Giải pháp chống khai thác lỗ hổng và thực thi mã độc trên máy trạm

Hiep Nguyen
CCIE, CISSP
Security Solution Consultant

Exploits

≠

Malware

Là một đoạn mã thực thi để khai thác lỗ hổng của phần mềm

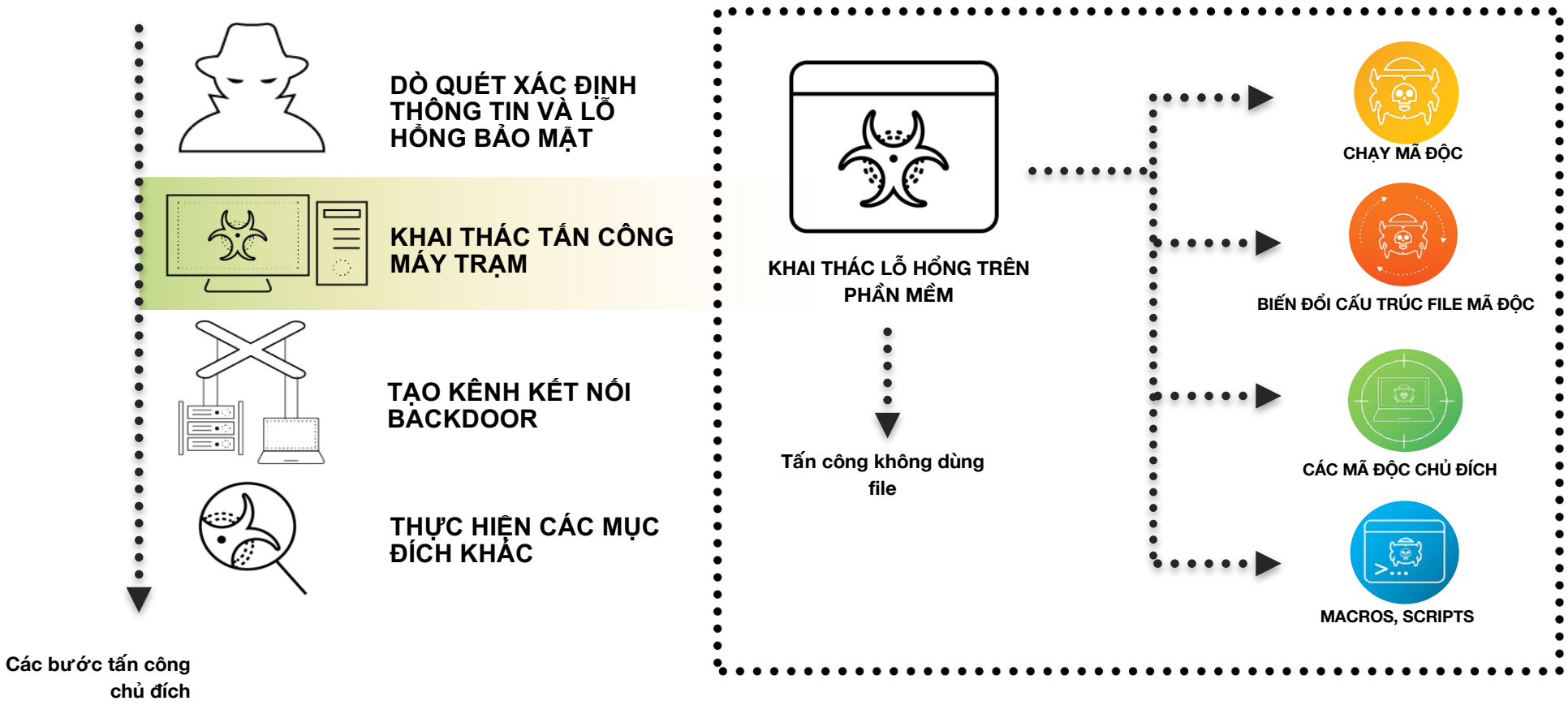
Khai thác các phần mềm phổ biến (Office, Adobe PDF, Flash, Trình duyệt…)

~ Mã độc

Là một chương trình chạy (.exe, .com, .dll)

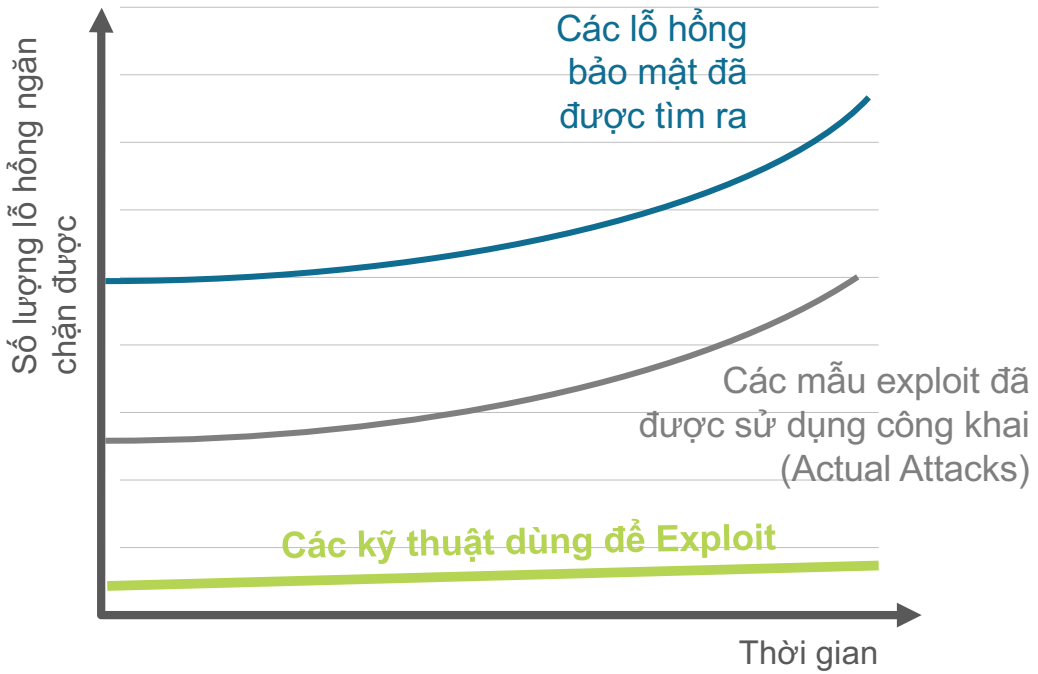
Thực thi các tác vụ, hành động xấu

Các bước tấn công mã độc



Exploits

Các cách ngăn chặn khai thác lỗ hổng bảo mật của phần mềm

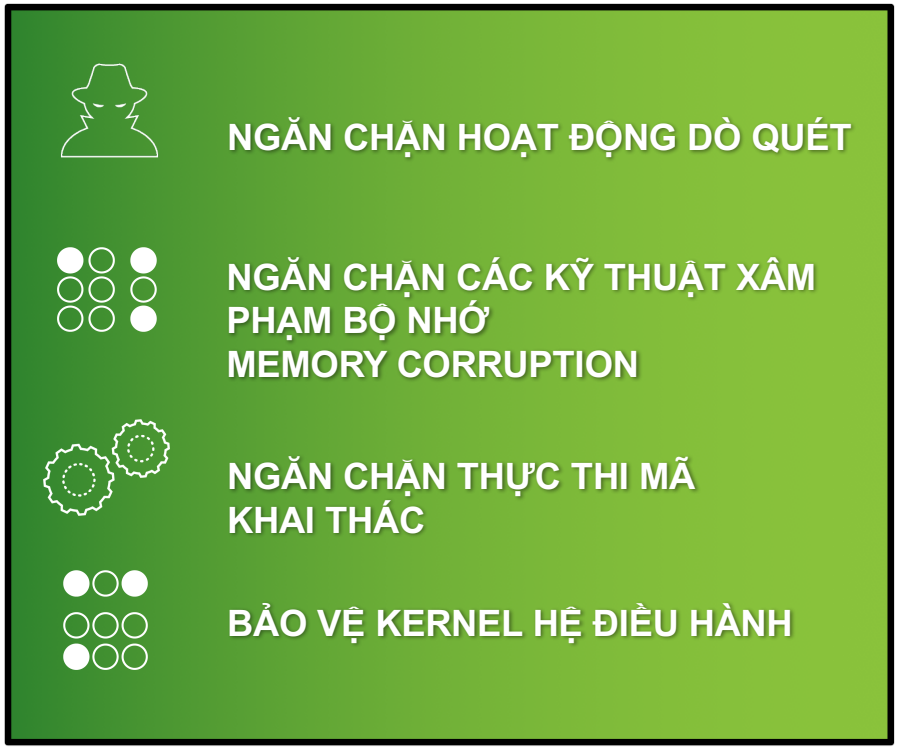


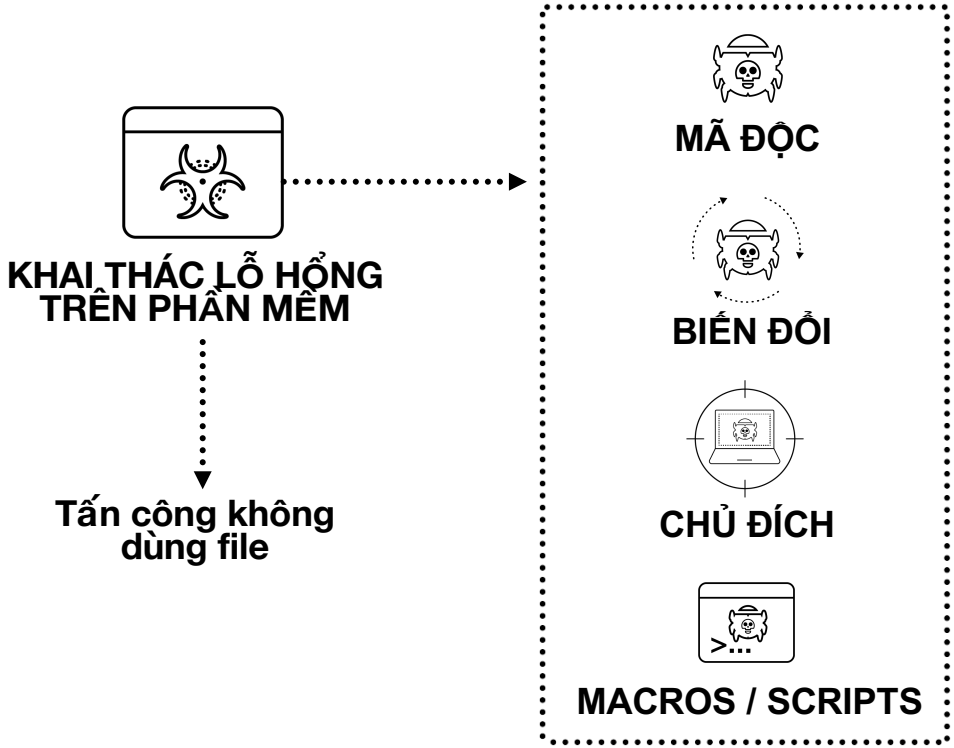
Patching — Sau khi đã có nghiên cứu về lỗ hổng và hãng phát hành bản vá

Signature / Behavior — Cần có mẫu exploits để hãng viết signature chặn từng mẫu

Traps — **Không cần patch, không cần mẫu, không signature, không scan**

Các phương pháp ngăn chặn Exploit

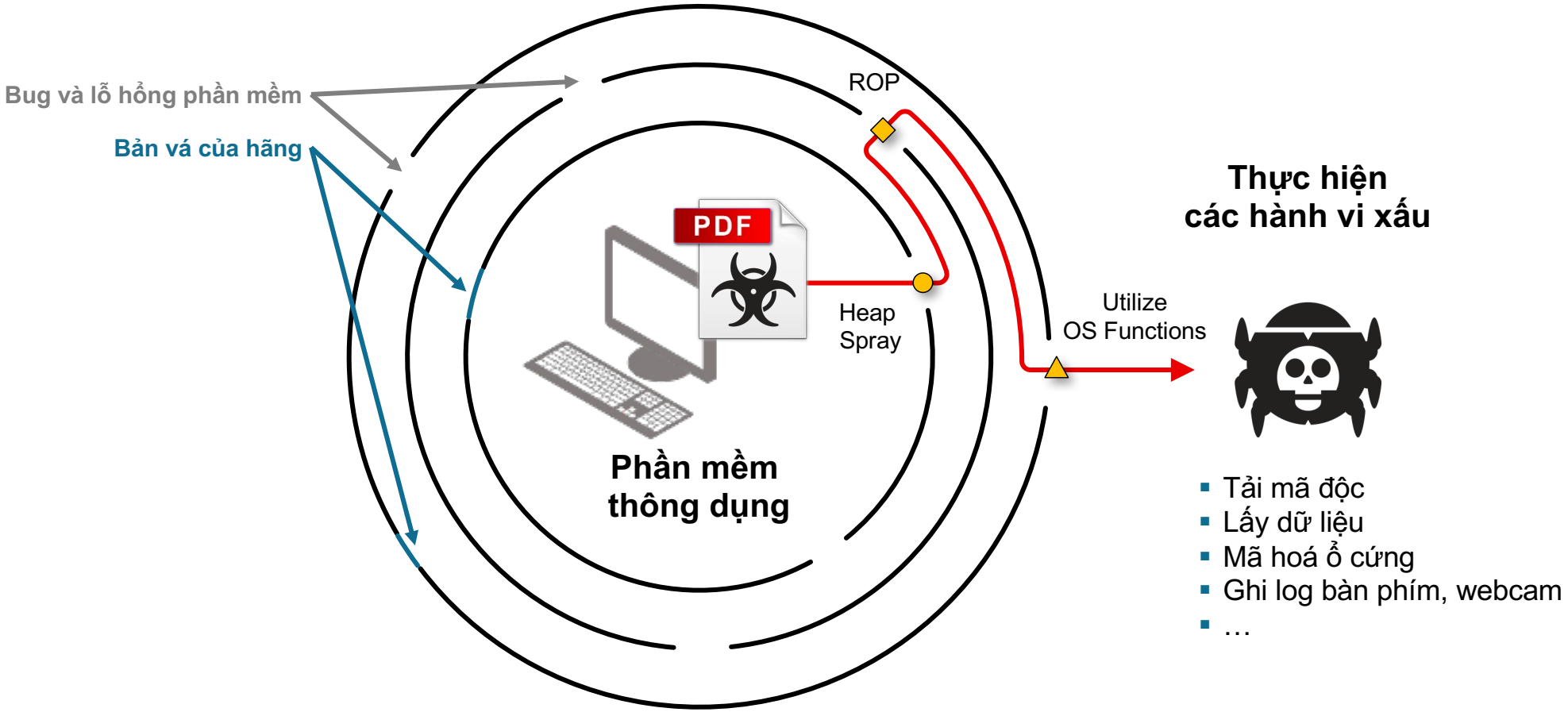




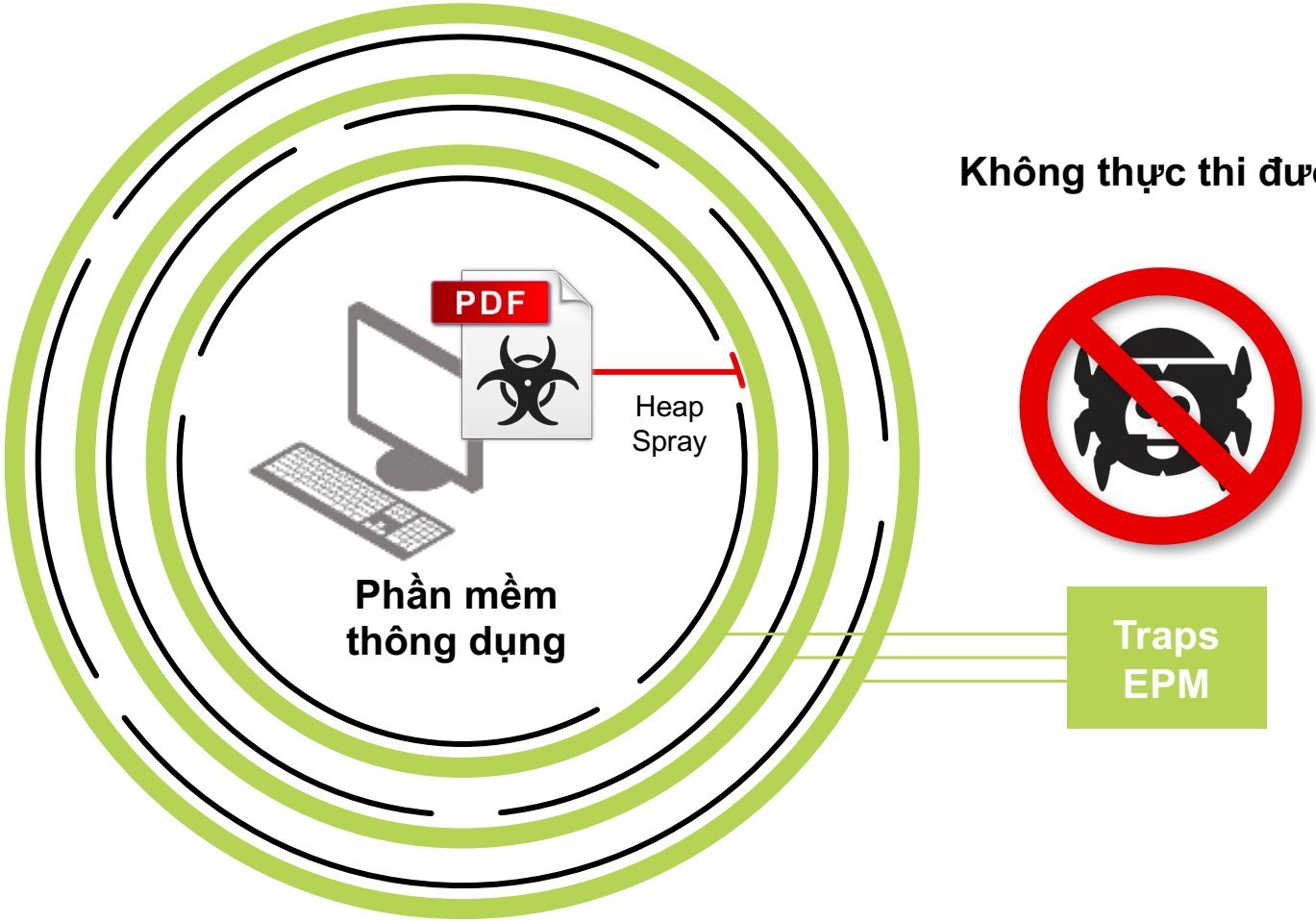
CÁC KỸ THUẬT ĐỂ KHAI THÁC LỖ HỔNG PHẦN MỀM

Control Panel Protection	Data Execution Prevention	UASLR	DLL-Hijacking Protection
Exception Heap Spray Check	Exploit Kit Fingerprinting Protection	SysExit	Hot Patch Protection
Just-in-Time (JIT) Mitigation	Kernel Privilege Escalation Protection	Library Pre-allocation	Memory Limit Heap Spray Check
Null Dereference Protection	ROP Mitigation	Structured Exception Handler Protection	Shellcode Pre-allocation

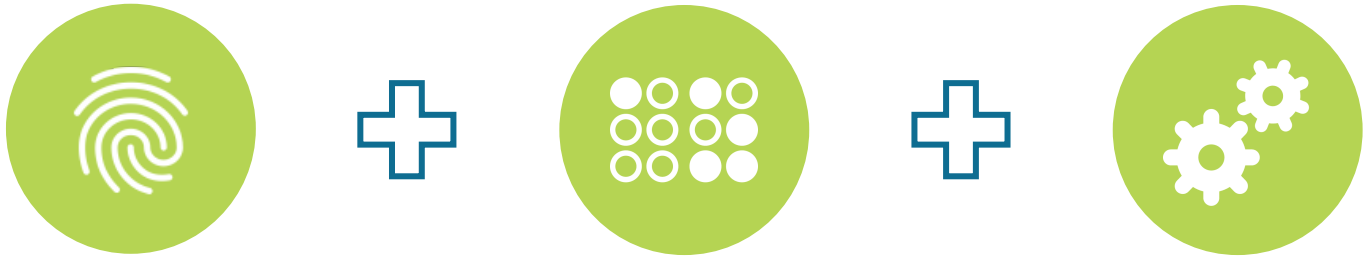
Exploits sử dụng các phần mềm thông dụng để tấn công



Traps ngăn chặn từng kỹ thuật Exploit



Các tính năng ngăn chặn Exploit



Chống dò quét lấy thông tin

Tự động ngăn chặn các exploit kit dò quét xác định lỗ hổng

Ngăn chặn các kỹ thuật khai thác

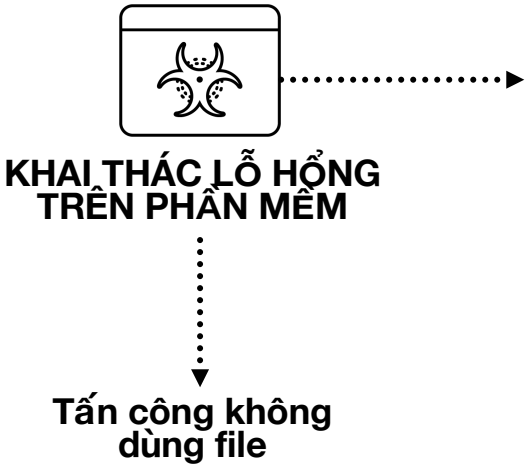
Chặn theo từng kỹ thuật khai thác lỗ hổng mà exploit sử dụng

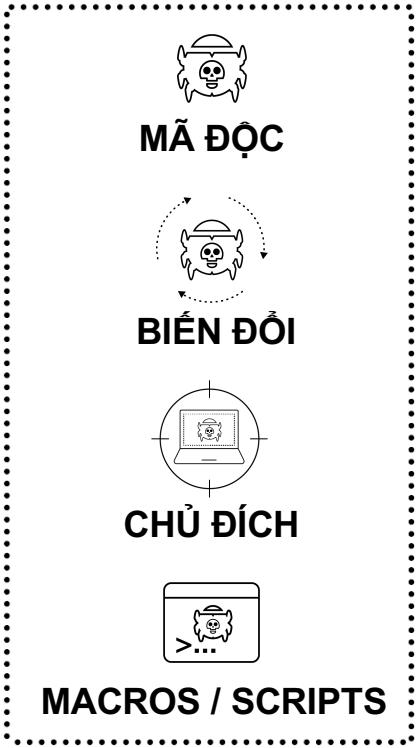
Bảo vệ Kernel

Bảo vệ các exploit chiếm quyền hoặc can thiệp các tiến trình ở kernel

Malware

Các phương pháp ngăn chặn Mã độc





GIẢM BỚT ĐIỂM TẤN CÔNG
Kiểm soát chính sách, Tiến trình con, Thư mục thực thi

NGĂN CHẶN MÃ ĐỘC ĐÃ BIẾT
Dùng thông tin từ Wildfire

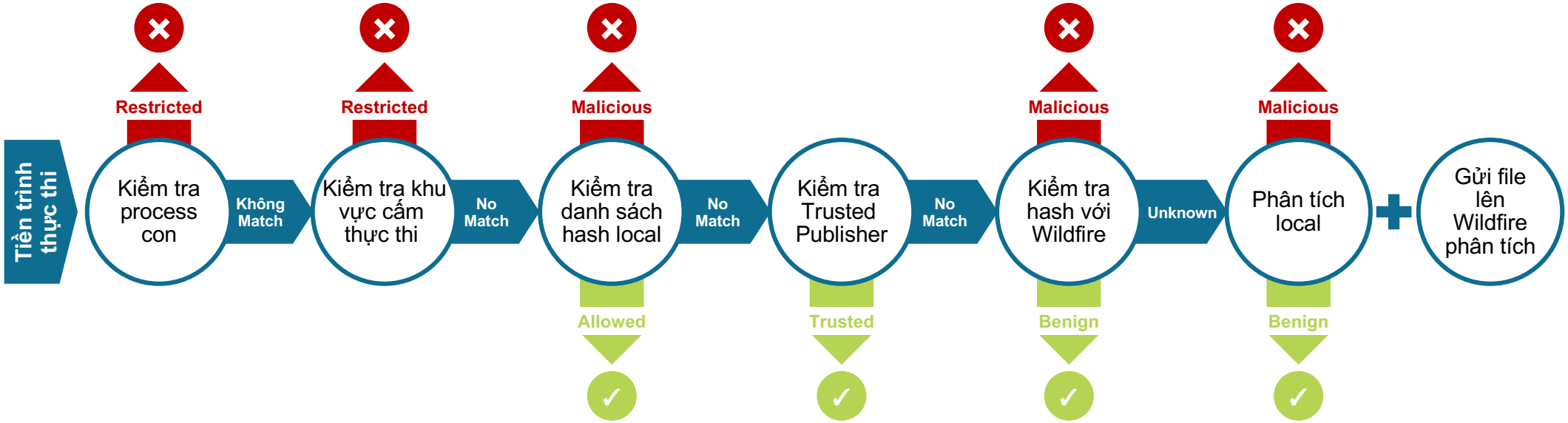
NGĂN CHẶN MÃ ĐỘC CHƯA BIẾT
Phân tích local và học máy

PHÁT HIỆN CÁC TẤN CÔNG PHỨC TẠP
Phân tích động trên Wildfire

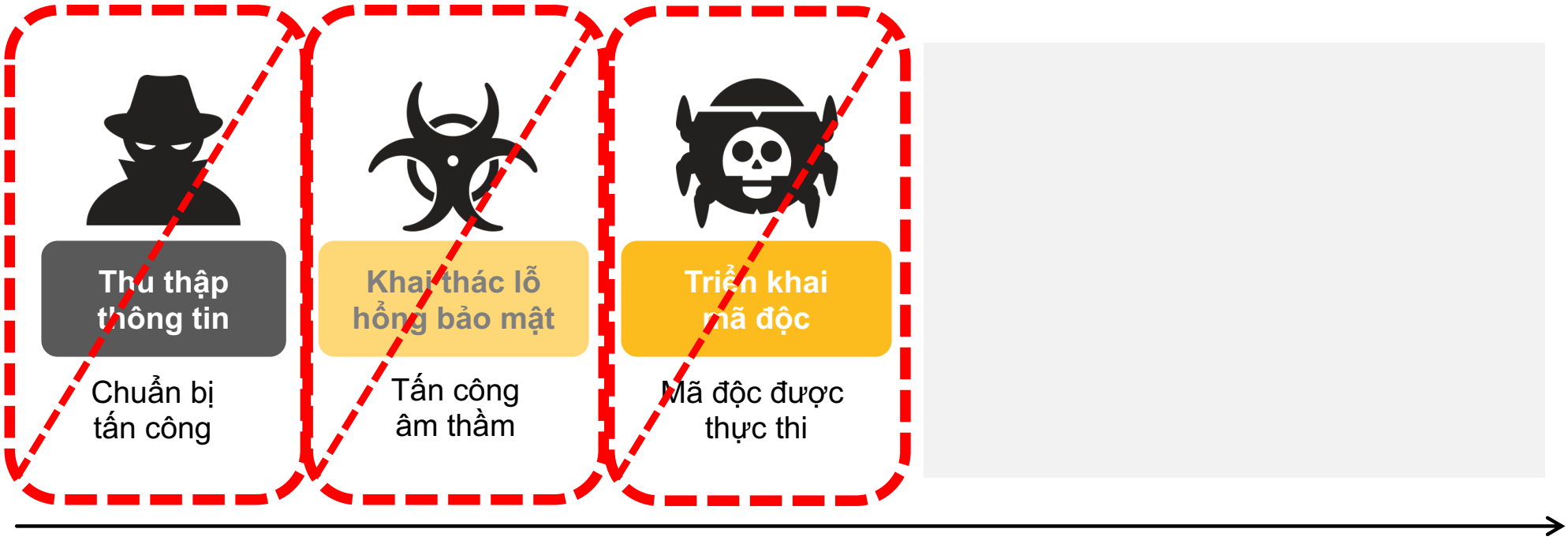
Các kỹ thuật chống Mã độc

Wildfire Intelligence	**Phân tích Local trên máy**	**Phân tích động trên Wildfire**	**Ngăn chặn các tiến trình xấu**	**Chống mã hoá dữ liệu**
Chặn mã độc đã biết	Chặn mã độc chưa biết	Chặn mã độc chưa biết và tấn công phức tạp	Chặn tấn công bằng script based, không dùng file	Bắt sự kiện mã hoá trên file mồi

Quy trình kiểm tra và ngăn chặn Mã độc



Ngăn chặn một bước, sẽ ngăn chặn được cả cuộc tấn công



Traps ngăn chặn các bước của cuộc tấn công

Đánh giá hiệu quả AV với AV-TEST

Có thể thay thế AV

100% phát hiện các mẫu (không dùng signature)

Điểm năng lực hệ thống cao nhất

Điểm tổng cao hơn các AV truyền thống

Test với phương pháp không update

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Based on 4.0
Q3, 2017

Mô hình triển khai

Bảo vệ cho nhiều hệ điều hành

Workstations

- Windows XP* (32-bit, SP3 or later)
- Windows Vista (32-bit, 64-bit, SP1 or later; FIPS mode)
- Windows 7 (32-bit, 64-bit, RTM and SP1; FIPS mode; all editions except Home)
- Windows Embedded 7 (Standard and POSReady)
- Windows 8* (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit; FIPS mode)
- Windows Embedded 8.1 Pro
- Windows 10 Pro (32-bit and 64-bit, CB and CBB)
- Windows 10 Enterprise LTSB
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- macOS 10.12 (Sierra)

Servers

- Windows Server 2003* (32-bit, SP2 or later)
- Windows Server 2003 R2 (32-bit, SP2 or later)
- Windows Server 2008 (32-bit, 64-bit; FIPS mode)
- Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode)
- Windows Server 2012 (all editions; FIPS mode)
- Windows Server 2012 R2 (all editions; FIPS mode)
- Windows Server 2016 (Standard edition)

Virtual Environments

- VMware ESX, Horizon View
- Citrix XenServer, XenDesktop, XenApp
- Oracle Virtualbox
- Microsoft Hyper-V

* Microsoft no longer supports this operating system.

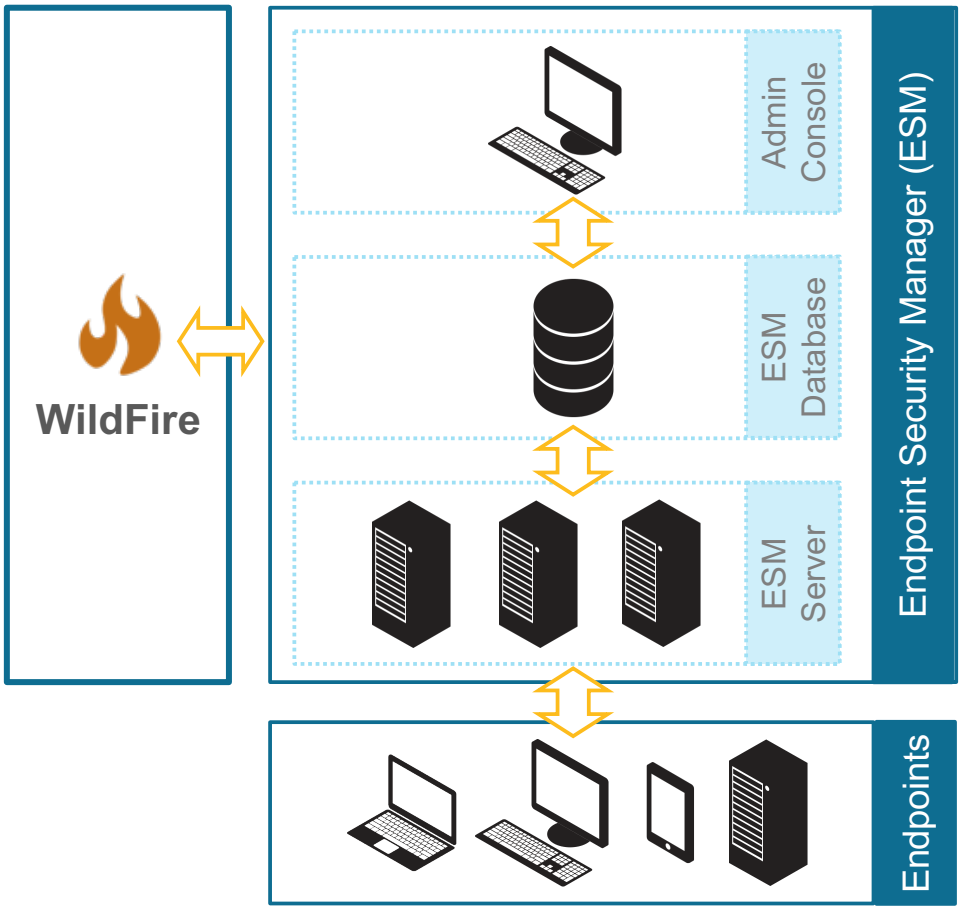
Mô hình triển khai

Mô hình linh hoạt

- Hỗ trợ máy ảo và máy vật lý
- Hỗ trợ Windows & Mac
- Hỗ trợ150,000 endpoints/ESM DB

Dùng rất ít tài nguyên

- 0.1% CPU Load
- 50 MB RAM
- 200 MB HD
- Không scan
- Không dùng signature



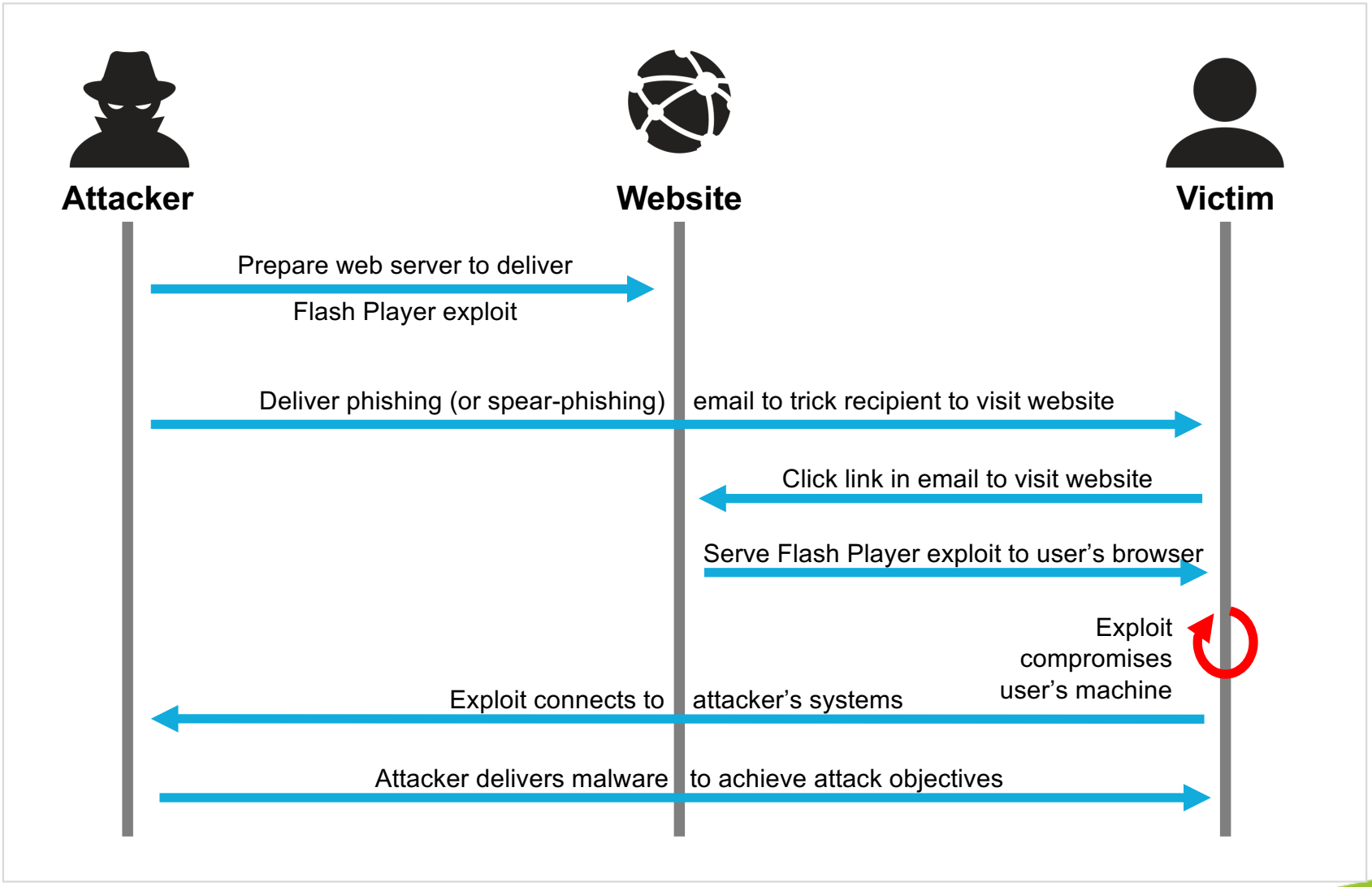
Hands-on Lab

Class Link:

https://use.cloudshare.com/Class/uypzo

Student Passphrase

DTS IS THE BEST


Attacker
Website
Victim
Prepare web server to deliver
Flash Player exploit
Deliver phishing (or spear-phishing)
email to trick recipient to visit website
Click link in email to visit website
Serve Flash Player exploit to user's browser
Exploit
compromises
user's machine
Exploit connects to
attacker's systems
Attacker delivers malware
to achieve attack objectives