Jurnal E-Komtek
Vol. 7, No. 2 (2023) pp. 329-335
https://jurnal.politeknik-kebumen.ac.id/index.php/E-KOMTEK
p-ISSN : 2580-3719 e-ISSN : 2622-3066

Implementation and Analysis of WiFi Human Interface Device (HID) USB Using ATMEGA32U4 and ESP8266

Gilang Ryan Fernandes[1], Ika Mei Lina[2]
[1,2]Department of Informatics Engineering, Universitas Indraprasta PGRI, Indonesia, 12530

gilangfernandes@gmail.com

https://doi.org/10.37339/e-komtek.v7i2.1478

Published by Politeknik Piksi Ganesha Indonesia

Artikel Info
Submitted:
24-10-2023
Revised:
06-12-2023
Accepted:
06-12-2023
Online first :
13-12-2023

Abstract

Advances in technology have resulted in hacking occurring everywhere. Hacking is the act of illegally accessing data and information. It is not uncommon for many hacking cases to harm various parties due to ignorance. The results of hacking at this time are widespread, one of which is a ransomware virus that can encrypt data, a keylogger is software that can monitor keyboard activity, and a WiFi USB human interface device which is where this attack is a virtual keyboard. This research assembles the components used for Human Interface Device (HID) by utilizing ATMEGA32U4 as a virtual keyboard and ESP8266 as WiFi media. This technique is used to obtain target information and data. This research aims to make people more careful and overcome hacking. It is hoped that people will be more concerned about system and data security. Based on the research results, WiFi HID USB attacks can be dangerous for computer owners who need to be more aware of various hacker attacks because this technique can directly take target access.

Keywords: HID USB, BadUSB, Hacking; Cyber Security, Wifi

Abstrak

Kemajuan teknologi mengakibatkan peretasan terjadi dimana-mana. Peretasan merupakan tindakan mengakses data dan informasi secara ilegal. Tidak jarang banyak kasus peretasan yang merugikan berbagai pihak karena ketidaktahuan. Hasil dari peretasan pada saat ini sudah meluas, salah satunya adalah virus ransomware yang dapat mengenkripsi data, keylogger adalah software yang dapat memonitor aktivitas keyboard, dan USB human interface device WiFi yang merupakan tempat serangan ini adalah keyboard virtual. Penelitian ini merangkai komponen-komponen yang digunakan untuk Human Interface Device (HID) dengan memanfaatkan ATMEGA32U4 sebagai keyboard virtual dan ESP8266 sebagai media WiFi. Teknik ini digunakan untuk mendapatkan informasi dan data target. Penelitian ini bertujuan agar masyarakat lebih berhati-hati dan mengatasi peretasan. Harapannya masyarakat lebih peduli terhadap keamanan sistem dan data. Berdasarkan hasil penelitian, serangan WiFi HID USB dapat berbahaya bagi pemilik komputer yang perlu lebih waspada terhadap berbagai serangan hacker karena teknik ini dapat secara langsung mengambil akses target.

Kata-kata kunci: *HID USB, BadUSB, Peretasan, Keamanan Dunia Maya, Wifi*

1. Introduction

Technology is an inseparable part of today's life, where all activities are related to technology. In the current era, technology is one way to survive, which means people are competing to create systems, applications, and artificial intelligence for the needs of individuals, organizations, and companies. Currently, technology is part of people's lives because it can make work easier and provide the right solutions in the current era.

With the presence and development of technology, data and information are well organized. The story of technology is in line with the development of the world of hacking, where hacking is an act of accessing data and information illegally and is, of course, very dangerous for data security. Data is precious information, so the security of this data must also be maximized. It is not uncommon for many hacking cases to harm various parties because they are unaware of the developments and dangers of hacking. Hacking is an act of cybercrime involving hacking into a system [1].

The development of hacking at this time is rampant, one of which is the ransomware virus, which can encrypt data; keylogger is software that can monitor keyboard activity and USB human interface device WiFi, where this USB human interface WiFi attack is a virtual keyboard. This technique is used to obtain target information and data. This technique allows hackers to access all critical files on the target computer. The USB WiFi, a human interface device, will enable hackers to carry out activities with WiFi devices without the target realizing it. This tool can run on various operating systems without antivirus detection.

This research aims to make people more careful and able to anticipate these attacks. With the above objectives, it is hoped that the public will be more concerned with system and data security. This USB WiFi human interface device was created using an ATMEGA32U4 as a virtual keyboard and an ESP8266 as a WiFi medium to assist users in giving code execution commands to the ATMEGA32U4.

2. Method

In this research, the author will use a Human Interface Device (HID) connected to WiFi to implement and analyze how a virtual keyboard works to gain access to the target computer. This research aims to make the public, especially organizations and companies, more aware of various types of hacker attacks, both long-distance and short-distance.

2.1 WiFI Human Interface Device (HID) USB Series

The author will assemble the components used for the Human Interface Device (HID) in this research. Human Interface Device (HID) is a system that all computers have to be able to take input from users, one of which is using the keyboard [2]. This circuit aims to ensure that each hardware is connected and runs well. WiFi HID USB Series is presented on Figure 1.

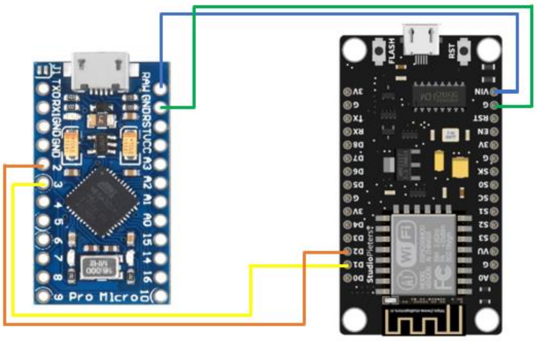


Figure 1. WiFi HID USB Series

It can be seen in the picture above that the author created a circuit between the ATEMEGA32U4 as a virtual keyboard and the ESP8266, whose task is to receive commands via WiFi connected to the attacker's device. The course above shows that VIN is connected to RAW, Ground is connected to Ground, D1 is associated with 3, and D2 is connected to 2.

2.2 ATEMEGA32U4

The ATMega32U4 is a microcontroller produced by Atmel, which has a RISC (Reduce Instruction Set Computer) instruction set. So, data processing can run faster than if using a CISC (Completed Instruction Set Computer) instruction set [3]. In this research, the ATMega32U4 is helpful as a signal processor. The analogue signal is converted into a digital signal of 16-bit analogue-to-digital resolution [4].

The ATMEGA32U4 microchip is one of the chips misused by hackers in carrying out their actions because this chip uses 8-bit ASCII code to communicate. With 2.5 kilobytes of storage memory, this size looks very small compared to the current size of storage memory for files, which are generally gigabytes. However, for hackers, the storage memory size of 2.5 Kilo Bytes is a prominent enough capacity to store payloads of up to 20,000 characters typed by the keyboard [5].

2.3 ESP8266

ESP8266 is a WiFi Serial Transceiver Module, which is a chip component that is assembled so that it can be integrated. This chip can be used as a controller for communication to the internet via WiFi [6]. The NodeMCU ESP8266 can be used as a host or WiFi client because of its onboard processing and storage capabilities. This makes it possible to integrate it into various sensors and specific device applications via GPIOs with easy implementation and relatively fast time. The high level of integration of the ESP8266 allows for minimal external circuitry requirements, including front-end modules designed to fill minimal PCB area [7].

2.4 WiFi Duck

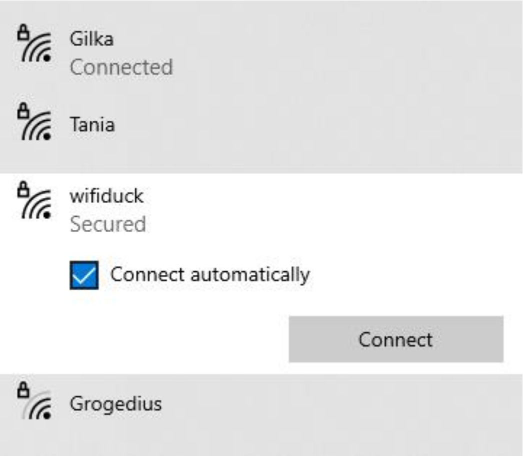
WiFi Duck is an open-source project that aims to study keystroke injection attacks and destructive USB attacks. Using a USB keyboard, this tool can provide access to the target computer with a USB port in seconds. With WiFi, duck attackers can attack by connecting to WiFi [8]. WiFi duck is a similar form of evil USB. It makes it easy to control and access scripts with a web interface connected to WiFi, so importing scripts via third-party applications such as Arduino IDE or saving hands to an SD card is unnecessary. BadUSB is a USB device manipulated by an attacker so that the computer can recognize it as a regular USB. However, BadUSB is an engineering technique that uses a virtual keyboard to run scripts embedded in the USB [9].

3. Results and Discussion

This implementation aims to research and raise awareness about computer security owned by users. The next goal is to make people more careful about the dangers of hacking because hacking and the development of the times are growing at an intersection. In this research, the author uses a computer or laptop as a target plugged in with the circuit created and coded above.

3.1 Implementation and Testing

In carrying out the implementation, the author first made a WiFi connection to the USB WiFi Human Interface Device (HID) circuit. WiFi SSID is presented in **Figure 2**.



Gilka
Connected

Tania

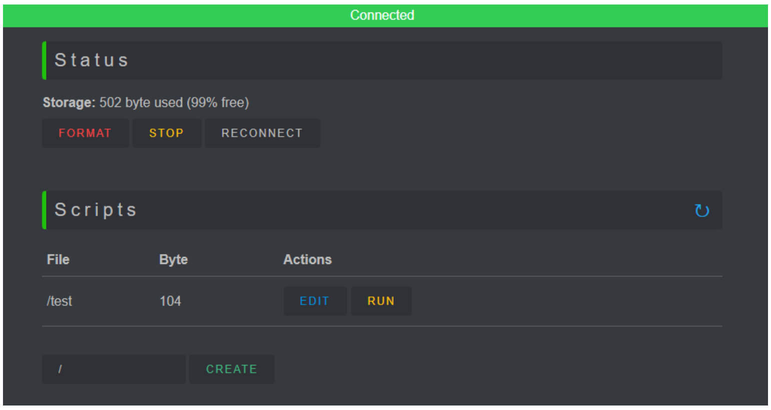
wifiduck
Secured

☑ Connect automatically

Grogedius

Figure 2. WiFi SSID

When the circuit is connected to the USB of the target computer or laptop, WiFi will also be visible with the name wifi-duck. The author connects to a WiFi called wifi-duck, where this WiFi is used to send commands to the targeted computer. The orders sent later will be made on the interface created on the ESP8266. After successfully connecting to the WiFi called wifi-duck, the next step is to open the browser and type 192.168.4.1; then, you will be directed to the WiFi Duck interface page. Interface page is presented on **Figure 3**.

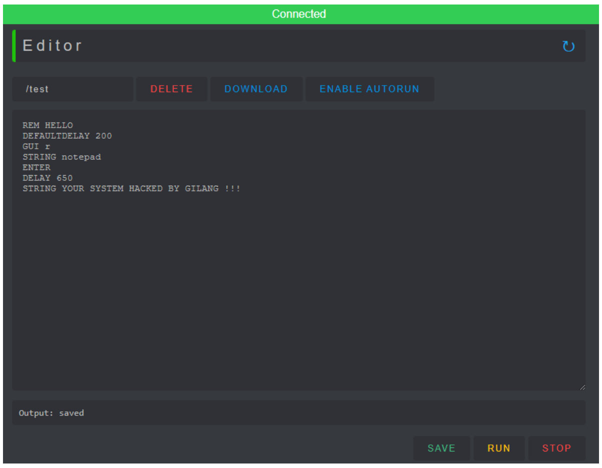


Storage: 502 byte used (99% free)

File	Byte	Actions
/test	104	EDIT RUN

Figure 3. Interface Page

In the picture above, there is a status that shows the storage space of the ATMEGA32U4, and in the scripts is a collection of commands that have been saved and are ready to be executed. The author will implement how the circuit above can take over the target computer or laptop in the following process. Editor interface is presented on **Figure 4.**



```
REM HELLO
DEFAULTDELAY 200
GUI r
STRING notepad
ENTER
DELAY 650
STRING YOUR SYSTEM HACKED BY GILANG !!!
```

```
Output: saved
```

Figure 4. Editor Interface

On the same page as the image above, there is a menu called editor, where the menu is a place to command the ATEMEGA32U4 as a Human Interface Device (HID). It can be seen in the image above that there is a script to open Notepad and write the sentence "YOUR SYSTEM HACKED BY GILANG." when this script is run by clicking the run button, the victim's computer will move itself according to the command that was made previously. In the Editor menu, there is also an Enable Autorun button where the attacker or hacker can immediately save the script that has been created. When the WiFi Duck circuit is plugged into the target computer or laptop, it will directly run automatically without being connected to WiFi.

3.2 Analysis and Anticipation

In the implementation above, it can be analyzed that attacks carried out by hackers require direct contact with the target computer or laptop. The target computer belongs to the attacker or hacker when the USB or circuit is plugged in.

The script above is an example of an attacker doing whatever they want to the target, including opening a notepad and writing the desired words. In other cases, an attacker or hacker can even insert a virus or RAT, which can monitor all target activities anywhere and at any time. A Remote Access Trojan (RAT) is a virus that can allow an attacker to gain remote access to aspects and the ability to control an infected device **[10]**.

From the explanation above, it is necessary to anticipate and avoid these attacks by constantly maintaining and monitoring all ports or computer activity. Ensure every USB connected to our computer comes from someone we know and are responsible for. If the USB port is not in use, you should cover it with a USB cover and ensure the antivirus is constantly updated to avoid attacks such as viruses or RATs that are too severe. The final precaution is never to leave your computer or laptop turned on or on standby.

4. Conclusion

From the implementation and testing that has been carried out above, the author can conclude that WiFi Human Interface Device (HID) USB attacks can be a dangerous threat for computer or laptop owners who are less alert to various types of hacker attacks because this technique can directly take away target access and several attacks are not recognized by the antivirus. This USB WiFi Human Interface Device (HID) utilizes the ESP8266 as a WiFi transmitter. It becomes an interface for creating scripts and sending them to the ATEMEGA32U4 to execute them on the target computer.

References

[1] R. Canady and D. Wuidjaja, “Tindakan Hacking dan Profesi Hacker: Persoalan Etis antara Utilitarianisme dan Deontologi,” *J. Filsafat Terap.*, vol. 1, no. 1, pp. 59–78, 2022, doi: 10.11111/moderasi.xxxxxxx.

[2] H. E. Wahanani and M. Idhom, “Serangan Hid Usb Otomatis Pada Sistem Operasi,” *Pros. Semin. Nas. …*, no. September, pp. 4–7, 2019, [Online]. Available: http://santika.ijconsist.org/index.php/SANTIKA/article/view/4%0Ahttp://santika.ijconsist.org/index.php/SANTIKA/article/download/4/2

[3] A. Roihan, A. Permana, and D. Mila, "MONITORING KEBOCORAN GAS MENGGUNAKAN MICROCONTROLLER ARDUINO UNO dan ESP8266 BERBASIS INTERNET OF THINGS," *ICIT J.*, vol. 2, no. 2, pp. 170–183, 2016, doi 10.33050/init.v2i2.30.

[4] H. H. Idrus, Y. Mangarengi, and N. S. Mustajar, “Test of Polymerase Chain Reaction (PCR) Detection and The Specificity in Gen Hd Salmonella typhi in RS. Ibnu Sina,” *Annu. Basic Sci. Int. Conf.*, no. December, p. 353, 2018.

[5] N. Budhisantosa, “Forensik Komputer Human Interface Device Badusb Berbasis Microcontroller Atmega32U4 Arduino Leonardo Pada Registry Sistem Operasi Microsoft Windows 7,” vol. 3, pp. 97–102, 2018.

[6] S. Samsugi, Ardiansyah, and D. Kastutara, “Internet Of Things (IoT) Sistem Kendali Jarak Jauh Berbasis Arduino Dan Modul Wifi Esp8266,” *Pros. Semin. Nas. ReTII*, pp. 295–303, 2018.

[7] M. R. Hidayat, C. Christiono, and B. S. Sapudin, “PERANCANGAN SISTEM KEAMANAN RUMAH BERBASIS IoT DENGAN NodeMCU ESP8266 MENGGUNAKAN SENSOR PIR HC-SR501 DAN SENSOR SMOKE DETECTOR,” *Kilat*, vol. 7, no. 2, pp. 139–148, 2018, doi: 10.33322/kilat.v7i2.357.

[8] SpacehuhnTech, “SpacehuhnTech/WiFiDuck: Wireless keystroke injection attack platform.” https://github.com/SpacehuhnTech/WiFiDuck (accessed Oct. 24, 2023).

[9] A. T. Ramadhan, A. Budiyono, and A. Almaarif, “Usb Attack Berbasis Powershell Menggunakan P4Wnp1 Pada Personal Computer Implementation and Analysis of Usb Attack Based on Powershell Using P4Wnp1 in Personal Computer,” vol. 6, no. 2, pp. 7995–8001, 2019.

[10] M. Alvian, H. Nasution, and A. T. Laksono, “Investigasi Serangan Backdoor Remote Access Trojan (RAT) Terhadap Smartphone,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 4, pp. 505–510, 2020, doi: 10.30865/jurikom.v7i4.2301.