RESEARCH ARTICLE OPEN ACCESS

Unveiling the Positive Potential of the USB Rubber Ducky

Vishnu Nair*, Manisha Singh**

*(Msc.IT, Mumbai University/Keraleeya Samajam dombivali's model collegeCollege, Dombivali
Email: vjnair2001@gmail.com)

** *(Msc.IT, Mumbai University/Keraleeya Samajam dombivali's model collegeCollege, Dombivali
Email: arya10112001@gmail.com)

--*************************----------------------------------

Abstract:

The USB Rubber Ducky, often associated with malicious hacking tactics, can surprisingly be wielded for good. This paper delves into the capabilities of this versatile tool, exploring its potential applications in security awareness training, penetration testing, automation, and accessibility. By shedding light on its ethical uses, we aim to foster a nuanced understanding of the Rubber Ducky, highlighting its potential to contribute positively to the digital landscape.

Keywords **— USB Rubber Ducky, Cyber Security,Malicious Files.**

--*************************----------------------------------

I. INTRODUCTION

The USB Rubber Ducky, resembling a harmless duck-shaped flash drive, holds a complex duality. Originally designed for ethical penetration testing, it gained notoriety for its malicious exploitation by hackers. Its ability to mimic keyboard strokes and automate tasks on connected systems raises concerns about data breaches and system manipulation. However, dismissing the Rubber Ducky solely as a digital weapon would be a missed opportunity. This paper proposes that within its controversial shell lies a potential for significant good, waiting to be unleasheD

II. POWER IN DISGUISE:

The Rubber Ducky utilizes Ducky Script, a user-friendly language allowing users to script keystrokes,mouse movements, and system commands. This scripting capability unlocks possibilities beyond malicious intent. Consider these scenarios:

III. SECURITY AWARENESS TRAINING:

Simulate phishing attacks on training computers, deploying fake websites or emails with embedded Ducky scripts that trigger alerts or display warnings.

Showcase common social engineering techniques like keylogging or malware injection throughscripted scenarios.

Design interactive training sessions where participants have to "defuse" Rubber Ducky attacks usingsecurity procedures.

Automate data exfiltration from vulnerable systems using scripts to copy sensitive files or uploadthem to designated servers.

Perform privilege escalation by triggering specific exploit sequences through Ducky scripts, testingsystem defenses.

Generate simulated denial-of-service attacks by flooding target systems with scripted commands.

IV. Automation of Repetitive Tasks:

Fill lengthy online forms or registration pages automatically using Ducky scripts, saving time and effort.

Schedule daily tasks like system backups or software updates through automated Ducky scripts. Simplify routine office tasks like copying and pasting data between applications.

V. Accessibility Solutions:

Create custom keyboard shortcuts for individuals with motor disabilities using Ducky scripts,triggering complex actions with single keystrokes.

Automate repetitive tasks for visually impaired users, like reading emails or navigating web pages.

Develop accessible tools for individuals with cognitive disabilities, providing prompts and remindersthrough scripted sequences.

VI. Additional Considerations:

Security hardening: Implement measures to prevent unauthorized Ducky script execution oncomputers, such as requiring password authentication or restricting USB device access.

Open-source scripts and collaboration: Promote responsible development and sharing of Duckyscripts through open-source repositories with clear ethical guidelines.

Public awareness and education: Increase public awareness about the potential for both good and baduses of the Rubber Ducky, fostering ethical considerations and responsible use.

VII. CONCLUSIONS

The USB Rubber Ducky, like any tool, possesses the potential for both good and bad. By acknowledging its strengths and limitations, and promoting responsible usage through education and regulatory frameworks, we can unlock its power to enhance security, improve efficiency, and foster inclusivity in the digital world. As we move forward, let us embrace the Rubber Ducky not as a villain, but as an unexpected hero waiting to write its own positive story in the digital age.

REFERENCES

[1] OWASP Juice Shop: https://owasp.org/www-project-juice-shop/

[2] National Initiative for Cybersecurity Careers & Studies https://niccs.cisa.gov/ W3C Web Accessibility Initiative (WAI): https://www.w3.org/WAI/

[3] SANS Institute Penetration Testing with Kali Linux: https://www.sans.edu/cyber-security- programs/graduate-certificate-penetration-testing/

[4] Penetration Testing Execution Standard (PTES): http://www.pentest-standard.org/index.php/Main_Page

[5] Automation with Python and Robot Framework: https://docs.robotframework.org/docs/getting_started/rpa