Reviewing Fileless Malware

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

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

Sneaky little hobbitses

Gollum

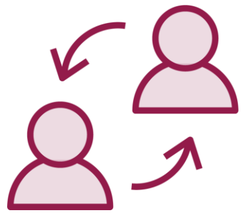
Organizations should focus on monitoring, detecting, and prevention instead of just the traditional approaches.

- Steal
- Install
- Inject

Why Use Fileless Malware

Stealth

LOL (Living-off-the-land)



Trustworthy

PowerShell

The good

The bad and ugly

Fileless Techniques

Techniques

- Phishing emails
- Legitimate applications
- Native applications
- Lateral movement
- Malicious websites
- Registry manipulation
- Memory code injection
- Script-based injection

Taxonomy

Type I

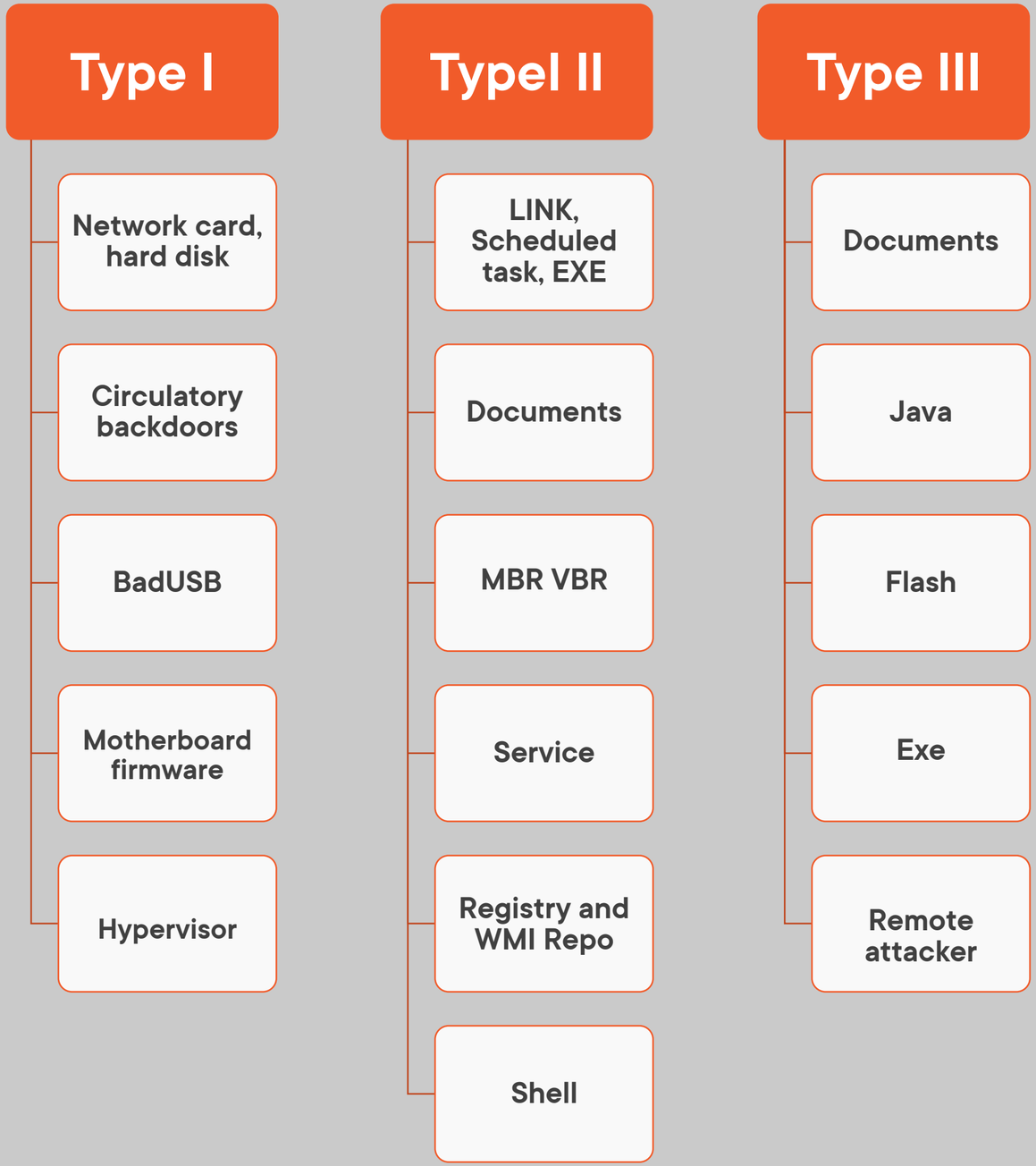
No file activity performed

Type II

Indirect file activity

Type III

Files are required to operate



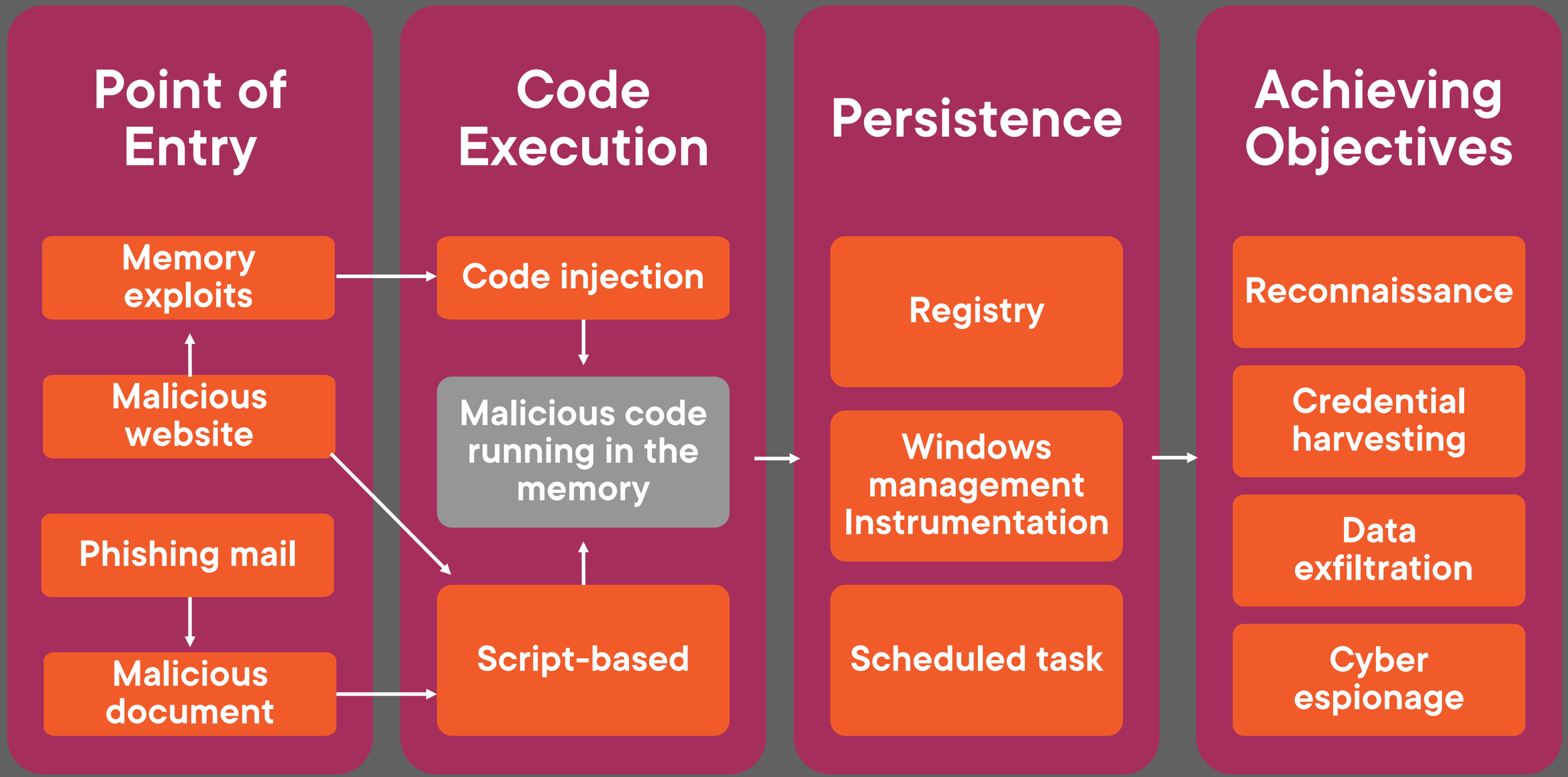
Classification Based on Point of Entry

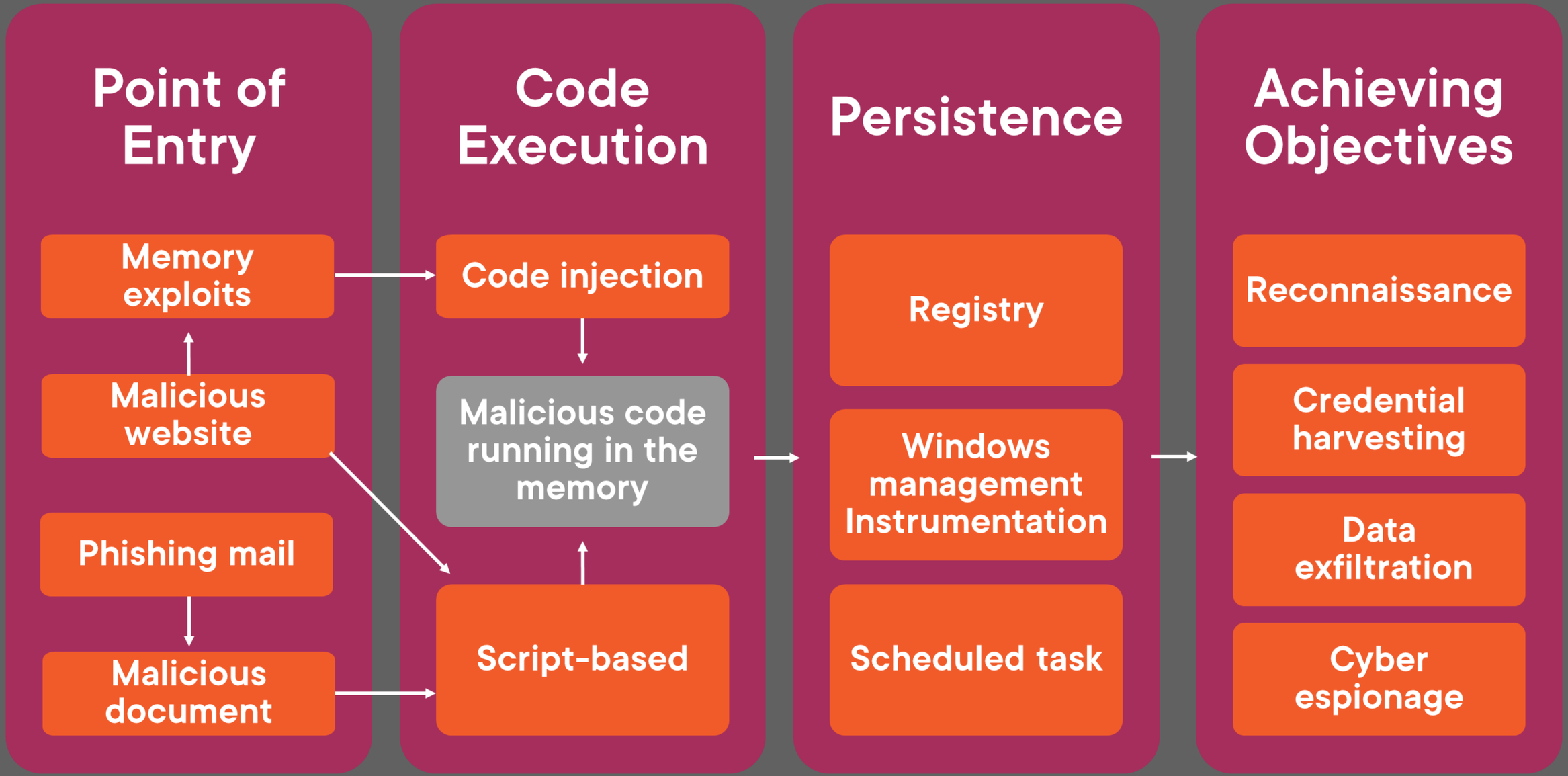
Exploits

Hardware

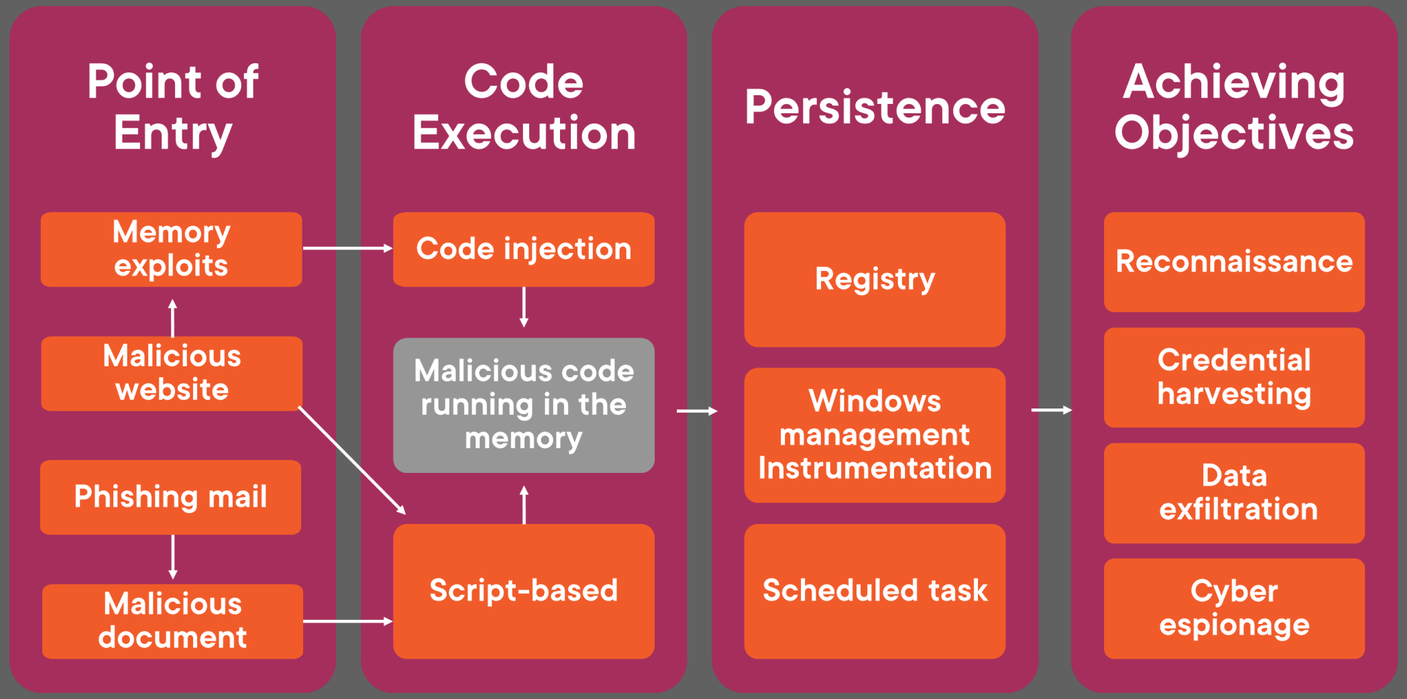
Execution and Injection

How Does Fileless Malware Work?



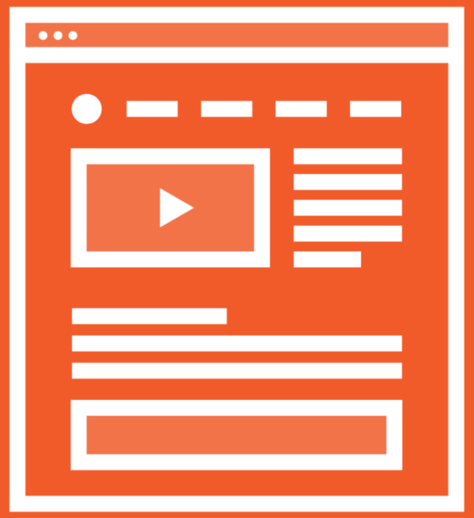


Deep Dive



Point of Entry

Memory Exploits



Malicious Website

Malicious email and documents

Code Execution

Code injection

Script-based injection

Persistence

Windows Registry

Windows Management Instrumentation (WMI)

Windows Task Scheduler

Achieving Objectives

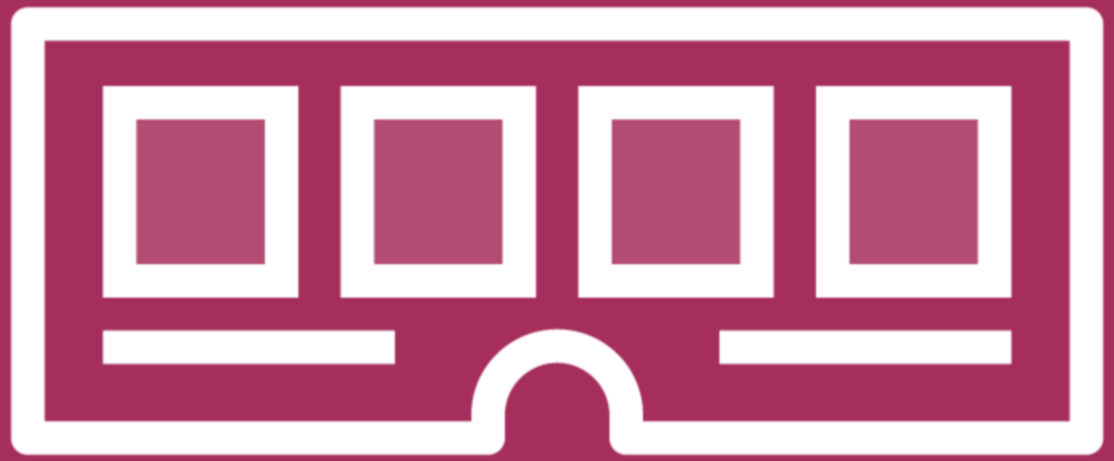
Persistence is what allows attackers bypass security solutions and achieve their objectives

Launching Fileless Malware

Launching Through Document Exploits

- **Trick the victim into downloading a malicious document**
- **The document runs a malicious macro**
- **The macro launches VBA or JavaScript**
- **The script exploits PowerShell to run additional code to spread the infection**

Launching through in-memory Exploits



Inject malicious payload inside the running memory that targets processes

Employ a reflective Dynamic Link Library (DLL) method into a host-side process

Launching through Script-based Injection

Performed using scripts with embedded binaries and shellcode

Used to find design flaws and vulnerabilities in applications

Used along with vulnerabilities in a system to inject malicious scripts into the memory via PowerShell to evade detection

Launching by Exploiting System Admin Tools

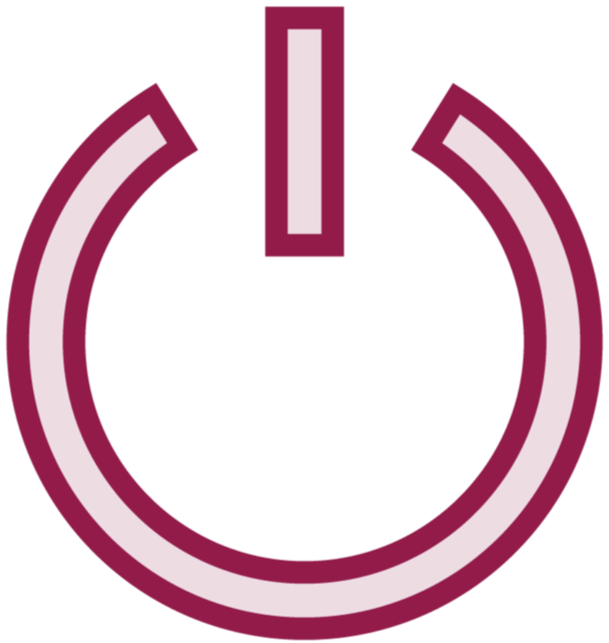
Exploits default system admin tools, features, and utilities

Modified tools are used to access payloads, maintain, persistence, steal, and export information and expand malware

Launching through Phishing

- **Send a phishing email with a malicious link**
- **Automatically redirected to a fake website**
- **Website scans for vulnerabilities in the system**
- **Exploits system tools to load and run malicious payloads in memory**
- **Creates a AutoStart registry key to store the malicious script**

Maintaining Persistence



Fileless Malware

- **Divergent**
- **Kovter and Poweliks**
- **Nodersok**
- **Dridex**
- **Vaporworm**
- **Sorebrect**

Learning Check

Learning Check

- RAM
- Phishing emails
- Type 1
- Persistence
- Powershell

Up Next:
Detecting Malware