Feasibility and Deployment of Bad USB

Stella Vouteva, System and Network Engineering Master research project

University of Amsterdam

Introduction

- Main elements of security
- Social Engineering
- Bad USB

Goals

- Run attack(s) in less than 10 seconds
- Attacks should work on user without admin rights
- Download an executable that can bypass Windows UAC and AV programs and run it
- Obtain access to the compromised device from a Kali Linux machine
- Installation of a root certificate on the Windows machine
- Add a backdoor

Tools

- Arduino
- Victim #1: Lenovo Z50-70 laptop with Windows 8.1
- Victim #2: Windows 7 Ultimate VM
- Kali Linux machine

Endpoint security circumvention

- Time benefits
- Confidentiality
- Integrity
- Availability

Feasibility requirements

- 'Typed' without human or mouse intervention
- Timing
- Assumptions
- Security threat considerations

Logon bypass on locked computers

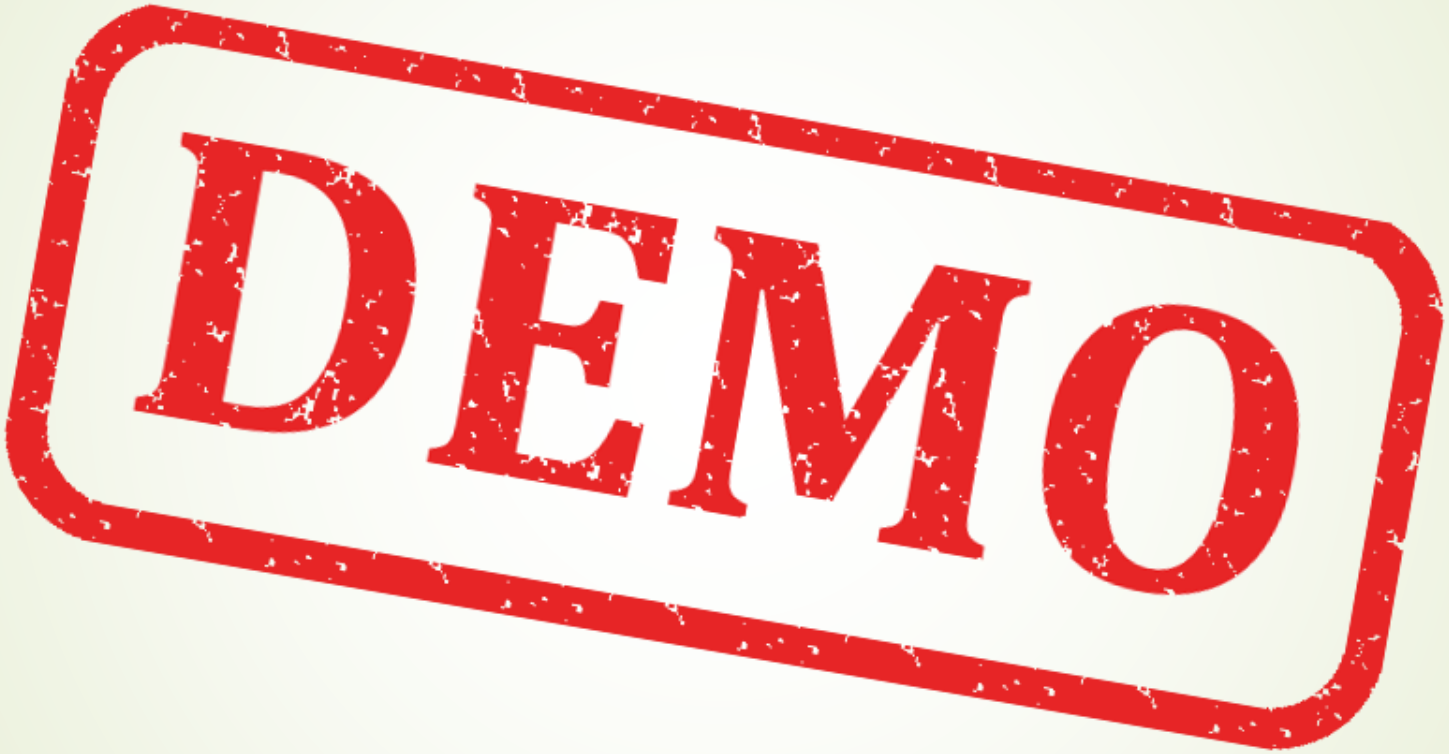
- Kon Boot
- Recovery disk/ Advanced options
- Booting from another OS
- Feasibility

Unlocked computers exploitation

- File Download
  - FTP, HTTP, SFTP?
- Bypass UAC and AV
  - Veil-Evasion
- Remote access
  - MSFVenom
  - Payloads
- Privilege escalation
- MITM
  - mitmproxy
- Keyloggers
- Persistent backdoor
- Feasibility

Scenario

- Preparation
  - Create an .exe file using Veil-Evasion
    - AES encryption
    - MSFVenom
    - Reverse TCP
  - Allow SSH to the Kali machine
- Execution on the victim computer
  - Plug the Arduino
- Kali Linux machine attacks
  - Persistent backdoor
  - Bypass UAC
  - Keylogger
  - Migrate process


DEMO

Conclusion

- Feasible for unlocked computers (with limitations)
- Unfeasible for bypassing login screen

Questions