School of Informatics & IT
TEMASEK POLYTECHNIC

Temasek Polytechnic
School of Informatics and
IT
Diploma in Cybersecurity &
Digital Forensics
AY 21/22 Semester

Major Project Reflection Report

Project Title:

Keyboard in Disguise (KiD)

Submitted To:

Mr. Shaun Tan

Submitted By:

Zachary Phoon Jun Ze, 1900353B

Supervisor:

Mr. Shaun Tan

Students' Declaration of Originality

I hereby declare that the course work(s) submitted, is a result of my own efforts. I affirm that there is NO plagiarism and copying, either partially or entirely, from someone else's design and works, without giving proper credit and acknowledgement to the source(s)/author(s).

I am aware that I shall be subjected to disciplinary actions deemed appropriate by the School of Informatics & IT and Temasek Polytechnic if I am found to have committed or abetted the offence of plagiarism in relation to this submitted work.

Zachary Phoon Jun Ze
1900353B
25/6/2021

Table of Contents

Acknowledgements

I would like to express our gratitude to my supervisor, Mr. Shaun Tan, for his guidance and active participation during the development of the project. Without his guidance, insightful input and numerous suggestions, the project would not have been a success.

Abstract

Keyboard in Disguise (KiD) is an offensive backdoor device disguised as a keyboard.
When the keyboard is plugged into the USB port of the attack system, malicious code will be executed. After this, the attacker will be able to access the victim’s machine without their knowledge and will be able to extract information without their consent.

Our goal is to make the attacking tool, a keyboard, to be inconspicuous as possible. The keyboard will function as normal while secretly compromising the victim's machine. The victim will be suspicious, giving the attacker a longer timeframe carrying out attacks and extracting information.

Chapter 1 Introduction

Since most computers have unsecured USB ports, an attack can be carried out on unsuspected victims by disguising the attack method as an ordinary USB device. This is display that this is always a possible vector of attack beside the normal ways of attacking a system physically or remotely.

Chapter 2 Reflection: Planning

The initial planning was manageable, we made the discussion and decisions easily and assigned our roles by our team leader. We were unsure on what to do at first as there are many existing Security Devices in the market. We had some inspiration with our seniors work of making a Malicious USB Mouse. We came into conclusion to make a new malicious USB Keyboard to bring aware of this type of vector of attack.

Chapter 3 Reflection: Execution

The team was assigned to find payload delivery methods and see if it works. We found many ways to deliver the payload, but the firewall must be turned off.
With this bottleneck, the team started to research on hardware required to run our commands on the host machine to retrieve payload. Due to chip shortages over the world, we had to order our chips from overseas.
While waiting of the delivery of chips, the team continued to find possibility to deliver the payload past the firewall and Windows Defender. The issue was the payload keeps getting caught at Windows Defender, was persistent, so we tried to find a way to reduce the terminal display up time. We tried to make the command prompt terminal smaller by altering the command used in Windows Run Module. Soon enough we manage to open a hidden PowerShell Terminal. With this we obtain a standard user PowerShell Terminal. This allow us to run the codes we need to retrieve the payload.
After some research we found out that the Microsoft has a function called “Real-time Protection”, I learned that we had to turn this off as it set the payload into a “playground” machine and see what effect of the payload do to the system to see if it is malicious or not. I learned new way to obtain administrator privileges terminal with simple PowerShell commands with some Arduino Keystroke sending. I had to learn new skills in obfuscation and ways to bypass Windows Defender.
When the hardware arrived, we begin our hardware trouble shooting. The first issue was that caused Windows to fail to recognize as a USB device as Arduino has a bootloader that has a 5 second delay for uploading new code. Hence, we manage to find existing scripts to remove that bootloader which aid to reduce the delay for the attack to be carried out. The other issue was a faulty USB Hub Chip, it could not allow us to use sequential order. Hence, I solder the Keyboard and the Arduino on slot 1 and 4. Since bare cables were exposed, we could not sleeve it up hence we used hot glue to insulate and prevent the devices from casing any short circuits. My team leader managed to bypass Windows Defender, but it doesn’t run on administrator level of shell hence I found the binds for the Digispark keystrokes to allow admin level access and added it to the Arduino USB chip.

Chapter 4 Reflection: Deliverable

During this project, I helped with research of payload delivery methods, research for post exploit remote procedure call, research on bypassing anti-virus and firewall and soldering of hardware together. Each research has contributed a significant role in refining the product that we all wished to achieve. I fell if the team and I had more time and budget, we will be able to produce not only the awareness product but the solution to it as well.

During the research phase of the earlier payload delivery methods, it acted as a refresher course as well as deepen my knowledge of what I have learned during Ethical Hacking lessons. This made me realize that with the knowledge of payload delivery, I will be able to defend the system more easily as the knowledge is at my fingertips and I do not require more research time which will help reduce the attacker's up time in the compromised system.

The most challenging part of this project was the bypassing of anti-virus and firewall. This was due to the constant failure as I forgot that anti-virus detects on a signature basis. I did not give up and continued to preserver along with the help of the team. I realize that the rapid cyber security has improved as most of our lives are on the internet now. I had to learn many ways such as obfuscation, compressing codes, making use of algorithm to alter the code to prevent it from detection. This took the longest time in the project as I do not have much experience in this topic and had to take more time to learn and research. I would like to admit that I felt the most burn out during the bypassing of anti-virus and firewall portion.

As for soldering of hardware together, it was the most fun as I am a more hands on learner. The troubleshooting and solving of issue while soldering was more time draining than brain draining as these issues were easily solved with the debugging skill instilled after many hours of learning how to code. Also, we received a faulty chip where our second USB solder slot was faulty hence it did not work at first. So, after some time, I soldered the keyboard connection to USB slot 1 and the female USB connector used for the connection of the Arduino Chip on USB slot 4. I feel my weakness was trusting all hardware obtained online was in 100% working condition. We did not consider that some products maybe faulty. If we did receive a failed product our timeline would be in a mess.

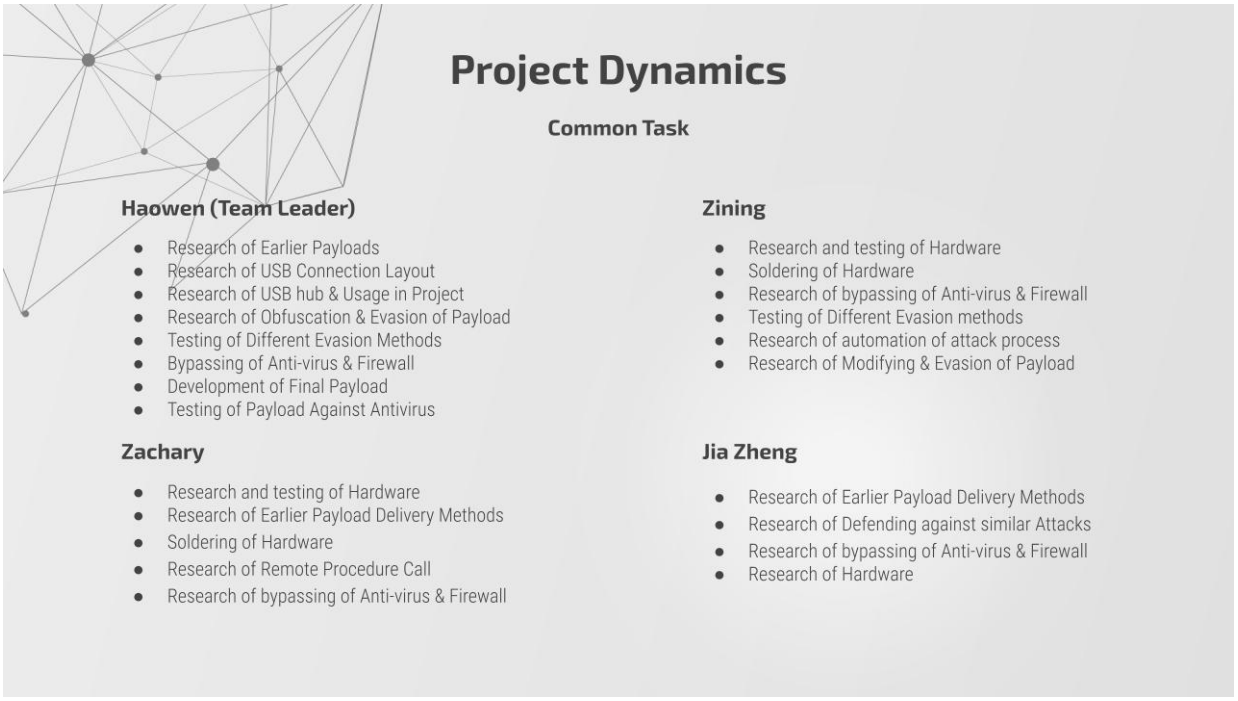
Research of Post-exploit Remote Procedure Call was the most interesting process

for this project. I had to learn PowerShell language better understand what I was doing and what each command issued meant. This also brought light to how our daily driving Operating System can do much more with some programming. It made me more curious what more can PowerShell do to improve our daily lives as well as impact it.

The research of payload delivery was useful for the team and I to have different idea of attacks which slowly lead to the final decision to use port 443 as it was a port that uses HTTPS.

One weakness that I notice was our knowledge of windows defender, this was because there were some options that caused us to render our payload first successful attack. The options were the real-time protection as well as sample submission. After a successful attack, the system will take note of the signatures and begin to defend against such attacks despite being successful on the first try. If we had knew about these options earlier, we could have prevented our research to get notice which would have reduced the time spent on that section significantly.

One thing I would like to improve is making a smaller version of the keyboard as more consumers are shifting to smaller sized keyboard due to lack of space, but this is just an awareness project. So, it also applied to all sizes and types of keyboards.



Chapter 5 Conclusion

Looking back, I do not regret what I have done during this process as this made me understand how malware are made and the many ways to hide it. This made me understand how important cybersecurity role on the internet, they require so much knowledge as well as keep informed about the fast pace changing standard to keep protect users like us.

All in all, I feel that I have learned a lot from this project, but I wish I had more time to build a solution along with this awareness product as this could make a complete circle where I have done the attack as well as a product to defend against it. I am beyond happy with the final deliverables as it has met all and more expectations, I set for it.

References/ Bibliography

Digistump. 2016. Digikeyboard.h
https://github.com/digistump/DigistumpArduino/blob/master/digistump-avr/libraries/DigisparkKeyboard/DigiKeyboard.h

Swisskyrepo. 2021. PayloadAllTheThings.
https://github.com/swisskyrepo/PayloadsAllTheThings

Red Team Experiments. 2019. Evading Windows Defender with 1 byte Challenge.
https://www.ired.team/offensive-security/defense-evasion/evading-windows-defender-using-classic-c-shellcode-launcher-with-1-byte-change

Elliot. 2020. Evading Antivirus with Better Meterpreter Payloads.
https://securityboulevard.com/2020/02/evading-antivirus-with-better-meterpreter-payloads/

Purpl3fox. 2021. Bypassing Defender on modern Windows 10 systems.
https://www.purpl3f0xsecur1ty.tech/2021/03/30/av_evasion.html

Cthivierge. 2018. How to disable NLA.
https://social.technet.microsoft.com/Forums/en-US/c07323c2-77fa-4eb4-91ed-7ba6fa23bd00/how-to-disable-nla?forum=winserversecurity

Appendix A1: Terms of Reference (TOR)
Temasek Polytechnic
School of Informatics & IT
Diploma in Cybersecurity and Digital Forensics

AY20/21 SEMESTER

MP Terms of Reference

Project Particulars

MP Supervisor	Mr. Shaun Tan
Project Title	Keyboard in Disguise
Student Matric Card Numbers	1900353B 1902298G 1901669J 1905357H
Student Names	Zachary Phoon Jun Ze Tan Jia Zheng Zheng Haowen Wang Zining

1. Introduction

Give a short introduction to the project. You may include information such as the purpose of the project, any relevant background information, the users and usage of the system, brief description of problems faced thereby leading to the need for this system, etc.

Purpose:
Obtaining access to the user's device using a malicious device disguised as a USB keyboard.

Background Info.:
Since most computers have unsecured USB ports, an attack can be carried out on unsuspected victims by disguising the attack method as an ordinary USB device.

Targeted Users: Users on Windows x64 devices.

Usage: Victim machine will be compromised by connecting the USB keyboard.

Brief Description:
A malicious device that is disguised as a keyboard, a payload will be delivered once the keyboard is connected into the USB port of a windows computer, allowing the attacker to view the contents of the victim machine and extract data.

2. Objectives of the Project

Describe the objectives that you want to achieve through this project. Objectives may be both technical and non-technical.

Objectives:
Implement an attack device that disguises itself as a keyboard, while making it as inconspicuous as possible.
Learning of circuitry for the keyboard.
Learning of configuring Arduino based device to execute the commands.

3. Scope of the Project

Developing internal circuitry for the keyboard to be used as an attacking tool.
Deliver malicious payload to the victim machine.
Develop malicious payload to compromise the victim machine.

4. Project Plan

Timeline			
Generate & Finalise Ideas	0%	19/4/21	25/4/21
Initial Research	0%	20/4/21	30/4/21
Making of Prototype	0%	1/5/21	21/5/21
Development of Software	0%	1/5/21	21/5/21
Testing of Prototype	0%	22/5/21	28/5/21
Bug Fixing and Finalising Sofware	0%	22/5/21	28/5/21
Finalising Prototype	0%	29/5/21	1/6/21
Final Testing	0%	2/6/21	6/6/21
Writing of Report	0%	7/6/21	13/6/21

5. Skills being assessed (to be completed by MP supervisor only)

To be advised by the supervisor.

Appendix A2: Project Plan

Timeline			
Generate & Finalise Ideas	0%	19/4/21	25/4/21
Initial Research	0%	20/4/21	30/4/21
Making of Prototype	0%	1/5/21	21/5/21
Development of Software	0%	1/5/21	21/5/21
Testing of Prototype	0%	22/5/21	28/5/21
Bug Fixing and Finalising Sofware	0%	22/5/21	28/5/21
Finalising Prototype	0%	29/5/21	1/6/21
Final Testing	0%	2/6/21	6/6/21
Writing of Report	0%	7/6/21	13/6/21

Appendix A3: Weekly Progress Report

School of Informatics & IT

Diploma in Cybersecurity & Digital Forensics

AY2021/2022 Semester

MP Weekly Project Progress Report

Project Title: Keyboard in Disguise	
Student Name: Zachary Phoon Jun Ze	**Adm No:** 1900353B
Supervisor Name: Mr. Shaun Tan	**Week No:** 1

Tasks Completed

Discussion of project ideas.

Planning of the project

Issue/Risk Tracking

Issue/Risk Name	Status

Meeting minutes with MP supervisor

We discussed on what possible project idea and we are suppose to decide what to do by the next meeting.

Weekly Self-Reflection *(no more than 150 words)*

Possible ideas maybe very costly, or requires more time to learn about the topic prior to start of project.

School of Informatics & IT

Diploma in Cybersecurity & Digital Forensics

AY2021/2022 Semester

MP Weekly Project Progress Report

Project Title: Keyboard in Disguise (KiD)	
Student Name: Zachary Phoon Jun Ze	**Adm No:** 1900353B
Supervisor Name: Mr. Shaun Tan	**Week No:** 2

Tasks Completed

Injecting a Script when thumbdrive is inserted

Issue/Risk Tracking

Issue/Risk Name	Status
Masking the Rubber Ducky	In Progress
Coding the programme to run the listener.	In Progress

Meeting minutes with MP supervisor

Decision on project Final. We require a item to mask the rubber ducky.

Will test out and get back on Thursday

Weekly Self-Reflection *(no more than 150 words)*

I learn about how usb drives work. Learning to run a listener using the run module as well as hiding the cmd shell from sight to prevent suspicion of user setting.

School of Informatics & IT

Diploma in Cybersecurity & Digital Forensics

AY2021/2022 Semester

MP Weekly Project Progress Report

Project Title: Keyboard in Disguise (KiD)	
Student Name: Zachary Phoon Jun Ze	**Adm No:** 1900353B
Supervisor Name: Mr. Shaun Tan	**Week No:** 3

Tasks Completed

Decision on project Final.

Research on Reverse Shell delivery.

Issue/Risk Tracking

Issue/Risk Name	Status
Anti-virus is blocking the web delivery.	

Meeting minutes with MP supervisor

Waiting for smaller bad usb and USB Hub to arrive. We agreed to begin coding and testing the script first before soldering it with the keyboard. We need to figure out delivery method to exploit the pc.

Weekly Self-Reflection *(no more than 150 words)*

Managed to learn newer ways to enter advance cmd and privilege mode.

I need to improve my knowledge on powershell scripting.

I need to have better knowlege of netstat to open TCP port for future attackes

School of Informatics & IT

Diploma in Cybersecurity & Digital Forensics

AY2021/2022 Semester

MP Weekly Project Progress Report

Project Title: Keyboard in Disguise (KiD)	
Student Name: Zachary Phoon Jun Ze	**Adm No:** 1900353B
Supervisor Name: Mr. Shaun Tan	**Week No:** 4

Tasks Completed

Able to access target machine via web delivery

Issue/Risk Tracking

Issue/Risk Name	Status
Bypass Windows Defender	On-going
Try to hide command inputs	On-going

Meeting minutes with MP supervisor

Dry test run without firewall, or any anti-virus was successful.

Supervisors has asked us to research on bypassing anti-virus as well as windows defender.

Weekly Self-Reflection *(no more than 150 words)*

knowledge on how the power shell delivery works.

I was happy that the project is going smoothly, I need to improve my

School of Informatics & IT

Diploma in Cybersecurity & Digital Forensics

AY2021/2022 Semester

MP Weekly Project Progress Report

Project Title: Keyboard in Disguise (KiD)	
Student Name: Zachary Phoon Jun Ze	**Adm No:** 1900353B
Supervisor Name: Mr. Shaun Tan	**Week No:** 5

Tasks Completed

Team has successfully hidden the cod command while executing the code

Issue/Risk Tracking

Issue/Risk Name	Status
Still unable to bypass anti-virus	On-going
Concealing of the bad USB in the keyboard	On-going

Meeting minutes with MP supervisor

The team met with supervisor in school to settle the soldering and testing on hardware level.

Failed in concealing due to hardware failure, decided to meet in the lab again and solve issues on Monday.

Weekly Self-Reflection *(no more than 150 words)*

There is no command way of turning o ff the antivirus. If we do want to avoid antivirus we need to find a way to write exceptions to the system.

School of Informatics & IT

Diploma in Cybersecurity & Digital Forensics

AY2021/2022 Semester

MP Weekly Project Progress Report

Project Title: Keyboard in Disguise (KiD)	
Student Name: Zachary Phoon Jun Ze	**Adm No:** 1900353B
Supervisor Name: Mr. Shaun Tan	**Week No:** 6

Tasks Completed

Soldering of the USB keyboard, USB hub and malicious USB together	Completed	
Concealing of the bad USB in the keyboard	Completed	

Issue/Risk Tracking

Issue/Risk Name	Status
unable to bypass anti-virus	On-going

Meeting minutes with MP supervisor

The team met with supervisor in school to settle the soldering and testing on hardware level. Successfully soldered the devices together. Looked into further developments of the project. Decided the main issue is the Antivirus and we need to solve it. We are to look into bypassing antivirus as well as prepare presentation slides

Weekly Self-Reflection *(no more than 150 words)*

Soldering was the toughest part as it had many trials and errors due to possible malfunction or chip development issues. Luckily, everything is working smoothly with minor slot issues.

School of Informatics & IT

Diploma in Cybersecurity & Digital Forensics

AY2021/2022 Semester

MP Weekly Project Progress Report

Project Title: Keyboard in Disguise (KiD)	
Student Name: Zachary Phoon Jun Ze	**Adm No:** 1900353B
Supervisor Name: Mr. Shaun Tan	**Week No:** 7

Tasks Completed

Preparation of the slides for presentation	completed	

Issue/Risk Tracking

Issue/Risk Name	Status
Bypassing of anti-virus	On-going

Meeting minutes with MP supervisor

We stated we are still bypassing the anti-virus. Supervisor wants to see if this attack can be prevented. Our solution is to find a way that allows only an approved list of usb devices to be connected to. Supervisor has assigned the defending task to Jia Zheng. The rest of the team will continue with finding a way to bypass the anti-virus and aid Jia Zheng if any help is needed.

Weekly Self-Reflection *(no more than 150 words)*

While researching on the bypass, we learned that windows defender detects on binary basis

Hence it will be hard to bypass, and we are looking into different ways of injecting the payload .

This made me learn more of windows 10 system and understanding how things are being defended.

School of Informatics & IT

Diploma in Cybersecurity & Digital Forensics

AY2021/2022 Semester

MP Weekly Project Progress Report

Project Title: Keyboard in Disguise (KiD)	
Student Name: Zachary Phoon Jun Ze	**Adm No:** 1900353B
Supervisor Name: Mr. Shaun Tan	**Week No:** 8

Tasks Completed

Gaining access to device remotely	Completed	

Issue/Risk Tracking

Issue/Risk Name	Status
Bypass Firewall	Ongoing

Meeting minutes with MP supervisor

Updated progress on the payload, presentation slides and defense. Supervisor wants us to research the remote procedure calls for full control of the device. More research of defense and possibility to run the payload on memory.

Weekly Self-Reflection *(no more than 150 words)*

Researching on the Remote Procedure Call brought light to certain windows defenses that I have not known was implemented before.

I learn powershell coding to turn off certain function without user knowledge.