N. R. Hryhoruk

THE USB DROP ATTACK`S THREAT TO SECURITY

Vinnytsia National Technical University

Анотація

Досліджено небезпеку від USB drop атак і визначено стратегії захисту від них.

Ключові слова: USB drop атаки, технології USB, хакери, безпека.

Abstract

The danger of USB drop attacks is investigated and strategies for protecting against them are identified.

Keywords: USB drop attacks, USB technologies, hackers, security.

Introduction

USB drop attacks represent a sophisticated form of social engineering and capitalizing on human psychology in various situations. Many pen testers and attackers have used Universal Serial Bus (USB) drop key attacks to successfully compromise victim systems. Essentially, USB sticks, commonly known as USB keys or USB pen drives, are strategically placed or left unattended in different locations. Unsuspecting users, assuming these devices are lost, inadvertently insert them into their systems, unknowingly triggering the download and installation of malware. Such attacks underscore the importance of vigilance among individuals and organizations to mitigate potential risks.

Research results

A USB drop attack is a type of cyber-attack where a USB drive, typically pre-loaded with malware, is physically left in a location with the intent that an unsuspecting individual will pick it up and plug it into a computer.In other words, a USB drop attack is the digital equivalent of the well-known Trojan Horse story, in which a seemingly innocuous object harbors a hidden danger. Just like the wooden horse that the Greeks used to infiltrate Troy, the USB drive appears harmless, even useful. But once it’s plugged into a computer, the malicious software hidden inside springs into action, compromising your system and potentially even your entire network.[1]

Various types of USB attacks underscore the diverse methods employed by attackers:

Social Engineering: USB sticks often contain files with enticing names such as "Top Secret," leading users to click on them. These files typically redirect users to phishing sites, tricking them into divulging confidential information, making payments, or unwittingly installing malware on their computers.

Malicious Code: This prevalent type of USB drop attack involves USB sticks harboring files that deploy malicious code upon execution, automatically installing malware on the victim's system. Attackers can subsequently pilfer sensitive data or encrypt files, especially in the case of ransomware.

Human Interface Device Spoofing: In this attack, a connected USB drive manipulates a computer into recognizing it as a keyboard. It then injects pre-configured keystrokes to grant hackers remote access to the computer, allowing them to pilfer confidential information or deploy various forms of malware.

USBKill: Though less common, USBKill attacks are designed to render computers inoperable. A USBKill stick, resembling an ordinary USB thumb drive, stores power using a capacitor and subsequently releases a high-voltage surge through the data pins of the USB connection, effectively rendering the computer unusable.[2]

The motivations behind USB drop attacks are multifaceted, with financial gain being the primary objective. Hackers resort to such attacks to steal logins and passwords, install ransomware for data encryption or exfiltration, remotely take over victims' computers for espionage purposes, and even destroy victims' computers. These attacks underscore the critical importance of cybersecurity awareness and robust defense mechanisms to safeguard against potential threats.

Once hackers gain access to your sensitive data or device, they may demand a ransom after encrypting your data or sell your confidential information on the dark web to profit from it.

USB technologies have been exploited in numerous attacks targeting critical industrial infrastructure, with at least 56% of such incidents involving USB technology. For example, the AutoRun feature introduced by

Microsoft in 2005 facilitated the spread of malware via USB drives. The Stuxnet attack of 2010 demonstrated the devastating impact of USB-based attacks on industrial systems, while the Copperfield malware in 2017 targeted Middle Eastern infrastructure via infected USB drives. More recently, USB Killer attacks have caused irreparable damage to computers within seconds of connection. These incidents highlight the ongoing threat posed by USB-based attacks and the need for robust cybersecurity measures to protect critical infrastructure.[3]

Why Are USB Drop Attacks Still Relevant? USB drop attacks may seem like a basic attack method, making it difficult to understand why they continue to be relevant even in an age where cybersecurity is a top priority for many organizations. The main reason why USB drop attacks continue to pose real security threats is that they exploit human curiosity and behavior, which even the most advanced cybersecurity systems struggle to control. Moreover, recent USB drop attack campaigns, such as Sogu and Snowydrive, have demonstrated their evolution into highly specialized and targeted operations.

For instance, the Sogu campaign didn't just indiscriminately distribute USB drives across random locations; it targeted key industries like pharmaceuticals, IT, and energy across multiple countries. The malware it used is designed to persist, adapt, and execute a variety of malicious activities ranging from data theft to setting up reverse shells and keylogging. On the other hand, Snowydrive utilizes a malicious DLL side-loaded by a legitimate Notepad++ updater to evade detection. In summary, USB drop attacks persist because they exploit human vulnerabilities, can be highly targeted, and have adapted to circumvent contemporary cybersecurity solutions.[4]

Research conducted by Elie Bursztein, from Google's anti-abuse research team, shows that the majority of users will plug USB drives into their systems without hesitation. As part of his research, he distributed nearly 300 USB sticks on the University of Illinois Urbana-Champaign campus and measured who plugged them in. The results showed that 98% of the USB drives were picked up, and for 45% of the drives, someone not only plugged them in but also clicked on the files.[5]

To prevent bad USB attacks, take control of your security by following some basic guidelines. Firstly, keep personal and work-related USB sticks separate to avoid cross-contamination. Exercise caution with USB drives from unknown sources; if you're unsure of their origin, refrain from using them altogether. It's also important to periodically change and update your USB keys to minimize the risk of malware infiltration. Regularly scan your USB drives and devices with antivirus software to detect and remove any malicious software. Disable autorun features on all your devices to prevent unknown files from launching without your permission. If you need to access information from an unfamiliar USB source, consider using a buffer device and scan it for malware before proceeding. If you've already connected a suspicious USB drive, immediately disconnect from the internet and restart your device to minimize potential damage. Alternatively, invest in quality antivirus software to provide ongoing protection against USB-based threats. By following these precautions, you can enhance your security and mitigate the risk of falling victim to bad USB attacks.

Conclusion

In conclusion, USB drop attacks remain a significant threat due to their exploitation of human vulnerabilities and behaviors, making them relevant even in today's cybersecurity landscape. These attacks capitalize on curiosity and trust, leading unsuspecting users to compromise their own security by plugging in unknown USB drives. However, by implementing simple precautions, such as keeping personal and work-related USB sticks separate, exercising caution with unknown USB drives, regularly updating and scanning devices, and disabling autorun features, individuals can mitigate the risk of falling victim to bad USB attacks. It is imperative to recognize the ongoing relevance of these attacks and take proactive steps to protect against them, as they continue to target human weaknesses and pose real security risks.

REFERENCES

1. The Editors of Encyclopaedia Britannica. Trojan horse | Story & Facts. Encyclopedia Britannica. URL: https://www.britannica.com/topic/Trojan-horse

2. What Is a USB Drop Attack and How Can You Prevent It? URL: https://www.makeuseof.com/what-is-a-usb-drop-attack/

3. Belanger C. USB Security Risks | What is the Single Biggest Threat Posed by USB Technology?. Blog. URL: https://blog.pulsarsecurity.com/usb-security-risks-biggest-threat-posed-by-usb-technologies

4. Types of USB Drop Attacks & Cybersecurity Threats with Examples. Managed IT Services & Technology Consulting | OSIbeyond. URL: https://www.osibeyond.com/blog/usb-drop-attacks-cause-cybersecurity-incidents/ (date of access: 21.02.2024).

5. Users Really Do Plug in USB Drives They Find / M. Tischer et al. 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 22–26 May 2016. 2016. URL: https://doi.org/10.1109/sp.2016.26

Григорук Надія Романівна – студентка групи 2БС-22Б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: grigoruknadiia15@gmail.com

Бойко Юлія Василівна - старший викладач кафедри іноземних мов, ВНТУ, e-mail: boiko@vntu.edu.ua

Hryhoruk Nadiia Romanivna - student of group 2BS-22B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: grigoruknadiia15@gmail.com

Boyko Yuliia Vasylivna - senior teacher of foreign languages department, VNTU, e-mail: boiko@vntu.edu.ua