Journal of Positive School Psychology http://journalppw.com
2023, Vol. 7, No. 1, 965-974

Survey On Micro-Controller Based Bad USB Attacks

B S Vishnu Charan[1] and Lalit Kulkarni[2]

[0000−0002−8359−307X]
[1,2]SCHOOL OF COMPUTER ENGINEERING & TECHNOLOGY, MIT World Peace University, Pune

Abstract. Every day, people all around the world make strides forward in the fields of electrical engineering and information technology. We have used several equipment in the past, including cameras, cellular phones, lighting, and wristwatches. However, at this time there is only one gadget that can accomplish everything, and that is the smartphone. Likewise, computer ports provide a similar function. Peripherals can be connected to a computer through its ports. In the past, when computers were still in their infancy, many ports had more than one purpose. In the end, USBs were developed to replace them. USB, or the Universal Serial Bus, allows a computer to talk to its peripherals such a mouse, keyboard, graphics card, camera, and scanner. Since the HID device class has been standardized, a standard USB driver may be used in place of the obsolete PS/2 connections. Numerous specialized tools may be used to launch attacks on HID. Sending a brief sequence of keystrokes using the on-board flash memory storage can completely corrupt the target system. BadUSB attacks are a type of USB attack that is similar to the more common USB drive attacks. This research systematically examines the available literature to uncover countermeasures to common forms of cybercrime. Perhaps over time, the quality of answers will improve. However, the purpose of this survey is to investigate BadUSB devices. We look into HID assaults, and we extend on the idea to allow scripts to be sent via the web.

Keywords: Human Interface Devices (HID) · Microcontroller · BadUSB.

1 OVERVIEW

As the name implies, a BadUSB is a USB device with altered firmware and is being utilized in an attack on other computers. This flaw is referred to as a HID attack. Any gadget that can receive data from people and provide it back to them is considered a Human Interface Device (HID). Changing the firmware makes the gadget think the USB device linked to it is a Mic, keyboard or Headphones. Recent studies have revealed that people are still susceptible to USB attacks, despite frequent warnings about the hazards of unsafe equipment. The original discovery of this vulnerability was made by Karsten Nohl, Sascha Krißler, and Jakob Lell at the 2014 Black Hat conference. It took them two months to patch the firmware of the USB device. They started by looking for firmware that could be cracked or patched online. A patch is a new version of some program or some corrected information. [14]

1.1 INTRODUCTION

Malware spread via USB drives is becoming increasingly sophisticated. In order to spread host-side vulnerabilities, attackers are increasingly aiming for the stack of the USB rather than just the USB devices themselves. They do this by introducing malicious code into the firmware of the device, which has the unrecognized and destructive capacity of demanding additional USB ports outside the specified objective of the device. This makes it possible for the devices like BadUSB to be carried out the attacks, in which a storage media device with malicious architecture is used as a keyboard to transfer malware to the victim's computer. A USB or thumb drive is the first thing that comes to mind when a user needs to move files between gadgets. The creation of USB (Universal Serial Bus) was a gamechanger in the history of technology.

Fig.1. PS/2 Connector

The picture above depicts what can only be described as a "USB." As a result of their harmful intent, though, these devices are commonly referred to as "BadUSBs." Several devices' firmwares were altered by hackers using these USBs. Firmware is a subset of software that is physically embedded into a device. Nonvolatile memory is used to store the software's instructions, ensuring that they will remain intact even if the device's power supply is cut. Thus, PCs or other systems with HID capability identify the BadUSB as a HID device and add the required drivers to make it operational, allowing it to take use of its environment.

*Supported by MIT-WPU.

Fig.2. BadUSB

2 LITERATURE REVIEW

According to Karystinos, E. et al., BadUSB is a critical flaw that has not been adequately addressed. By altering the firmware of a USB device, badUSB attacks may be carried out. Introduced here is Spyduino, an OS-agnostic Arduino that mimics a standard HID (Human Interface Device) (OS). Spyduino exploits the BadUSB flaw to steal private information and upload it to a remote server using the File Transfer Protocol. In this configuration, sensitive operating system and user information is sent to an FTP server using a Spyduino installed in a USB keyboard. It discusses potential growth and a number of potential responses.[1]

Researchers A. Ramadhanty and colleagues Many people take use of USB technology because it allows for simple plug-and-play integration with Windows, the most popular operating system now in use. For a long time now, USB has been a tool for cybercriminals to launch attacks against PCs. A keylogger is an example of an offensive tool. Exploiting these vulnerabilities in Windows 10 allows for the execution of keylogger attacks, which discreetly record PC keyboard activity. In this research, we ́ll employ a PowerShell script that makes use of BadUSB to initiate the Keylogger software. The Keyboard Injection Attack research utilizing an Arduino was finished, and the average execution time for the keylogger on an online PC was 7.474 seconds. The keylogger will send the data it collects back to the bad guy.[12]

Muslim, A. With each new version of Windows, Microsoft adds and removes browsers from its official list of supported software. Browsers make it simple to connect in to a website by storing usernames and passwords. However, doing so leaves your login information vulnerable to brute force and other forms of assault from hackers if you leave it stored in your browser. In order to do this, an application that can access the computer’s internal storage may be used to retrieve the browser login information and then display it. Rubber Ducky, Chrome Pass, and Passwordfox will all be used in an attack, as will Arduino Pro Micro, which will be used as a BadUSB. It took 14 seconds for the device to steal the credentials and send to the author’s email.[13]

USB-based attacks, as noted by security researchers such as Dave (Jing) Tian, Nolen Scaife, and others, have grown increasingly sophisticated in recent years. These days, attackers use a broad variety of techniques, from social engineering to signal injection, in their attacks. The security industry's response to these threats has been to deploy an increasingly diverse collection of countermeasures. This paper, provides a comprehensive survey and taxonomy of attacks by USB devices and countermeasures, consolidating insights from academic and professional literature and practice. Through our systematization, we have been able to extract primitives that can be used for both offense and defense across many USB communication levels. Using our classification method, we learn that USB assaults frequently exploit the trust-bydefault environment and cross over numerous layers of a software stack, revealing that no one line of security can fully prevent them. They created the verification of the newly published Type C USB Authentication standard, in which we find serious faults in the spec's architecture. Their analysis shows that while the standard has correctly identified the require of addressing the USB security issue, its shortcomings make doing so impossible. We wrap up by discussing potential avenues for further study into making USBbased computing more secure.[7]

A Mass Storage Device (MSD) is a device used to store data in large amount in such a fashion which is understandable by the machines. A Universal Serial Bus (USB) is a type of MSD, can be referred to as a BadUSB if the firmware on the device has been altered in such a way that it pretends to be

Paper	**Objective**	**Observations**	**Gap**
SoK: Plug & Pray[7]	To protect the host machine from USB attacks	They have outlined the techniques, nature, and defences for USB as- saults	"Tru in w it di prote these
Spyduino: Arduino as a HID Exploiting the BadUSB Vulnerability[1]	Arduino Pro Micro is used to perform HID attack which send file to attack's FTP server.	- Gain root privileges - Connect to drive	Sing and be m remo
Implementation and Analysis of Keyboard Injection Attack using USB Devices in Windows Operating System[12]	Arduino Pro Micro is used to perform HID attack which captures the keystrokes and mail them to the attacker	- Turns off Antivirus - User Account Control (UAC) level is Reduced - Downloads and run Keylogger - Send logged keys to Attacker	Sing
Implementation and Analysis of USB based Password Stealer using PowerShell in Google Chrome and Mozilla Firefox[13]	The surveyed paper discusses the use of BadUSB attack to run ChromePass.exe to extract and send passwords over email	- Turns off Antivirus - Execution policy Bypass - Download and run chrompass.exe - Send credentials to	Sing

something else, such as a keyboard, in order to escape being detected by an antivirus program. In this method, when the infected USB device is put in, a script that has already been developed is executed, and keystrokes are mimicked from a keyboard are generated. This can lead to an attacker installing backdoors, keyloggers, password sniffers, and other malicious software. This study makes an attempt to equip the attacker with hardware-software linked architecture with Wi-Fi as an additional layer system and makes it possible to compromise the victims' devices over the wire.[2]

		Attackers	

Table 1: Literature Survey Table

3 PROPOSED SYSTEM

This section explains the concept of Human Interface Devices (HID) and discusses the construction and Generalized Architecture of the system.

3.1 Universal Serial Bus Human Interface Device

As the name implies, a BadUSB is a USB device whose firmware has been altered and is being utilized in an attack on other computers. In the hacking world, this vulnerability is known as a HID attack. All gadgets that take data from people and give it back to humans are considered human interface devices (HID). When a USB is plugged in, the connected device analyzes the vendor ID(VID), product ID(PID), and description to install the right drivers. Such, the gadget's firmware is changed so that it thinks any USB device linked to it as a keyboard or mouse. [9,11]

3.2 Payload

The Ducky script is utilized by the payload. The standard keyboard instructions are used as input for the script; however, these commands may be altered and assigned aliases. Notepad or any other text editor is used to write the script, and then it is sent to Python as an input so that it may parse each line individually and look for the first word in each line in order to locate the command in the list of commands. Every single line that is entered into the payload has to begin with a Ducky command. This instructs the Python function to make use of the appropriate code in order to deliver keystrokes into the system that belongs to the victim.

3.3 Generalized System Architecture

Adding a wireless adapter to a regular USB is not an option. Since a microcontroller is easily customized with add-ons like the ESP wifi module, we utilize it to imitate HID attacks. Pico is used as a client in ESP to obtain data packages. That function holds off until ESP has sent data through UART.

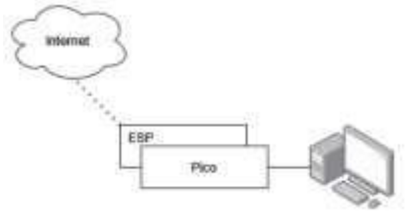

Fig.3. Generalized System Architecture

Universal Asynchronous Receiver/Transmitter (UART) is one such protocol that is widely used for device-to-device communication. With the right settings, UART may be used with serial protocols, allowing it to be utilized for tasks like sending serial data. Every byte of data is sent in a single packet when using serial transmission. For bidirectional data transport, we need two serial cables. Given the reduced number of components required for serial communications, this mode of transmission has the potential to reduce overall system cost.

3.4 Proposed Methodology

As shown in the following diagram, the device is activated after being inserted into the desktop computer. The hacker now has access to the ESP device and is able to upload the payload through the internet. The payload won't go off until some more execution activity is finished. The payload might be carried out with the aid of a TCP/IP connection.

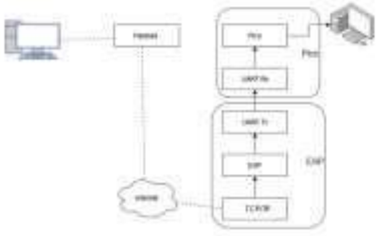

Fig.4. Proposed System Architecture

Pico acts as a serial device, therefore COM drivers are loaded on the victim's computer when it is connected. A computer's COM port serves as an input/output (I/O) interface for connecting serial devices. The Cipher Block Chaining (CBC) function of the Advanced Encryption Standard (AES) is used to encrypt data in communication between devices. [15]

4 CONCLUSION

We have conducted a thorough literature review on BadUSB. The model's framework that will guide our future efforts is now on display. The BadUSB payload has also been revealed to us. During the course of the project, we will be putting our knowledge of UART device-todevice communication protocols to use. TCP/IP communication is used to send payload to Pico from

ESP8266 and execute the payload on Pico.

References

1. E. Karystinos, A. Andreatos and C. Douligeris, **”Spyduino: Arduino as a HID Exploiting the BadUSB Vulnerability”**,2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2019. Available : 10.1109/dcoss.2019.00066 [Accessed 6 January 2022]
2. U. Shafique and S. Zahur, **”Towards Protection Against a USB Device Whose Firmware Has Been Compromised or Turned as ‘BadUSB’”**, Lecture Notes in Networks and Systems, pp. 975-987, 2019. Available: 10.1007/978-3030-12385-7 66 [Accessed 6 January 2022]
3. D. Tian, A. Bates, and K. Butler, **”Defending Against Malicious USB Firmware with GoodUSB”**, Proceedings of the 31st Annual Computer Security Applications Conference on - ACSAC 2015, 2015. Available: 10.1145/2818000.2818040 [Accessed 6 January 2022]
4. F. Griscioli, M. Pizzonia and M. Sacchetti, **”USBCheckIn: Preventing BadUSB attacks by forcing human-device interaction”**, 2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016. Available: 10.1109/pst.2016.7907004 [Accessed 6 January 2022].
5. N. Nissim, R. Yahalom and Y. Elovici, **”USB-based attacks”**, Computers Security, vol. 70, pp. 675-688, 2017. Available: 10.1016/j.cose.2017.08.002
6. L. Almazaydeh, J. Zhang, P. Wu, R. Wei, Y. Cheng and K. Elleithy, **”Bad USB MITM: A Network Attack Based on Physical Access and Its Practical Security Solutions”**, Computer and Information Science, vol. 11, no. 1, p. 1, 2017. Available: 10.5539/cis.v11n1p1
7. J. Tian, N. Scaife, D. Kumar, M. Bailey, A. Bates and K. Butler, **”SoK: ”Plug Pray” Today – Understanding USB Insecurity in Versions 1 Through C”**, 2018 IEEE Symposium on Security and Privacy (SP), 2018, pp. 1032-1047, doi: 10.1109/SP.2018.00037
8. M. Mamchenko and A. Sabanov, **”Exploring the Taxonomy of USB-Based Attacks”**, 2019 Twelfth International Conference ”Management of large-scale system development” (MLSD),

2019. Available : 10.1109/mlsd.2019.8910969 [Accessed 11 January 2022].

9. **”GitHub - dbisu/pico-ducky: Create a USB Rubber Ducky like device using a Raspberry PI Pico”**, GitHub, 2022. [Online]. Available: https://github.com/dbisu/picoducky. [Accessed: 11- Jan-2022].

10. Marwan Al-Zarouni, **”The Reality of Risks from Consented use of USB Devices”**, 2006 Te Proceedings of 4th Australian Information Security Management Conference.[Accessed 11 January 2022].

11. **”wonderhowto - NullByte Make your Own BadUSB”**, wonderhowto, 2019. [Online]. Available: https://null-byte.wonderhowto.com/howto/make-yourown-bad-usb0165419/. [Accessed: 11-Jan- 2022]

12. A. Ramadhanty, A. Budiono and A. Almaarif, **Implementation and Analysis of Keyboard Injection Attack using USB Devices in Windows Operating System**, 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE), 2020. Available: 10.1109/ic2ie50715.2020.9274631 [Accessed 20 February 2022]

13.] A. Muslim, A. Budiono and A. Almaarif,**Implementation and Analysis of USB based Password Stealer using PowerShell in Google Chrome and Mozilla Firefox**, 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE), 2020. Available: 10.1109/ic2ie50715.2020.9274566 [Accessed 20 February 2022]

14. Nohl, K. and Lell, J., 2022. **Black Hat USA 2014 - BadUSB - On Accessories that Turn Evil**. [online]Blackhat.com. Available at: ¡https://www.blackhat.com/us14/briefings.htmlbadusb-onaccessories-that-turnevil¿ [Accessed 20 July 2022]

15. DataLocker Inc. 2022. **”ECB versus CBC Mode AES encryption.”** [online] Available at: ¡https://datalocker.com/what-isthe-difference-betweenecbmode-versus-cbc-mode-aesencryption/¿ [Accessed 20 July 2022

16. B. S. Vishnu Charan, Lalit Kulkarni, **”Enhancement And Implementation Of Badusb Attacks Using Microcontroller”**, Journal of Positive School Psychology, 2022, Vol. 6, No. 9, 563-573 Available: https://www.journalppw.com/index.php/jpsp/article/download/12204/7918/14636