Maintaining Access: Executing Applications

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

Make it so, number one

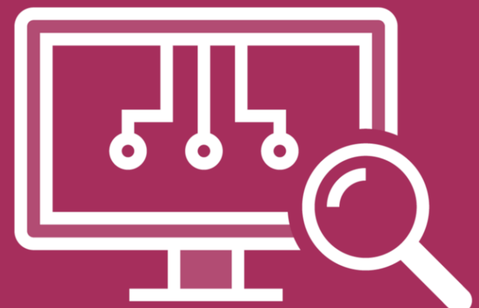
Jean-Luc Picard

Goals

Overall, We're Here to:

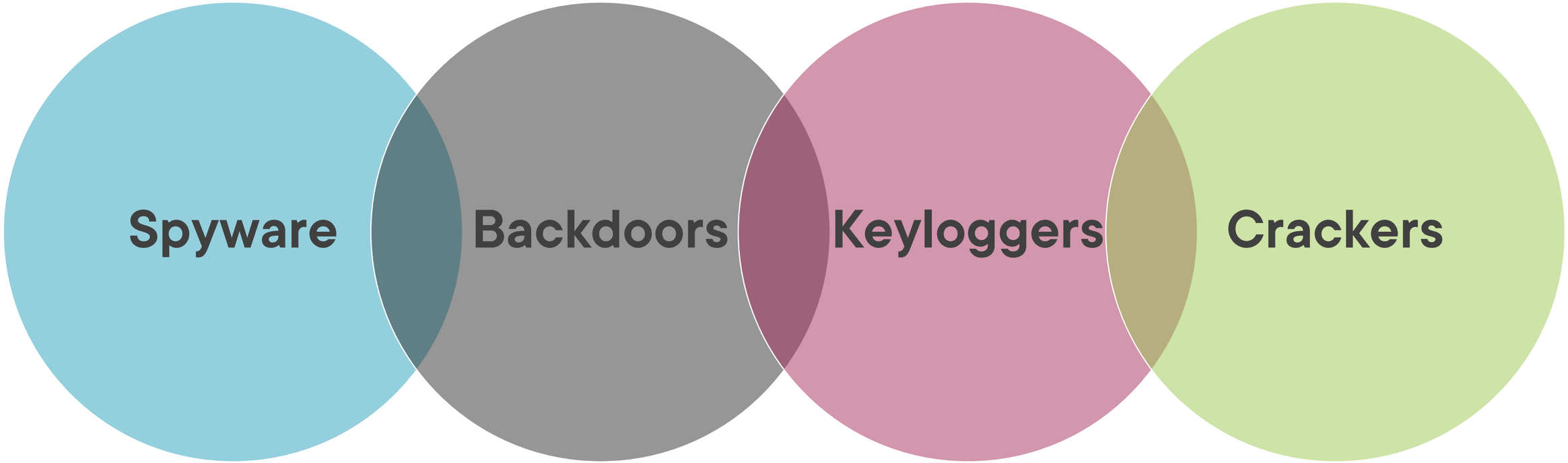
Make sure we can get back in

See what's going on here



Detect more information

How to Execute Applications



Too legit, to legit to quit

MC Hammer

Remote Code Execution

Remote Code Execution Technique

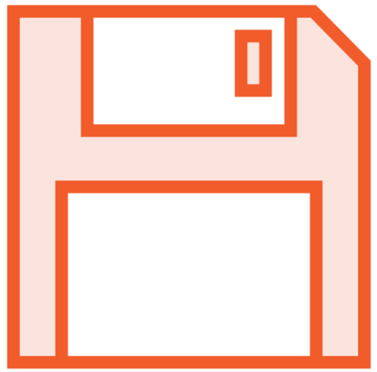
- **Exploitation for client execution**
- **Scheduled tasks**
- **Service execution**
- **Windows Management Instrumentation (WMI)**
- **Windows Remote Management (WinRM)**

Tools for Fun

- **Pupy**
- **Remote Exec**
- **PDQ Deploy**
- **Dameware Remote Support**
- **PsExec**

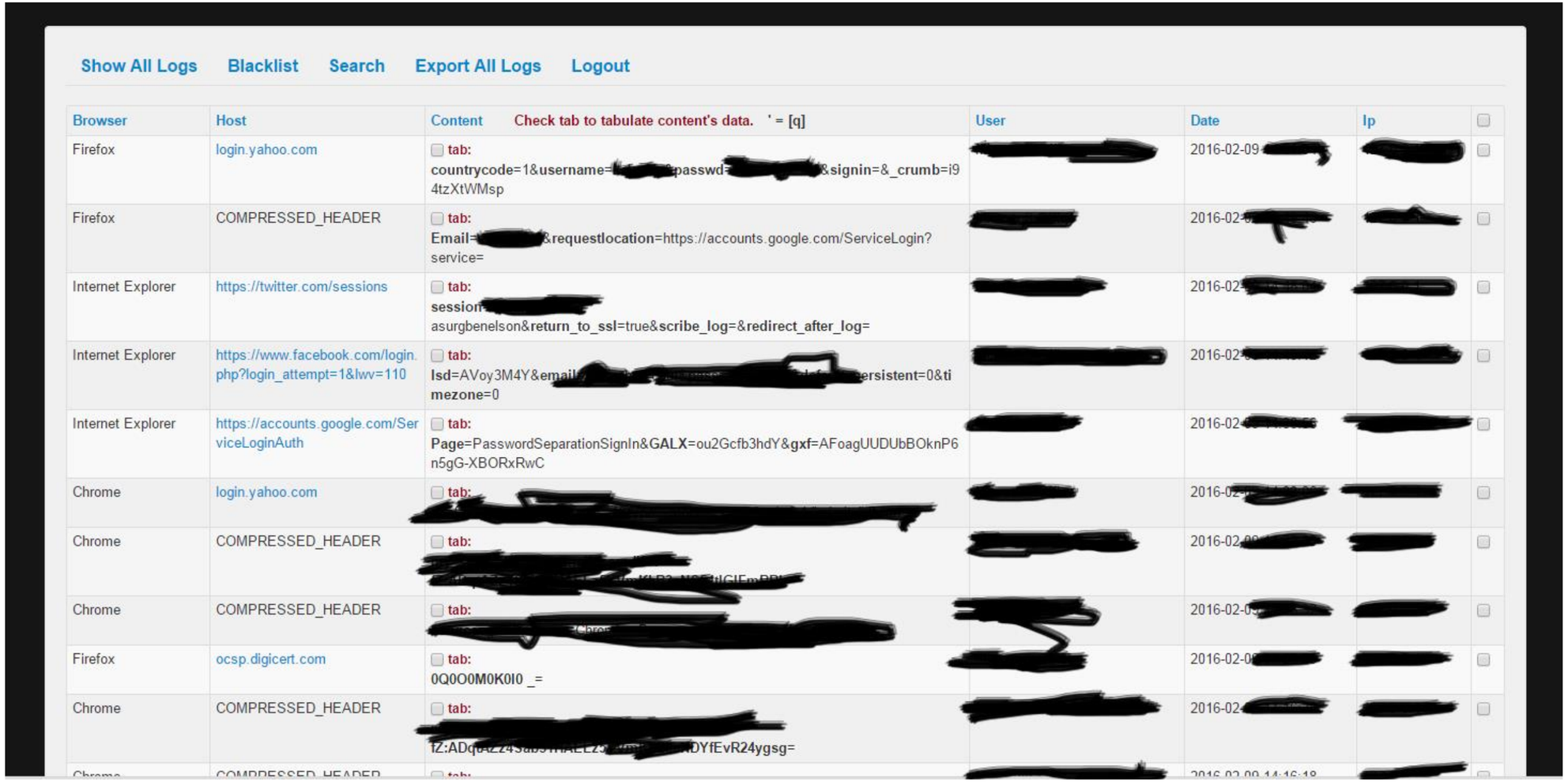
Keyloggers

Log THIS!



- **Software**
- **Hardware**
- **Monitors EVERY keystroke**
- **Reporting**
- **Legitimate use?**

Log THIS!

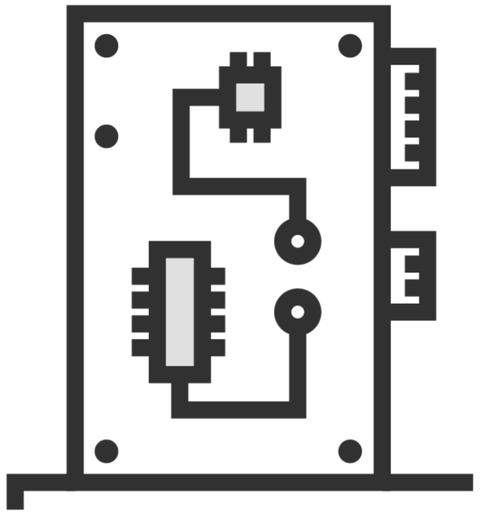


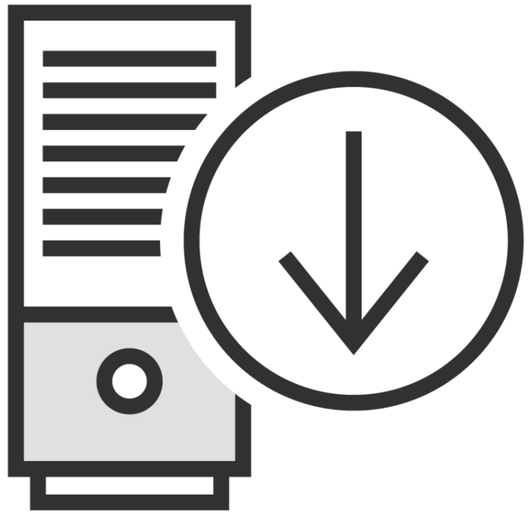
Log THIS!

- Capture screen shots
- Websites
- Passwords
- Emails
- Logon names
- Passwords hidden by *

Log THIS!

- Wi-Fi loggers
- Bluetooth loggers
- Acoustic loggers
- Rootkit loggers
- Driver loggers
- Hypervisor loggers





Spyware

Spyware

Capture keystrokes

Capture screenshots

Capture authentication credentials

Capture emails

Capture web forms

Capture habits

Who's Spying?

Marketing Companies

Organized Crime

Online Attackers

Trusted Insiders

Types of Spyware

Desktop

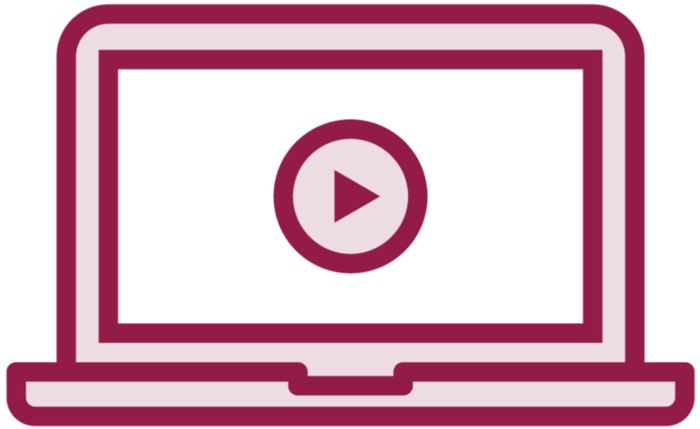
Video

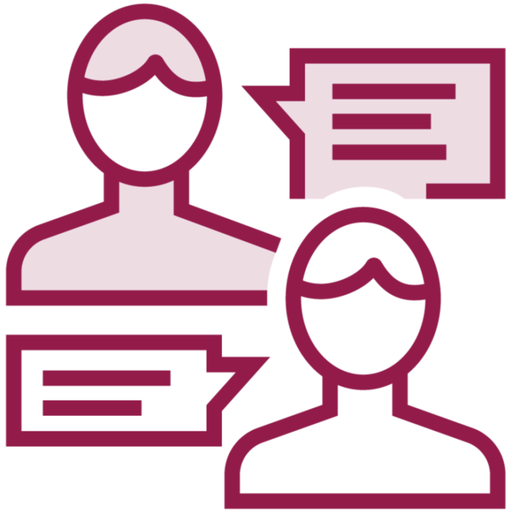
Printing

USB

Audio

Email/internet





Types of Spyware

Screen Capture

GPS

Monitoring

IoT

Don’t “Think” That’s All!

Backdoors

Backdoors

Remote admin utility

Total control of target

Uses exploits

Some are for “good”…but

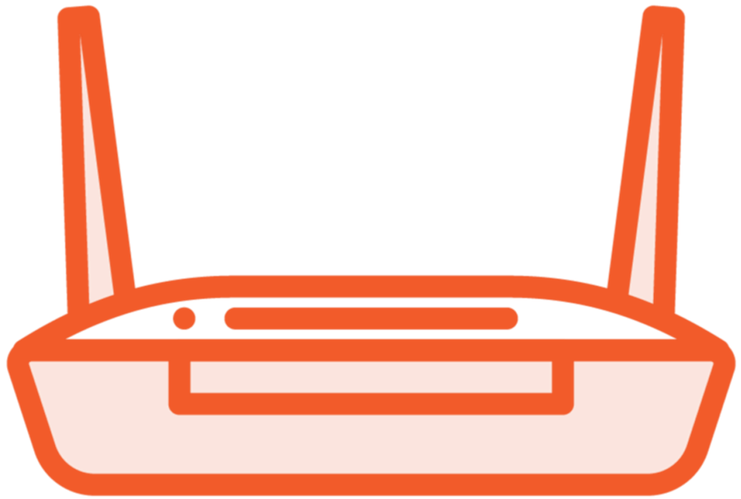
Two components – client/server

Automation built-in

Disable Security

Disable Security

Types of Backdoors



SERCOM

Types of Backdoors

Types of Backdoors

RemoteExec

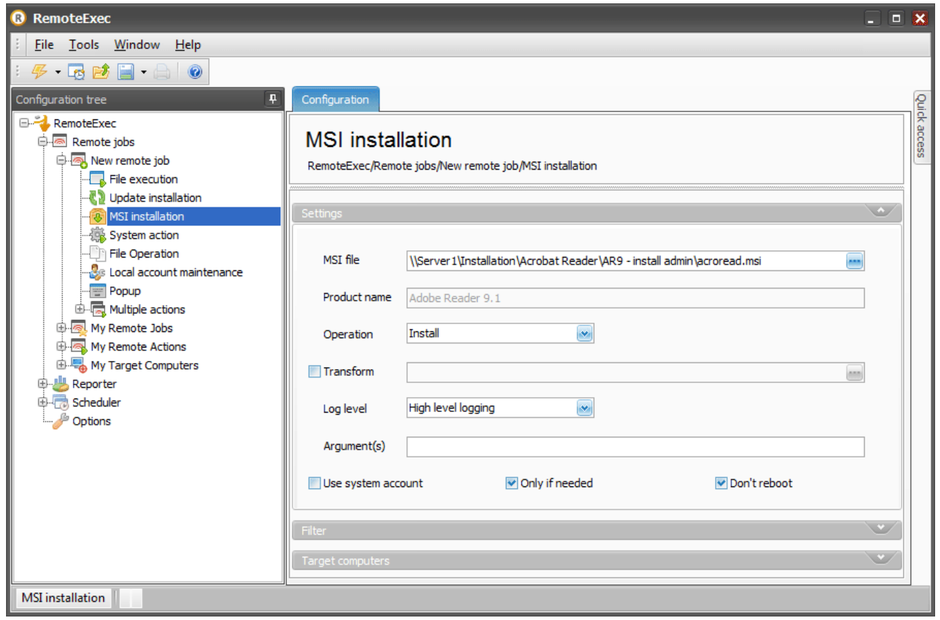
Install apps

Execute scripts

Copy/modify/delete files

Change admin password

Wakeup/reboot/power off



Learning Check

Learning Check

- Keylogger
- Crackers
- Audio spyware
- GPS spyware
- Physical inventories

Learning Check

- Metasploit
- Client component
- Nation States
- Printing spyware
- Video spyware

Key Terms

- **Keylogger**
- **Spyware**
- **Backdoor**

Next Up:

Maintaining Access: Hiding Your Tools