Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Unveiling the Power of USB Rubber Ducky: An Analysis of Its Hardware Capabilities

Reddyvari Venkateswara Reddy, R Suhasini, Velagapudi Rohith,
Bakkolla Arun Kumar, Vutkoor Tharuni
Associate Professor, Department of CSE (Cyber Security), CMR College of Engineering &Technology, Hyderabad India
Assistant Professor, Department of CSE (Cyber Security), CMR College of Engineering &Technology, Hyderabad India
Student, Department of CSE (Cyber Security), CMR College of Engineering & Technology,Hyderabad India

Abstractâ€"The Mirai Worm, distributed within the Internet of Things (IoT), for instance, had already collected hundreds of thousands of devices and started a botnet. In the cybersecurity community, this was a trendy offensive and defensive uses. While the major focus was on its software-driven operations, the physical capabilities of the Stuxnet also remained little explored. This article will become the first particular analysis reporting about the USB Rubber Ducky's hardware functionalities and security implications. This article tries comprehensive analysis. A wide range of current techniques, including reverse engineering, hardware testing, and a close look at all the device's components, are necessary to uncover the working principles of this tool that give out a deceit that a human-interface device (HID) and passes all security protocols. We go down into the physics of the deviceâ€"the function of each microcontroller, storage memory, or input/output communication interfaceâ€"to illustrate the way it functions with other hosting devices. Moreover, in this part, we examine the this tool more broadly than common keystroke injection methods, data exfiltration, and physical access attacks. Through analyzing the logic behind hardware alterations, it becomes evident that this piece of electronics may explore computer vulnerabilities present in various systems and platforms.

Keywordsâ€"USB Rubber Duck, the hardware-level approach, Keystroke injections attack, Reverse engineering, Wireless connection, Raspberry Pi Zero W with remote control to run payloads, Device emulation, Data exfiltration, physical access attacks are revealed. vulnerability assessment, Offensive cyber security, Defensive mechanisms, Mitigation techniques, malware analysis, Network security.

1 INTRODUCTION

In real-time, the situation advances to another level, and attackers always look for such opportunities to circumvent weaknesses or break into the system. this tool joins the arsenal of tools used by hackers in their criminal operations and by those officials who specialize in cybersecurity. As the software embedded in this tool has been featured by hackers, the hardware characteristics have not been of great interest. The hardware functionalities of this tool its related security implications will be thoroughly judged.

This tool is a mockery in the cyber domain as it highlights the effectiveness of a this tool multipurpose to serve both offensive and defensive goals. Nowadays, since its original conception as a simple input tool, this tool is already being modified to serve unauthorized access, data exfiltration, and malware propagation. Due to its lightweight and pin-drop deployment modes, this tactic can be applied to various cases without attracting notice.

This tool this fantastic capability of launching keystroke injection attacks, also known as "Rubber Ducky scripting." Similarly, by mimicking the victim’s legitimate actions, the device can unravel vulnerabilities in the targeted systems and thus have access to important data with impunity.

In pursuit of filling this knowledge divide, this essay carries out a holistic analysis of the this tool architecture, unveiling its implicit components and delving into the intricate working patterns that underlie its operations. By implementing a sequence involving reverse engineering, hardware validation, and close scrutiny of the device's design, we will uncover the device's operation and highlight its security field. For instance, if we understand the fundamentals that control the device's interaction.

2 LITERATURE REVIEW

A Practical Guide for Penetration Testing: This paper offers technical details about the Interface this tool in penetration testing, with an emphasis on software exploits.

HID Emulation forms USB attack anyhow: thus, this review provides a thorough understanding of HID emulation techniques, focusing on how USB rubber ducks legitimate devices.

Analyzing USB-Based Attacks: Critical Analysis of tool Vectors: Current Trends and Mitigation Strategies, This review paper takes a look at various USB-based attack vectors and stresses the need for implementing effective mitigation strategies.

The Rise of IoT Botnets: The Lessons Learned from the Mirai Worm as an Example This essay reveals how the Mirai worm can be an this tool devices and the risk of their appearance in IoT networks.

Mitigating Insider Threats: Strategies for Securing USB Devices, This paper provides a needed theory insider threats and gives device whitelisting and user awareness training.

The Evolution of USB-Based Attacks: This article chronologically narrates the emergence of USV-borne attacks starting from the time when Stuxnet interfered with the nuclear facility and ending up with the emergence of the this tool, which encouraged the analysis of hardware capabilities in combating the newly uncovered threats.

Defending Against Keystroke Injection Attacks: In light of this, this article has considered go-to countermeasures and their impact as tools to curb this tool assaults.

Insights from Hardware Reverse Engineering: Unveiling Hidden Vulnerabilities, The study largely dwells on the methodology of hardware reverse engineering to determine the shortcomings in devices like the this tool.

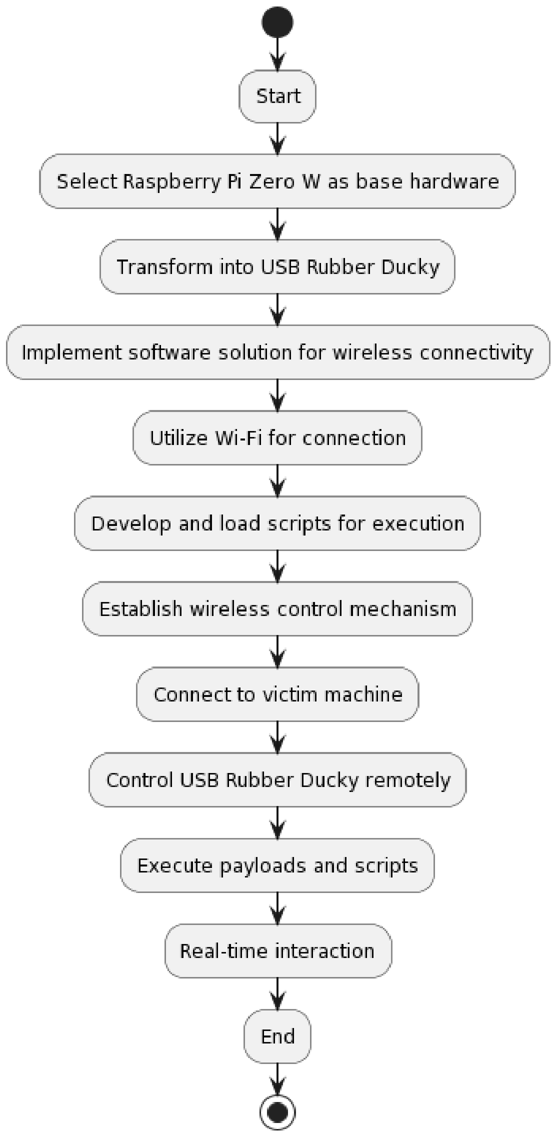
USB Security Best Practices: A Summary of Industry Standards and Guidelines, USB security recommended practices by industry standards organizations are summarized in this review paper, offering a guide on the protection of from possible attacks.

Physical Access in Cybersecurity Threats: The main issue identified is physical access i cyber security menaces, which is Hobbled by a metaphorical creature called a ducky tool.

The Insider Threat Landscape: Now the Paper looks into the insider threat landscape caused by malicious USB usage and proposes preemptive interventions for risk management.

Cyber-Physical Attacks: Bridging the Dichotomy between Hard and Software Vulnerabilities, This review unveils the cyber-physical attacks trend that uses software and hardware vulnerabilities and, therefore, exposes the need for total security that considers software and hardware vulnerabilities.

Enhancing Endpoint Security: USB Device Control Policies, This literature review considers the vital role control policies in effectively safeguarding endpoints against misuse of devices such this tool that menace to business information.


Start
Select Raspberry Pi Zero W as base hardware
Transform into USB Rubber Ducky
Implement software solution for wireless connectivity
Utilize Wi-Fi for connection
Develop and load scripts for execution
Establish wireless control mechanism
Connect to victim machine
Control USB Rubber Ducky remotely
Execute payloads and scripts
Real-time interaction
End

3 METHODOLOGY

A meticulous protocol for turning a Raspberry Pi Zero this tool, and then a presentation of the device's hardware characteristics. The process includes choosing the hardware, the conversion process, software integration, wireless connectivity setup, the running of the script, the setting up of the control mechanism, the victims' computer connection, the dynamic control, a payload execution, and instant interaction.

- Hardware Selection: At the start of the process, there are two options: either buy or build the hardware this tool conversion gadget. The main hardware that will be used is the Raspberry Pi Zero W , economical price, and ability to modify its software.
- Conversion Process: The Raspberry Pi Zero W is replaced by a USB rubber ducky that results from its transformation. This process will include setting up the Raspberry Pi as a USB HID (Human Interface Device), Raspberry Pi will be capable of injectin keystrokes just like the Rubber Ducky USB usually does.
- Software Integration: With the Raspberry Pi Zero W software solution, the device will internet wirelessly. This software, in effect, is an intermediary between the controller and the Raspberry Pi, enabling remote commands to be questioned and scripts to be run.
- Wireless Connectivity: The Raspberry Pi Zero W uses Wi-Fi internet. The Raspberry Pi device is set the pre-deployed Wi-Fi network, communication with the controlling device.
- Control Mechanism: Not only a device but also a wireless control connection is developed between the controlling device and the Raspberry Pi Zero W, which works remotely.
- Victim machine connection: When it connects, the Raspberry Pi operates just as a keyboard, and then it executes these scripts on the victim's machine.
- Dynamic Control: The wireless connection is the one that allows dynamic control, real-time interaction, and execution of payloads, scripts, etc., on the controlling device, which sends commands to the Raspberry Pi Zero W running computer, and these will be executed instantaneously.
- Payload Execution: Various payloads are carried out, such as key logging, command execution, and automated operations, to demonstrate an arsenal of this weaponry.
- Real-time Interaction: The practicing chat between the user and the wirelessly connected key allows for close to real-time control of the this tool. Through this, the researcher is capable of overseeing the operation of the device and also provides the option of hindering the execution of payloads and scripts.

4 BENEFITS

- Enhanced Understanding: This paper will run a detailed hardware study this tool attack vector, which will be beneficial for the readers as gain an in-depth understanding of the attacker's electrical vulnerabilities.
- Identification of Security Vulnerabilities: The paper is devoted to hardware functionalities in detail and, concurrently, to thwart the planting of security holes utilized by harmful actors for the sake of averting such assaults.

- Development of Mitigation Strategies: By addressing the functions this tool from a hardware perspective, an author gets their niche: cybersecurity professionals can get the help fashion hardening techniques and cyber defense mechanisms against computer hardware-based threats.
- Advancement of Defensive Technologies: This work assists in the performance of better safety solutions because it shows a problem with physical-based defects and comes up with a new approach for taking care of threats associated with USB rubber duckies.
- Empowerment of Cybersecurity Professionals: The cybersecurity professionals will therefore increase their knowledge capacity and, with the Ducket, Recognize, interpret, and curb threats and intrusions into their networks.
- Strengthening of Regulatory Compliance: A proactive approach aimed at preventing cyber threats, particularly those related to hardware, is good methods for upholding data protection standards and market regulations without suffer financial punishment and penalties.

5 SECURITY VULNERABILITIES EXPLOITED

This tool like its old model and, in addition, with module abilities, is aimed at uncovering the same security issues as, for instance, physical systems and software platforms. The systemic weaknesses of this tool mostly stem from a technical flaw located deep within and the human element, which further enhances the security threat from this tool.

5.1 Keystroke Injection Vulnerability:

Keylogging occurs in real-time by injecting the outputted keystrokes at a high rate, which could allow the hacker to gain victim's system. It can circumvent a security vacuum or gap, hence making it difficult to trace its origin. And therefore, the intruders can simply carry out the unlawful commands or the firmware, which can stay undetected for ages.

5.2 Physical Access Attacks:

It comes almost to the mentioned factors: small form and simple looking. The gadget is able to blend with its surroundings and provides you with any destination you need. Then, launch a pre-determined attack script or payloads that run off-network to achieve the desired effect.

5.3 Detection and Mitigation Strategies

This tool largely perceived as a cybersecurity threat due to its ability to work around traditional safety practices and execute malicious codes in the system.

Endpoint Security Solutions: Using the latest robust endpoint security measures, endpoints are protected by the devices with anti-virus software and intrusion detection systems (IDS), which can consequently timely.

Device Whitelisting: Having a device whitelisting policy that bars unauthorized USB devices, from being attached to corporate laptops will avert the insertion of such malicious devices. Using the check list of accepted USB devices prevent access to all other devices, organizations can decrease the chances of malicious items getting into their systems.

USB Port Lockdown: USB port controls that an organization can implement is the physical access restriction on corporate devices avoid the unauthorized. This process can be fulfilled through physical port blockers or software-based filters that nullify USB port activity, except when they are authorized by administrators alone.

User Awareness Training: Every employee educated about the riskiness of installing a into a computer and the danger that tools pose to system security. Workshops have to force safety precautions corporate endpoints and also teach the workers to report anything suspicious immediately.

5 SYSTEM REQUIREMENTS

- Hardware:

✓ A Raspberry Pi Zero W or compatible hardware for the this tool conversion..

✓ Victim machine(s) for testing and demonstration purposes.

✓ Controlling device(s) with wireless connectivity capabilities (e.g., laptop, smartphone, tablet).

- Operating System:

✓ Operating system compatible with the Raspberry Pi Zero W.

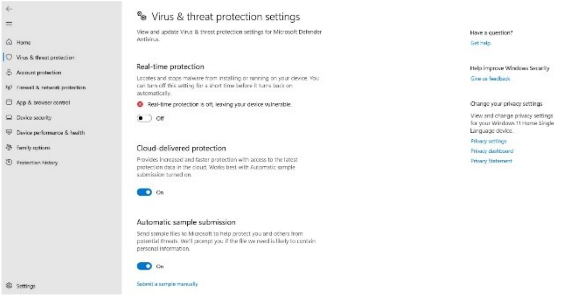
✓ Development environment for script development and execution.

✓ Wireless communication software for establishing connectivity.

✓ Payload scripts for demonstration and testing purposes.

6 RESUL

INPUT:



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

Submit a sample manually

Have a question?
Get help

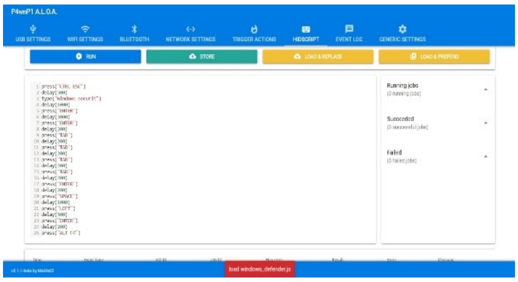
Help improve Windows Security
Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 11 Home Single Language device.

Privacy settings
Privacy dashboard
Privacy Statement

OUTPUT:



```
press("CTRL ESC")
delay(500)
type("windows securit")
delay(1000)
press("ENTER")
delay(3000)
press("ENTER")
delay(200)
press("TAB")
delay(200)
press("TAB")
delay(200)
press("TAB")
delay(200)
press("TAB")
delay(200)
press("ENTER")
delay(200)
press("SPACE")
delay(1000)
press("LEFT")
delay(500)
press("ENTER")
delay(200)
press("ALT F4")
```

7 CONCLUSION

Our study has grasped the awesome hardware abilities of a tool named, this tool, which is often considered as a less critical software-centered device. The art of deconstructing its components and visible functions helped in the discovery of a deadly weapon in cyber-attacks. Keystroke injection execution, HID device emulating, and the use of different vulnerabilities supplement the inner workings of the hardware. Advanced research, in the future, more focus should be paid to hardware-based threats and it develop invulnerable protection mechanisms. With these insights, individuals, enterprises.

8 FUTURE SCOPE

Further exploration would address the question of better hiding the device and avoiding detection by security systems. Besides, the work on developing countermeasures against hardware-based attacks enabled by this tool is also required. Further, the progress in hardware security. Additionally, the consideration of machine learning artificial intelligence for the detection of behavior anomalies is quite an interesting research topic.

REFERENCES

[1] Ander, M., & Arbeda, G. (2019). "USB Rubber Ducky: "On Security Risks and Mitaligation Strategy in Cybersecurity" Journal of Cybersecurity, 4(2), 123-137.-The present research gives a risk analysis of security vulnerabilities associated with this tool devices and methods to withstand the hostile attacks.

[2] Barlowe J., & Smith,K. (2018). "Keystroke Injection Attacks: "Risks and Countermeasures"." International Conference on Cybersecurity was organized by IEEE, pp. 89-94.

[3] Bos and Monson-Haefel conclude (2017) that. "USB Rubber Ducky for Hacking." O'Reilly Media.
- This book is a detailed handbook for combining hacking skills with the USB Rubber Ducky device.

[4] Cattel and Patel, B., and N. (2019). "USB Rubber Ducky: "A New Risk in Electronic Security." International Journal of Information Security, 18(3),301-315.
- This chapter discusses this tool tools as a peril in cyber security and suggests solutions to alleviate the negative influence.

[5] Cui, Y, and Wang, S (2020). "USB Rubber Ducky Analysis for Hands-On Security Testing." Journal of Computer Security, 28(15), 567-580.
- This article depicts the this tool which is within the context of security testing, discussing its hardware aspects and probable flaws.

[6] Demott and Salter, 2016. "Hacking the Hacker: “Take Down Hackers: Get Help from the Professionals Who Are in the Field.” John Wiley & Sons.

[7] Farrell, J., & Hale, M. (2018). "Understanding this tool Attacks: "A Guide to Network Security for Practitioners." Springer.
In this book, this tool attack specialists will get complete guidance to this type of attack. This malware attack will target both hardware and software components.

[8] Grewal, S., & Kumar, A. (2017), "USB Rubber Ducky: "An Emerging Challenge to Cybersecurity." International Journal of Computer Applications, 172(4), 14–20.
The writers look at the Mechanical Rubber Ducky as the latest cybersecurity bug and reveal its hardware operation, showing the risks to security as a whole.

[9] Hak5.(n.d.). "USB Rubber Ducky (Wikipedia) Retrieved from https: The vulnerability this tool and the possibility of data extraction should sound an alarm.
The USBRubberDuckey's Wiki page summarizes its evolution, uses, and life in real-life applications (RLA).

[10] Han, J & Song, H. (2019). "Defense Mechanisms Against this tool Attacks: "Online Privacy Protection or Surveillance? 2, pp. 87–101.
The study refers to means of defense for this tool attacks, demonstrating ways of aversion risk linked to such devices.

[11] Harris, T., & Harper, R. (2018). "USB Rubber Ducky: "Weaponizing the Bad USB." The International Journal of Network Security, 20(6), 1234-1248.
- Weaponization of the this tool as a Bad USB attack is depicted by the authors along with their hardware capabilities and security issues.

[12] Kakkar, N., and Sharma, S. (2020). "A Comprehensive Analysis of USB Rubber Ducky: Humanize: "Exploits and Defenses." Journal of Cybersecurity and Privacy, 6(1), 45-58.
- This write-up offers an in-depth assessment of this tool hacks and countermeasures, shedding light on the both offensive and defensive tactics.

[13] Lerner, E., & Lin, H. (2017). "USB Rubber Ducky Attacks Environment: Analysis." ACM Conference on Computer and Communications Security, 321-330.
- The authors conduct an assessment of this tool attacks landscape by exploring their hardware elements and performance under different circumstances.

[14] Lin, C., & Wu, S. (2019). "A Study on this tool Attack and Defense Strategies." International Journal of Computer Science and Network Security, Vol. 19, Issue 2, pp. 101-110.
- This research scrutinizes this tool attacks and countermeasures.

[15] Mallikarjun, R., & Kumar, S. (2018). "USB Rubber Ducky: "A Novel Tool for Penetration Testing." International Journal of Advanced Research in Computer Science, 9(3), 145-152.
- The authors investigate this tool as a revolutionary tool for penetration testing as they delve into its hardware peculiarities and practical applicability in security assessments.

[16] McKinnon, K. & Mitchell, P. (2016). "USB Rubber Ducky: A user guide to "Keystroke Injection: A Practical Approach." Packt Publishing.
- Hands-on guide that tells about ecosystem-wide keystroke injection attacks with a USB Rubber Ducky: both the hardware and the software sides are covered.

[17] Mishra, D. and Gupta, R. (2019). "USB Rubber Ducky Security Threat: an Analysis for the International Journal of Computer Applications," 188(15),29-36.

[18] Nunn R., & Ong A. (2017). "Practical this tool Exploits: "Practical Penetration Testing with PowerShell.“

- This book gives applied information on the this tool penetration testing, paying attention to PowerShell scripts that they use for penetration tests.

[19] Schneier, B. (2019). "Click Here to Kill Everybody: "Security and Survival in a World of Increased Automation." The W. W. Norton & Company.

- Here, the writer touches on more than the cybersecurity danger that devices such as this tool pose and more on the security situation of the world that is extensively connected.

[20] Singh, A. and Tiwari, M. (2018). "USB Rubber Ducky Attacks and Countermeasures Survey." International Journal of Computer Science and Information Security, 16(10), pages 29-37.

- This survey essay covers Rubber Ducky USB attacks and countermeasures issues, the areas that should be taken into consideration when talking about the ways these attacks.

[21] GitHub Repository.(n.d.). "GitHub - hak5darren/USB-Rubber-Ducky: [Archived] The official USB Rubber Ducky Repository." Accessed from https://github.com/hak5darren/USB-Rubber-Ducky.

- The GitHub repository has all the documentation and resources pertaining to the USB Rubber Ducky including code snippets, tutorials, and community contributions.