Attacking a medical lab with a rootkit to raise awareness about cybersecurity

Milestone 5 / Final presentation

Teacher / Client : Jamal EL HACHEM

Group 6 : Maximilien CHAUX, Madigan LEBRETON, Bertrand MARTIN, Alan PICARD

École d'ingénieurs
ensibs
Université Bretagne Sud

Plan

- The problem
- Our scenario
- Our toolset
- The attack cycle : the Cyber Kill Chain & Mitre Att&ck framework
- Our awareness package
- Feedback

The problem

The context :

- Poor cybersecurity practices
- Lack of awareness
- Lack of real demonstration

The problem :

- How to efficiently raise awareness of cybersecurity risks towards companies ?

Our solution :

- Improve awareness of cybersecurity risks through the demonstration of a stealthy attack using a rootkit

The scenario : who are we

- A company that offers pentesting services and does security awareness
- “HealthSIBS” just bought a local medical lab “Vannalyz” , we are contracted to attack the Vannalyz network.

The scenario : why a rootkit

- Ransomware attacks make the front page but rootkit attacks do happen
- Poor knowledge about rootkits among sysadmin relatively to other malware
- The technical challenge motivated us + we gained technical knowledge about Windows Internals and kernel drivers

The scenario : sticking to reality

- Real attack targeting a medical lab in Brittany in 2021
- We conducted an interview with a lab technician
- Real rootkits have been found using the same techniques we've been using

Our toolset

Our technical solution is composed of four different packages, each of them comprised of several components.

Delivery package

Components :
Spearphising
Script Rubber Ducky

Exploitation package

Composants :
Userland app
Userland librairies

Rootkit package

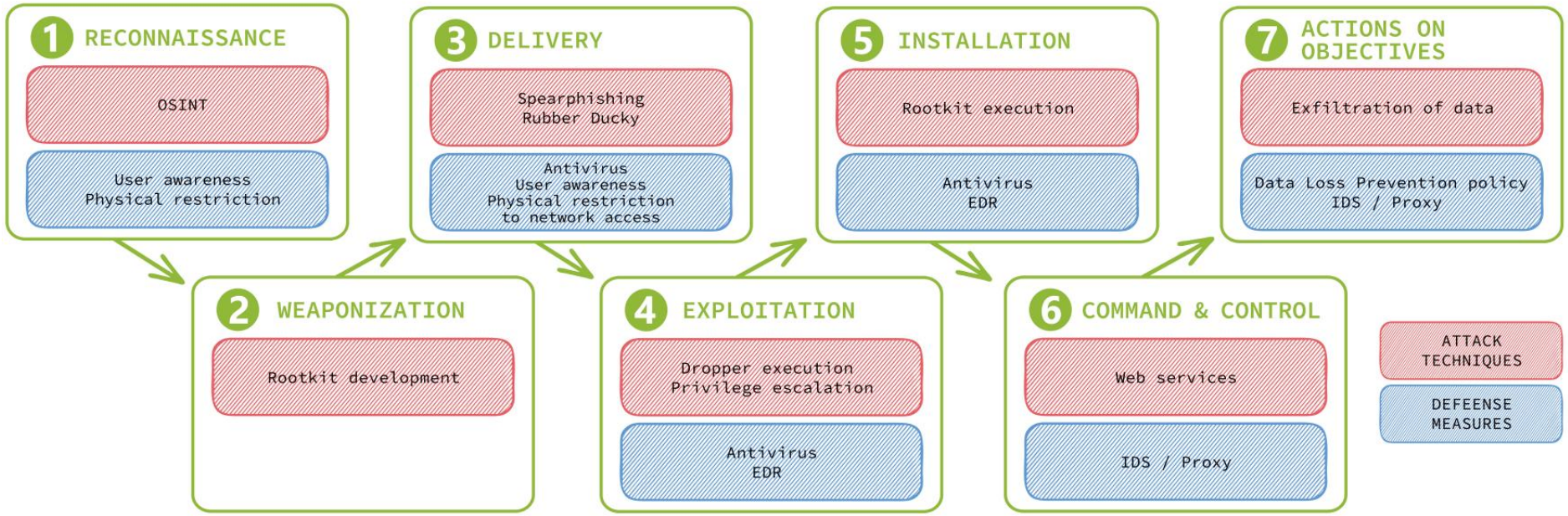
Components :
Kernel driver
Userland app

Command & Control Package

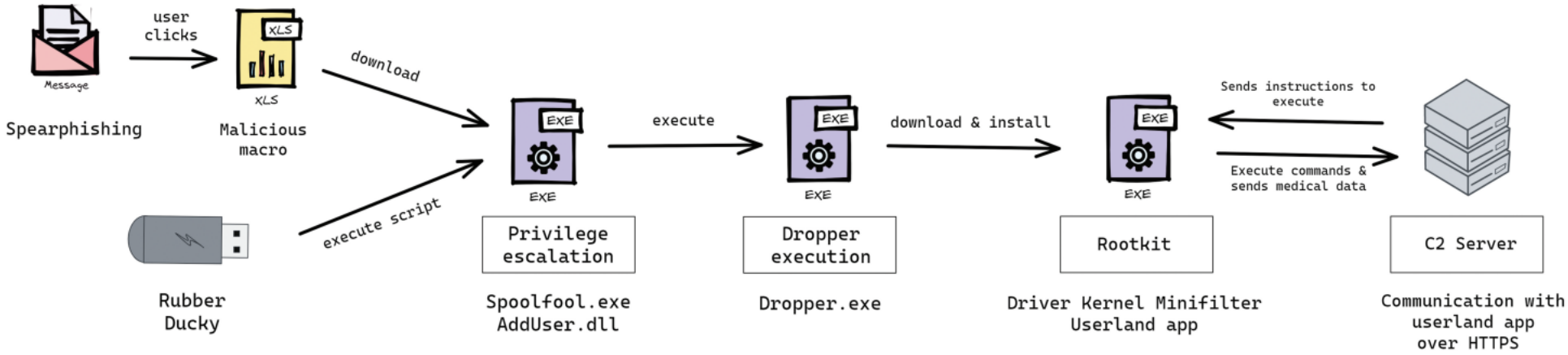
Components :
HTTPS server app

The Cyber Kill Chain

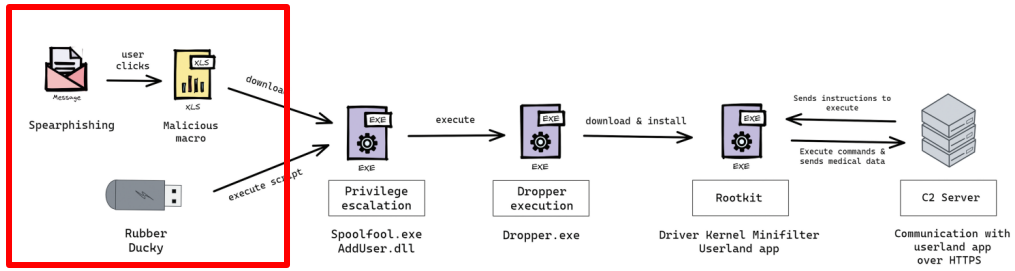
We are using the Cyber Kill Chain – a framework developed by Lockheed Martin - to visualize the different stages of the attack, which allows us to present both the attack techniques and the best way to defend an organization against a rootkit at each stage of the attack.



The attack cycle



Delivery package



Spearphishing

Malicious Macro into excel file

1. Download zipped dropper
2. Unzip dropper
3. Install dropper

Downloading exe was considered malicious

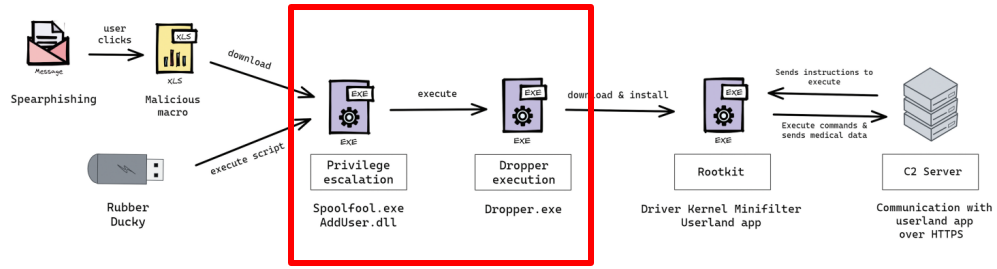
Rubber Ducky

Type of usb key that registers as keyboard

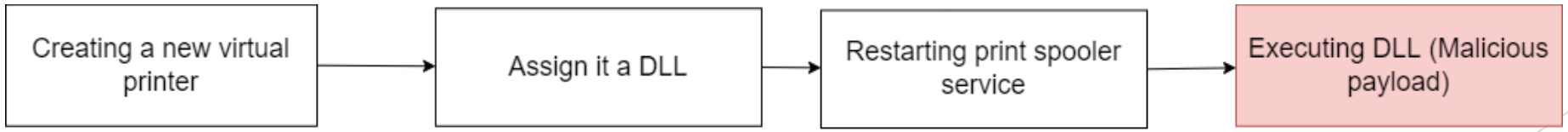
1. Plug the rubber ducky into usb port
2. Rubber ducky types commands
3. Dropper installed

Physical access needed
No connection to C2 necessary

Exploitation Package

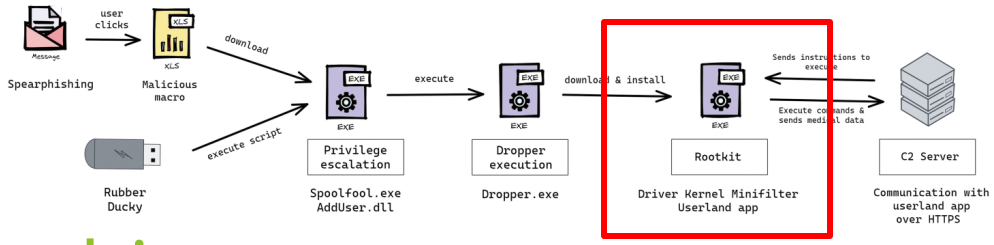


- We used SpoolFool vulnerability
- Very recent (February 2022)
- In line with the famous PrintNightmare vulnerability
- Used to gained administrator privileges

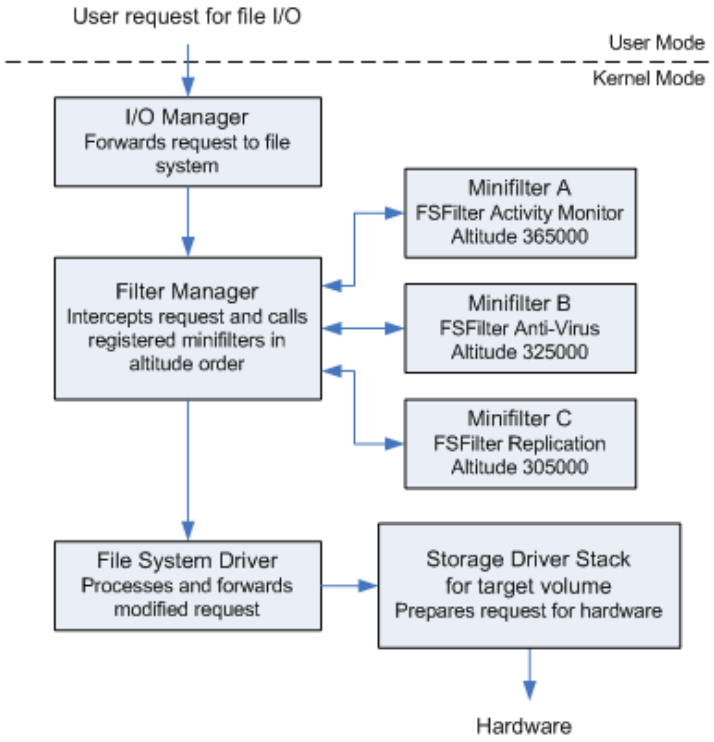


Rootkit Package

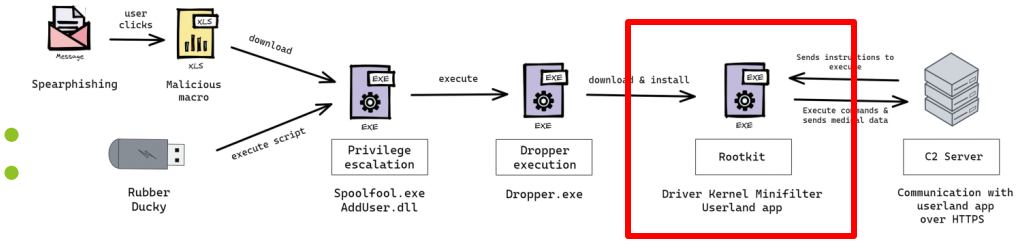
Our kernel MiniFilter driver

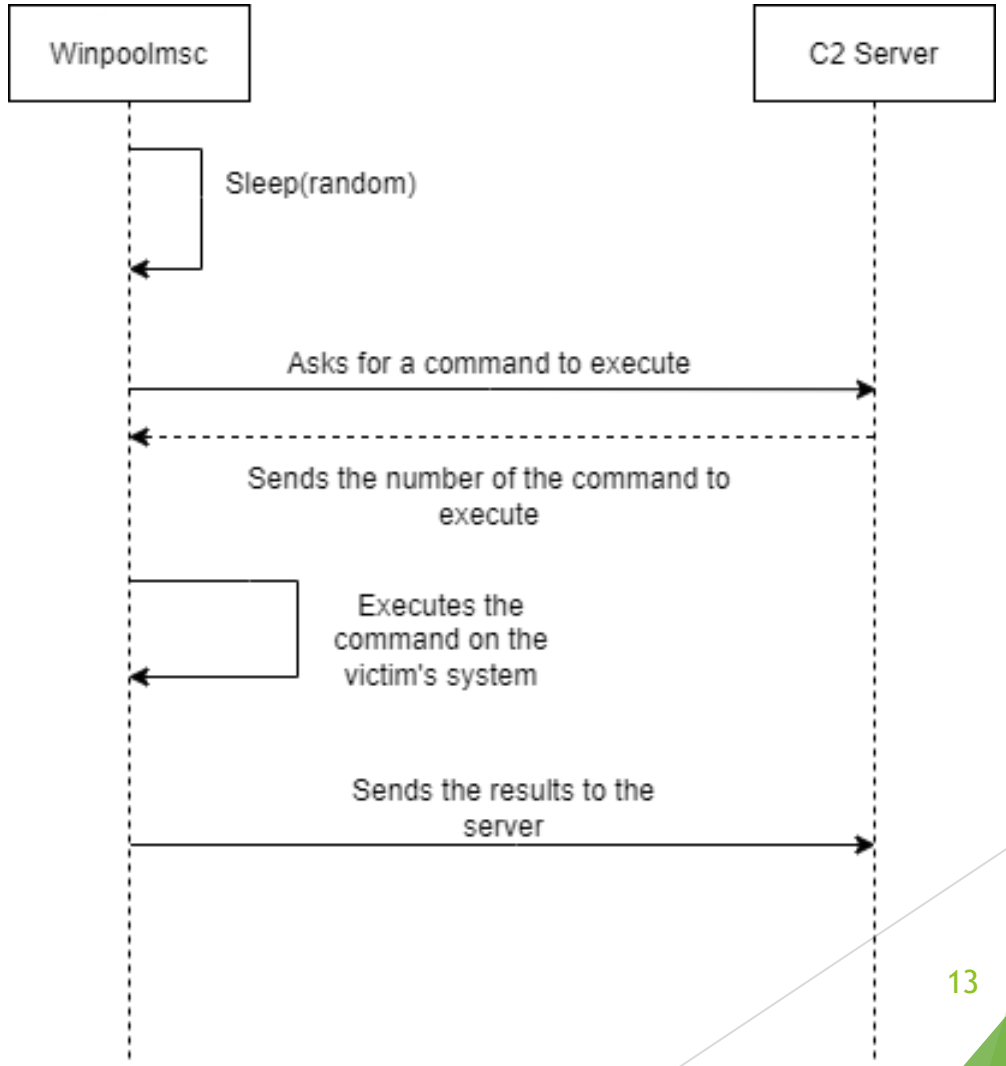


Used for hiding files

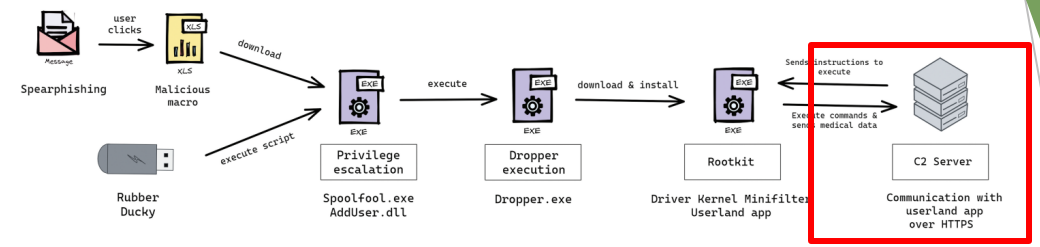


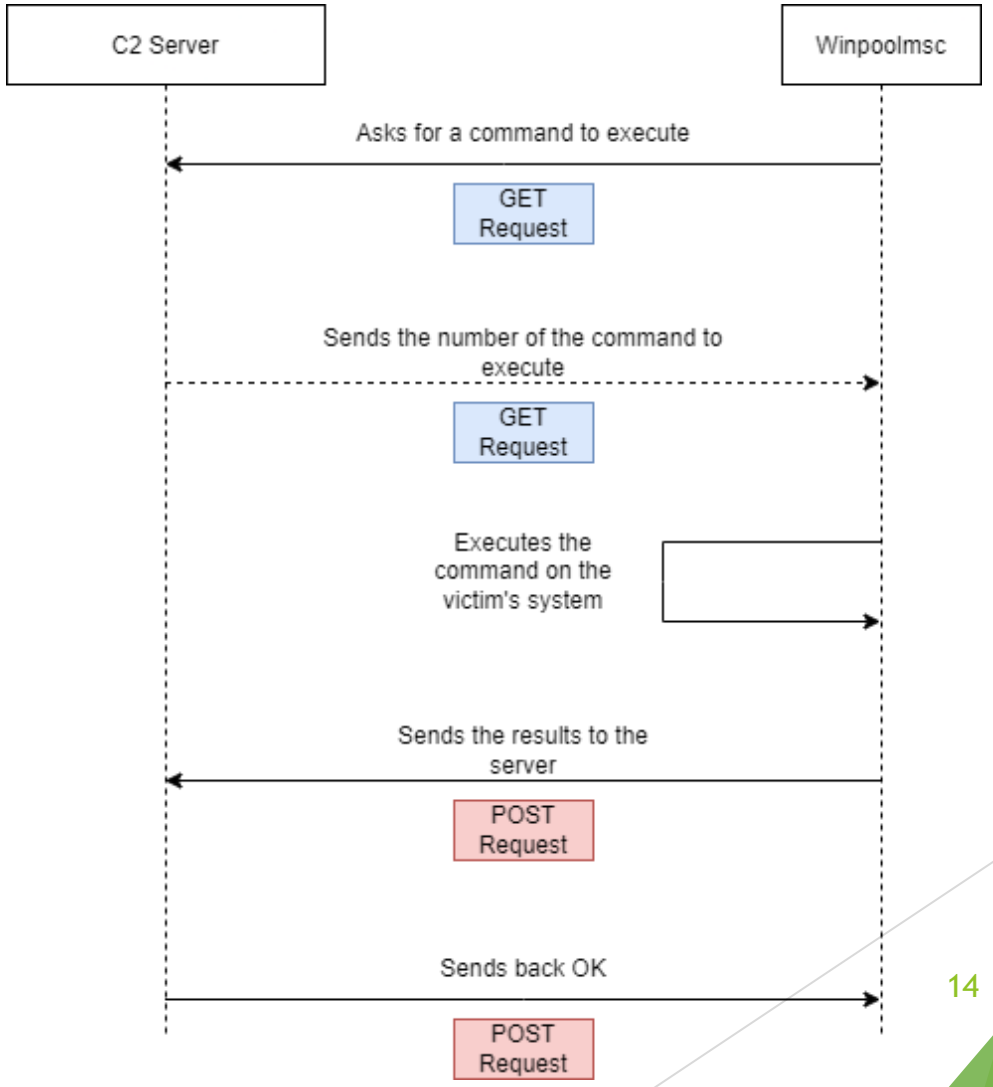
Our Userland app : Winpoolmsc





And its parallel : The Command & Control server





Demonstration

Justification

Choice	Justification	Existing
Communication via HTTPS	Blend in with legitimate traffic	Common practice among malwares
MiniFilter	Used to manipulate files at the kernel level	Microsoft Documentation (msdn)
Privilege escalation	Use of a recent vulnerability within Windows	This vulnerability has been exploited by several malwares
Cyber Kill Chain	Brings a higher-level perspective than ATT&CK Framework	Used by malware analysts to categorize malwares and present defense measures

Our awareness package

2 documents :
- 1 poster about kernel-mode rootkits
- 1 technical note about rootkits and defense measures

Defense measures	Type	Defense limitations
User awareness	Human	- Human factor (mistakes, curiosity, blackmail, corruption...)
Microsoft Driver Signature Enforcement	Technical	- Microsoft mistakes (Netfilter malware example) - BYOVKD (RobinHood malware example, using Gigabyte driver)
Antivirus Endpoint Detection Response	Technical	- Only user level is supervised (not kernel level) - EDR products detect but do not block malicious actions
Network security (Proxy, IDS/IPS, Sandbox for downloaded files...)	Technical	- Amount of traffic - Use already known patterns and malicious code

Feedback

Strengths	Weaknesses
- Good work organization - Passionate about the subject	- State of the art
Opportunities	**Threats**
- Project presentation at DGA MI	- Code publication on GitHub ? - Amount of work

Thank you