

# Maintaining Access: Executing Applications

---



## **Dale Meredith**

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

[dalemeredith.com](http://dalemeredith.com) | [Twitter: @dalemeredith](https://twitter.com/dalemeredith) | [Linkedin: dalemeredith](https://www.linkedin.com/in/dalemeredith)

Make it so, number one

**Jean-Luc Picard**

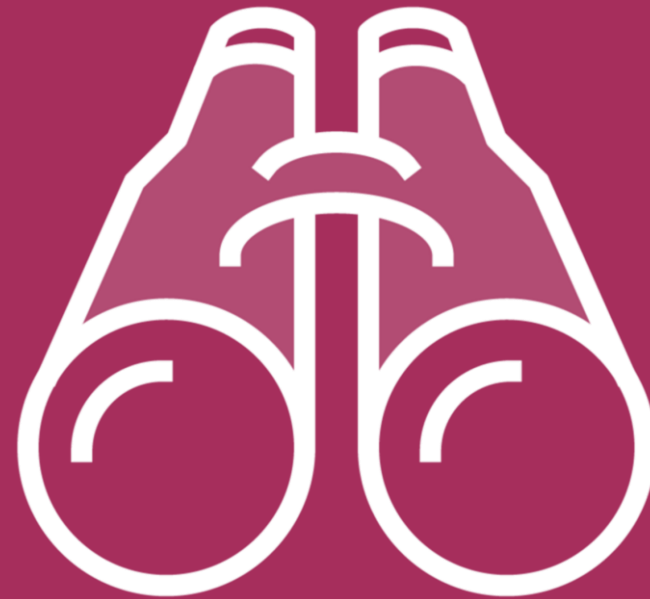
# Goals

---

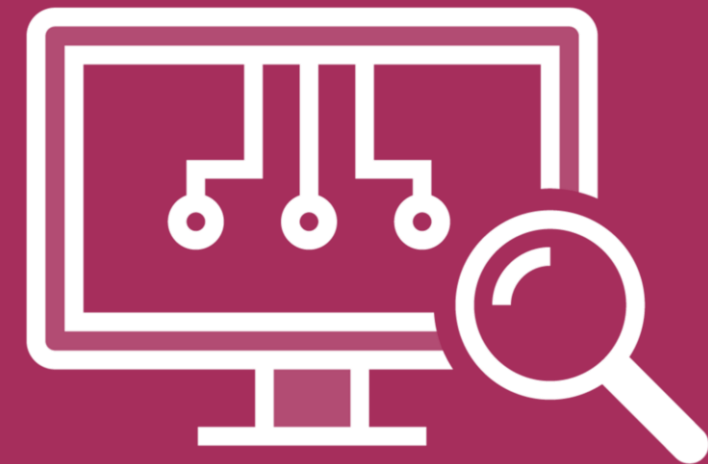
Overall, We're Here to:



**Make sure we  
can get back in**

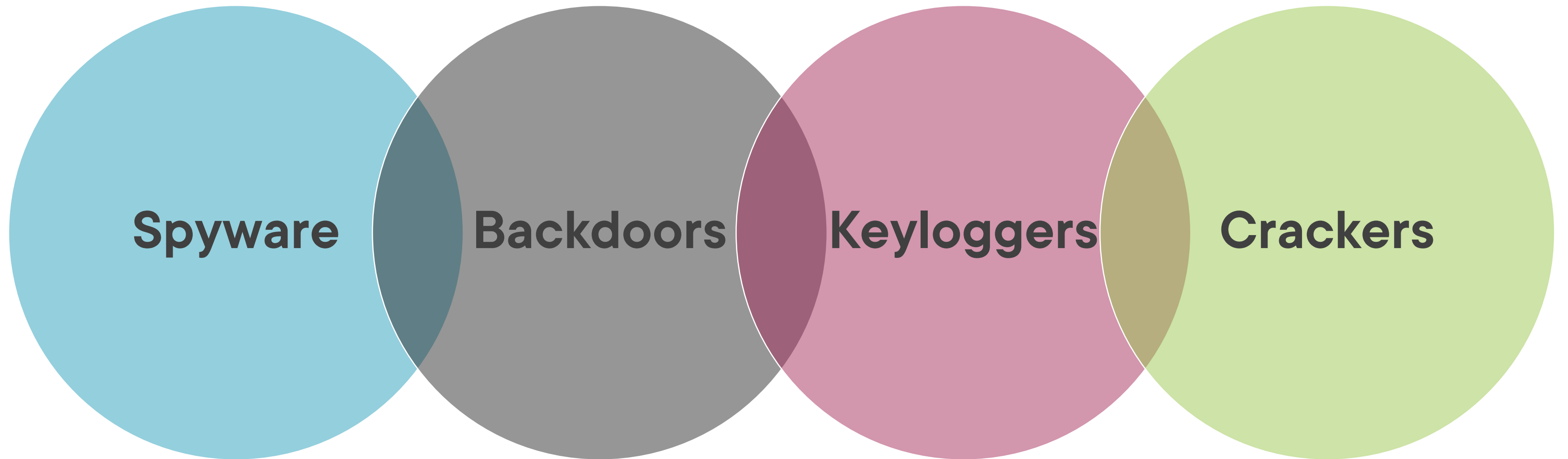


**See what's  
going on here**



**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 management interface with navigation links: [Show All Logs](#), [Blacklist](#), [Search](#), [Export All Logs](#), [Logout](#)

Browser	Host	Content <small>Check tab to tabulate content's data. ' = [q]</small>	User	Date	Ip	
Firefox	login.yahoo.com	<input type="checkbox"/> tab: countrycode=1&username=[REDACTED]&passwd=[REDACTED]&signin=&_crumb=i94tzXtWmsp	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Firefox	COMPRESSED_HEADER	<input type="checkbox"/> tab: Email=[REDACTED]&requestlocation=https://accounts.google.com/ServiceLogin?service=[REDACTED]	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Internet Explorer	https://twitter.com/sessions	<input type="checkbox"/> tab: session=[REDACTED] asurgbenelson&return_to_ssl=true&scribe_log=&redirect_after_log=[REDACTED]	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Internet Explorer	https://www.facebook.com/login.php?login_attempt=1&lwv=110	<input type="checkbox"/> tab: lsd=AVoy3M4Y&email=[REDACTED]&persistent=0&timezonedelay=0	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Internet Explorer	https://accounts.google.com/ServiceLoginAuth	<input type="checkbox"/> tab: Page=PasswordSeparationSignIn&GALX=ou2Gcfb3hdY&gxf=AFoagUUDUbBOknP6n5gG-XBORxRwC	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Chrome	login.yahoo.com	<input type="checkbox"/> tab: [REDACTED]	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Chrome	COMPRESSED_HEADER	<input type="checkbox"/> tab: [REDACTED]	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Chrome	COMPRESSED_HEADER	<input type="checkbox"/> tab: [REDACTED]	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Firefox	ocsp.digicert.com	<input type="checkbox"/> tab: 0Q000M0K010_=[REDACTED]	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Chrome	COMPRESSED_HEADER	<input type="checkbox"/> tab: [REDACTED]	[REDACTED]	2016-02-09	[REDACTED]	<input type="checkbox"/>
Chrome	COMPRESSED_HEADER	<input type="checkbox"/> tab: [REDACTED]	[REDACTED]	2016-02-09 14:16:18	[REDACTED]	<input type="checkbox"/>

# Log THIS!



**Capture screen shots**

**Websites**

**Passwords**

**Emails**

**Logon names**

**Passwords hidden by \***

# Log THIS!

WiFi



**Wi-Fi loggers**

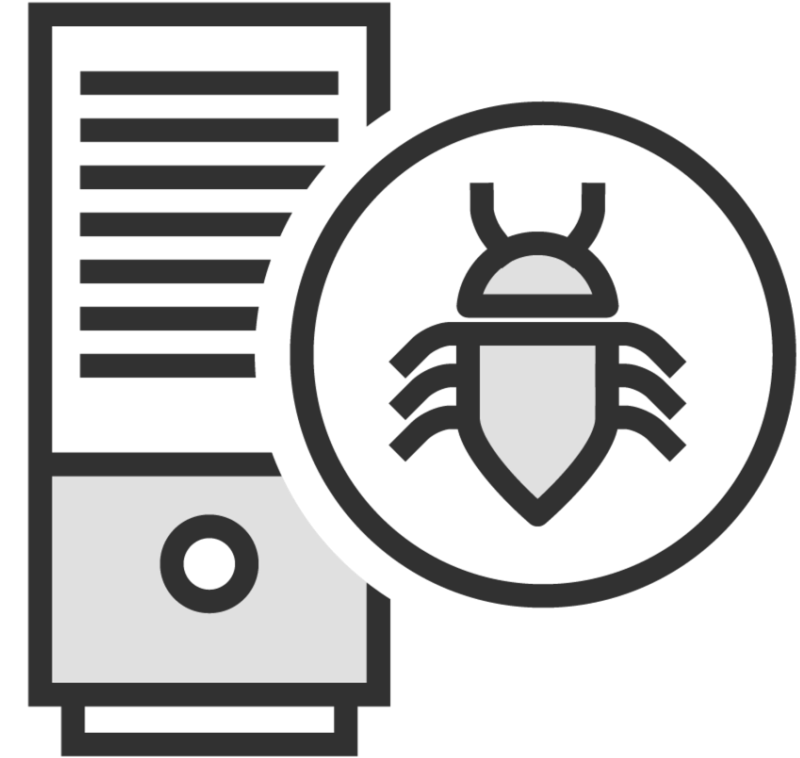
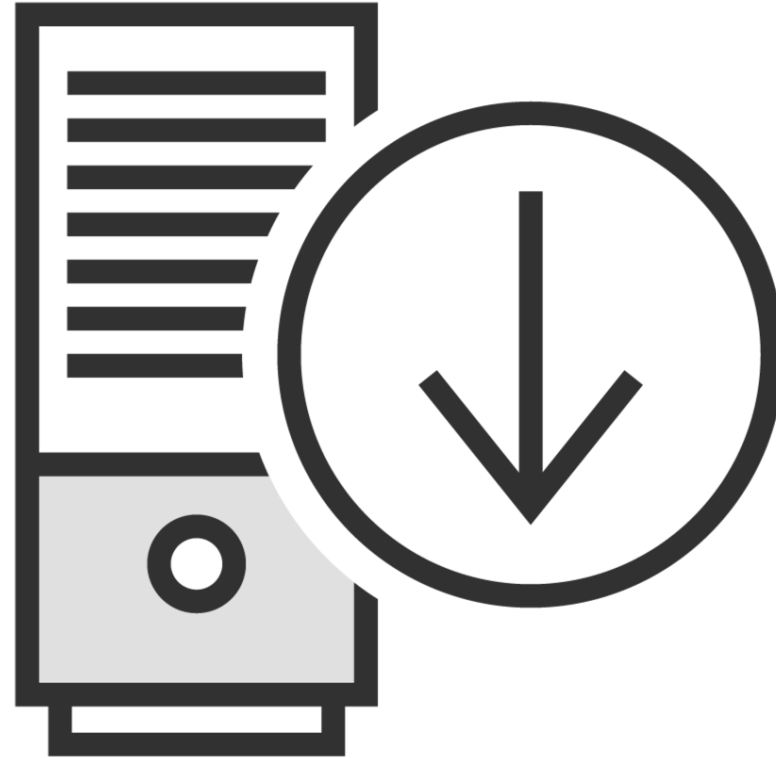
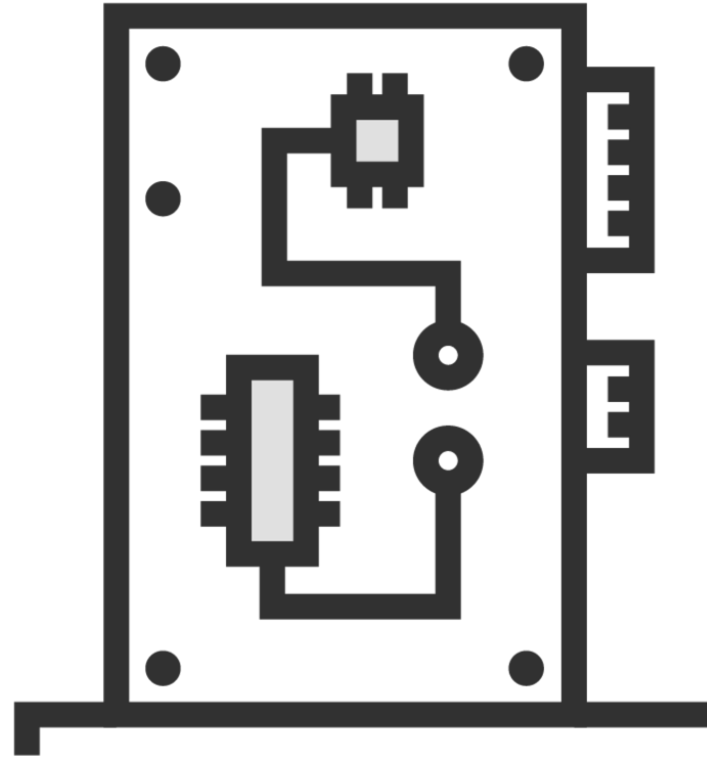
**Bluetooth loggers**

**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

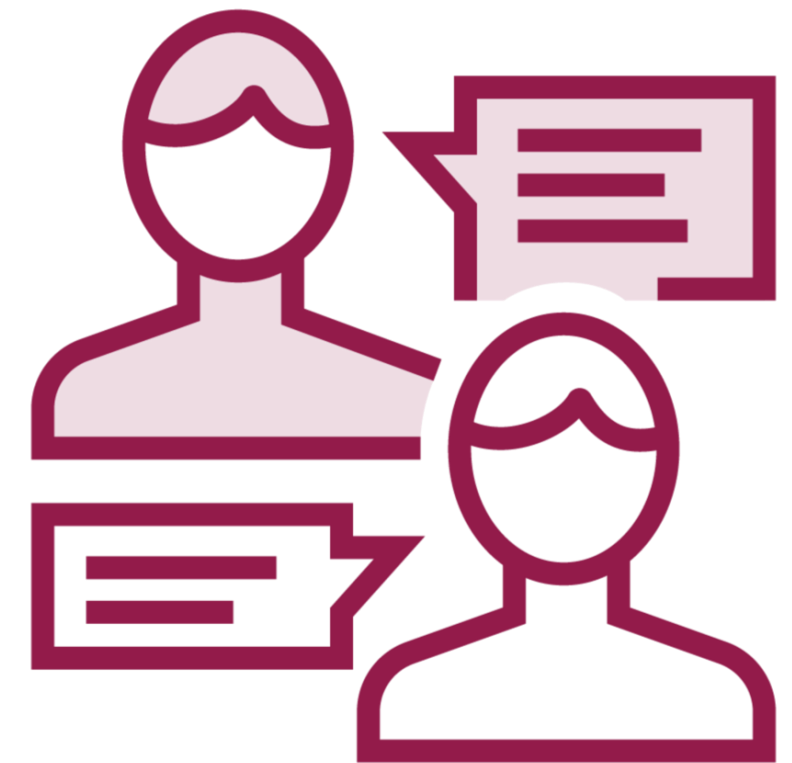
Video

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

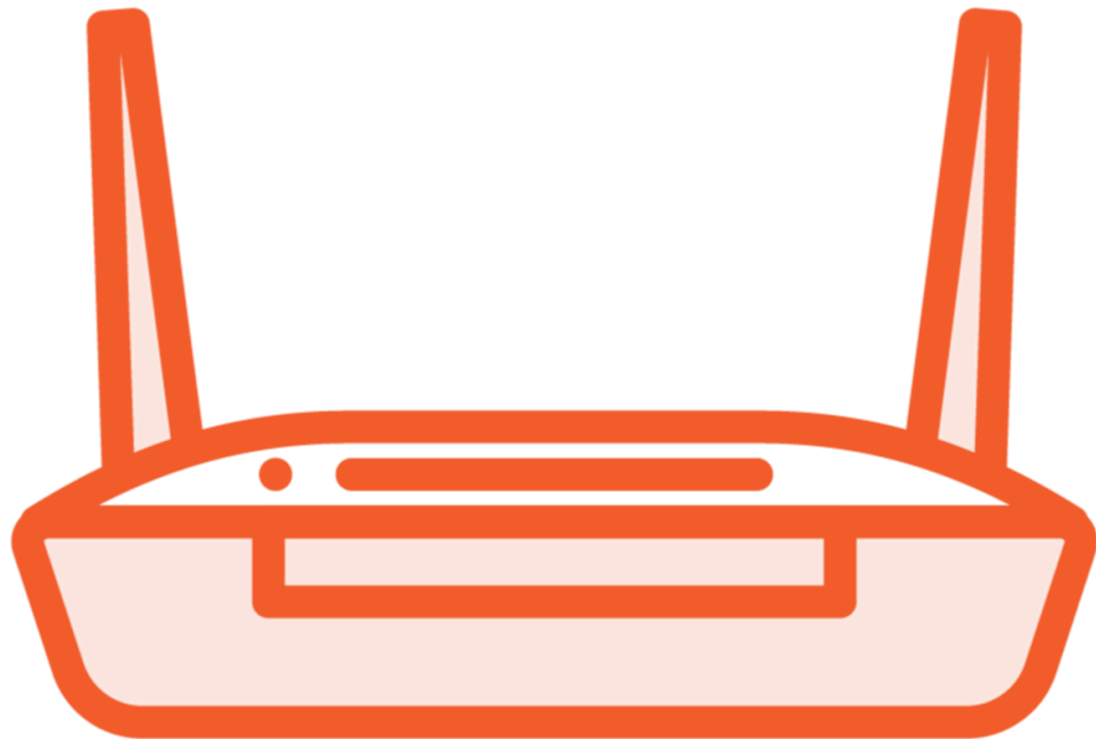
# Disable Security



# Disable Security

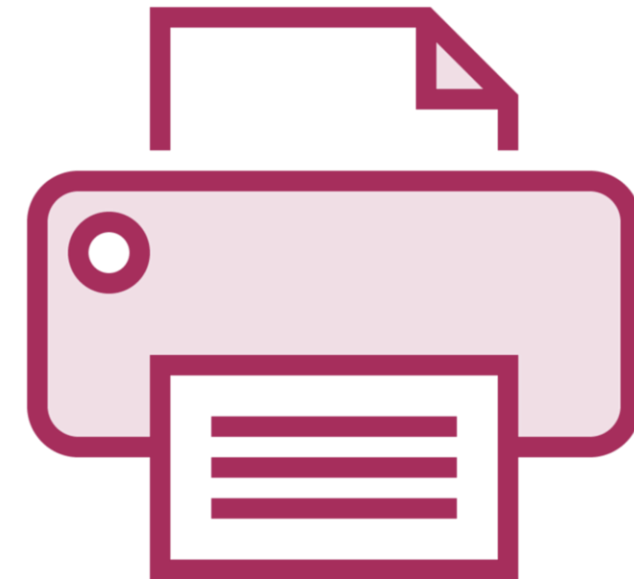


# Types of Backdoors



**SERCOMA**

# Types of Backdoors



# Types of Backdoors

**RemoteExec**

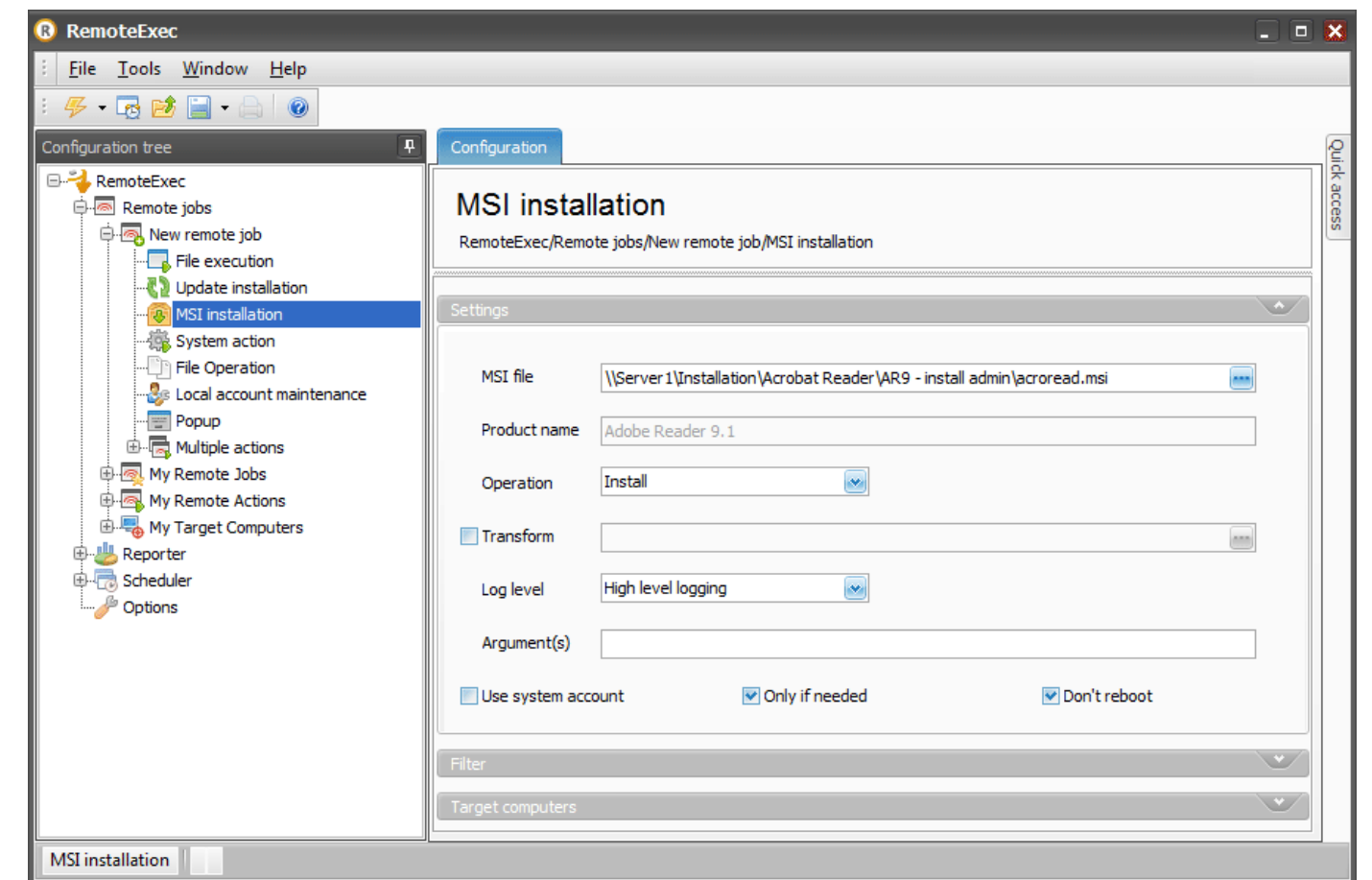
**Install apps**

**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

---