Sri Lanka Institute of Information Technology

USB Drop Attacks

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT20128272	Rathnayake R.M.K.G.

Date of submission

Table of Contents

Abstract

USB drop attack is generally a malware attack that distributes by using a malicious USB drive. Attackers use these kinds of attacks that can limitedly target a single person, organization, or incidentally distribute. So these attacks become more sophisticated in the current society. Script kiddies to nation-state hacking groups are using this method to accomplish their attacks **[1]**. There are many types of USB malware attacks, and it is gradually increasing threat in the present society.

Even though users can use cloud services as an alternative solution, there is still have great awareness of the security risks regarding USB devices. Millions of USB devices are still manufacturing and distributed annually for use in daily use and different industries, and an abundant USB drive on a parking lot or in a classroom is not an unusual scene. Cybercriminals take advantage of it and succeed in their attacks. Most users plug these malicious USB drives with the altruistic intention of finding the owner. This human curiosity helps cybercriminals for a successful attack.

According to one research, the researchers investigated the anecdotal view that end-users will pick up and plug in USB flash drives with a controlled experiment. They dropped 297 flash drives on a large university campus. They discovered that the attack is effective, with an expected progress rate of 45 -- 98%. First drive that picks up connected in less than six minutes **[2]**.

At present, most organizations and financial companies introduce different privacy policies and safety measures to their employees to prevent USB malware attacks. However, the attacker changes their tactics and hacking techniques to attract and mislead their victims to accomplish their tasks. Due to these reasons, it is a critical step forward in defending against USB attacks and allowing the safe deployment of USB devices in the enterprise.

1. Introduction to USB Drop Attacks

At present, a USB drive is one of the easiest ways to transfer data. Unfortunately, a cybercriminal can use these USB drives to distribute their attacks.

A USB drop attack occurs when an attacker intentionally includes malicious code or file inside a USB drive with the vicinity of a victim taking it and plugging it into a computer and obtain additional access. In this situation, the USB drive acts as the medium for the hackers' attacks. Attackers will try to manipulate multiple targets by using their social engineering skills. Also, the attackers will manipulate their victims to click files loaded on the devices. These USB drop attacks are very effective and extremely hard to defend against them. Their achievement is saving with humans' curiosity [1].

Researchers from the University of Illinois researched in 2016 by leaving 297 USB flash drives around the university, and staff and students picked up 98% of the dropped drives. In this scenario, at least half of them plugged those drives into a computer to view the content [3]. These situations make enormous opportunities for a hacker to distribute their attacks and malware.

USB devices have been using in this society for almost 20 years, and they are offering an easy and convenient way to store and transfer digital files between computers without directly connecting or the internet.

However, cybercriminals exploited this capability to succeed in their attacks. There are incidents in the past that happen because of USB drop attacks.

1. Stuxnet

In January 2010, several centrifuges of the SCADA system at a specific Iranian nuclear plant failed down. A few days after that, the computers at the facility crashed due to unknown reasons. Experts found a worm named Stuxnet, and they firmly believe that it had made its way into the systems through a USB drive because the nuclear plant had no connection with the internet. One of the employees might plug the USB drive into an employee's computer, and then the worm spread to other computers. This worm exploited several zero-day vulnerabilities and destroyed 1/5 of the centrifuges. Thus, the nuclear plant reduced its efficiency by about 30 percent. The experts thought Israel and the united states made this worm, but they denied it [1] [4] [5].

2. The U.S. Military cyberattack

In 2008, a malicious USB drive left in the parking lot of a U.S. defense facility in the Middle East, and someone plugged it into a laptop. Then the malicious code is unleashed and spread undetected to both classified and unclassified systems. It was caused to leaked sensitive data via backdoors to a remote server. The military took almost 14 months to clean the worm from its networks [4].

Kaspersky Lab data for 2017 shows that each of 12 months or less, around one in four users worldwide is stricken by a 'local' cyber incident caused by removable media like USB devices [6].

This report explains the present stage for removable media malware attacks, especially USBs, and provides advice and suggestions on defending and avoiding these kinds of attacks.

2. Types of USB Drop Attacks

There are many different types of USB malware attacks that attackers use to accomplish their tasks.

Types of USB malware attacks

- USB human interface device (H.I.D.) spoofing
- Malicious file/code
- Social engineering links
- USB kill
- Zero-day attack

USB human interface device (H.I.D.) spoofing

USB human interface device (H.I.D.) spoofing can allow an attacker to input and get output from the target computer. If the attacker has direct physical access to the victims' computer, they can plug in their H.I.D. to the target computer. Even though the device is a USB drive that requires only 3-5 volts of power, it pretends to be a fully functional keyboard or mouse [7]. After the plugin, it will execute a pre-configured set of keystrokes to drop a malicious payload onto the target computer, and it will obtain access to the hacker to the target computer [8]. The original payloads that are separated and executed are incredibly configurable, and this program will work on Linux, Windows, and Mac OS X [7]. It is a versatile attack since this can use across different platforms. These kinds of attacks need specific USB drives such as Hak5's USB rubber ducky and Maltronic's Maldunio. These devices need a specific programming language called DuckyScripts to program them [1].

However, there are some drawbacks to this type of attack. The attacker must finish the attack before the victim unplugs the USB drive. So attacker must complete the attack quickly. If the attacker does not hide the keystrokes well, the victim might notice it, and it will cause attacks' failure [1].

To prevent this kind of attack, implement stringent controls for locking systems after inactivity because of the basic H.I.D. Attack requires the computer to be unlocked. Organizations and financial companies should make knowledgeable employees be on the lookout *(BOLO)* for devices like the Teensy, especially if they are discovered being plugged into their computer [7]. Third, if the organization has a security guard, they should train to recognize these devices and questionable the device.

Malicious file/code

Malicious code is hazardous computer programming scripts designed to create or exploit system vulnerabilities and cause undesired modifications, destruction, or continuous access to computer systems. Back doors, security breaches, information and data theft, and other potential damages to files and computing systems would result from this malicious code/files [9].

In this scenario, the attacker makes a malicious file by including malicious code inside the file then save it on a USB drive. Once the victim clicks on a file in this malicious USB drive, hoping to find any critical information in it. Instead, the file will launch malicious code to download malware from the internet. Then it starts infects and damages the computer and its data. This attack is one of the most basic USB drop attacks [1] [8].

Different types of malicious code/files can spread by using the harmless USB drive.

1. Viruses

This malware can travel via documents and other file downloads and allowing the virus to infiltrate the computer and self-replicating them self that connects to macro-enabled programs to execute. Once the virus executes, it will self-propagate and spread through the system and other connected networks.

2. worms

This malware is also self-replicating and self-spreading code like viruses but does not need any additional performance. Once a computer worm has arrived on the targeted computer, these malicious threats can execute entirely independently without any support from a user-run program.

3. Trojans

Trojans are trick files that transfer malicious code containing viruses, worms, or any other code, requiring users to use the file or program to execute. These threats cannot self-replicate or spread autonomously.

4. Cross-site scripting (XSS)

Cross-site scripting conflicts with the user is web browsing by injecting malicious instructions into web applications that often change web content, block confidential information, or complete an infection to the user's device itself.

5. Backdoor attacks

In this scenario, cybercriminals get remote access to the hazarded system by using a malicious code. Apart from exposing sensitive data, such as private company information, it can also allow an attacker to become an advanced persistent threat (APT).

The U.S. Government Accountability Office has warned about the intimidation of malicious code on national security [9].

This type of attack does not need any specific USB drives such as Hak5's USB rubber ducky and Maltronic's Maldunio. Hackers use everyday typical flash drives to distribute their attacks. Because of these harmless-looking USB drives, attackers accomplish their target almost every time. The attacker can easily disguise these attacks with the proper knowledge, such as steganography or giving enticing names to the malicious file [1].

Nevertheless, even though the malicious codes' implementation can hide from the victim's view, the target machines' countermeasures can cause attacks' failure [1].

Users can take some critical steps to prevent malicious code/file attacks [9].

- Users can install reliable anti-virus software on their computers.
- Users can install anti-scripting software to prevent running unauthorized JavaScript and related code.
- Organizations and other financial companies can make high-level permissions required to run scripts and applications automatically to avoid using admin-level accounts for regular use.
- Users can appropriate data backups to protect valuable files and documents.

Social engineering links

In this type of attack, the attacker includes a file with malicious phishing links inside a typical USB drive, which tricks victims into revealing their login credentials, redirect victims to phishing sites to extort victims or download malicious files. It has also known as "USB baiting." The attacker leaves their malware-infected USB drive as bait in a conspicuous area such as the parking lot or cafeteria of the targeted company or organization. Attacker names the file with much interest to get the advantage of humans' curiosity [8] [4]. When the victim plugs the infected USB drive into their work or home computer and the malicious phishing link inside a USB drive will lead victims to malicious sites.

This type of attack does not need any specific USB drives such as Hak5's USB rubber ducky and Maltronic's Maldunio. Hackers use everyday typical flash drives to distribute their attacks. Because of these harmless-looking USB drives, attackers accomplish their target almost every time [1].

However, there are few drawbacks to this attack. The victim must connect with the internet to succeed in this attack. Furthermore, this type of attack may quite difficult on gullible victims [1].

In this kind of attack attacker manipulate the victims to do something without letting them think. Users should consider the details around the link, such as company name, address which are real, existing ones. Users should stay in control by finding the website themselves using a search engine to ensure user land where the user intends to land and avoid letting link redirects to a web page itself. Furthermore, users must beware of downloading by using those suspicious links [10].

USB kill

This attack is most destructive that can cause damage to the physical components of the target computer. It can destroy pretty much everything, such as personal laptops to company computers, photo booths, kiosks, and even cars [11]. This malicious USB drive gathers power from the USB power port then it reaches a specific voltage (240V). After that, it discharges that voltage directly into the USB data line. This process will continue till the device can no longer discharge. It destroys the circuits of the machine [12]. These USB Kill devices can destroy iPhones, iPads, and other devices, like phones, tablets, and digital cameras, using micro-USB, USB-C, and Lightning adapters [11].

a Hong Kong-based company has created a more powerful version of a USB Kill drive with a higher voltage and amp output and a three-times faster pulse rate of up to 12 times a second. They also sell a test shield for €13.95 (about $15) to test the USB Kill stick while guarding the host computer [11].

Most computers are vulnerable to this attack. There are two types of versions in the USB kill drive. The "Standard" version comes with a logo, so it is easy to detect, but the "Anonymous" version, which looks like a typical black USB stick, comes with no branding [1]. It costs €49.95 (about $53) when writing a USB kill drive [11].

The possibility of happening this kind of attack is increasing because anyone can purchase online this dangerous USB drive. In the College of Saint Rose in Albany, New York, a former student arrested that he destroyed tens of thousands of dollars worth of campus computers using a USB kill drive [13].

Organizations and other financial companies can prevent these attacks by prohibiting using USB drives inside the organization and covering the USB port physically to prevent USB Killers from being inserted into a computer [14].

Zero-day attack

In this scenario, the malicious code inside in USB drive uses the unpatched vulnerabilities and damages the system. It takes advantage of current existing vulnerabilities. While this is similar to the malicious code attack, it specifically exploits hidden vulnerabilities and cannot be fixed until a patch is deployed [4].

A newly discovered software vulnerability refers to a "zero-day" because an official patch or update to fix the issue has not been released. Zero-day attacks are perilous because the only people who know about them are the attackers themselves. The developers have "zero days" to fix the problem that has just been exposed and maybe already exploited by hackers, which refers to "zero days." Once the particular vulnerability has infiltrated a network, cybercriminals can either attack instantly or anticipate optimal time. Because of that, the vendor has to fix the issue to protect its users quickly.

However, a software vendor may fail to release a patch before hackers manage to exploit the security breach, known as a zero-day attack [15]. Any information that can be used or sold is an attractive target in a zero-day attack. Zero-day malware is estimated for over 50% of all malware blocked in Q3 2020, increasing 14% yearly [16].

Stuxnet is one of the best examples of zero-day attacks that happen by using a malicious USB drive.

Even though zero-day attacks are brutal to prevent, some actions will help prevent this kind of attack.

1. Use advanced AI and heuristics systems to prevent zero-day attacks searching for unusual patterns not typically seen from a user or application and develop fixes and distribute them immediately and efficiently.
2. educate employees and users on reliable security practices, tips that will help keep them secure online and protect the organization from zero-day attacks.Evolution of USB Drop Attacks.

Researchers from the Ben-Gurion University of the Negev in Israel analyzed the types of USB drop attacks in a completely different way. They have identified 29 ways to distribute attacks using USB drives.
They analyzed these 29 exploitation methods into four categories, depending on how the attack is carried out [17].

The first category is reprogrammable microcontroller USB attacks such as Rubber Ducky, PHUKD/URFUKED attack platforms, USBdriveby, Evilduino, Unintended USB channel. The second category is maliciously reprogrammed USB peripheral firmware attacks such as Smartphone-based HID attacks, Hidden Partition Patch, Virtual Machine Break-Out. As the third category, the researchers analyzed attacks based on unprogrammed USB devices such as USB Backdoor into Air-Gapped Hosts, Data Hiding on USB Mass Storage Devices, AutoRun Exploits. Finally, they categorized the USB killer attacks in the Electrical attacks that is as a fourth category [17].

3. Evolution of USB Drop Attacks

A Brief History of USB drives

In 1995, inventors introduced the USB 1.0 intending to develop a standardized device-connection protocol. Before that, users had to use many different ports and drivers with computers to connect devices and transfer data. In 2000, Trek Technology introduced their first commercially available USB. It could contain data only up to 8 megabytes. By 2002 many companies started to marketing these flash drives, and patent clashes abounded. After that, USB 2.0 came with the ability to transfer data at about 30 M.B./second in 2004. the USB 1.0 could only transfer data at about 1 M.B./second. In 2010, USB 3.0 was available, and it could transfer data up to 4.8 GB/second [8].

USB attacks and cases

Not only the Stuxnet attack, but some incidents also happened because of malicious USB drives and caused so damages such as system crashes, shutdowns, or infection.

Mariposa botnet

In 2008, the Mariposa botnet was an attack methodology that uses for cyber scamming and denial-of-service attacks. This botnet included 12.7 million unique I.P. addresses. Mariposa botnet was affected by one of the U.S. companies for the first time that the initial attack vector may have been a USB drive shared at an industry conference.

According to a 2010 U.S. Department of Homeland Security advisory, an instructor has shared a malicious USB drive with students at a training event in an industry conference. Employees started their training and inserted the malicious USB drive into their laptops, and then it spread the Mariposa botnet into multiple business systems [18].

U.S. Department of Defense bans USB drives (2008)

U.S. CERT issued a warning in 2008 that malicious code was spreading via USB drives. At the same time, due to the possibility of the spread of malware, the U.S. Department of Defense temporarily banned the use of USB drives and other removable storage devices [19].

Operation Copperfield (2017)

The Industrial Safety and Security Source described how an employee used a USB drive to download and view a movie on a critical infrastructure computer in the Middle East. Due to that, employees' action released a piece of malware known as Copperfield that could end in data leakage, remote control of an I.C.S. workstation, and network scanning.

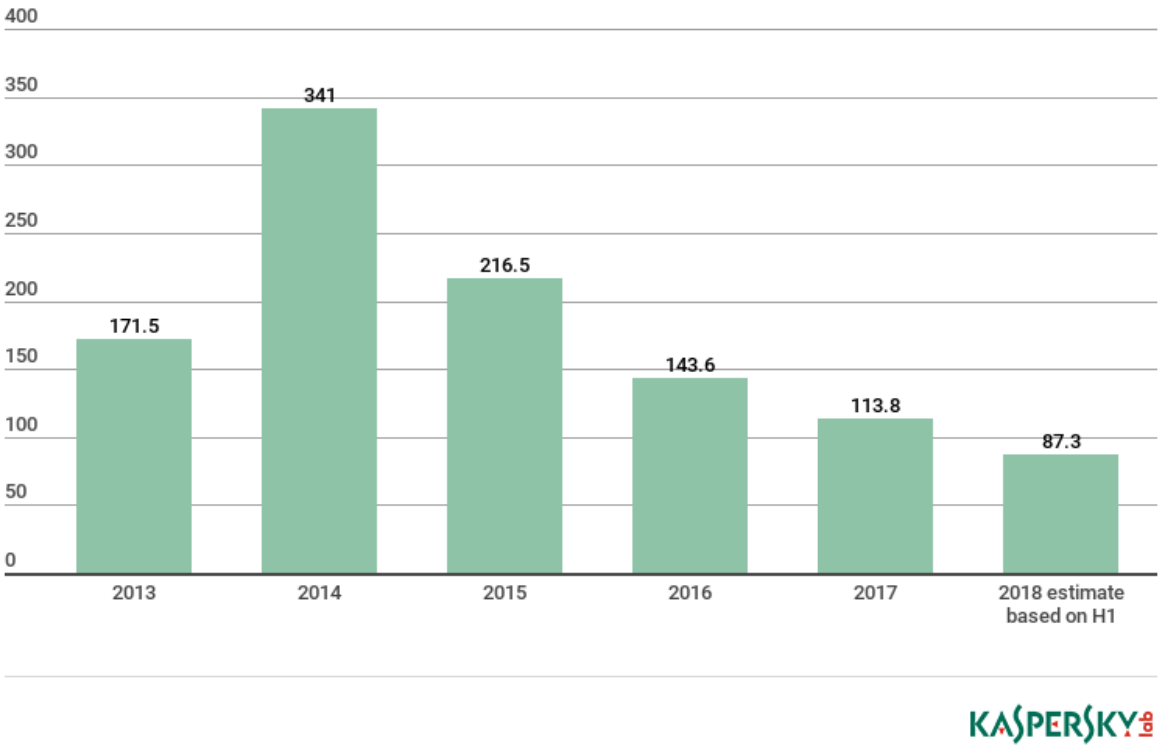
The Copperfield malware is potent because it can send information about the machine to the attacker, including the antivirus products installed, and it can update itself.

Also, it can upload any file from the machine to the attacker's server and run any command on the machine, download and run any added executable, such as malware, keystroke loggers, screen scrapers, and audio recorder. Also, the infect a USB drive to spread the infection to other devices [19] [20].

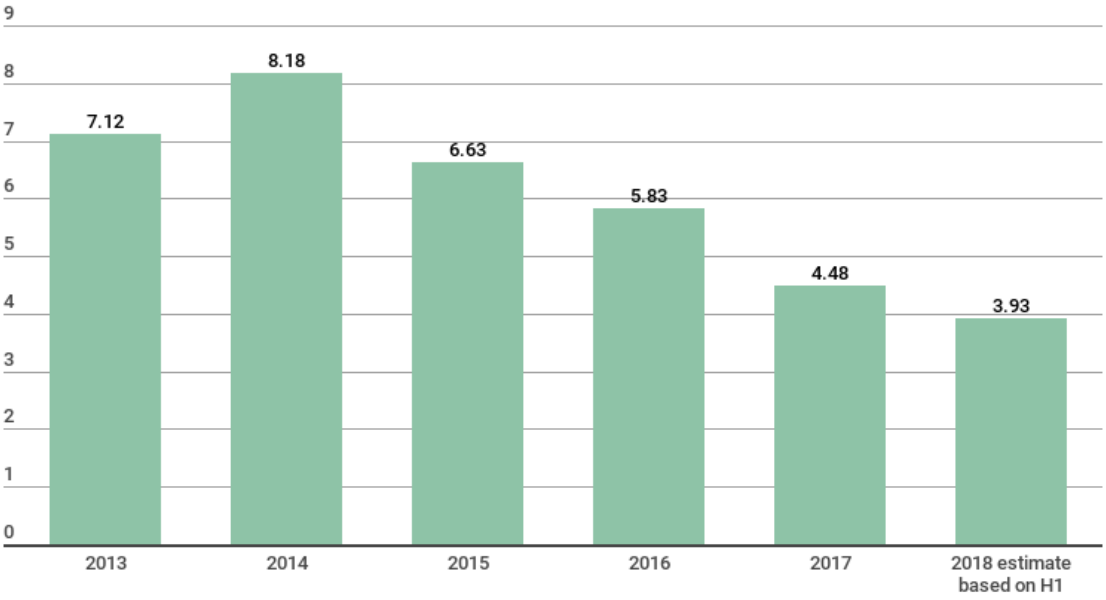
Incidents that are happened because of infected removable media are defined as local threats. Those infections can be detected directly on a user’s computer. As an example, during a scheduled installation or user-initiated security scan. Local threats vary from threats targeting computers over the internet (web-borne threats), far more accepted. Local threats can also happen because of an encrypted malicious program covered in a complicated installer. We can use the detections triggered in the drive root of affected computers, a strong indicator that the infection source is removable media, to isolate the data for malware spread by removable media such as USB devices.

According to the Kaspersky Lab researchers, the number of removable media threat detections has failed regularly since 2014, but the overall rate of decline may be decreasing down. The ratio between a user affected by a removable media threat and the total number of local threats detected was 1:42 in 2014. It had dropped by around half to 1:25 in 2017. 1:22 is the estimate for 2018 [21].

These figures fain compared to web-borne threats. Kaspersky Lab's file antivirus detected 113.8 million possible removable media threats in 2017, while its web antivirus repelled just under 1.2 billion attacks launched from online resources. With this information, it can be easy to neglect the permanent risks presented by removable media, even though around four million users worldwide will be infected this way in 2018 [21].



Total number (in millions) of malware detections triggered in the drive root of user computers, a strong indicator of infection by removable media, 2013 – 2018. Source: KSN



Number of unique users (in millions) with malware detections triggered in the drive root of computers, a strong indicator of infection by removable media, 2013 – 2018. Source: KSN

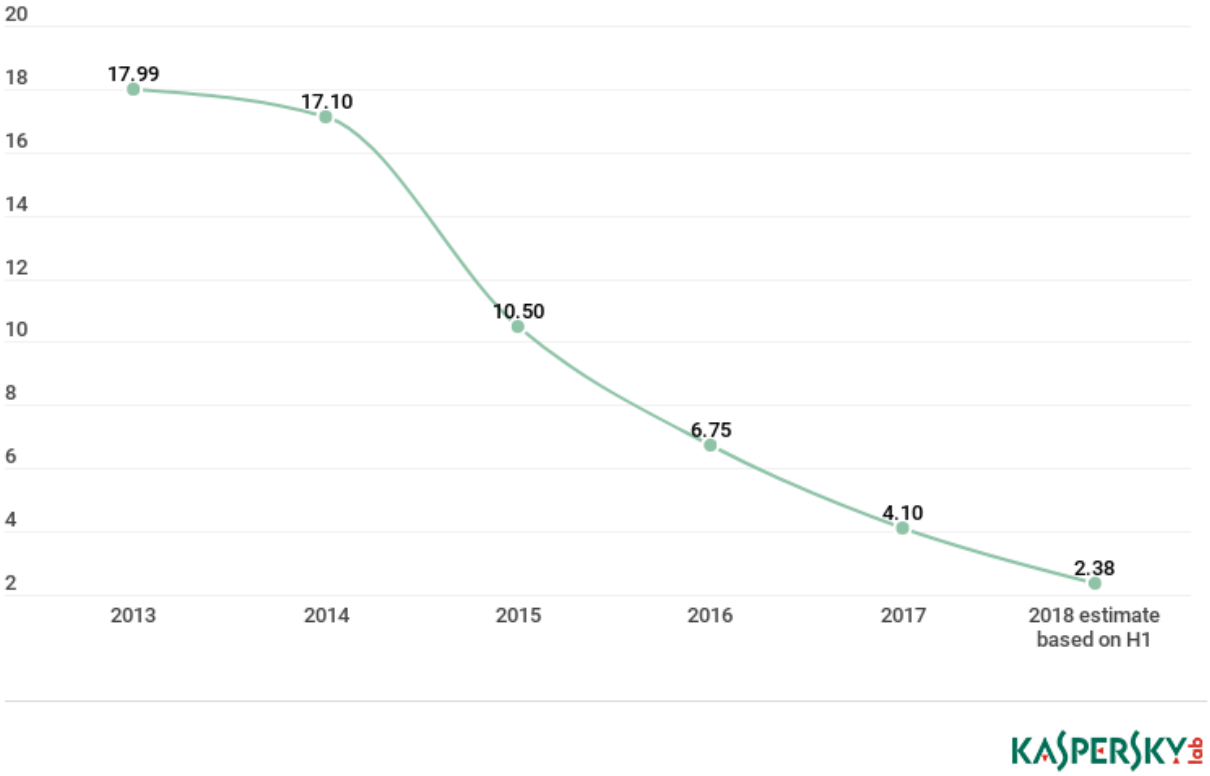
USB devices attract attackers because attackers can target computer networks that are not connected to the internet, such as those powering critical national infrastructure by using a USB drive. The most famous example of this scenario is Stuxnet. The Stuxnet worm targeted Iran's nuclear power plant to interrupt operations in 2009 and 2010 [21].

USB devices can use to inject malware into the facilities' air-gapped networks. The devices incorporated an exploit to a Windows L.N.K. vulnerability (CVE-2010-2568) that allowed remote code execution [21]. Other advanced threat actors have all integrated exploits for this vulnerability into removable media to use in attacks.

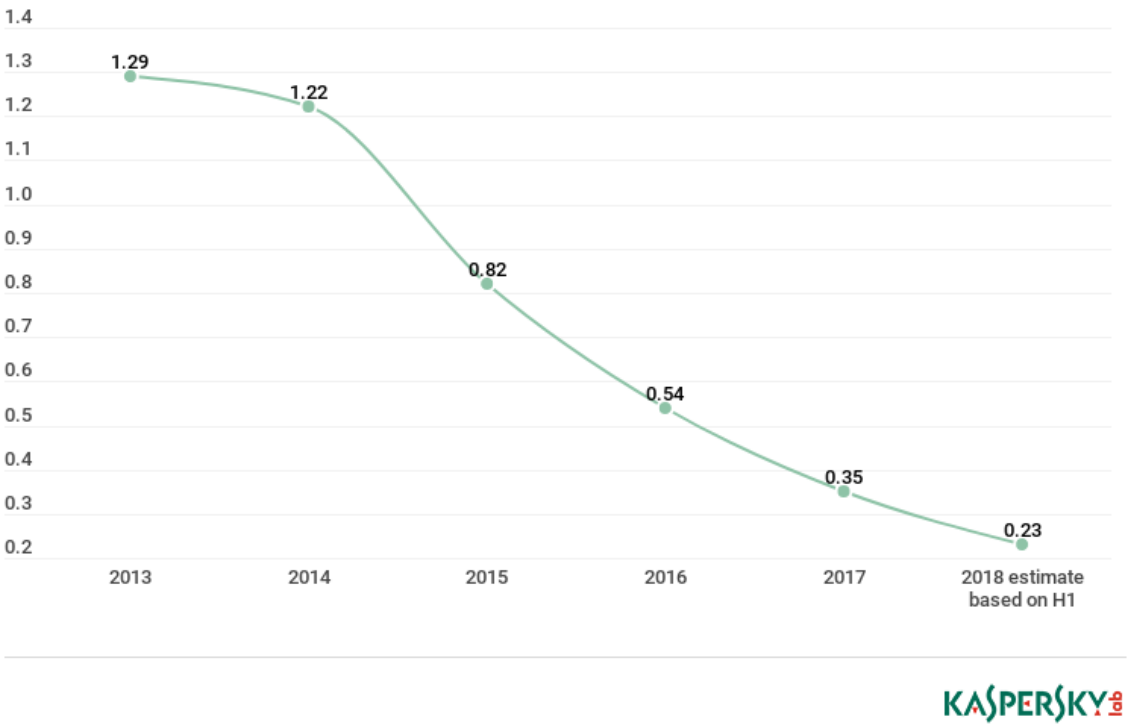
Additionally, the structure of most USB devices allows them to be transformed to provide hidden storage sections for the removal of stolen data. For example, the ProjectSauron 2016 toolkit was found to include a particular module designed to move data from air-gapped networks to internet-connected systems that involved USB drives that had been formatted to alter the size of the partition on the USB disk, reserving some covered space (several hundred megabytes) at the end of the disk for malicious intentions [21].

The Stuxnet survivor CVE-2010-2568

In March 2015, Microsoft fixed the last of the vulnerable L.N.K. code track. However, one in four Kaspersky Lab users who encountered an exploit through any attack medium in 2016, including web-borne threats, faced an exploit for this vulnerability. Nevertheless, CVE-2010-2568 emphasizes malware distributed by USB devices and other removable media, notwithstanding quickly decreasing numbers of detections and victims, and still ranks among the top 10 drive root threats detected by K.S.N. [21].



Total drive root (removable media) detections (in millions) of an exploit for CVE-2010-2568, 2013 – 2018. Source: KSN



Users with drive root (removable media) detections (in millions) of an exploit for CVE-2010-2568, 2013 – 2018. Source: KSN

If the exploit exposures indicate the amount of malware being transmitted via removable media, the following demonstrates the kind of malware being shared in this way.

Malware delivered via removable media

At least since 2016, The top malware expanded via removable media has stayed moderately consistent. For example, the family of Windows L.N.K. malware was containing links for downloading malicious files or paths for launching a malicious executable named Trojans has settled between the top three threats spread by removable media [21]. Attackers use this malware to destroy, block, modify or copy data or disrupt a device's operation or network. In 2017 a top detected USB threat called The WinLNK Runner Trojan is used in worms for launching executable files.

22.7 million attempted WinLNK.Agent infections were detected and striking nearly 900,000 users in 2017. Twenty-three million attacks estimate for 2018, hitting just over 700,000 users representing a 2% rise in detections and a 20% decline in the number of users targeted year-on-year [21].

The numbers for WinLNK Runner Trojan are expected to fall more sharply, with a 61% drop in detections from 2.75 million in 2017. In 2018 estimated 1 million, a decline of 51% in the number of targeted users (from around 920,000 in 2017 to just over 450,000 in 2018) [21].

Other top malware spread within USB devices includes the Sality virus first detected in 2003 but heavily modified [22]. The Dinihou worm automatically copies itself onto a USB drive and generating malicious shortcuts to launch the worm as promptly as the new victim opens them [23].

4. Future developments in USB Drop Attacks

Even though put so much effort to make aware employees not to put found USB devices into their computers, some researches prove that effort becomes useless. In 2016, Google's anti-abuse research team dropped 297 USBs on a university campus, and 98% of found devices that were picked up and 45% were plugged into computers [24].

These USB drives are also easy to lose. In 2008, a research study found that an estimated 9,000 USB drives were found in people's pant pockets at the dry cleaners and if these abandoned drives are not encrypted and can be accessed by the wrong hands [25].

Therefore it is essential to keep safe user-owned USB drives because hackers can use the data inside those USB drives or infected those devices, so the owner of that USB drive will plug them without any uncertainty. Also, if someone uses USB drives to transfer data from one computer to another, there is a possibility of infecting their computers with a virus that came with those data.

How to protect the user-owned device

- If the USB drive does not include a hardware switch for write protection, the owner can use a software write protector, such as USB Write Protect 2.0 [26]. It will completely block any data from being deleted and protect the device from malware being written onto owners' drive.
- The owner can use a decent USB anti-virus such as ClamWin to ensure no virus inside that USB drive [26].
- Users can install an encryption program like VeraCrypt or BitLocker to Windows for password protection on their USB device to ensure privacy and secure their data [26].
- Users can establish USB Firewalls in their computers to keep safe from malicious USB drives and user-owned USB drive that infected unintentionally [26].

- Users can use keypad flash drives [27] that can lock the device physically, and there are some USB drives such as Ironkey [28] that can be self-destructed when someone entered an incorrect password too many times.

An essential procedure to moderating the threat of infected USB drives is focusing on the human aspect. I.C.S. security managers help to reduce the threat by offering multiple guides.

For example, the National Cybersecurity and Communications Integration Center (ICS-CERT) gives the following guidelines for using USB drives [19]

- authorize strict policies for the use of USB drives on all enterprise and I.C.S. networks
- warning users about the USB drive attack vector and caution them that USBs of the unknown or uncertain source should never be plugged into a business, personal, or I.C.S. computer.

The U.K. National Cyber Security Centre has also offered some direction regarding USB drive policies [19]. Their supervision intimates that the user:

- control how USB drives can be used
- block access to physical ports for most users
- use antivirus tools
- only allow approved USB drives within the organization.

USB virus check kiosks

USB virus check kiosks can check USB drives for malware before using them. Olea manufactured a portable media cybersecurity kiosk named California Cyber Security Kiosk to safeguard networks and I.C.S. systems against malware threats caused by removable media.

The kiosk can scan USB drives brought in by contractors, vendors, employees, or anyone else and using up-to-date antivirus systems. For example, the kiosk can be installed at the entrance of a companies' building to ensure that USB drives are clean before crossing the plant origin.

Organizations can be implementing policies and procedures to prohibit the use of unknown USB drives, although it requires training and enforcement. Companies must have technical barriers, including antivirus to their machines and probably physically blocking USB ports [19] [29].

5. Conclusion

Considering the facts mentioned in the report above, many highly sophisticated USB drive malware attacks were discovered in the global cybersecurity industry. The danger of the impact on the victim cannot be overstated because they make direct losses to those infected individuals or organizations. Even though many high-tech security measures were invented, such as USB virus check kiosks, the malware also gets updated based on the tech level.

As we advance to the future, it is more likely to encounter more and more USB malware attacks. It is wise for the users to properly follow the security constraints to face this USB malware and to prevent their loss by taking the first step by installing a reliable antivirus guard and be conscious about the background. All these new malware are introduced so they can take action to prevent them before getting attacked by cybercriminals.

6. References

[1] S. Briere, "USB Drop Attack from Cybrary," Cybrary, [Online]. Available: https://www.cybrary.it/course/usb-drop-attack/. [Accessed April 2021].

[2] M. Tischer, Z. Durumeric, S. Foster, S. Duan, A. Mori, E. Bursztein and M. Bailey, "Users Really Do Plug in USB Drives They Find," IEEE, 18 August 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7546509. [Accessed April 2021].

[3] M. a. D. Z. a. F. S. a. D. S. a. M. A. a. B. E. a. B. M. Tischer, "Users really do plug in usb drives they find," IEEE, 2016. [Online]. Available: https://elie.net/publication/users-really-do-plug-in-usb-drives-they-find/. [Accessed April 2021].

[4] "What is a USB Drop Attack," Manage engine, [Online]. Available: https://www.manageengine.com/data-security/security-threats/usb-drop-attack.html. [Accessed April 2021].

[5] KASPERSKY, "The echo of Stuxnet," SecureList, 05 August 2014. [Online]. Available: https://securelist.com/the-echo-of-stuxnet-surprising-findings-in-the-windows-exploits-landscape/65367/. [Accessed April 2021].

[6] "Despite their Decreasing Numbers, USBs are Still Leveraged to Conduct Attacks," WATERISAC, 25 September 2018. [Online]. Available: https://www.waterisac.org/portal/despite-their-decreasing-numbers-usbs-are-still-leveraged-conduct-attacks. [Accessed April 2021].

[7] M. McLarnon, "The Human Interface Device (HID) Attack, aka USB Drive-By," CyberPoint, 18 October 2016. [Online]. Available: https://www.cyberpointllc.com/posts/cp-human-interface-device-attack.html. [Accessed April 2021].

[8] J. Talamantes, "USB Drop Attacks: The Danger Of “Lost And Found” Thumb Drives," Redteam Security, [Online]. Available: https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives. [Accessed April 2021].

[9] "What is Malicious code?," Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/definitions/malicious-code. [Accessed April 2021].

[10] "What is Social Engineering?," Webroot, [Online]. Available: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering. [Accessed April 2021].

[11] Z. Whittaker, "This laptop-bricking USB stick just got even more dangerous," ZDnet, 16 March 2017. [Online]. Available: https://www.zdnet.com/article/this-weaponized-usb-stick-gets-even-more-dangerous/. [Accessed April 2021].

[12] "USB Killer: A device that can destroy a PC in seconds," DECCAN CHRONICLE, 12 September 2016. [Online]. Available: https://www.deccanchronicle.com/technology/in-other-news/120916/usb-killer-a-device-that-can-destroy-a-pc-in-seconds.html. [Accessed April 2021].

[13] C. Welch, "Student used 'USB Killer' device to destroy $58,000 worth of college computers," The Verge, 17 April 2019. [Online]. Available: https://www.theverge.com/2019/4/17/18412427/college-saint-rose-student-guilty-usb-killer-destroyed-computers. [Accessed 29 April 2021].

[14] G. Belding, "USB killer: What it is and how to protect your devices," Infosec, 6 June 2019. [Online]. Available: https://resources.infosecinstitute.com/topic/usb-killer-how-to-protect-your-devices/. [Accessed April 2021].

[15] K. Chivers, "Zero-day vulnerability: What it is, and how it works," Norton, 28 August 2019. [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html. [Accessed April 2021].

[16] B. Day, "What Are Zero-Day Attacks & How Can I Prevent Them?," Gardian digital, 22 February 2021. [Online]. Available: https://guardiandigital.com/blog/zero-day-attack. [Accessed April 2021].

[17] C. Cimpanu, "Here's a List of 29 Different Types of USB Attacks," Bleeping computer, 13 March 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/heres-a-list-of-29-different-types-of-usb-attacks/. [Accessed April 2021].

[18] W. Ashford, "Mariposa botnet hit hardest where security awareness is low," Computer weekly.com, 11 March 2010. [Online]. Available: https://www.computerweekly.com/news/1280092325/Mariposa-botnet-hit-hardest-where-security-awareness-is-low. [Accessed April 2021].

[19] E. Hayden, "USB attacks: Big threats to ICS from small devices," Search security, February 2019. [Online]. Available: https://searchsecurity.techtarget.com/feature/USB-attacks-Big-threats-to-ICS-from-small-devices. [Accessed April 2021].

[20] G. Hale, "ICS Alert: USB Malware Attack," ISS Source, 20 December 2017. [Online]. Available: https://isssource.com/ics-alert-usb-malware-attack/. [Accessed April 2021].

[21] Kaspersky, "USB threats from malware to miners," Securelist, 25 September 2018. [Online]. Available: https://securelist.com/usb-threats-from-malware-to-miners/87989/. [Accessed April 2021].

[22] K. threats, "VIRUS.WIN32.SALITY," Kaspersky, 29 September 2015. [Online]. Available: https://threats.kaspersky.com/en/threat/Virus.Win32.Sality/. [Accessed April 2021].

[23] K. threats, "WORM.VBS.DINIHOU," Kaspersky, 29 September 2015. [Online]. Available: https://threats.kaspersky.com/en/threat/Worm.VBS.Dinihou/. [Accessed April 2021].

[24] G. Cluley, "Does dropping malicious USB sticks really work? Yes, worryingly well…," The State of Security, 4 August 2016. [Online]. Available: https://www.tripwire.com/state-of-security/featured/does-dropping-malicious-usb-sticks-really-work-yes-worryingly-well/. [Accessed April 2021].

[25] "How to safely and securely use USB memory sticks," Norton, [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-how-to-safely-and-securely-use-usb-memory-sticks.html?aid=usbdrives. [Accessed April 2021].

[26] R. Lecount, "USB Flash Drive Malware: How It Works & How to Protect Against It," hashedout, 16 December 2019. [Online]. Available: https://www.thesslstore.com/blog/usb-flash-drive-malware-how-it-works-how-to-protect-against-it/. [Accessed April 2021].

[27] L. Mearian, "Back to the future: Toshiba touts a USB flash drive with keypad passkey," Computerworld, 4 February 2015. [Online]. Available: https://www.computerworld.com/article/2879710/back-to-the-future-toshiba-touts-a-usb-flash-drive-with-keypad-passkey.html. [Accessed April 2021].

[28] Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/IronKey. [Accessed April 2021].

[29] "CyberSecurity Kiosks Help Companies," Kiosk Manufacturer Association, 5 April 2019. [Online]. Available: https://kioskindustry.org/cybersecurity-kiosks-help-companies/. [Accessed April 2021].