ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

The USB Threat No One is Talking About

Research on Firmware-Based Attacks Reveals the Urgent Need to Improve Supply Chain Security for all USB-Enabled Devices

October 2018

Authored by:

Drew Spaniel, Lead Researcher, Institute for Critical Infrastructure Technology

Parham Eftekhari, Executive Director, Institute for Critical Infrastructure Technology

The USB Threat No One is Talking About

Research on Firmware Based Attacks Reveals the Urgent Need to Improve Supply Chain Security for all USB-Enabled Devices

Authored by

Drew Spaniel, Lead Researcher, Institute for Critical Infrastructure Technology

Parham Eftekhari, Executive Director, Institute for Critical Infrastructure Technology

ICIT Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Support ICIT

Through objective research, publications and educational initiatives, the Institute for Critical Infrastructure Technology, a 501(c)(3) cybersecurity think tank located in Washington, D.C., is arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cyber criminals, nation states, and cyber terrorists.

Our mission is to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

Financial capital from generous individual and corporate donors is the lifeblood of the institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark.

Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our national security, and the protection of our personal information.

http://icitech.org/support-icit/

Contents

Introduction

Cables and devices that run on the Universal Serial Bus (USB) protocol are ubiquitous, popular, and pervasive. They are used to charge phones, connect devices to PCs, etc. In fact, USB connections are probably the most frequent user-initiated device interactions. Consider how many times a friend or co-worker asked to borrow a USB cable to charge their phone. Think of how many times a day you connect a device into one of a handful of USB ports on your PC. USB connections are a part of everyday life, yet for years USB devices have remained vulnerable to an unmitigated security vulnerability due to a lack of focus by manufacturers on supply-chain security and holistic, layered security-by-design.

USB devices are well-known vehicles that attackers can use to infiltrate networks. Past methodologies vary from flash drives dropped in parking lots to infected thumb drives disseminated at career fairs. The vector is favorable to threat actors because it bypasses airgap defenses by manipulating a complicit or unaware employee into inserting the infected device into sensitive systems. Afterward, malware hidden on the device installs on the system and spreads across the company network. In the past, dangerous malware such as BlackEnergy, Epic Turla, and many others have been delivered on infected thumb drives. The vector may soon evolve into a new and more dangerous derivative if it has not already. As we will explore in this paper, researchers have repeatedly demonstrated that USB devices can be leveraged to deliver malware using methodologies that do not require flash storage and are significantly more difficult to detect.

In writing this paper, it is the intent of the authors to educate readers on the fact that virtually every device with a USB cable can be weaponized and used as an attack vector to infiltrate an organization's layered defenses. The solution lies in improved supply chain security on the part of manufacturers coupled with awareness and stricter policies by organizations to minimize their risk exposure.

The USB Protocol is Vulnerable, and Threats are Possible

The fallibility and vulnerability behind the USB protocol have been known since at least 2014 and remains unaddressed. Consequently, at the time of this writing, any device featuring a USB connector can be turned malicious [1]. BadUSB, BadUSB 2.0, and USBHarpoon are attack vectors in which an adversary reprograms the USB controller chip in a device by altering its firmware and injects malicious code. Devices ranging from thumb drives to USB cables, to keyboards, and practically every other device with a USB connector have no protection against such reprogramming [2]. The weakness is the result of both the USB protocol and the poor security practices of device manufacturers. It cannot be fixed by issuing a downloadable patch,

by scanning connected devices, or by reformatting drives. Changes in security culture, practices, and expectations will be required from stakeholders at every level.

BadUSB Demonstrates That USB Firmware is Vulnerable

USB drives are frequently handed out as promotional material, shared among colleagues, lost, found, and otherwise exchanged among computer users. Security conscious users are aware of the devices' potential to carry malware, and they reformat the drives or employ antimalware scans to keep their systems, networks, and organizations safe. However, the risk from USB devices is not just in what they could carry in flash memory but is also inherent in their underlying components. USB devices have long been fundamentally flawed. In 2014, after months of reverse engineering the firmware that runs the basic communication functions of USB devices, researchers at SR Labs found that the controller chips which facilitate communications with PCs and let users transfer files could be weaponized to deliver malicious code. By altering the firmware of the device connector, adversaries can inject malicious code capable of compromising a system, altering files, delivering commands, or redirecting internet traffic. The infected device could replace software that is being installed with versions poisoned with malware, and it could install backdoors or rootkits on the system, impersonate a keyboard, alter the DNS setting to siphon traffic, act as a man-in-the-middle and secretly spy on communications, etc. It can do everything a user and a keyboard can do on a PC, which is basically everything [3].

Because the malware lies in the firmware of the device, scanning or reformatting the drive will not mitigate the risk. Even if the drive appears empty, the malicious code could still be present. The scanning and cleaning processes do not interact with the code that is being weaponized. There is no trivial remediation to the mitigate the vulnerability. Old-fashioned USB cyber-hygiene will not prevent infection because even if users are aware of the attack vector, it is difficult for them to verify the integrity of the device firmware. The problem cannot be patched because the attack vector exploits the very design of the USB protocol. The devices do not rely on the “code-signing” countermeasure that would ensure that any code added to the device be accompanied by the manufacturer’s unforgeable cryptographic signature. Manufactures do not even upload trusted versions of the firmware to compare against the shipped code. In fact, when researchers Nohl and Lell of SR Labs contacted a Taiwanese manufacturer of USB devices about the vulnerability present in their devices, the warning was met with denials that the attack vector was possible instead of immediate action to fix the problem. A warning WIRED issued to the USB Implementers Forum, the nonprofit corporation that oversees the USB standard, was met with the statement, "Consumers should always ensure their devices are from a trusted source and that only trusted sources interact with their devices. Consumers safeguard their personal belongings, and the same effort should be applied to protect themselves when it comes to technology.” While the advice is sound, it does little to reduce the

chances that malware will rapidly spread across the vector due to the poor cyber-hygiene of everyday users [3].

BadUSB 2.0 Proved that the Threat was Even Worse

Risk increases over time when vulnerabilities are left unmitigated because technology and human understanding continues to advance when device manufacturers fail to respond to the disclosed weakness responsibly. In 2016, researchers demonstrated an evolution in the BadUSB vector in the form of a proof of concept of an inline hardware implant capable of compromising USB fixed-line communications. The new attack, dubbed BadUSB 2.0, is an active or passive man-in-the-middle attack against low-speed USB-HID devices, such as keyboards and mice. It could enable an attacker to eavesdrop, replay input credentials and code, modify data, fabricate information, exfiltrate data, etc. It functions similar to hardware keyloggers, but it introduces new techniques to bypass keyboard-based one-time-password systems, automatically replay user credentials, and interact with the command shell over USB. Furthermore, it is more difficult to detect. Some keyboard emulation devices are easy to detect and block because they register as an additional USB device; potentially raising user suspicions at the presence of, for instance, two keyboards. BadUSB registered as a secondary USB device. BadUSB 2.0 functions as an inline hardware implant which means that it will not register as a secondary device; thereby giving it similar stealth potential as an obfuscated keylogger. It can capture all keystrokes and store them in the '/tmp' folder. It can modify regular expressions using weaponized code to either change user keystrokes, strategically frustrate the user, or alter input. Start or Run generic commands can be issued to the target operating system. Finally, PowerShell exfiltration and other techniques can be used to steal data [4].

The Threat is Evolving

BadUSB is not limited to thumb drives. Keyboards, mobile devices, mice, and any other device with a USB connector and firmware that can be reprogrammed can be infected. Worse, the threat can travel both from computer to USB and vice versa. Any USB connected to a PC could have its firmware reprogrammed by malware on the PC. Any PC connected to an infected USB device could be infected with the malware [3]. The potential epidemic could intensify through "Juice Jacking" attacks in which an attacker spreads malware to mobile devices through public charging terminals [5]. Afterward, the malware could spread to PCs that are later interfaced with infected mobile devices, and those systems would further spread the malware to additional devices and so on. If leveraged effectively, an attacker could widely spread a system-agnostic malware through a global distribution network of connected devices and unwitting users. This hypothetical vector has been proven possible through research into a methodology dubbed USBHarpoon.

USBHarpoon Weaponizes Any USB Device

Several independent research groups have built prototype malicious USB charging cables that are capable of compromising connected devices within a few seconds. A researcher using the Twitter handle MG developed an initial prototype and demonstration videos; meanwhile, Olaf Tan and Dennis Goh of RFID Research Group, Vincent Yiu of SYON Security, and Kevin Mitnick later collaborated to demonstrate the hypothetical attack to a wider audience. The device, dubbed BadUSB cable or USBHarpoon by each group respectively, is based on the BadUSB research. Once connected, the malicious cord acts as an infected peripheral device, enabling an attacker to type or launch commands [1] [6].

USB cables are relatively ubiquitous and are often seen as innocuous due to their lack of memory. Users have become at least partially suspicious of unknown flash drives, but that caution likely does not transfer to cables because the attack vector seems outside the imagination of many consumers. Most see cables only as a way to transfer power and files from point A to point B. As a result, even cautious users may not suspect that charging cables could be capable of infecting a system.

The USBHarpoon attack vector is similar to the BadUSB attack; although it is based on an alternate chip and a different firmware. As with BadUSB, USBHarpoon features altered firmware on its controller chip that makes it appear to the connected system as a human interface device (HID) ranging from an input device like a keyboard that issues a rapid succession of commands to a network card that modifies the system's DNS settings to redirect traffic. The USBHarpoon leverages the charging cable instead of the USB drive to create a "code bomb."

The researchers were even able to modify the connectors so that both data and power could pass through the cable to fulfill user expectations. The cable used in the demonstration worked with the 24-pin USB-C connector used with MacBook chargers, traditional USB devices, and micro USB connectors. In both appearance and function, USBHarpoon looks and behaves like a traditional USB cable except that the device can compromise any connected device [1]. One evolution in the attack hierarchy is that unlike BadUSB, USBHarpoon could be easily be used to compromise mobile devices as well as PCs [7].

The attack vector is successful on unlocked machines where it can launch commands and download and execute a payload after connection. On Windows, a Run prompt can be launched to execute commands. On Mac and Linux, a terminal can be launched and fed commands. The adversary's commands could modify or delete files, but the function would most likely be used to download and execute a payload such as a rootkit, backdoor, or other malware. On either category of operating system, the activity is visible to the user. It essentially appears as if someone else is controlling the system. However, researchers believe it is possible for an

attacker to implement mechanisms only to trigger the attack when a user is not present. These could range from system clock checks to user activity monitors. Instead of delaying the action, researchers believe that it may also be possible to trigger the attack using Bluetooth and radio signals [1].

Our Reliance on USB Makes BadUSB a Major Problem

USB is one of the fastest and most reliable ways to transfer a file; however, convenience and its dependability popularized it to the point that now that it has been discovered vulnerable, it may be difficult or impossible to mitigate the risk to consumers, organizations, and critical infrastructure. Outside of designed secure facilities, asking users to forgo USB altogether is an unrealistic pipe-dream. Similarly, without significant imposed market incentives and other leverage, history has demonstrated that manufacturers most likely will not consider making the changes necessary to ensure that each device's firmware and hardware are secure before distribution.

Four years after the disclosure of the weakness and as many years of inactivity, the potential for an epidemic is mounting. Without significant changes, users will continue to rely on inherently vulnerable USB devices that could be unknowingly spreading hidden malware. Suppliers could be spreading infected devices from the conveyor belt. Employees may be connecting poisoned devices and cables from home to their sensitive work systems. Insider threats posing as contractors could be stealing national security secrets by plugging in a single otherwise innocuous cord. All it takes for the figurative epidemic to burst is for one sophisticated adversary to attach a complex malware to the attack vector and release a single infected device into the public. The clock is ticking to raise awareness of the risk and to take action to mitigate the threat.

USB Condoms Don't Always Work

Attacks that rely on USB connections are not easy to mitigate because the vector leverages both the open nature of the USB protocol as well as the trust or curiosity of a user. Some have proposed mitigating the vector with USB condoms, an electronic accessory that blocks the data pins on a USB cable and allows only power to go through; however, as demonstrated by the researcher MG in a video, USB condoms can also be infected and cannot be trusted unless each can be audited prior to use [1].

Avoiding USB Is A Growing Option, but Not a Long Term Solution

USB grew in popularity because the protocol was universal across devices, hardware ports were easy to include, and the small drives were easy to transfer. Now, with email, the cloud, and other non-physical file transfer options, it may be reasonable for some organizations to avoid USB altogether. Ports could be filled with solder, or super glue and personnel could be

instructed not to connect BYOD devices. The obvious risk is that the flaw will still be present under the "band-aid" solution unless IT does a thorough job of removing drivers, disconnecting the blocked ports, etc. because otherwise a rogue employee could unblock a port and connect an infected device to compromise the system. Organizations' Information Security team should regularly audit all assets and networks for rogue and recognized USB devices.

Some systems that are isolated from the internet or legacy systems, in general, may rely heavily on USB ports for updates and other data transfer. Some have suggested "treating USB devices like hypodermic needles" to reduce risk. While the strategy might prove effective from a risk perspective, it seems cost ineffective and doomed to fail to an employee's perchance for convenience eventually.

The Supply Chain Needs to be Secured

The public sector should begin to evaluate acquisitions using security as a critical determinant. USB devices should be evaluated, and only secure devices should be purchased from trusted parties. Vendors should ensure the security of their devices and any subcomponents purchased from third-parties. It will be difficult to persuade consumers to recognize and care about the risk; however, until the public exerts financial pressure on the insecure vendors, it is unlikely that USB suppliers will improve their practices. Lawmakers may be able to influence the discussion by levying sanctions against companies that are found to include malware in their devices; however, since the BadUSB flaw is so well hidden, the potential of legislative influence will be difficult to realize.

A Paradigm Shift is Required

No technical patch can mitigate the BadUSB and USBHarpoon threat. In the short-term, the best solution is to raise awareness of the risk and to instruct consumers to not connect their PCs and mobile systems to USB devices that they do not trust, and vice versa. Trust cannot be assumed because the device appears blank. It can only be trusted if it has a verified supply chain that ensures that it was never influenced by malicious parties.

Since most devices and USB cables are manufactured in foreign factories, it is nearly impossible for consumers to discern where or by whom the components of their device were made. The majority of USB cables included in public and private sector devices are likely outsourced from third-party subcontractors. Trust cannot be ensured because the chain of custody is unknown. For instance, every major company operating in China is subject to the whims of a government liaison who promotes the Thirteenth Five-Year Plan. If the liaison injects malware into the firmware of some devices or cables on behalf of a nation-state Advanced Persistent Threat (APT) group, United States national security could later become jeopardized when the infected device is later purchased and connected to a sensitive network. Meanwhile, cybercriminals

could remotely compromise the firmware stored on the server of the USB device manufacturer and infect the devices before distribution. The infected systems could later be leveraged in crypto-mining or botnet schemes.

In the long term, companies need to change their USB policies. Manufacturers should verify the integrity of firmware on their devices, and they should ensure that it cannot be reverse engineered or altered. Meanwhile, consumers should only purchase devices from vendors who implement code-signing and other security on their products. Businesses and government entities that depend on security should only purchase from suppliers whose supply chain security can be trusted. This long-term shift does not seem likely in the near future. Consumers do not know or care who manufactures components such as USB drives or cables. The convenience and interoperability offered by the devices far outweigh security concerns for most. The other often repeated suggestion, of "treating USB devices like hypodermic needles" is likewise unlikely. Consumers do not want to live in a state of perpetual paranoia and fear. Instead, many will default to ignorance of the threat [3].

A malware that leverages BadUSB or USBHarpoon could spread fast. Regardless of their apathy, consumers should be made cognizant of the threat. Device makers, who have undoubtedly heard of the threat since 2014, will need to be convinced through the strategic delivery of information, stakeholder engagement, or market pressures, that the threat is real and worth remediating. With USB 4.0 on the horizon, a new security model should prevent the attack vector from ever developing into an epidemic [3].

ICIT Contact Information

Phone: 202-600-7250

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

Sources

[1] Ilascu, I. (2018). USBHarpoon Is a BadUSB Attack with A Twist. Retrieved from https://www.bleepingcomputer.com/news/security/usbharpoon-is-a-badusb-attack-with-a-twist/

[2] P. Paganini, "USBHarpoon a look-like charging cable that can hack into your computer", *Security Affairs*, 2018. [Online]. Available: https://securityaffairs.co/wordpress/75644/hacking/usbharpoon-attack.html. [Accessed: 27- Sep- 2018].

[3] A. Greenberg, "Why the Security of USB Is Fundamentally Broken", *WIRED*, 2014. [Online]. Available: https://www.wired.com/2014/07/usb-security/. [Accessed: 27- Sep- 2018].

[4] D. Kierznowski, "BadUSB 2.0: USB man in the middle attacks", *Intranet.royalholloway.ac.uk*, 2016. [Online]. Available: https://intranet.royalholloway.ac.uk/isg/documents/pdf/technicalreports/2016/rhul-isg-2016-7-david-kierznowski.pdf. [Accessed: 27- Sep- 2018].

[5] J. Fitzpatrick, "What Is “Juice Jacking”, and Should I Avoid Public Phone Chargers?", *How-To Geek*, 2016. [Online]. Available: https://www.howtogeek.com/166497/htg-explains-what-is-juice-jacking-and-how-worried-should-you-be/. [Accessed: 27- Sep- 2018].

[6] "MG", "USB - MG", *MG*, 2018. [Online]. Available: https://mg.lol/blog/tag/usb/. [Accessed: 27- Sep- 2018].

[7] C. Singh, "USBHarpoon: How "Innocent" USB Cables Can Be Manipulated To Inject Malware", *Fossbytes*, 2018. [Online]. Available: https://fossbytes.com/usbharpoon-usb-cable-malware-transfer/. [Accessed: 27- Sep- 2018].