf>

KATWALA, 2019. How BBC One's The Capture created a realistic take on CCTV. *Wired*, 4/09/2019 from: <https://www.wired.co.uk/article/bbc-drama-the-capture-realistic-cctv>

KITCHEN, E.A., 2022. *hak5/usbrubberducky-payloads* [viewed 30/06/ 2022]. From: [GitHub - hak5/usbrubberducky-payloads: The Official USB Rubber Ducky Payload Repository](https://github.com/hak5/usbrubberducky-payloads)

KOCH, L., 2019. What's Driving the Top Five Retail Ecommerce Markets Worldwide? accessed March, 5, 2020 from: [https://contentstorage-na1.emarketer.com/8a9d217d5c3f214c602da3f50ba5183b/Whats\\_Driving\\_the\\_Top\\_Five\\_Retail\\_Ecommerce\\_Markets\\_Worldwide\\_eMarketer.pdf](https://contentstorage-na1.emarketer.com/8a9d217d5c3f214c602da3f50ba5183b/Whats_Driving_the_Top_Five_Retail_Ecommerce_Markets_Worldwide_eMarketer.pdf)

KONDRATEV, M.I., A.A. GAMOVA and V.V. GUROV, 2020. USB Devices with Hardware Backdoor. *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, pp.141-143 from: <https://ieeexplore.ieee.org/abstract/document/9039065>

KOPPE, P. et al., 2017. Reverse engineering x86 processor microcode. *usenix*, 1163-1180 from: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/koppe>

LAKSHMANAN, 2022. Researchers Warn of 'Raspberry Robin' Malware Spreading via External Drives. *The Hacker News*, May from: <https://thehackernews.com/2022/05/researchers-warn-of-raspberry-robin.html>

LYSNE, O. et al., 2016. Vendor malware: detection limits and mitigation. *Computer*, 49(8), 62-69 from: <https://ieeexplore.ieee.org/abstract/document/7543430>

MCCURDY, 2022. Kingston's new USB drive features a frankly unreal amount of military-grade security. *techradar*, 12/09/22 from: <https://www.techradar.com/news/kingston-reveals-its-most-secure-usb-drive-ever>

MAHBOUBI, A., S. CAMTEPE and H. MORARJI, 2018. Reducing USB attack surface: A lightweight authentication and delegation protocol. *IEEE*, 1-7 from: <https://ieeexplore.ieee.org/abstract/document/8538400>

MARKETTOS, T. et al., 2019. Thunderclap: Exploring vulnerabilities in operating system IOMMU protection via DMA from untrustworthy peripherals. *Cambridge* from: <https://www.repository.cam.ac.uk/handle/1810/288484>

MUDIYANTO, 2022. *Make a USB Rubber Ducky with less than \$3* [viewed 20/09/ 2022]. Available from: <https://infosecwriteups.com/make-usb-rubber-ducky-with-less-than-3-fa72dac9e4de>

A.K. PERZANOWSKI, 2007. The magnificence of the disaster: Reconstructing the Sony BMG rootkit incident. *Berkeley Tech.LJ*, 22, 1157 from: [https://heinonline.org/HOL/Page?handle=hein.journals/berktech22&div=51&g\\_sent=1&collection=journals](https://heinonline.org/HOL/Page?handle=hein.journals/berktech22&div=51&g_sent=1&collection=journals)

NCSC, 2020. Buying and selling second-hand devices [viewed 09/06/ 2022]. Available from: <https://www.ncsc.gov.uk/guidance/buying-selling-second-hand-devices>

NCSC, 2022. The National Cyber Security Centre [viewed 13/09/ 2022]. Available from: <https://www.ncsc.gov.uk/>

NETAC, 2022. Netac [viewed 08/09/ 2022]. Available from: <https://www.netac.com>

NETWORKCHUCK, 2021. *bad USBs are SCARY!! (build one with a Raspberry Pi Pico for \$8)* [viewed 30/06/ 2022]. Available from: [https://www.youtube.com/watch?v=e\\_f9p-JWZw](https://www.youtube.com/watch?v=e_f9p-JWZw)

NISSIM, N., R. YAHALOM and Y. ELOVICI, 2017. USB-based attacks. *Computers & Security*, 70, 675-688 from: <https://www.sciencedirect.com/science/article/pii/S0167404817301578>

NIST, 2022. NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) [viewed 13/09/ 2022]. Available from: <https://www.nist.gov/itl/applied-cybersecurity/nice>

NORTH DATA, 2022. EUROPEAN COMPANIES SEARCH ENGINE [viewed 08/09/ 2022]. Available from: <https://www.northdata.com/>

O. LYSNE, et al., 2016. Vendor Malware: Detection Limits and Mitigation, *IEEE*, pp.62-69 from: <https://ieeexplore.ieee.org/abstract/document/7543430>

THE OFFICE OF NATIONAL STATISTICS, 2022. *Data tables for: Retail Sales Index - Internet Reference Tables*. [www.ons.gov.uk](http://www.ons.gov.uk) gov.uk from: <https://www.ons.gov.uk/businessindustryandtrade/retailindustry/datasets/retailsalesindexinternetsales>

OFFICE FOR NATIONAL STATISTICS, 2022. UK trade with China: 2021 [viewed 09/09/ 2022]. Available from: <https://www.ons.gov.uk/economy/nationalaccounts/balanceofpayments/articles/uktrade-with-china2021/2022-06-01#uk-trade-in-goods-with-china>

OKORIE, O. et al., 2020. Manufacturing in the time of COVID-19: an assessment of barriers and enablers. *IEEE Engineering Management Review*, 48(3), 167-175 from: <https://ieeexplore.ieee.org/abstract/document/9149579>

OPEN THREAT EXCHANGE, 2022. Alien Vault OTX [viewed 30/08/ 2022]. Available from: <https://otx.alienvault.com/indicator/ip/13.224.245.97>

OPSS, 2021. Government Issues Online Marketplace Product Safety Message [viewed 31/05. 2022]. Available from: <https://www.gov.uk/government/news/government-issues-online-sales-product-safety-message>

ORI OR-MEIR, NIR NISSIM, YUVAL ELOVICI, AND LIOR ROKACH, 2019. Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. ACM,

OWAIDA, 2020. Buying a secondhand device? Here's what to keep in mind [viewed 09/06/2022]. Available from: <https://www.welivesecurity.com/2020/04/22/buying-secondhand-device-what-keep-in-mind/>

PANDEY, S. et al., 2020. Cyber security risks in globalized supply chains: conceptual framework from: [https://www.researchgate.net/publication/338668641\\_Cyber\\_security\\_risks\\_in\\_globalized\\_supply\\_chains\\_conceptual\\_framework](https://www.researchgate.net/publication/338668641_Cyber_security_risks_in_globalized_supply_chains_conceptual_framework)

PENG, H. and M. PAYER, 2020. {USBfuzz}: A Framework for Fuzzing {USB} Drivers by Device Emulation. usenix, 2559-2575 from: <https://www.usenix.org/conference/usenixsecurity20/presentation/peng>

PLEWS, 2022. *SeeCure Devices* [viewed 19/09/ 2022]. Available from: <https://seecuredevices.com>

RANKIN, 2022. Anti-Interdiction on The Librem 5 USA [viewed 12/09/ 2022]. Available from: <https://puri.sm/posts/anti-interdiction-on-the-librem-5-usa/>

ROKICKI, T., 2018. E-commerce market in Europe in B2C. Information Systems in Management, 7 from: <https://bibliotekanauki.pl/articles/94731>

SAMMONS, J., 2012. The basics of digital forensics: the primer for getting started in digital forensics. Elsevier from: <https://books.google.co.uk/books?id=H-59BAAAQBAJ>

SCROXTON, 2022. MI5, FBI chiefs warn of Chinese cyber espionage threat. Computer Weekly, 7/07/2022 from: <https://www.computerweekly.com/news/252522463/MI5-FBI-chiefs-warn-of-Chinese-cyber-espionage-threat>

SUN, C., J. LU and Y. LIU, 2021. Analysis and Prevention of Information Security of USB. IEEE, , 25-32 from: <https://ieeexplore.ieee.org/abstract/document/9588135>

TAHIR, R., 2018. A study on malware and malware detection techniques. International Journal of Education and Management Engineering, 8(2) <https://www.mecspress.org/ijeme/ijeme-v8-n2/IJEME-V8-N2-3.pdf>

THE OFFICE OF NATIONAL STATISTICS, 2022. Data tables for: Retail Sales Index - Internet Reference Tables. [www.ons.gov.uk](http://www.ons.gov.uk) Available from: <https://www.ons.gov.uk/businessindustryandtrade/retailindustry/datasets/retailsalesindexinternetsales>

THE PHRASE FINDER, 2022. What's the meaning of the phrase 'Loose lips sink ships'? [viewed 13/09/ 2022]. Available from: <https://www.phrases.org.uk/meanings/loose-lips-sink-ships.html>

THREATMINER, 2022. SSL [viewed 05/09/ 2022]. Available from: <https://www.threatminer.org/ssl.php?q=d69b561148f01c77c54578c10926df5b856976ad>

CTSI, 2022. Looking for Consumer Help and Advice? [viewed 19/09/ 2022]. Available from: <https://www.tradingstandards.uk/consumer-help/>

UK Guns and Ammo Store 2022c. [viewed 07/06/ 2022]. Available from: [onili244aue7jkvzn2bgaszcb7nznkpyihdhh7evflp3iskfq7vhlzid.onion](https://onili244aue7jkvzn2bgaszcb7nznkpyihdhh7evflp3iskfq7vhlzid.onion)

UK Passports 2022d. [viewed 07/06/ 2022]. Available from: [wosc4noitfscyywccasl3c4yu3lftpl2adxuvprp6sbg4fud6mkrwqqd.onion](https://wosc4noitfscyywccasl3c4yu3lftpl2adxuvprp6sbg4fud6mkrwqqd.onion)

ULLRICH, C., 2019. New Approach Meets New Economy-Enforcing EU Product Safety in E-commerce from: <https://journals.sagepub.com/doi/abs/10.1177/1023263X19855073>

ULLRICH, C., 2021. Unlawful Content Online from: <https://www.nomos-elibrary.de/10.5771/9783748927051/unlawful-content-online>

WEST and LANSANG, 2018. Global manufacturing scorecard: How the US compares to 18 other nations [viewed 12/09/ 2022]. Available from: <https://www.brookings.edu/research/global-manufacturing-scorecard-how-the-us-compares-to-18-other-nations/>

WHICH?, 2021. How to avoid fake and dangerous products [viewed 31/05. 2022]. Available from: <https://www.which.co.uk/reviews/online-shopping/article/online-shopping/how-to-avoid-fake-and-dangerous-products-ax1RW5d7peY8>

## APPENDIX 1. USB PACKAGING

Figures 1 & 2- USB 1 as sent in packaging.

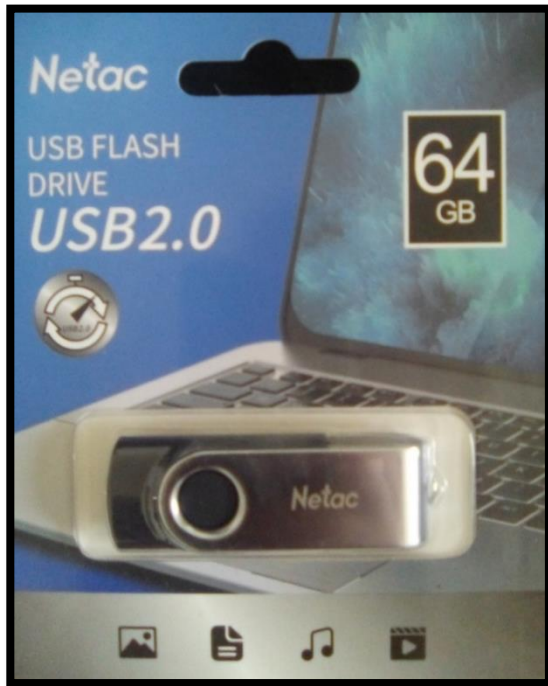


Figure 1

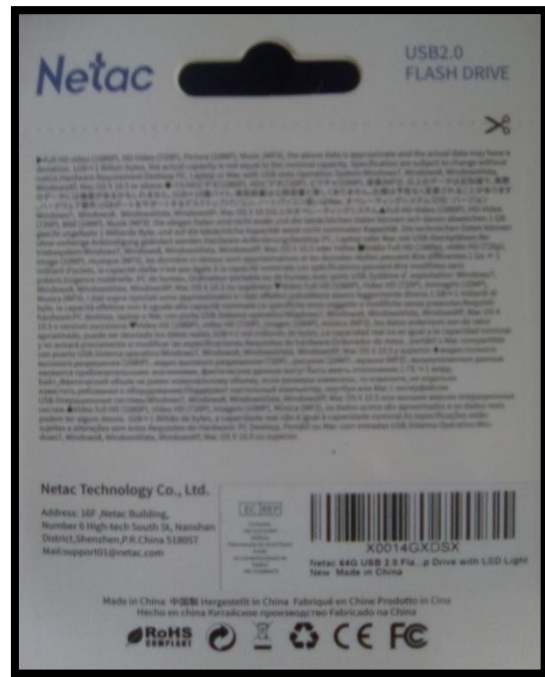


Figure 2



Figure 3

Figure 3- USB 1 can be accessed without fully opening the packaging.

Figure 4 & 5- USB 2 device in packaging which had to have the packaging fully removed to access.



Figure 4



Figure 5

Figures 6 & 7- USB 3 device as it was sent in packaging.



Figure 6



Figure 7

Figure 8 - The packaging is accessible without opening the remainder.



Figure 8

Figure 9- USB 4 device as sent in packaging.



Figure 9

Figure 10- The Amazon USB 1 order and store



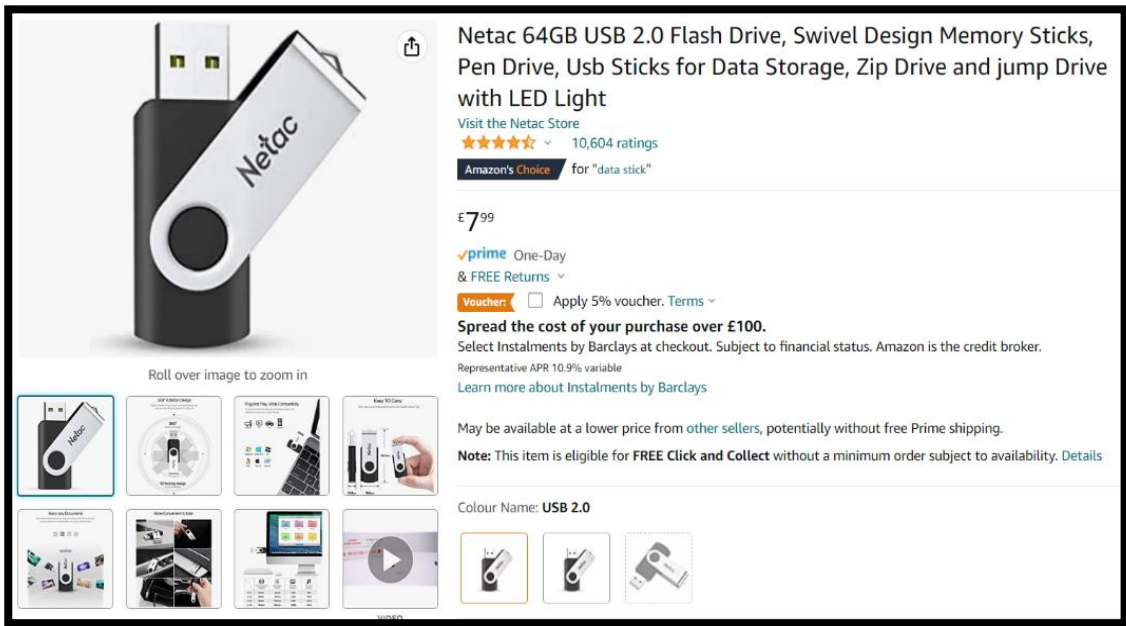


Figure 10

Figure 3- The Amazon USB 2 order and store.

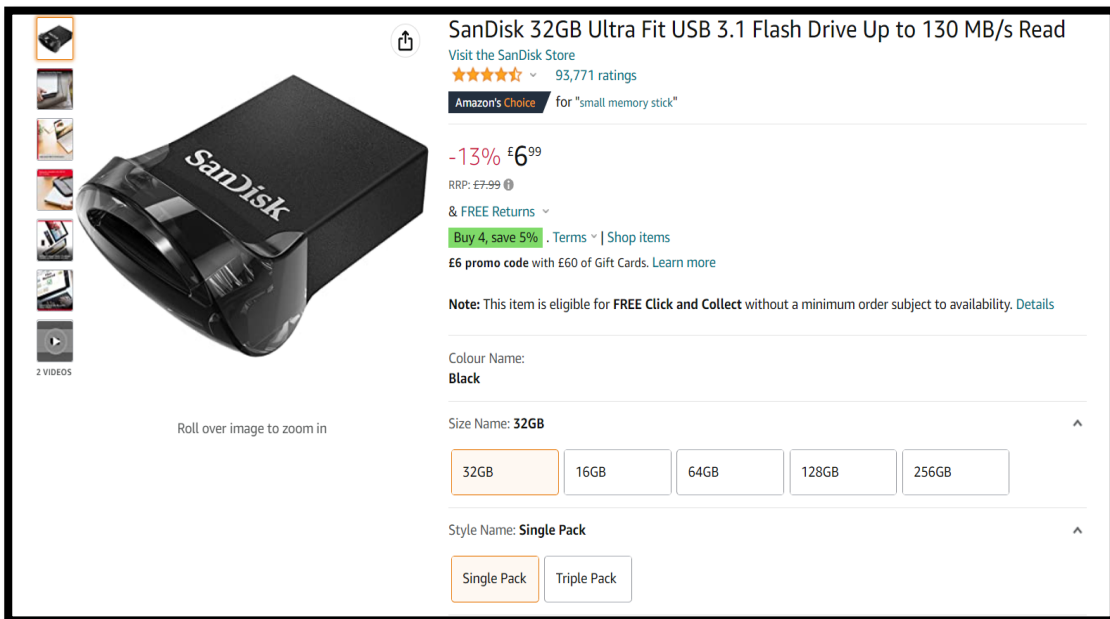


Figure 11

Figure 4- The eBay USB 3 order and seller



Figure 12

Figure 13 & 14- The original seller is featured in the order history of figure 2 but has set the item to unavailable, the same device is still being sold by many eBay sellers with the same, specifications, marketing, descriptions, and delivery origin from China.

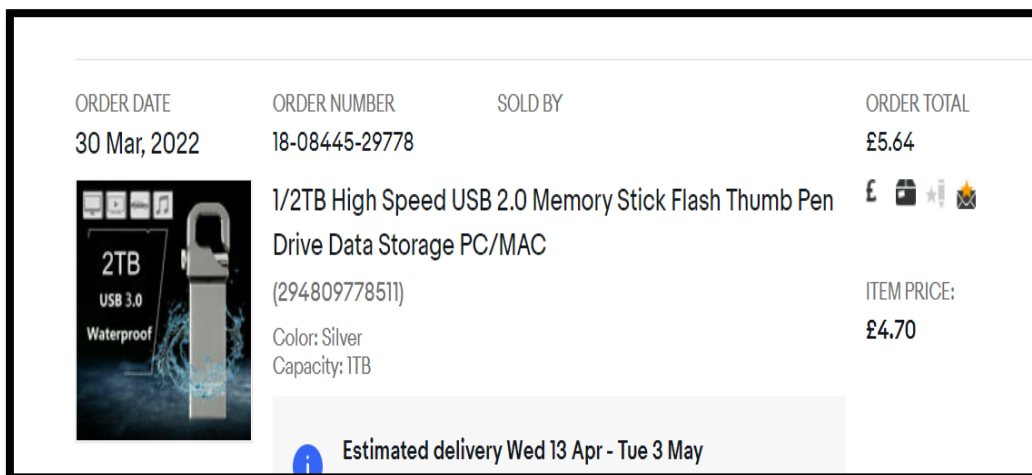


Figure 13

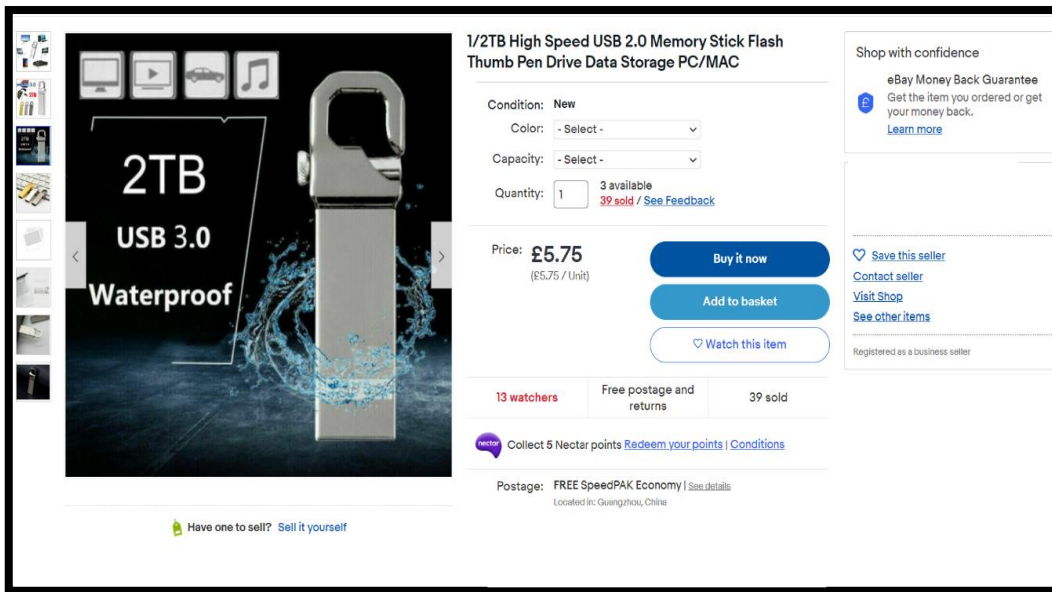


Figure 14

## APPENDIX 2. UNALLOCATED BLOCK RESULTS

Figure 1- USB 1 results from Autopsy showed out of the ( ) unallocated blocks, ( ) contained HEX values.

0x00000000:	00 00 FC 7F 02 00 00 00	11 00 C4 7F 25 00 FC 7F	.....\$...
0x00000010:	10 01 7C 7C 43 02 88 FF	01 10 44 4B 04 23 74 75	..  C....DK.#tu
0x00000020:	20 F0 FC 68 41 1D 12 2D	F1 11 D2 26 F5 A6 0C 0D	..hA...-...&....
0x00000030:	30 0D 4F 46 4E DA 8F EA	E1 C5 A1 1E C6 D7 BC 04	0.OFN.....
0x00000040:	40 98 7A CB 7C 6A B2 65	D1 EB 2E EC 8F D5 EE C0	@.z. j.e.....
0x00000050:	50 D1 BF D6 3F 6F 2D 3A	C1 43 3D 95 0D 56 69 3F	P...?o-:..C=.Vi?
0x00000060:	60 F8 96 BE 8C 4E 69 4C	B1 8D D8 2A 9F 92 C2 38	`....NiL...*...8
0x00000070:	70 4D B0 82 04 25 3F 7E	A1 89 54 A8 B3 78 63 E8	pM...\$?~...T..xc.
0x00000080:	80 10 F4 DC 27 9C 28 46	91 F7 4C F2 D5 36 55 F9	....'.(F..L..6U.
0x00000090:	90 81 82 32 1A 2E 4B 8E	81 97 A5 F5 18 35 EA 88	...2..K.....5..
0x000000a0:	A0 E0 B3 64 F7 B3 5E FB	71 29 8A E6 1E 6C 40 1F	...d..^q)...l@.
0x000000b0:	B0 6D 18 82 40 7F 50 BB	61 6D 6E 9F 77 E2 CF 7B	.m..@.P.amn.w...{
0x000000c0:	C0 68 78 57 63 B2 9C E0	51 23 0E 20 92 DC A6 80	.hxWc...Q#. ....
0x000000d0:	D0 11 D4 E0 E0 0F D5 A9	41 0B 6D 2C FD FF 4F D4	.....A.m,..O.

Figure 2

Figure 2- USB 2 results from Autopsy of the unallocated blocks containing no machine code.

```

0x00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Figure 2

Figure 3 & 4 - USB 3 results from Autopsy of the unallocated blocks containing no machine code instead they are either switched off with 00000000 or fully on with FFFFFFFF.

```

0x00000000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Figure 3

```
0x00000000: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000010: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000020: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000030: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000040: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000050: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000060: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000070: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000080: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000090: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x000000a0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x000000b0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x000000c0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x000000d0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x000000e0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x000000f0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000100: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000110: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0x00000120: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
```

Figure 4

Figure 5 - The results of USB 4 showing that no HEX data can be read using Autopsy.

```
(offset 0-16,384 could not be read)
```

Figure 5

Figure 6- USB 4 example of text found in 11 unallocated spaces of out of 957.

```
                                06CV
jKWNI
oX(
t&U/
)OX=
C:%W4
J.[d
vWtf+
+                                $M
:,:S:
][:_k3
g.Wmw
~ZF[
g\&w
7+L:
Y):13V
SA{!g
```

Figure 6

### APPENDIX 3. DELETED FILES & MATCHING FILES

Figure 1 & 2 - Matching filename, type and MD5 hash found on USB 1 and USB 4.

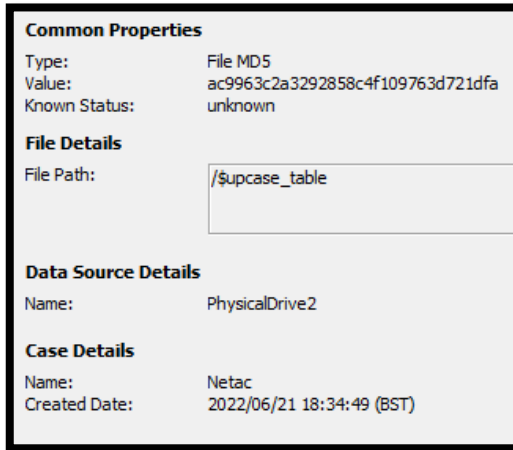


Figure 1

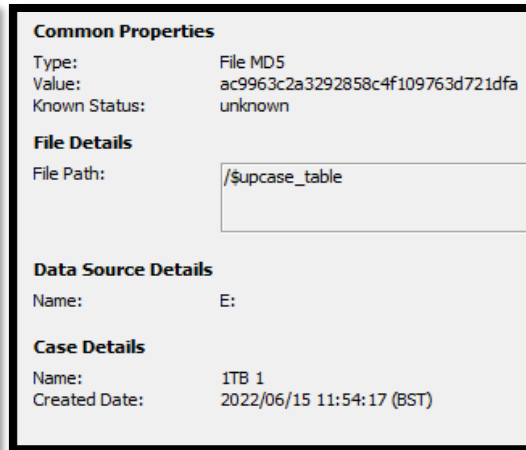


Figure 2

Figure 3 - Carved video files located on USB 4.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Flags(Dir)	Size
f1587576.swf			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	Unallocated	260931584
f1901688.swf			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	Unallocated	100106240
f1915094.swf			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	Unallocated	93224960

Figure 3

### APPENDIX 4. BINWALK AND ENTROPY RESULTS

Figure 1 shows the entropy results of USB 1, it does not go up to the same value and stays below 1 as well as having a second rising and falling edge. This test was repeated on further random data sets of varying sizes to assess the credibility of the entropy reading as being conclusively not generated from random binary.

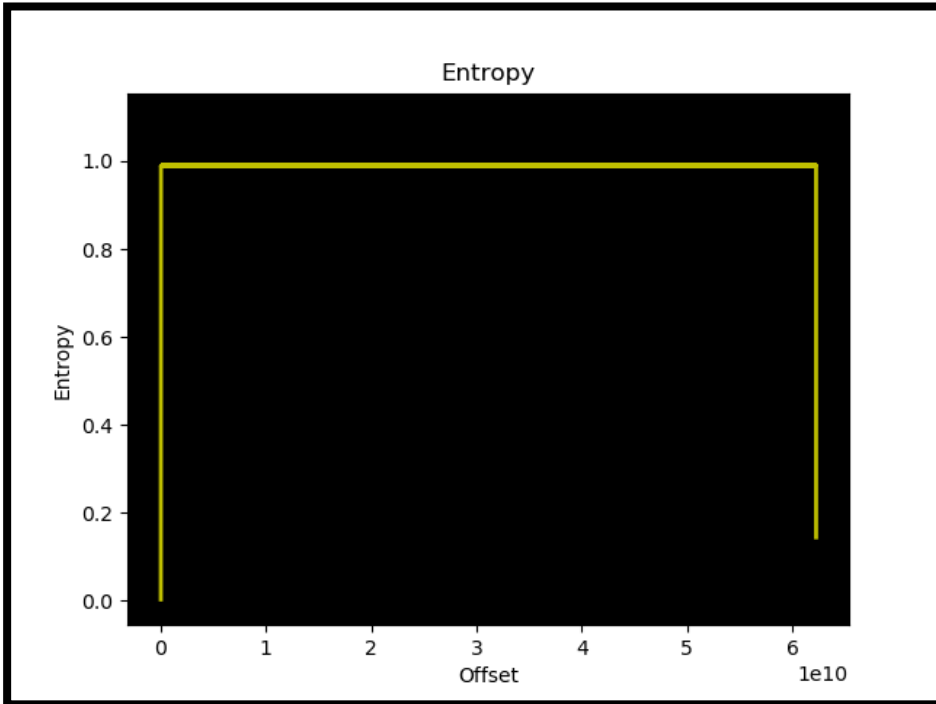


Figure 1- USB 1 Results

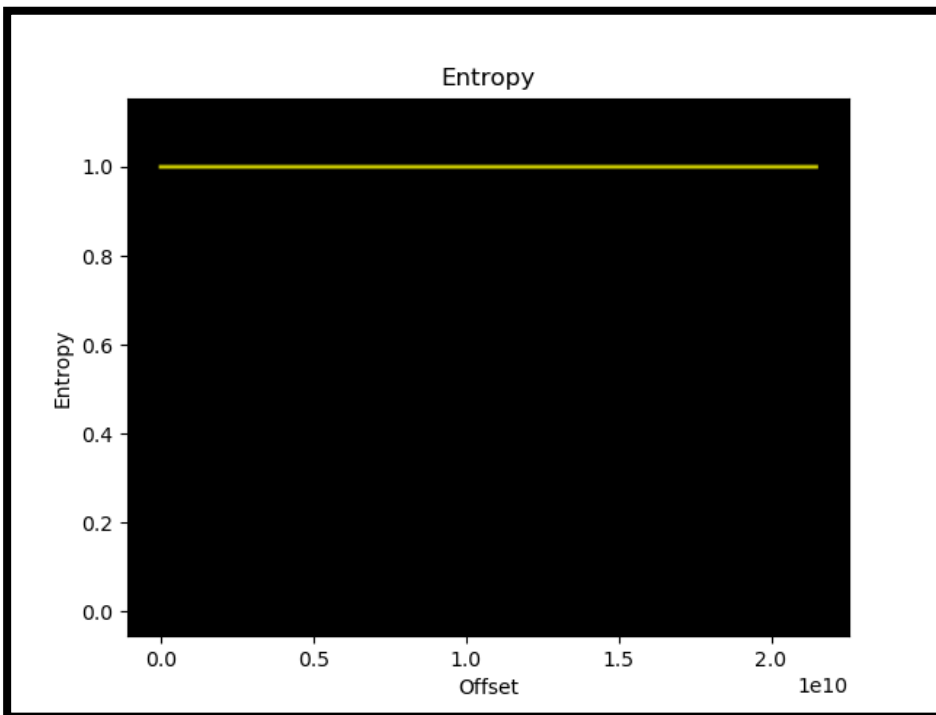


Figure 2 - All Random Data Result

Figure 3- USB 1 large block of encrypted signatures. In random data the encryption signatures were not in a large block in the binary or with the same algorithm as shown on USB 1 here.

```

L0422505474 0x26D3AD002 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422505986 0x26D3AD202 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422506498 0x26D3AD402 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422507010 0x26D3AD602 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422507522 0x26D3AD802 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422508034 0x26D3ADA02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422508546 0x26D3ADC02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422509058 0x26D3ADE02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422509570 0x26D3AE002 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422510082 0x26D3AE202 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422510594 0x26D3AE402 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422511106 0x26D3AE602 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422511618 0x26D3AE802 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422512130 0x26D3AEA02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422512642 0x26D3AEC02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422513154 0x26D3AEE02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422513666 0x26D3AF002 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422514178 0x26D3AF202 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422514690 0x26D3AF402 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422515202 0x26D3AF602 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422515714 0x26D3AF802 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422516226 0x26D3AFA02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422516738 0x26D3AFC02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422517250 0x26D3AFE02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422517762 0x26D3B0002 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422518274 0x26D3B0202 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422518786 0x26D3B0402 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422519298 0x26D3B0602 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422519810 0x26D3B0802 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit
L0422520322 0x26D3B0A02 mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, keymode: 8bit

```

Figure 3

Figure 4 - This shows the 2652 Intel microcode signatures for updating Intel processors, this was located only in a block as seen here and was not found at all in varying sized random data sets.

```

4453391876 0x109715E04 Intel x86 or x64 microcode, sig 0x19715f10, pf_mask 0x4c5429b7, 1E0F-09-37, rev 0x-75c53def, size 4136829889
4453392388 0x109716004 Intel x86 or x64 microcode, sig 0x19732110, pf_mask 0x4c596fb7, 200F-09-37, rev 0x-75c51fef, size 4143741889
4453456388 0x109725A04 Intel x86 or x64 microcode, sig 0x1a4e0db0, pf_mask 0x4e09db7, 1A0F-09-38, rev 0x-75b679ef, size 712774594
4453456900 0x109725C04 Intel x86 or x64 microcode, sig 0x1a509d10, pf_mask 0x4ef1e3b7, 1C0F-09-38, rev 0x-75b65bef, size 719686594
4453457412 0x109725E04 Intel x86 or x64 microcode, sig 0x1a525f10, pf_mask 0x4ef729b7, 1E0F-09-38, rev 0x-75b63def, size 726598594
4453457924 0x109726004 Intel x86 or x64 microcode, sig 0x1a542110, pf_mask 0x4efc6fb7, 200F-09-38, rev 0x-75b61fef, size 733510594
4453521924 0x109735A04 Intel x86 or x64 microcode, sig 0x1b2f0b10, pf_mask 0x518f9db7, 1A0F-09-39, rev 0x-75a779ef, size 1597510594
4453522436 0x109735C04 Intel x86 or x64 microcode, sig 0x1b319d10, pf_mask 0x5194e3b7, 1C0F-09-39, rev 0x-75a75bef, size 1604422594
4453522948 0x109735E04 Intel x86 or x64 microcode, sig 0x1b335f10, pf_mask 0x519a29b7, 1E0F-09-39, rev 0x-75a73def, size 1611334594
4453523460 0x109736004 Intel x86 or x64 microcode, sig 0x1b352110, pf_mask 0x519f6fb7, 200F-09-39, rev 0x-75a71fef, size 1618246594
4567292420 0x110385A04 Intel x86 or x64 microcode, sig 0x10f7db10, pf_mask 0x32e79e10, 1A0F-10-01, rev 0x-fef79ef, size 4195883263
4567292932 0x110385C04 Intel x86 or x64 microcode, sig 0x10f99d10, pf_mask 0x32ee4d10, 1C0F-10-01, rev 0x-fef5bef, size 4202795263
4567293444 0x110385E04 Intel x86 or x64 microcode, sig 0x10fb5f10, pf_mask 0x32f22a10, 1E0F-10-01, rev 0x-fef3def, size 4209707263
4567293956 0x110386004 Intel x86 or x64 microcode, sig 0x10fd2110, pf_mask 0x32f77010, 200F-10-01, rev 0x-fef1fef, size 4216619263
4567357956 0x1103C5A04 Intel x86 or x64 microcode, sig 0x11d8db10, pf_mask 0x358a9e11, 1A0F-10-02, rev 0x-fe079ef, size 785651968
4567358468 0x1103C5C04 Intel x86 or x64 microcode, sig 0x11da9d10, pf_mask 0x358fe411, 1C0F-10-02, rev 0x-fe05bef, size 792563968
4567358980 0x1103C5E04 Intel x86 or x64 microcode, sig 0x11dc5f10, pf_mask 0x35952a11, 1E0F-10-02, rev 0x-fe03def, size 799475968
4567359492 0x1103C6004 Intel x86 or x64 microcode, sig 0x11de2110, pf_mask 0x359a7011, 200F-10-02, rev 0x-fe01fef, size 806387968
4567423492 0x1103D5A04 Intel x86 or x64 microcode, sig 0x12b9db10, pf_mask 0x382d9e11, 1A0F-10-03, rev 0x-fd179ef, size 1670387969
4567424004 0x1103D5C04 Intel x86 or x64 microcode, sig 0x12bb9d10, pf_mask 0x3832e411, 1C0F-10-03, rev 0x-fd15bef, size 1677299969
4567424516 0x1103D5E04 Intel x86 or x64 microcode, sig 0x12bd5f10, pf_mask 0x38382a11, 1E0F-10-03, rev 0x-fd13def, size 1684211969
4567425028 0x1103D6004 Intel x86 or x64 microcode, sig 0x12bf2110, pf_mask 0x383d7011, 200F-10-03, rev 0x-fd11fef, size 1691123969
4567489028 0x1103E5A04 Intel x86 or x64 microcode, sig 0x139adb10, pf_mask 0x3ad09e11, 1A0F-10-04, rev 0x-fc279ef, size 2555123970
4567489540 0x1103E5C04 Intel x86 or x64 microcode, sig 0x139c9d10, pf_mask 0x3ad5e411, 1C0F-10-04, rev 0x-fc25bef, size 2562035970
4567490052 0x1103E5E04 Intel x86 or x64 microcode, sig 0x139e5f10, pf_mask 0x3adb2a11, 1E0F-10-04, rev 0x-fc23def, size 2568947970
4567490564 0x1103F6004 Intel x86 or x64 microcode, sig 0x13a02110, pf_mask 0x3ae07011, 200F-10-04, rev 0x-fc21fef, size 2575859970
4567545564 0x1103F5A04 Intel x86 or x64 microcode, sig 0x147b0b10, pf_mask 0x3d739e11, 1A0F-10-05, rev 0x-fb379ef, size 3439859971
4567546076 0x1103F5C04 Intel x86 or x64 microcode, sig 0x147d0d10, pf_mask 0x3d78e411, 1C0F-10-05, rev 0x-fb35bef, size 3446771971
4567546588 0x1103F5E04 Intel x86 or x64 microcode, sig 0x147f5f10, pf_mask 0x3d7e2a11, 1E0F-10-05, rev 0x-fb33def, size 3453683971
4567547100 0x1103F6004 Intel x86 or x64 microcode, sig 0x14812110, pf_mask 0x3d837011, 200F-10-05, rev 0x-fb31fef, size 3460595971
4567620100 0x110405A04 Intel x86 or x64 microcode, sig 0x155cdb10, pf_mask 0x40169e11, 1A0F-10-06, rev 0x-fa479ef, size 29628675
4567620612 0x110405C04 Intel x86 or x64 microcode, sig 0x155e9d10, pf_mask 0x401be411, 1C0F-10-06, rev 0x-fa45bef, size 36540675
4567621124 0x110405E04 Intel x86 or x64 microcode, sig 0x15605f10, pf_mask 0x40212a11, 1E0F-10-06, rev 0x-fa43def, size 43452675
4567621636 0x110406004 Intel x86 or x64 microcode, sig 0x15622110, pf_mask 0x40267011, 200F-10-06, rev 0x-fa41fef, size 50364675

```

Figure 4



## APPENDIX 5. USB DEVICES IN RESEARCH STUDY

This appendix features images of the USB devices and their packaging as delivered the same address.



Figure 1, Emtec USB



Figure 2, Gigastone USB



Figure 3, Pink 1 USB



Figure 4, Integral USB



Figure 5, Kingston USB



Figure 6, Netac3 USB



Figure 7, White Netac USB



Figure 8, Pink2 USB



Figure 9, Unbranded Swivel USB



Figure 10, Vansunny USB



Figure 11, Qumox USB



Figure 12, Transend USB

The remaining USB devices came in handwritten envelopes with no further packing or in Post Office labelled small packages as pictured in figure 13.



Figure 13, Post Office Packaging



Figure 14, Golden USB



Figure 15, Hook USB



Figure 16, Mini Silver USB



Figure 17, Netac 2 USB



Figure 18, Purple USB



Figure 19, Sandisk Refurb 1 USB



Figure 20, Sandisk Refurb 1 USB



Figure 21, Silver Keychain USB



Figure 22, Waysta USB

## APPENDIX 6. VENDOR CORRESPONDENCE

The light blue rows are the researcher's emails with the dark blue being that of the seller or store. Individual tables represent each conversation.

Communication via eBay
<p>Hello</p> <p>I have found something concerning with my purchase of this order and would like to discuss it please. Can you tell me about where the stock originates from? Does it come directly from a vendor and can you give me details about them please.</p>
<p>Thanks for the message</p> <p>We have certificates from our supplier who by the way supply to so many sellers just like us. This is a mass produced item with the manufacturers having official licenses from their country to produce, sell and distribute the USBs and also many other products. We do not source from illegal vendors or black market. We sell with integrity on Ebay. We hope this concludes the matter now, we unfortunately cannot respond to your messages</p>

in a fitting timeframe as we have to prioritise the day to day running of our Ebay store.  
Thank you and have a lovely weekend ahead.

Communication via eBay

Hello

There seems to be an issue with this item, can I ask where the country of origin your supplier comes from please and if it was securely packaged? This won't be raised for refund or with eBay I would just like to understand what I have.

China

Communication via eBay for Netac 2

Hello there was a problem with this order, I wont ask for a refund or raise it with eBay I would just like to know the country of origin and if the product securely packaged? I think some sellers are falling victim to unsafe products and speaking to sellers selling USB's that have the same problems to track the issue to the vendors. The more information you can share the better.

Thank You

Dear Helen,

Thank you for contacting us about the issue with " Swivel Design Memory Sticks, Pen Drive, Usb". We are truly sorry that the item that you received did not function as promised. We understand your disappointment and apologise for any inconvenience that this may have caused you.

The country of origin is China. The order has been prepared for shipping from the fulfilment depot we work with.

Could you please be more specific what is the issue with order you have received?

We are apologising again for any inconvenience that may have caused to you.

Sincerely,

Hello

It was forensically analysed as part of a research project, and I found Microcode signatures on the not so empty blocks you save onto. Does this make any sense to you as this is very technical. Basically, it likely had something hidden on it that shouldn't be there that is concerning and if you didn't put it there the supplier did, from chats with others this seems

likely. I am trying to locate the vendor, is your supplier in Shenzhen, Guangdong?

Thanks

Dear Helen,

Thank you for contacting us about the issue with "Swivel Design Memory Sticks, Pen Drive, Usb".  
Yes the supplier is in Shenzhen, Guangdong.  
Please let us know if have to remove this listing form our store

Sincerely,

Hello

I sure can, the results are now published on my website <https://seecureddevices.com>, which will be accompanied by the white paper when it is published. Was the company Netac as it says on it, I have other devices from the direct factory, from Guangdong? I found advanced malware hidden on it.

Thanks

Communication via eBay

Have you received your item?  
If not, please let me know, we will help you.  
if you receive it , may i know that do you like our project? If yes, please leave a five star positive feedback; if not, please contact us , we will make best effort to solve it for you.  
We will give you a satisfactory solution.  
Hope your understanding and support :)  
Thanks in advance for your kindly.  
Best Regard.

Hello

Do you also trade as [redacted] ?

ah?

Hello

I received the same message from 3 sellers on the same day, word for word. The probability of that from independent sellers is 0%. I found an issue with the product, can you let me know where this was manufactured at all, company name would be fantastic



but if that's not something you feel comfortable with can you confirm the city and country please. I won't raise this issue for refund, I would just like to discuss it.

Our company has 23 stores on ebay, run by different people. We are honest sellers and have been selling products on ebay for 16 years.  
Most of our products are produced in China and we have a total of 10 warehouses, two in the UK, two in the US, one in Germany, one in Australia and four in China.  
If there is any problem with the product, you can leave us a message and we will provide the most suitable solution.  
best wishes

Hello,

You have been great! The openness and honesty from all the sellers i have spoken to is great and shows you work hard to please the customers. I have indeed found issues with it which are now published online at <https://seecuredevices.com/>. There is a white paper available soon, which contains more technical information. I have not identified you in anyway as this would be unethical, but you can see the issues with the products, they contain advanced malware. The paper will provide the technical evidence in due course.

Thanks

Integrity and protection of buyer rights are what we do all the time.  
Regarding the USB Memory Stick, we are no longer ready to continue selling it. The products we will sell in the future will expand to new energy sources, and we attach great importance to the environment.  
best wishes

Communication via eBay

Have you received your item?  
If not, please let me know, we will help you.  
if you receive it , may i know that do you like our project? If yes, please leave a five star positive feedback; if not, please contact us , we will make best effort to solve it for you.  
We will give you a satisfactory solution.  
Hope your understanding and support :)  
Thanks in advance for your kindly.  
Best Regard.

I did but it came with an issue I'm trying to look into, can you let me know where your vendor is located please and if they use secure packaging? I think we may have a rough one. Also you sent the same message from three different accounts, and they came packaged together, are they all from yourself?

Our supplier is in China, I checked the order, the three accounts are all of our company, but they are operated by different colleagues.  
best wishes

Hello

Thanks so much for your replay, can you by any chance let me know the company name you trade under please I would like to alert them of a manufacturing fault.

Our process is to report product problems to colleagues in the purchasing department, and the colleagues in the purchasing department will contact the factory, and they will decide whether to change the supplier according to the number of products in question. We don't know the name of the factory, if you have after-sales questions, you can leave us a message at any time

Hello

For more information please head to <https://seecureddevices.com/> where the findings are, a white paper will soon accompany it. All your products were found to contain advanced malware. Any chance I can have a statement or further information, is the factory based in Guangdong? I have not included anything to identify you and have left your seller names from the website and white paper as this would be unethical.

Thanks

I only know that the factory is in Guangzhou, but I don't know the exact location because I'm not from the purchasing department

Communication via Amazon

Hello, there is an issue with this product and I'm concerned about the address on the product not matching the address provided by the seller. Can you confirm did you provide the goods or did Kova Associates LTD?

What's wrong with the product? You tell me and I can help you solve it. Vansunny

Before i discuss my finding i would like to know who im speaking to about it first, you say Vansunny, then another company is the registered one on Amazon a SHENZHENSHI MAILIWEI KEJIYOUXIANGONGSI under the store RAOYI GOOD USB. On the bag it came with a different residential address that I know quite well. It is a small flat above a chip shop, with the registered company of Kova Associates owned by Mr. Yun Gao. So can you confirm who i am speaking to and why there are many companies in this chain for me before i disclose the issues with the product, which are highly complex.

I am RAOYI GOOD USB store customer service, about the product on the ask you can talk to me, I will give you a satisfactory answer, about the package with multiple addresses, you can take pictures and send me, I help you verify.

Attachments:

[kovafront.jpg](#) [kova.jpg](#)

I would like to find out why this product contains a different address, is that the vendor label or manufactures, can you confirm who this is? You have your sticker saying Vansunny and there's another on the product which means that you must be trading under both? So why two names and two owners, this makes tracking down the vendor difficult, was this intentional? I wont be raising this to Amazon I would just like to know what is going on and who to speak to about the highly technical issues found. Thanks

The first address is our manufacturer address in China, and Kova Associates LTD is one of our distributors in the UK, it is only responsible for sales and not involved in other matters, I am the customer service of RAOYI GOOD USB store, I am responsible for the after-sales service of the product, if there is any problem with the USB flash drive you received, I can help you to refund or replace it. Best regards, Vansuny

There is a problem, it has been investigated for a cyber-security research project and was found to have signatures in the binary of the unallocated spaces that match an Intel x86 Microcode, which would indicate malicious firmware, as no firmware should be on a USB let alone in secret hidden away in the binary, its considered so. Is this something you are aware of,? il this likely a few rough employees placed something on the device, or in transit or something across all products and can you explain any legitimate reasons for the blocks to contain firmware? Do them come securely packaged?

Thanks

There was no response, however days later the Amazon account's two-factor authentication telephone number changed, there were no other conversations via this Amazon account.

Email from Amazon Customer Service after discussion and review about hacked and locked account.

amazon Your Account | Amazon.co.uk

Message From Customer Service

Hello Sally,

It's Gavin again, we spoke on the phone.

I'm glad we were able to get you into your account today.

As also discussed, Two-Step Verification is a feature that adds an extra layer of security by asking you to enter a unique security code in addition to your password on computers and devices.

To sign up for Two-Step Verification, follow the steps from this Help page:

██

Lastly, I would advise that you have your email address and any other commonly/frequently used passwords changed as a precaution.

If you have any other questions or queries, please don't hesitate to let us know.

Customer Service can be reached by phone and chat 24 hours a day, 7 days a week using the link below: <https://www.amazon.co.uk/icon>, <https://www.amazon.co.uk/contact-us>

I hope this information helps, and I hope you have a lovely day.

We'd appreciate your feedback. Please use the buttons below to vote about your experience today.

Did I solve your problem?

Your feedback is helping us build Earth's Most Customer-Centric Company.

Warmest regards,

██

Amazon.co.uk

## Appendix 7. AMAZON STORE RESEARCH

LikesunGmbH - Netac 1 EU vendor



Figure 1, Netac 1 distributor label used to track the company trading in the UK.



Figure 2, residential address registered as the EU distributor address (Google 2022).

**REGISTRATION · ADDRESS · MANAGING DIRECTOR: KE**  
**CAPITAL · CORPORATE PURPOSE · ARTICLES OF ASSOCIATION · PROXY**

Hrb 1 Sept 2016 German Trade Register Announcement, Germany

**OVERVIEW**

like sun GmbH

- Change Corporate Purpose: Trade in and export...
- Change Capital: €25,000
- Change Proxy: Ist nur ein Geschäftsführer...
- Change Address: Planckstr. 59, D-45147 Essen
- Articles of association: 07/07/2016
- Change Managing Director

**TEXT**

HRB 27519: like sun GmbH, food, 45147 Essen. GmbH. Partnership agreement of July 7, 2016. **Business address:** 45147 Essen. The alike is the trade in and export of food, cosmetics, non-prescription medicines and household goods, and the implementation of logistics services. **Share capital:** EUR 25,000.00. **General representation scheme:** If only one managing director is appointed, he shall represent the company alone. If several directors are appointed, the company is represented by two directors or by a managing director together with an authorized representative. **Managing Directors:** | . Ke, Essen, ....., authorized to carry out legal transactions on behalf of the company with the power to represent itself or as a representative of a third party.

Figure 3, public company information (Northdata, 20202)



Figure 4, Picture from Netac store from Amazon of Netac factory (Amazon 2022)



Figure 5, matching factory from Netac company website (Netac, 2022)

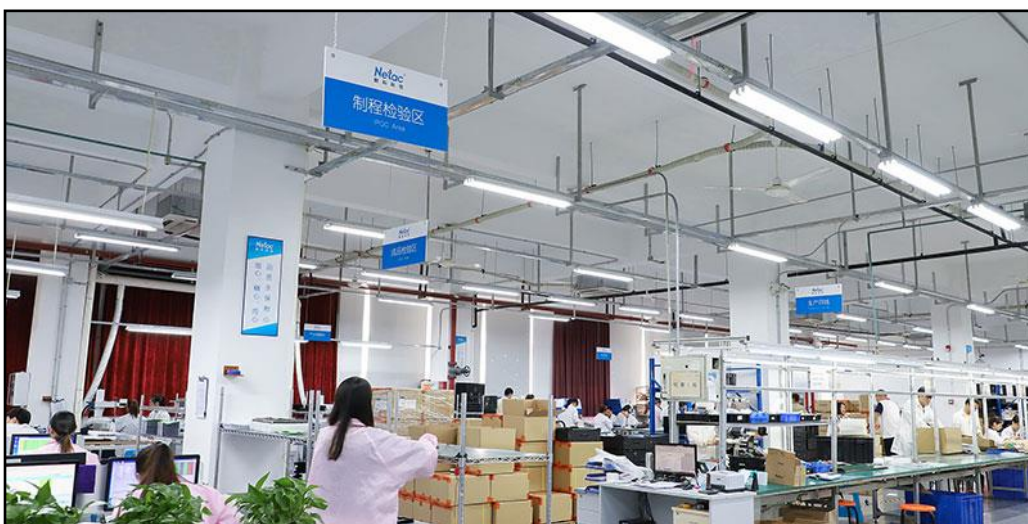


Figure 6, matching factory from Netac company website (Netac, 2022)

UKCA SERVICE LTD- Netac 2 vendor



Figure 7, Netac 2 distributor label used, features different name and surname matching Kova Associates LTD.



Figure 8, residential address registered as the UK distributor address (Google 2022)

**Ukca Service Ltd**  
21 Ellesmere Avenue, Worsley, Manchester, M28 0AL

**Overview**

- PEOPLE & CONTACTS
- FINANCIALS
- CONTROL & OWNERSHIP
- CREDIT RISK
- COMPETITION
- PROPERTY
- DOCUMENTS

**Key Data**

Ukca Service Ltd is an active company incorporated on 9 December 2020 with the registered office located in Manchester, Greater Manchester. Ukca Service Ltd has been running for 1 year 7 months. There is currently 1 active director according to the latest confirmation statement submitted on 29th April 2022.

[BUY A REPORT](#) [UPGRADE TO PRO](#)

<b>Name</b> Ukca Service Ltd	<b>Company No.</b> 13072963
<b>Status</b> ACTIVE	<b>Private Limited Company with Share Capital</b>
<b>Confirmation</b> Submitted	<b>Incorporation</b> 9 December 2020
<b>Confirmation Details:</b> <ul style="list-style-type: none"> <li>Last submitted on 29 April 2022 (2 months ago)</li> <li>Next confirmation dated 29 April 2023</li> <li>Due by 13 May 2023 (9 months remaining)</li> <li>Last change occurred 1 year 2 months ago</li> </ul>	<b>Incorporation Details:</b> <ul style="list-style-type: none"> <li>Incorporated 1 year 7 months ago</li> </ul>
<b>Size</b> Micro	<b>Classification</b> Other business support service activities n.e.c. (82990)
<b>Size Details:</b> Less than 10 employees or under £2 million turnover	

**Financials**

<b>Year Ended</b> Dec 2021	<b>Total Assets</b> £657
<b>Total Liabilities</b> £0	<b>Net Assets</b> £657
<b>Cash in Bank</b> Unreported	<b>Employees</b> 1
<b>Turnover</b> Unreported	<b>Debt Ratio (%)</b> 0%

[VIEW FINANCIALS >](#)

**Watch List**

Stay updated with Ukca Service Ltd  
Monitor changes to this company's activity with instant email notifications.

[ADD TO WATCH LIST](#)

Figure 9, company data (Endole, 2022)

<b>LIANG,</b>			
Correspondence address			
<b>Worsley, Manchester, England, M28 0AL</b>			
Role	<b>ACTIVE</b>	Date of birth	Appointed on
<b>Director</b>		<b>July 1984</b>	<b>12 April 2021</b>
Nationality		Country of residence	Occupation
<b>Chinese</b>		<b>China</b>	<b>Director</b>
<b>ZOU,</b>			
Correspondence address			
<b>London, United Kingdom, E15 4PH</b>			
Role	<b>RESIGNED</b>	Date of birth	Appointed on
<b>Director</b>		<b>October 1988</b>	<b>9 December 2020</b>
			Resigned on
			<b>12 April 2021</b>

Figure 10, company data ((Companies House) gov.uk 2022)

Kova Associates LTD - Vansunny vendor



Figure 11, Vansunny UK distributor label





Figure 12, residential address registered as the UK distributor address (Google 2022)

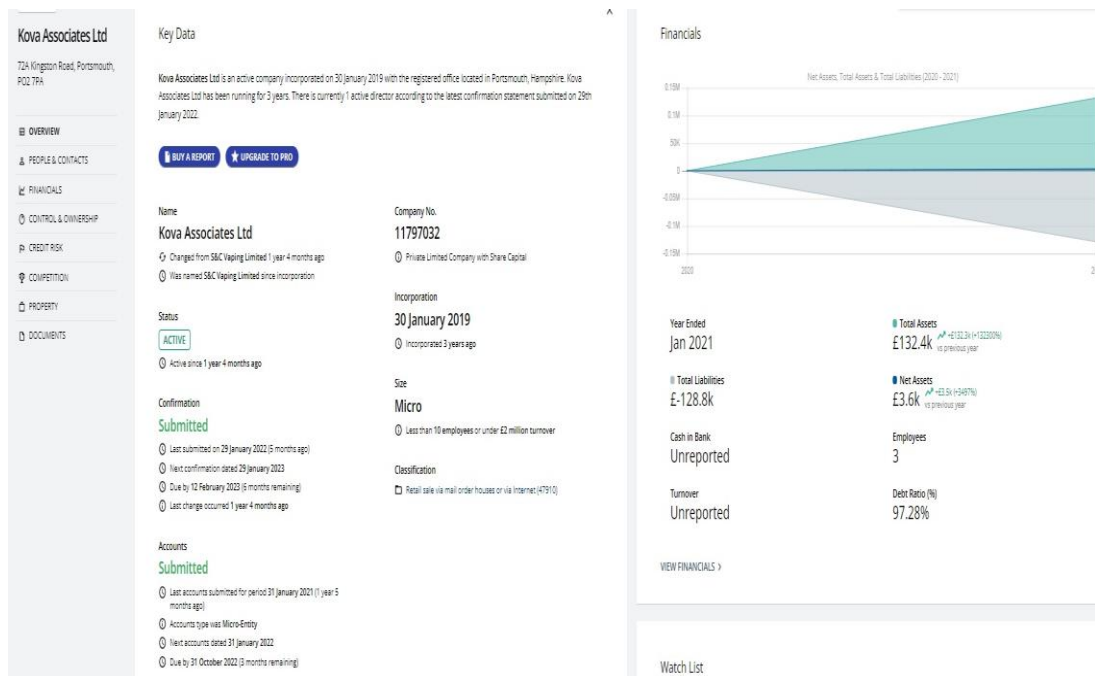


Figure 13, company data (Endole, 2022)

**GAO.**

Correspondence address

**Kingston Road, Portsmouth, England, PO2 7PA**

Role	<b>ACTIVE</b>	Date of birth	Appointed on
<b>Director</b>		<b>April 1984</b>	<b>1 February 2021</b>
Nationality	<b>Chinese</b>	Country of residence	Occupation
		<b>England</b>	<b>Managing Director</b>

**WEN.**

Correspondence address

**Thomson Crescent, Croydon, London, United Kingdom, CR0 3JT**

Role	<b>RESIGNED</b>	Date of birth	Appointed on	Resigned on
<b>Director</b>		<b>June 1989</b>	<b>30 January 2019</b>	<b>1 August 2020</b>
Nationality	<b>Chinese</b>	Country of residence	Occupation	
		<b>United Kingdom</b>	<b>Managing Director</b>	

**ZHANG.**

Correspondence address

**Randolph Avenue, London, United Kingdom, W9 1PE**

Role	<b>RESIGNED</b>	Date of birth	Appointed on	Resigned on
------	-----------------	---------------	--------------	-------------

## Appendix 8. KINGSTON & SANDISK CORRESPONDENCE

Statement from Sandisk on Microcode in US

Dear Mr. Plews,

Thank you for your understanding and cooperation and kindly note that as we discussed, there are no updates that are being performed in our USB drives, not firmware updates or as you asked, they do not include microcode for updates.

Thank you for your cooperation and allowing us to be of service to you!

Best regards,

SanDisk® Global Customer Support

Communication with Kingston

Dear Kingston Press

I am a cyber-security researcher at Solent University and I'm wondering if you can help me with a technical question. Do USBs often come with microcode, I can see your devices do not contain it, nor do many others. However, I have found a number that do and I can't seem to find why this would be the case so I am asking trusted manufactures if they are aware of microcode being used in USB devices. I would like to add the statement into my project, if possible, which is looking into the safety of USB's being sold via online marketplaces, particularly those unbranded.

Thanks Helen Plews

Dear Helen,

I hope you are well,

Thank you for getting in touch with Kingston Technology for a statement on this subject. Please could you kindly clarify what you mean by microcoding? Pasi, who is part of our Technical Resources team would then love to help you with that 😊

Best Wishes,

Hello

Sorry it is very technical! Its the x86 Intel Microcode, AMD microcode or similar used to update the host machines chip it is plugged into. They are often used by the chip manufacturer to quickly apply software updates to host machines. Can you possibly explain why, if you don't use them this is not needed and if they would be a possible security risk if they were used on USB drives.

Thanks Helen

Hi Helen,

Kingston doesn't offer updating such as this on our products. The only updates available are firmware updates for SSDs through our freely available Kingston SSD Manager (KSM at SSD Manager - Kingston Technology), and if necessary we also have software updaters available for encrypted USB drives, for example to offer improved OS support:

DataTraveler Locker Plus G3 USB3.0 Flash Drive - Technical Support - Kingston Technology

Some of our older discontinued products may also still have firmware updates available on [kingston.com](http://kingston.com). These updates are only for the associated product, not for updating the host system the product is used in. We recommend customers purchase our products from reputable sources, and if needing to apply software/firmware updates to obtain these updates from [kingston.com](http://kingston.com) and not from ftp sites, device updater depositories and such. A genuine Kingston product would not contain malicious code, microcode or anything that's not intended for the valid use of the product. There is a risk obtaining used USB drives

through auction sites, suspicious sources as there's no way to tell whether they have been loaded with malware, software intended to do harm.

I hope that helps.

Kindly,

## BIBLIOGRAPHY

ADMX, 2022. *Boot-Start Driver Initialization Policy 2022*]. Available from: [https://admx.help/?Category=Windows\\_10\\_2016&Policy=FullArmor.Policies.0EF0F32B\\_7305\\_4FC7\\_BBEB\\_D43DCC622C81::POL\\_DriverLoadPolicy\\_Name](https://admx.help/?Category=Windows_10_2016&Policy=FullArmor.Policies.0EF0F32B_7305_4FC7_BBEB_D43DCC622C81::POL_DriverLoadPolicy_Name)

ALLEN, R., 2021. Reducing the security risks of USB devices.

ALSAID, A. and C.J. MITCHELL, 2005. Installing Fake Root Keys in a PC.

ANON, 2012. *Reprogram USB flash drive microprocessor's firmware?2022*]. Available from: [https://www.reddit.com/r/netsec/comments/112kuv/reprogram\\_usb\\_flash\\_drive\\_microprocessors\\_firmware/](https://www.reddit.com/r/netsec/comments/112kuv/reprogram_usb_flash_drive_microprocessors_firmware/)

ANON, 2015a. *Extract files from a bin firmware 2022*]. Available from: <https://reverseengineering.stackexchange.com/questions/8063/extract-files-from-a-bin-firmware>

ANON, 2015b. *Firmware analysis and file system extraction?2022*]. Available from: <https://reverseengineering.stackexchange.com/questions/2704/firmware-analysis-and-file-system-extraction>

ANON, 2016. *Firmware extraction problems - binwalk is blank 2022*]. Available from: <https://reverseengineering.stackexchange.com/questions/12267/firmware-extraction-problems-binwalk-is-blank>

ANON, 2017a. *How unallocated memory space is represented?2022*]. Available from: <https://cs.stackexchange.com/questions/74315/how-unallocated-memory-space-is-represented>

ANON, 2017b. *Tool for measuring entropy quality?2022*]. Available from: <https://unix.stackexchange.com/questions/31779/tool-for-measuring-entropy-quality>

ANON, 2017c. *What is Intel microcode?2022*]. Available from: <https://stackoverflow.com/questions/4366837/what-is-intel-microcode>

ANON, 2020a. *Compute entropy of different file extensions to find randomness of data?2022*]. Available from: <https://stackoverflow.com/questions/64781278/compute-entropy-of-different-file-extensions-to-find-randomness-of-data>

ANON, 2020b. *Is this event a security concern: Windows 10: Event 360, User Device Registration?2022*]. Available from: <https://security.stackexchange.com/questions/164695/is-this-event-a-security-concern-windows-10-event-360-user-device-registratio>

ANON, 2021a. *Are there USB flash drives with read-only firmware?2022*]. Available from: <https://security.stackexchange.com/questions/172856/are-there-usb-flash-drives-with-read-only-firmware>

ANON, 2021b. *Binwalk - Compressed data is corrupt* 2022]. Available from: <https://stackoverflow.com/questions/36778409/binwalk-compressed-data-is-corrupt>

ANON, 2021c. *How do I install Intel microcode on a live USB stick?*2022]. Available from: <https://www.quora.com/How-do-I-install-Intel-microcode-on-a-live-USB-stick>

ANON, 2021d. *Two Hidden Instructions Discovered in Intel CPUs Enable Microcode Modification* 2021]. Available from: <https://news.ycombinator.com/item?id=27427096>

ANON, 2021e. *Use binwalk to extract all files* 2022]. Available from: <https://stackoverflow.com/questions/36530643/use-binwalk-to-extract-all-files>

ATOMIC SHRIMP, 2021. *Fake USB Flash Devices Are Everywhere!*[viewed 30/06/ 2022]. Available from: <https://www.youtube.com/watch?v=HFY5hd273lI>

BAILEY, R., 2022a. *Mscorsvw.exe Virus* 🦋 (Coin Miner Trojan) Removal 2022]. Available from: <https://howtofix.guide/mscorsvw-exe-virus/>

BAILEY, R., 2022b. *Ngen.exe Virus* 🦋 (Coin Miner Trojan) Removal 2022]. Available from: <https://howtofix.guide/ngen-exe-virus/>

BARKER, A. *et al.*, 2020a. *Artifice: Data in Disguise*. <https://par.nsf.gov>,

BARKER, A. *et al.*, 2020b. *Artifice: Data in disguise*.

BENCHERCHALI, N., 2020a. *Hunting Malware with Windows Sysinternals—Process Monitor*.

BENCHERCHALI, N., 2020b. *Hunting Malware with Windows Sysinternals—Process Monitor* 2022]. Available from: <https://nasbench.medium.com/hunting-malware-with-windows-sysinternals-process-monitor-e67476f44514>

BRITTON, 2021. *Huawei accused of stealing trade secrets, spying in Pakistan*. [www.reuters.com](http://www.reuters.com),

BULLER, I., 2021. *EVTX Forensics - Investigate Windows Events* 2022]. Available from: <https://www.security-hive.com/post/evtx-forensics-investigate-windows-events>

CAMACHO, P., 2019. *Ransomware MongoLock Immediately Deletes Files, Formats Backup Drives*. *trendmicro*, Jan

CANELLA, C. *et al.*, 2020. *KASLR: Break It, Fix It, Repeat*.

CAVIGLIONE, L. *et al.*, 2020. *Tight arms race: Overview of current malware threats and trends in their detection*. *IEEE Access*, 9, 5371-5396

CHEKOLE, E.G. and H. GUO, 2021. *DARUD: Detecting and Arresting Rogue USB Devices in the V2X Ecosystem*.

CHERQI, O. *et al.*, 2018. *Analysis of hacking related trade in the darkweb*. *2018 IEEE international conference on intelligence and security informatics (ISI)*. IEEE, pp.79-84

CISA, 2022. *China Cyber Threat Overview and Advisories* 2022]. Available from: <https://www.cisa.gov/uscert/china>

CLOUDFLARE, 2022. *What is the Mirai Botnet?*

CONACHER, J., RENAUD, K. and OPHOFF, J., 2020. *Caveat Venditor, Used USB Drive Owner* 2022]. Available from: <https://arxiv.org/abs/2006.11354>

CONACHER, J., K. RENAUD and J. OPHOFF, 2020. *Caveat Venditor, used USB drive owner*. *Used USB Drive Owner (June 19, 2020)*,

CRENSHAW, A., 2022. *Malicious USB Devices*.

- DEFAULTREASONING, 2020. *Unhide the Recovery Partition on a Basic Disk with DiskPart*. 2022]. Available from: <https://defaultreasoning.com/2009/05/29/unhide-the-recovery-partition-on-a-basic-disk-with-diskpart/>
- DEMME, J. *et al.*, 2013. On the feasibility of online malware detection with performance counters.
- DENG, S., B. HUANG and J. SZEFER, 2022. Leaky Frontends: Security Vulnerabilities in Processor Frontends.
- DENNEY, K. *et al.*, 2019. USB-Watch: A Dynamic Hardware-Assisted USB Threat Detection Framework.
- DESAI, A.R., *et al.*, 2013. *Interlocking obfuscation for anti-tamper hardware* 2022]. Available from: <https://dl.acm.org/doi/pdf/10.1145/2459976.2459985>
- DISKPART, 2022. *Free to Create Windows 10 to Go USB (All Win10 Versions Supported)* 2022]. Available from: <https://www.diskpart.com/windows-10/create-windows-10-to-go-usb-0528.html>
- DUIVENVOORDE, B., 2022. The Liability of Online Marketplaces under the Unfair Commercial Practices Directive, the E-commerce Directive and the Digital Services Act. *Journal of European Consumer and Market Law*, 11(2),
- DYS2P, 2021. *Random Mosaic - Detecting unauthorized physical access with beans, lentils and colored rice* [viewed 30/06/ 2022]. Available from: <https://dys2p.com/en/2021-12-tamper-evident-protection.html>
- DZWONKOWSKI, M. and R. RYKACZEWSKI, 2021. Reversible Data Hiding in Encrypted DICOM Images Using Cyclic Binary Golay (23, 12) Code.
- ELBAHRAWY, A. *et al.*, 2020. Collective dynamics of dark web marketplaces.
- ESMAEILI-NAJAFABADI, E. *et al.*, 2021. Risk-averse outsourcing strategy in the presence of demand and supply uncertainties.
- FAQCODE4U., 2019. *Use Binwalk To Extract All Files* 2022]. Available from: <https://www.faqcode4u.com/faq/195068/use-binwalk-to-extract-all-files>
- FILE INSPECT, 2021. *What is WerFaultSecure.exe?*2022]. Available from: <https://www.fileinspect.com/fileinfo/werfaultsecure-exe/>
- FILE.INFO, 2022. *What does the drvinst.exe file do?*2022]. Available from: [https://file.info/windows/drvinst\\_exe.html](https://file.info/windows/drvinst_exe.html)
- FILE.NET, 2022a. *What is MpCopyAccelerator.exe?*2022]. Available from: <https://www.file.net/process/mpcopyaccelerator.exe.html>
- FILE.NET, 2022b. *What is VSSVC.exe?*2022]. Available from: <https://www.file.net/process/vssvc.exe.html>
- FROST, J., 2022. *P-Values, Error Rates, and False Positives* 2022]. Available from: <https://statisticsbyjim.com/hypothesis-testing/p-values-error-rates-false-positives/>
- FUJITA, R., T. ISOBE and K. MINEMATSU, 2020. ACE in Chains: How Risky Is CBC Encryption of Binary Executable Files?
- GAJEK, S. and M. LEES, 2020. IIoT and cyber-resilience.
- GENKIN, D. and Y. YAROM, 2021. Whack-a-Meltdown: Microarchitectural Security Games [Systems Attacks and Defenses].

- GHADGE, A. *et al.*, 2018. Managing cyber risk in supply chains: A review and research agenda.
- GIT HUNTER, 2019. *Update firmware 2022*]. Available from: <http://git.hunter-ht.cn/fact-gitdep/binwalk/blob/b84af6833314fa24ecbcbad9a6c3dce0eadd4f83/src/binwalk/magic/firmware>
- GLASSWIRE, 2022. <https://www.glasswire.com/process/wermgr.exe.html> 2022]. Available from: <https://www.glasswire.com/process/wermgr.exe.html>
- GLOBALSIGN, 2022. *GlobalSign Root Certificates 2022*]. Available from: <https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-certificates>
- GOLDSMITH, J., 2000. Unilateral Regulation of the Internet: A Modest Defence. *EJIL*, 11(1), 135-148
- GOODIN, D., 2014. *This thumbdrive hacks computers. "BadUSB" exploit makes devices turn "evil" 2022*]. Available from: <https://arstechnica.com/information-technology/2014/07/this-thumbdrive-hacks-computers-badusb-exploit-makes-devices-turn-evil/>
- GOODIN, D., 2020. *In a first, researchers extract secret key used to encrypt Intel CPU code 2022*]. Available from: <https://arstechnica.com/gadgets/2020/10/in-a-first-researchers-extract-secret-key-used-to-encrypt-intel-cpu-code/>
- GOWTHAM, V., 2022a. *What Is drvinst.exe? Is It A Virus Or Malware? Uninstall or Fix?2022*]. Available from: <https://howtodoninja.com/files/exe/drvinst-exe/safe-virus-malware-uninstall-fix-drvinst-exe/>
- GOWTHAM, V., 2022b. *What Is ngen.exe? Is It A Virus Or Malware? Uninstall?2022*]. Available from: <https://howtodoninja.com/files/exe/ngen-exe/safe-virus-malware-uninstall-fix-ngen-exe/>
- GULMEZOGLU, B., 2021. XAI-based Microarchitectural Side-Channel Analysis for Website Fingerprinting Attacks and Defenses.
- HAMILTON, 2020. The US says Huawei has been spying through 'back doors' designed for law enforcement – which is what the US has been pressuring tech companies to do for years. *businessinsider.com*,
- HE, D. *et al.*, 2014. Enhanced three-factor security protocol for consumer USB mass storage devices.
- HEROUX, M., 2017. *FALSE-POSITIVE FINDINGS AND HOW TO MINIMIZE THEM 2022*]. Available from: <https://scientificallysound.org/2017/11/22/false-positive-findings/>
- HIRSH, M., 2022. We Are Now in a Global Cold War. <https://foreignpolicy.com>,
- INTOWINDOWS, 2020. *Using Rufus To Create Windows To Go USB Drive 2022*]. Available from: <https://www.intowindows.com/rufus-to-create-windows-to-go-usb-drive/>
- JAMES\_369, 2022. *Found some Chinese text in a Problem Report, should I be concerned?2022*]. Available from: <https://forums.tomshardware.com/threads/found-some-chinese-text-in-a-problem-report-should-i-be-concerned.3767157/>
- JAYS TECH VAULT, 2020. *I Bought a \$3 2TB USB Drive and Got More Than Just Malware* Available from: <https://www.youtube.com/watch?v=q2mDGIFlODI>
- JING TIAN, D. and A.B. BATES K, 2015. Defending Against Malicious USB Firmware with GoodUSB.
- JOESANDBOX, 2021. *Windows Analysis Report WPD.exe 2022*]. Available from: <https://www.joesandbox.com/analysis/501343/0/lighthtml>

- JOESANDBOX, 2022. *Analysis Report* <http://8.250.37.254> 2022]. Available from: <https://www.joesandbox.com/analysis/405755/0/lighthtml>
- KALI, 2022. *Tool Documentation: binwalk Usage Example* 2022]. Available from: <https://www.kali.org/tools/binwalk/>
- KASPERSKY, K., 2008. Remote Code Execution through Intel CPU Bugs.
- KASPERSKY., K., 2008. Remote Code Execution through Intel CPU Bugs.
- KAUFMANN, D., A. BIERE and M. KAUERS, 2019. Incremental column-wise verification of arithmetic circuits using computer algebra.
- KHASAWNEH, K. *et al.*, 2015. Ensemble Learning for Low-Level Hardware-Supported Malware Detection.
- KIM, D., B. JUN KWON and T. DUMITRAS, 2017. Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI.
- KITCHEN, E.A., 2022. *hak5 / usbrubberducky-payloads* [viewed 30/06/ 2022]. Available from: <https://github.com/hak5/usbrubberducky-payloads>
- KOCH, L., 2019. What's Driving the Top Five Retail Ecommerce Markets Worldwide? *accessed March, 5, 2020*
- KOCHER, P. *et al.*, 2019. Spectre Attacks: Exploiting Speculative Execution.
- KOJM, T., 2022. *clamscan(1) - Linux man page* 2022]. Available from: <https://linux.die.net/man/1/clamscan>
- KOLLEND, B. *et al.*, 2018. An Exploratory Analysis of Microcode as a Building Block for System Defenses.
- KONDRATEV, M.I., A.A. GAMOVA and V.V. GUROV, 2020. USB Devices with Hardware Backdoor.
- KONDRATEV, M.I., A.A. GAMOVA and V.V. GUROV, 2020. USB Devices with Hardware Backdoor. *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*. IEEE, pp.141-143
- KOST, E., 2022. *What is DLL Hijacking? The Dangerous Windows Exploit* 2022]. Available from: <https://www.upguard.com/blog/dll-hijacking>
- KUMAR, A. *et al.*, 2019. Vulnerability Assessment of Authorization System for USB-Based Storage Devices.
- KUMAR, A. *et al.*, 2019. Vulnerability Assessment of Authorization System for USB-Based Storage Devices.
- LAKSHMANAN, 2022. Researchers Warn of 'Raspberry Robin' Malware Spreading via External Drives. *The Hacker News*, May
- LAKSHMANAN, R., 2020. *Intel CPUs Vulnerable to New 'SGAxe' and 'CrossTalk' Side-Channel Attacks* 2022]. Available from: <https://thehackernews.com/2020/06/intel-sgaxe-crosstalk-attacks.html>



LEONHARD, W., 2022. *Mysterious WPD driver is installing on Windows PCs, triggering errors* 2022]. Available from: <https://www.computerworld.com/article/3178410/mysterious-wpd-driver-is-installing-on-windows-10-pcs-triggering-errors.html>

LI, C. and J.L. GAUDIOT, 2020. Challenges in Detecting an “Evasive Spectre”.

LI, C. and J.L. GAUDIOT, 2021a. Detecting Spectre Attacks Using Hardware Performance Counters.

LI, C. and J.L. GAUDIOT, 2021b. Detecting Spectre Attacks Using Hardware Performance Counters.

LODGE, 2022. *Using hexdump analysis for firmware extraction: A how-to* [viewed 19/09/2022]. Available from: <https://www.pentestpartners.com/security-blog/using-hexdump-analysis-for-firmware-extraction-a-how-to/>

MAHBOUBI., A., S. CAMTEPE and H. MORARJI, 2018. Reducing USB Attack Surface: A Lightweight Authentication and Delegation Protocol.

MALWARE BYTES, 2014. *Nasty virus which deletes files, creates a new user account and blocks taskmanager* 2022]. Available from: <https://forums.malwarebytes.com/topic/162880-nasty-virus-which-deletes-files-creates-a-new-user-account-and-blocks-taskmanager/>

MARKETTOS, A THEODORE ROTHWELL, COLIN GUTSTEIN, BRETT F PEARCE, ALLISON NEUMANN, PETER G MOORE, SIMON W WATSON, ROBERT NM, 2019. Thunderclap: Exploring Vulnerabilities in Operating System IOMMU Protection via DMA from Untrustworthy Peripherals.

MARTIN, D., 2022. *Boffins release tool to decrypt Intel microcode. Have at it, x86 giant says* 2022]. Available from: <https://www.theregister.com/2022/07/20/intel-cpu-microcode/>

MELARAGNO, A. and W. CASEY, 2022. Detecting Ransomware Execution in a Timely Manner. <https://ui.adsabs.harvard.edu>,

MESKAUSKAS, T., 2022. *How to remove HxTsr.exe malware* 2022]. Available from: [https://www.pcrisk.com/removal-guides/15096-hxtr-exe-virus#:~:text=HxTsr.exe%20\(Hidden%20Executable%20To,to%20disguise%20their%20malicious%20programs.](https://www.pcrisk.com/removal-guides/15096-hxtr-exe-virus#:~:text=HxTsr.exe%20(Hidden%20Executable%20To,to%20disguise%20their%20malicious%20programs.)

MICROSOFT, 2015. *VSS giving event id 8224 but no new shadow copies* 2022]. Available from: <https://social.technet.microsoft.com/Forums/en-US/799ea0d5-ba4b-432d-90a7-5af84bfb00ef/vss-giving-event-id-8224-but-no-new-shadow-copies?forum=smallbusinessserver2011essentials>

MICROSOFT, 2016. *“The VSS service is shutting down due to idle timeout” - event 8224 on Windows 10.* 2022]. Available from: <https://answers.microsoft.com/en-us/windows/forum/all/the-vss-service-is-shutting-down-due-to-idle/40ae9d42-1892-4ae8-99cf-b306f043f280>

MICROSOFT, 2019. *WerFault.exe* 2022]. Available from: <https://social.technet.microsoft.com/Forums/ie/en-US/4032dc41-c813-4058-bba2-27317b38bf63/werfaultexe?forum=w8itproappcompat>

MICROSOFT, 2022a. *Chinese text in a WER archived report.* 2022]. Available from: <https://answers.microsoft.com/en-us/windows/forum/all/chinese-text-in-a-wer-archived-report/c07894fe-0f01-4a78-9bb1-52a42ef84050>

MICROSOFT, 2022b. *event-6281* 2022]. Available from: <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-6281>

MICROSOFT, 2022c. *VIRUS CREATING HIDDEN PARTITIONS* 2022]. Available from: <https://answers.microsoft.com/en-us/insider/forum/all/virus-creating-hidden-partitions-and-windows/8cc242ac-ad03-49e6-b37c-f041397f3ba1>

MILLER, J., 2011. Evaluating Third Party Root Certificates for Corporate PKI Trust Stores.

MITRE CORPORATION, 2021. *Process Injection: Dynamic-link Library Injection* 2022]. Available from: <https://attack.mitre.org/techniques/T1055/001/>

MITRE CORPORATION, 2022a. *BlackEnergy* 2022]. Available from: <https://attack.mitre.org/software/S0089/>

MITRE CORPORATION, 2022b. *Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder* 2022]. Available from: <https://attack.mitre.org/techniques/T1547/001/>

MITRE CORPORATION, 2022c. *System Network Connections Discovery* 2022]. Available from: <https://attack.mitre.org/techniques/T1049/>

MOGHIMI, D., 2020. Data Sampling on MDS-resistant 10th Generation Intel Core (Ice Lake).

MONJUR, M. *et al.*, 2022. Hardware Security in Advanced Manufacturing.

MSRC TEAM, 2021. *Investigating and Mitigating Malicious Drivers* 2022]. Available from: <https://msrc-blog.microsoft.com/2021/06/25/investigating-and-mitigating-malicious-drivers/>

MULLIGAN, D.K. and A.K. PERZANOWSKI, 2007. The magnificence of the disaster: Reconstructing the Sony BMG rootkit incident. *Berkeley Tech.LJ*, 22, 1157

MULRENAN, S., 2022. Cyber espionage: China intensifies tech cold war.

MUSHTAQ, M. *et al.*, 2020. WHISPER: A Tool for Run-Time Detection of Side-Channel Attacks.

MUSHTAQ, M. *et al.*, 2020. WHISPER: A Tool for Run-Time Detection of Side-Channel Attacks .

NCOMPUTERS, 2017. *Entropy and serial correlation test* 2022]. Available from: <https://ncomputers.org/entropyarray>

NETWORKCHUCK, 2021. *bad USBs are SCARY!! (build one with a Raspberry Pi Pico for \$8)* [viewed 30/06/ 2022]. Available from: [https://www.youtube.com/watch?v=e\\_f9p-JWZw](https://www.youtube.com/watch?v=e_f9p-JWZw)

NILSSON, A., P.N. BIDEH and J. BRORSSON, 2020. A Survey of Published Attacks on Intel SGX.

NISSIM, N., R. YAHALOM and Y. ELOVICI, 2017. USB-based attacks.

NIST, 2011. *Microsoft Windows 7 Cryptographic Primitives Library (bcryptprimitives.dll) Security Policy Document* Available from: <https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp1329.pdf>

NYAKOMITTA, P.S. and S.O. ABEKA, 2020. A Survey of Data Exfiltration Prevention Techniques. *International Journal of Advanced Networking and Applications*, 12(3), 4585-4591

OLIVEIRA, J., M. FRADE and P. PINTO, 2018. System Protection Agent Against Unauthorized Activities via USB Devices.

OLIVEIRA, J., M. FRADE and P. PINTO, 2018. System Protection Agent Against Unauthorized Activities via USB Devices. *IoTBDs*. pp.237-243

ORI OR-MEIR, NIR NISSIM, YUVAL ELOVICI, AND LIOR ROKACH, 2019. Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. *ACM*,

PANDEY, S. *et al.*, 2020. Cyber security risks in globalized supply chains: conceptual framework.

PENG, H., 2020. USBFuzz: A Framework for Fuzzing USB Drivers by Device Emulation.

PRADHAN, D., S. SOM and A. RANA, 2020. Cryptography Encryption Technique Using Circular Bit Rotation in Binary Field.

PRADO, S., 2022. *Reverse engineering my router's firmware with binwalk* 2022]. Available from: <https://embeddedbits.org/reverse-engineering-router-firmware-with-binwalk/>

PRIYA, A. *et al.*, 2018. A Novel Multimedia Encryption and Decryption Technique Using Binary Tree Traversal.

PROCESS LIBRARY, 2022. *wmiadap* 2022]. Available from: <https://www.processlibrary.com/en/directory/files/wmiadap/25569/>

REDHAT, 2021. *Intel June 2021 Microcode Update* 2022]. Available from: <https://access.redhat.com/articles/6101171>

REFIRM LABS, 2021. *ReFirmLabs / binwalk* 2022]. Available from: <https://github.com/ReFirmLabs/binwalk/blob/master/src/binwalk/magic/firmware>

REFIRM LABS, 2015. *Better way to extract files that doesn't need processing* 2022]. Available from: <https://github.com/ReFirmLabs/binwalk/issues/38>

ROKICKI, T., 2018. E-commerce market in Europe in B2C. *Information Systems in Management*, 7

RUFUS, 2022. *Rufus* 2022]. Available from: <https://rufus.ie/en/>

RUSSINOVICH, M., 2022. *Autoruns for Windows v14.09* 2022]. Available from: <https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns>

S. VAN SCHAİK *et al.*, 2021. CacheOut: Leaking Data on Intel CPUs via Cache Evictions. - 2021 *IEEE Symposium on Security and Privacy (SP)*. pp.339-354

SAHAY, M., 2022. *Create Windows To Go USB Drive Using Rufus in Windows 10* 2022]. Available from: <https://www.thepecinsider.com/create-windows-to-go-usb-drive-rufus/>

SALAZAR GREG, 2021. *The Fake 1TB USB Flash Drive Scam* [viewed 24/05/ 2022]. Available from: <https://www.youtube.com/watch?v=tPHYVJHN6LY>

SAMMONS, J., 2012. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. First ed.

SAMMONS, J., 2014. *The Basics of Digital Forensics*. Second Edition ed.

SAMMONS, J., 2012. *The basics of digital forensics: the primer for getting started in digital forensics*. Elsevier

SHAFIQUE, U., 2019. Towards Protection Against a USB Device Whose Firmware Has Been Compromised or Turned as 'BadUSB'.

SHAFIQUE, U. and S. BIN ZAHUR, 2019. Towards Protection Against a USB Device Whose Firmware Has Been Compromised or Turned as 'BadUSB'.

SHAH, Z. *et al.*, 2022. Forensic Investigation of Remnant Data on USB Storage Devices Sold in New Zealand.

- SHIN, Y., 2021a. Multibyte Microarchitectural Data Sampling and Its Application to Session Key Extraction Attacks.
- SHIN, Y., 2021b. Multibyte Microarchitectural Data Sampling and its Application to Session Key Extraction Attacks.
- SINGH, D. *et al.*, 2022. Juice Jacking: Security Issues and Improvements in USB Technology.
- SLASHDOT, 2020. *Hackers Can Now Reverse Engineer Intel Updates Or Write Their Own Custom Firmware* 2022]. Available from: <https://developers.slashdot.org/story/20/10/28/217212/hackers-can-now-reverse-engineer-intel-updates-or-write-their-own-custom-firmware>
- STOCKTON, B., 2020. *Why Dwm.exe Causes High CPU Usage and How To Fix It* 2022]. Available from: <https://helpdeskgeek.com/help-desk/why-dwm-exe-causes-high-cpu-usage-and-how-to-fix-it/>
- SUN, C., J. LU and Y. LIU, 2021a. Analysis and Prevention of Information Security of USB.
- SUN, C., J. LU and Y. LIU, 2021b. Analysis and Prevention of Information Security of USB.
- SUN, C., J. LU and Y. LIU, 2021. Analysis and Prevention of Information Security of USB. *IEEE*, , 25-32
- SUPER USER, 2019. *Accessing the firmware of an USB flash drive* 2022]. Available from: <https://superuser.com/questions/176075/accessing-the-firmware-of-an-usb-flash-drive>
- SUPER USER, 2022. *How do I create a 1GB random file in Linux?* Available from: <https://superuser.com/questions/470949/how-do-i-create-a-1gb-random-file-in-linux>
- SUPERUSER, 2017. *Manipulating firmware of USB flash drives* 2022]. Available from: <https://superuser.com/questions/854918/manipulating-firmware-of-usb-flash-drives>
- SUPERUSER, 2018. *"the VSS service is shutting down due to idle timeout" event ID: 8224* 2022]. Available from: <https://superuser.com/questions/332925/the-vss-service-is-shutting-down-due-to-idle-timeout-event-id-8224>
- SYSTEM EXPLORER, 2017a. *Top file variants for security.evtx* 2022]. Available from: <https://systemexplorer.net/file-database/file-variants/security-evt-x>
- SYSTEM EXPLORER, 2017b. *What is the "security.evtx" ?* 2022]. Available from: <https://systemexplorer.net/file-database/file/security-evt-x>
- TANG, A., S. SETHUMADHAVAN and S.J. STOLFO, 2014. Unsupervised Anomaly-Based Malware Detection Using Hardware Features.
- TECHDOCS, 2022. *Downloading Firmware from a USB Device* 2022]. Available from: <https://techdocs.broadcom.com/us/en/fibre-channel-networking/fabric-os/fabric-os-software-upgrade/9-1-x/Obtaining-Firmware90x/Downloading-Firmware-from-a-USB-Device.html>
- THOMAS, V., P. RAMAGOPAL and R. MOHANDAS, 2009. The rise of autorun-based malware. *McAfee Avert Labs.*, *McAfee Inc.*,
- THOMASSEN, J., 2008. FORENSIC ANALYSIS OF UNALLOCATED SPACE IN WINDOWS REGISTRY HIVE FILES .
- THREATMINER, 2022. *Threatminer - SSL* 2022]. Available from: <https://www.threatminer.org/ssl.php?q=d69b561148f01c77c54578c10926df5b856976ad>
- THURNER, S. *et al.*, 2015. Improving the Detection of Encrypted Data on Storage Devices.

- TIAN, D.J., A. BATES and K. BUTLER, 2015. Defending Against Malicious USB Firmware with GoodUSB.
- TIAN, Q. and W. GUO, 2019. Reconfiguration of manufacturing supply chains considering outsourcing decisions and supply chain risks.
- TIBBETTS, T., 2022. *What is WWAHost.exe (Microsoft WWA Host)?*2022]. Available from: <https://www.majorgeeks.com/content/page/wwahost.html>
- TICU, M., 2021a. USB Traffic Analyzer - digUSB.
- TICU, M., 2021b. USB Traffic Analyzer - digUSB.
- TSAKALIDIS, G., K. VERGIDIS and M. MADAS, 2018. Cybercrime Offences: Identification, Classification and Adaptive Response.
- ULLRICH, C., 2019. New Approach meets new economy: Enforcing EU product safety in e-commerce.
- ULLRICH, C., 2021. Unlawful Content Online.
- VAN SCHAİK, S. *et al.*, 2021a. CacheOut: Leaking Data on Intel CPUs via Cache Evictions.
- VAN SCHAİK, S. *et al.*, 2021b. CacheOut: Leaking Data on Intel CPUs via Cache Evictions.
- VANISHREE, K. and M. PURNAPRAJNA, 2020. CPU Performance Modeling through Analysis of Primitive Operations.
- VARIOUS, 2022. *Unallocated Space* 2022]. Available from: <https://www.sciencedirect.com/topics/computer-science/unallocated-space>
- VIBIEN, P., 2022. SilGeo: A Method for the Detection of Counterfeit, Compromised, or Tampered Electronic Devices.
- VU PHAM, D. *et al.*, 2010. Optimizing Windows Security Features to Block Malware and Hack Tools on USB Storage Devices.
- WANG, G. *et al.*, 2019. oo7: Low-Overhead Defense Against Spectre Attacks via Program Analysis  
 Publisher: IEEE  
 Cite This  
 PDF .
- WATTANAJANTRA, A., 2009. *Researchers expose potential exploit of Intel CPUs* 2022]. Available from: <https://www.itpro.co.uk/610265/researchers-expose-potential-exploit-of-intel-cpus>
- WILLIAMS, A.I., 2021. *UNDOCUMENTED X86 INSTRUCTIONS ALLOW MICROCODE ACCESS* 2022]. Available from: <https://hackaday.com/2021/03/26/undocumented-x86-instructions-allow-microcode-access/>
- WILLIAMS, E., 2017. *34C3: HACKING INTO A CPU'S MICROCODE* 2022]. Available from: <https://hackaday.com/2017/12/28/34c3-hacking-into-a-cpus-microcode/>
- XIN, 2018. *How to extract Microcodes from Intel's Linux package and patch them into AMI BIOS image files (on Windows and Linux/UNIX)* 2022]. Available from: <http://wp.xin.at/archives/4397>
- YINN, A., FANN, D. and SIVARAM, A.T., 2002. *Efficient embedded memory testing with APG* 2022]. Available from: <https://ieeexplore.ieee.org/document/1041744>

ZHAO, L. *et al.*, 2020. Exploiting Security Dependence for Conditional Speculation Against Spectre Attacks.

ZHAO, L. *et al.*, 2021. Exploiting Security Dependence for Conditional Speculation Against Spectre Attacks.