Traps Advanced Endpoint Protection

Fredrik Lundgren

System Engineer

RADPOINT

caforssztxqzf2nm.onion

caforssztxqzf2nm.onion

BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

37:11:19

Price for decryption:

= 0.05

Enter your personal key or your assigned bitcoin address.

The Impact of Ransomware

WannaCry ~$750M (2017)
Locky ~$220M
Cryptowall ~$100M
CryptXXX ~$73M
Cerber ~$54M

38% Global Rise in
Cyber Insurance Demand

Nov 2016: 1 BTC = 700$
Nov 2017: 1 BTC = 7000$

Over $1 Billion Dollars in 2016 on ransom alone

The Impact of Ransomware

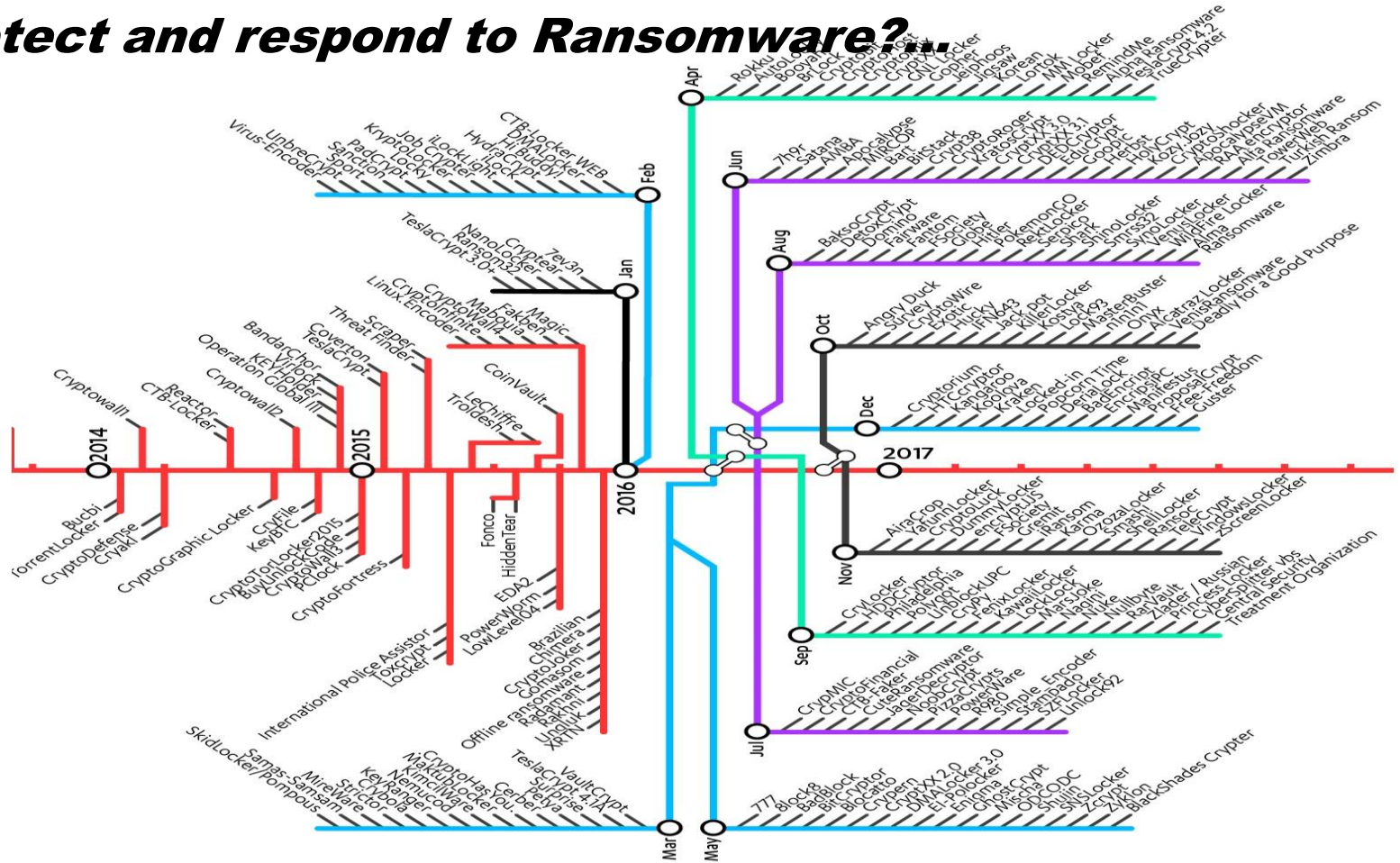
How did it impact your business?

- Honda, Renault, and Nissan had to stop production
- UK National Health Service forced to run on emergency-only basis during attack
- Public Transit systems affected gave free ridership until the issue was resolved

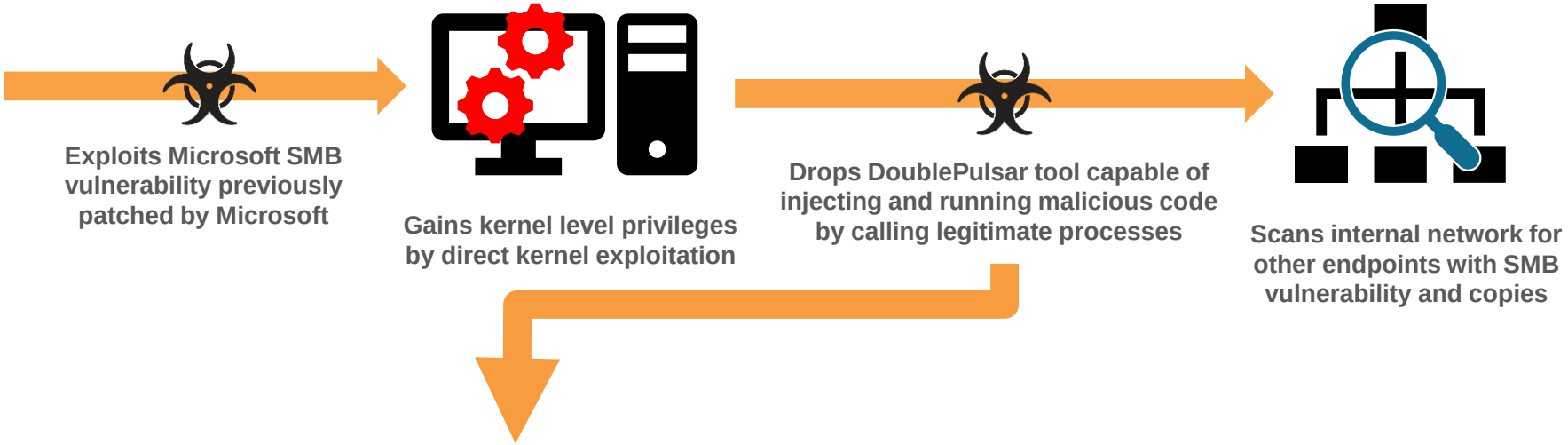
How many man hours did it take to…?

- Find backups and restore files?
- Get systems *back* online?
- Analyze and determine if the attack was *just ransomware?*

Detect and respond to Ransomware?...



WannaCry



Exploits Microsoft SMB vulnerability previously patched by Microsoft

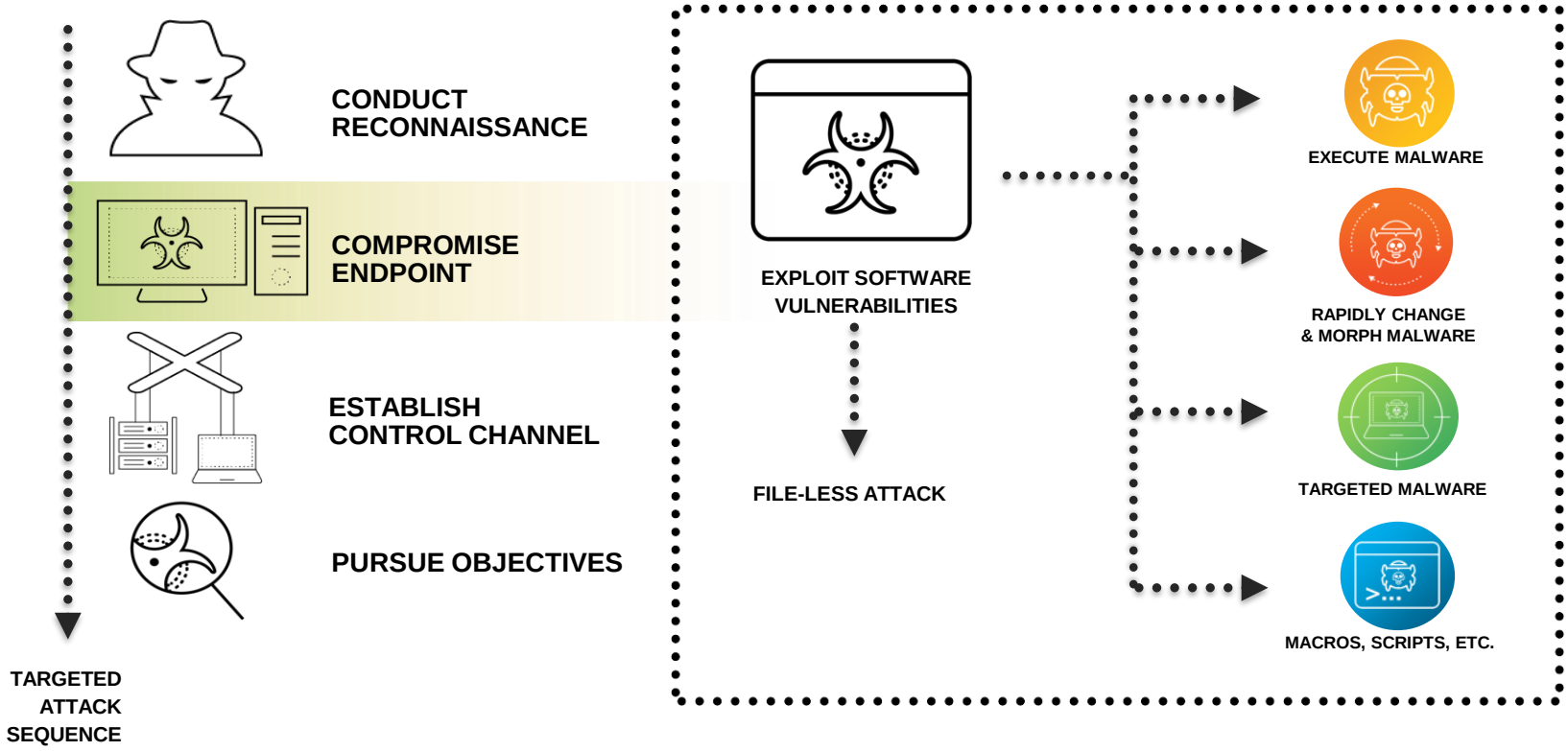
Gains kernel level privileges by direct kernel exploitation

Drops DoublePulsar tool capable of injecting and running malicious code by calling legitimate processes

Scans internal network for other endpoints with SMB vulnerability and copies

Runs WannaCry Ransomware, encrypting users machine

The Need For A Multi-Method Prevention Approach



Isn't Windows Defender Enough?

Solution	Scenario			
	Detection rate before execution offline	Detection rate before execution online	Detection rate at execution offline	Detection rate at execution online
Palo Alto Networks Traps 4.1.0	*See **	*See **	99,81 %	99,79 %
CylanceProtect 1450	98,66 %	99,73 %	98,66 %	99,73 %
Kaspersky Endpoint Security 10	75,84 %	76,30 %	93,88 %	94,24 %
Sophos Endpoint Protection 2017 (11.5.6) with Intercept X (3.7.0)	53,38 %	72,06 %	65,73 %	87,34 %
Symantec Endpoint Protection Cloud	51,06 %	56,31 %	60,13 %	68,48 %
McAfee ENS 10.5	45,40 %	47,05 %	60,25 %	63,81 %
TrendMicro OfficeScan	25,13 %	28,19 %	55,41 %	59,39 %
Windows Defender	37,90 %	38,16 %	48,05 %	48,38 %

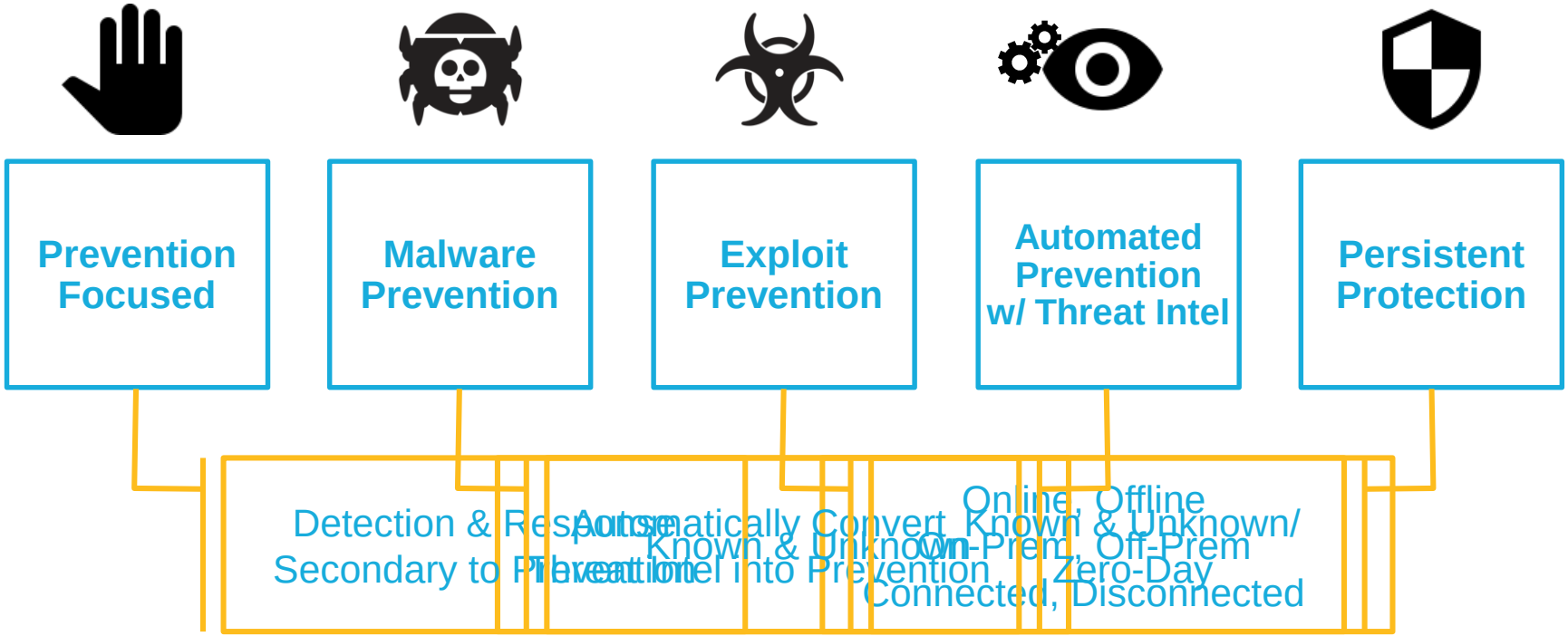
8000 malware samples tested
Source: SecureLink Germany Endpoint Protection Solutions Report 10/2017

Isn't Windows Defender Enough?

Solution	Scenario
	Detection rate Offline for Holiday Test-Scenario
Palo Alto Networks Traps 4.1.0	**99,81 %**
CylancePROTECT 1450	**98,66 %**
Kaspersky Endpoint Security 10	**75,59 %**
Sophos Endpoint Protection 2017 (11.5.6) with Intercept X (3.7.0)	**47,30 %**
McAfee ENS 10.5	**45,21 %**
Trend Micro OfficeScan	**25,26 %**
Symantec Endpoint Protection Cloud	**17,04 %**
Windows Defender	**11,81 %**

8000 malware samples tested – Holiday Test: 14 days offline
Source: SecureLink Germany Endpoint Protection Solutions Report 10/2017

Five Fundamental Capabilities of Any Endpoint Product



To Prevent Ransomware:

1. Delivery Methods
2. Payload

The Attack Sequence

Attack Sequence

Conduct Reconnaissance

Compromise Endpoint

Establish Control Channel

Pursue Objectives

Delivery

- Web-Based Exploitation
- Malware Download
- Email Attachments

Malicious Action

- Exploit Good Applications
- Run Malware
- Run Scripts
- Run MS Office Macros
- Exploit Operating System
- Escalate Privileges

Traps Multi-Method Exploit Prevention

Reconnaissance Protection

Automatic Prevention of Vulnerability Profiling Used by Exploit Kits

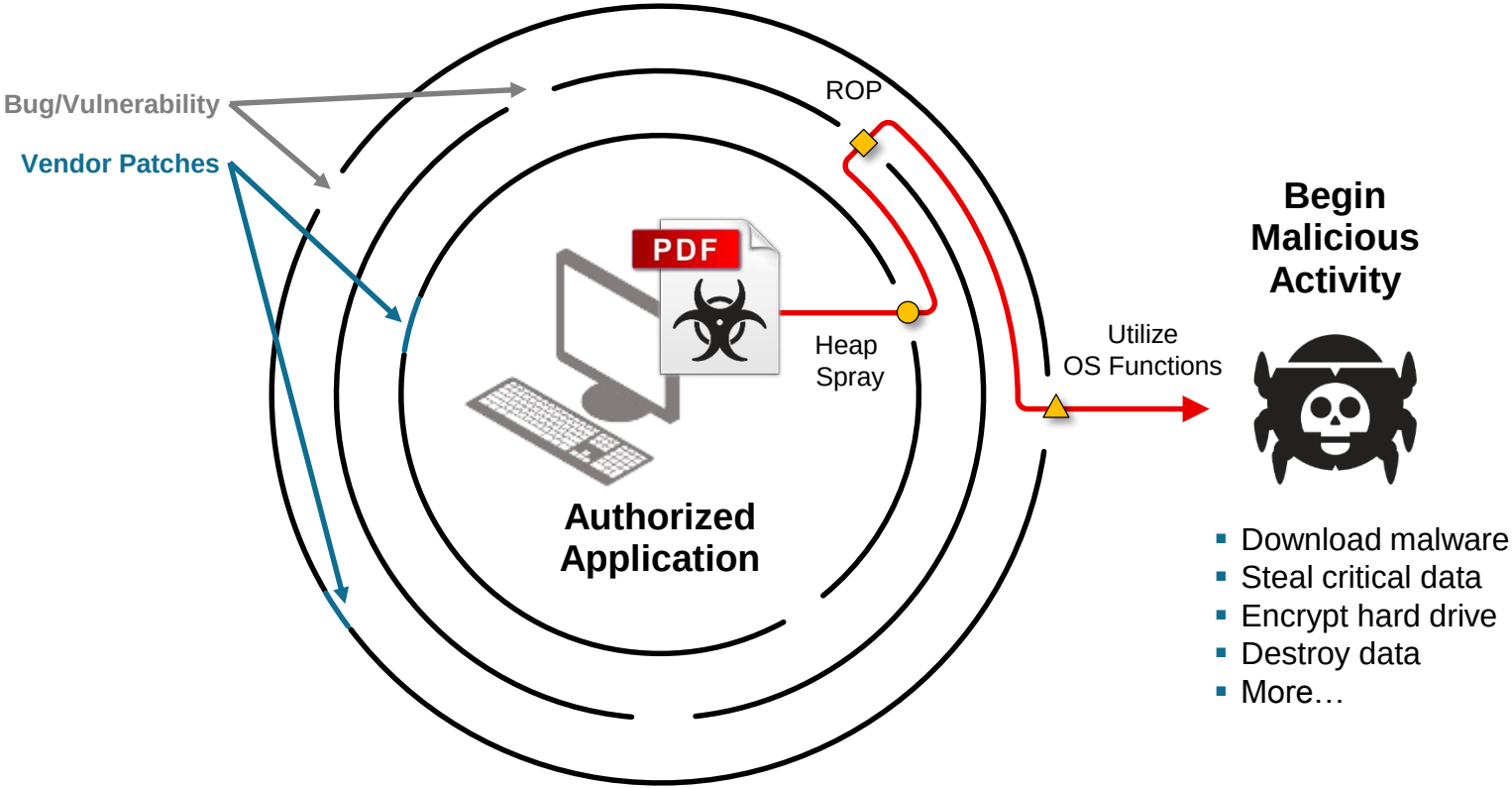
Technique-Based Exploit Prevention

Blocking of Exploit Techniques Used to Manipulate Good Applications

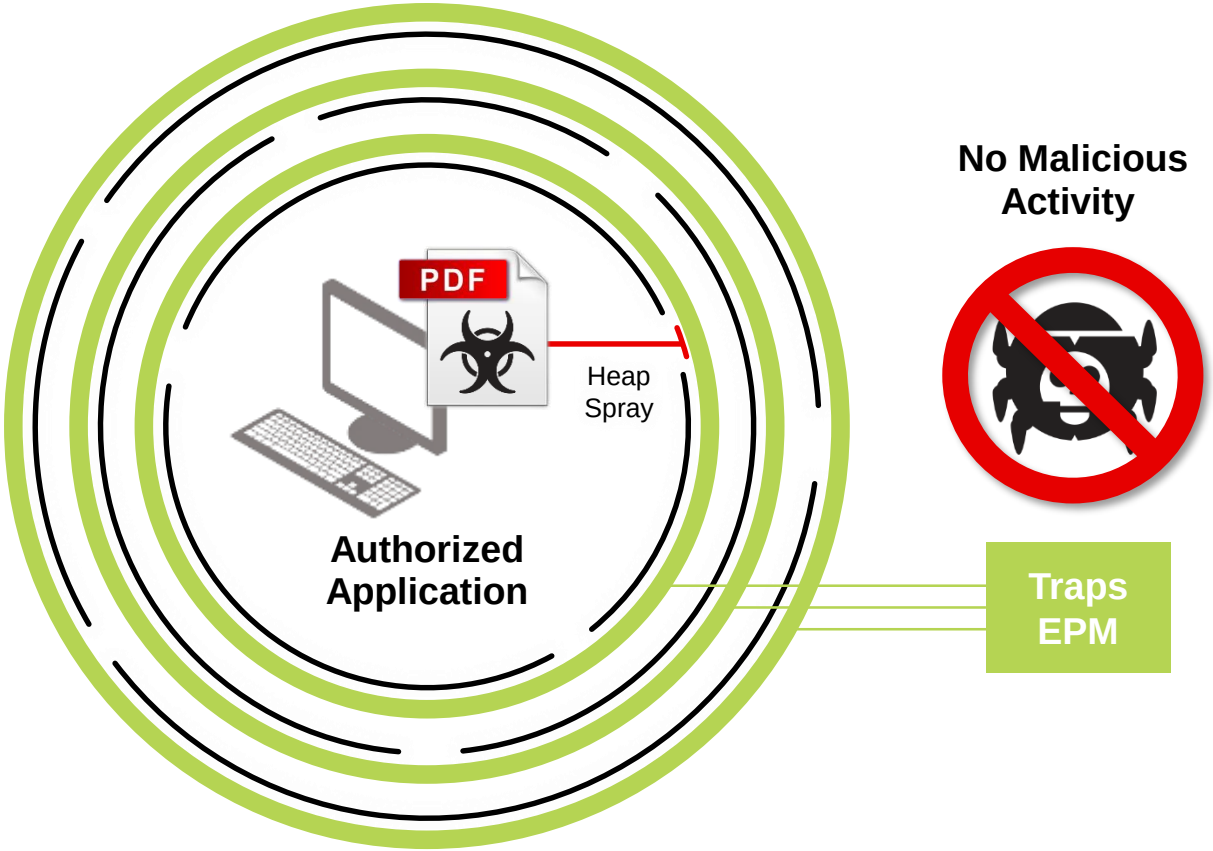
Kernel Protection

Protection Against Exploits Targeting or Originating from the Kernel

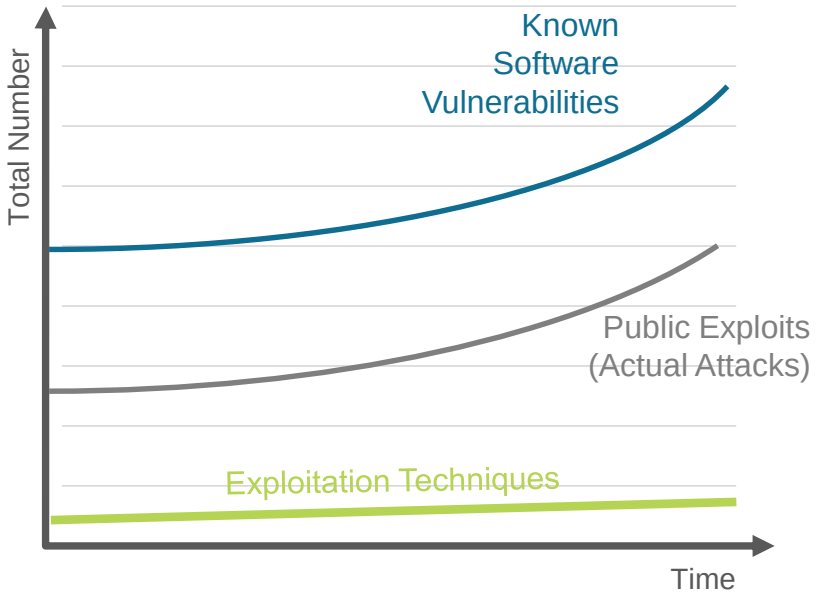
Exploits Subvert Authorized Applications



Traps Blocks Exploit Techniques



Blocking Exploitation Techniques Is the Most Effective Approach

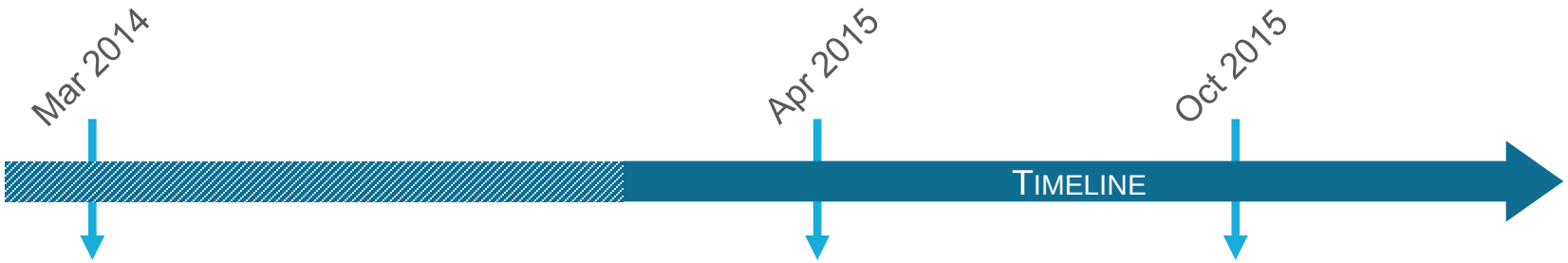


Patching — Requires Prior Knowledge, Proactive Application

Signature / Behavior — Requires Prior Knowledge of Weaponized Exploits

Traps — Requires No Patching, No Prior Knowledge of Vulnerabilities, and No Signatures

Value of Technique-based Exploit Prevention



Traps Version 2.3.6 Released

Vulnerability Discovered in Adobe Flash Player (CVE-2015-0359)

Attackers Attempted to Exploit Vulnerability.

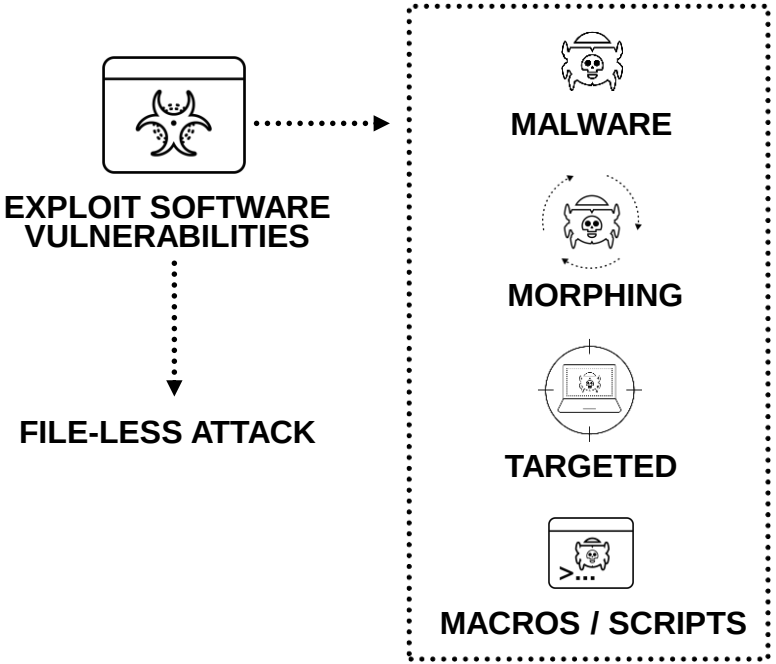
Traps Blocked the Attempt.

Traps v2.3.6

No Updates or Patches Since Installation

Traps Prevents Zero-day and Unknown Exploits That Have Yet to be Discovered

Multi-Method Malware Prevention



REDUCE THE ATTACK SURFACE
Policy Controls, Child Processes, Execution Restrictions

PREVENT KNOWN MALWARE
WildFire Threat Intelligence

PREVENT UNKNOWN MALWARE
Local Analysis via Machine Learning

DETECT ADVANCED THREATS
WildFire Inspection & Analysis

Traps Multi-Method Malware Prevention

Threat Intelligence

Prevents Known Threats

Local Analysis

Prevents Unknown Threats

Dynamic Analysis

Detects Advanced Unknown Threats

Malicious Process Prevention

Prevents Script-Based & File-Less Threats

Ransomware Protection

Additional Ransomware Protection

Preventing Known Threats

WildFire Threat Intelligence

- **Delivers over 230,000 new protections daily in 5min intervals**
- **A 2-way street across 19,500 customers and millions of sensors**
    - *Enterprises*
    - *Governments*
    - *Tech Partners*
    - *3rd Party Intel Feeds*
    - *Human Analysis from Unit 42*
    - *Other Palo Alto Networks components*
- **Continuously analyzed and utilized by the entire Next-Gen Security Platform of Palo Alto Networks**

Platform Benefits For Stand-Alone Traps Deployments

1. **Automatic blocking of malware first encountered elsewhere**

2. **Increased effectiveness of Local Analysis as machine learning model is trained**

Preventing Unknown Threats

Local Analysis

- Windows and Mac, for online or offline users
- No signatures or scanning and invisible to end users
- Based on Machine-Learning trained from WildFire

WildFire Analysis

- Runs in the cloud enabling significant computing power without affecting users
  - Static Analysis via Machine Learning
  - Dynamic Analysis
  - Bare-Metal Analysis
- Acts as a secondary check to reduce potential FPs

Preventing Unknown Threats

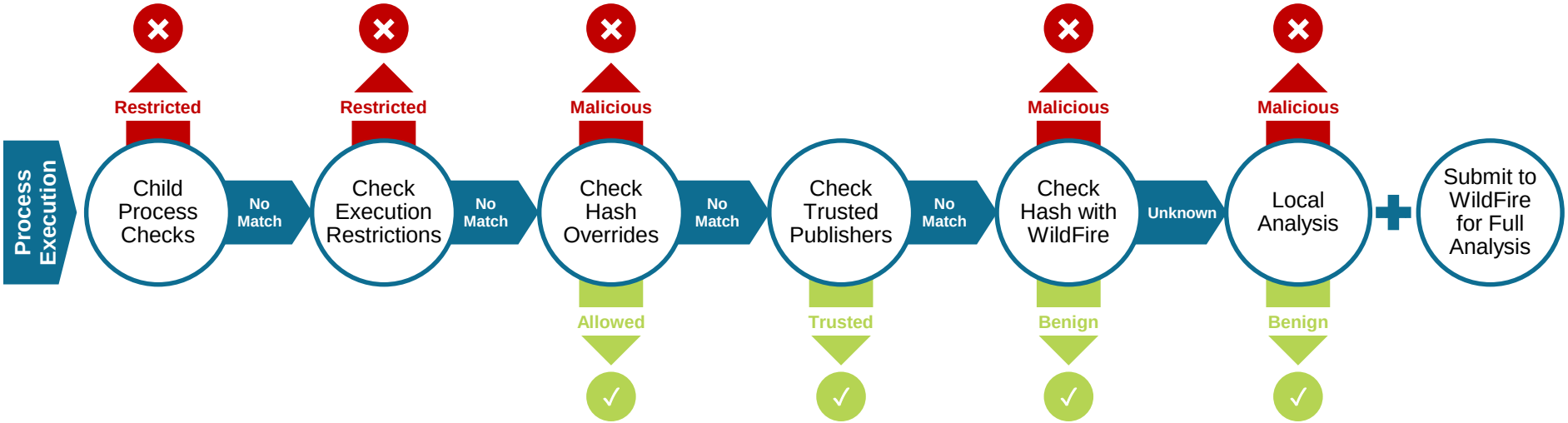
Granular Child Process Protection

- Customizable protection against script-based and file-less attacks
- Delivered out-of-the-box and automatically updated based on new threat intelligence without user action

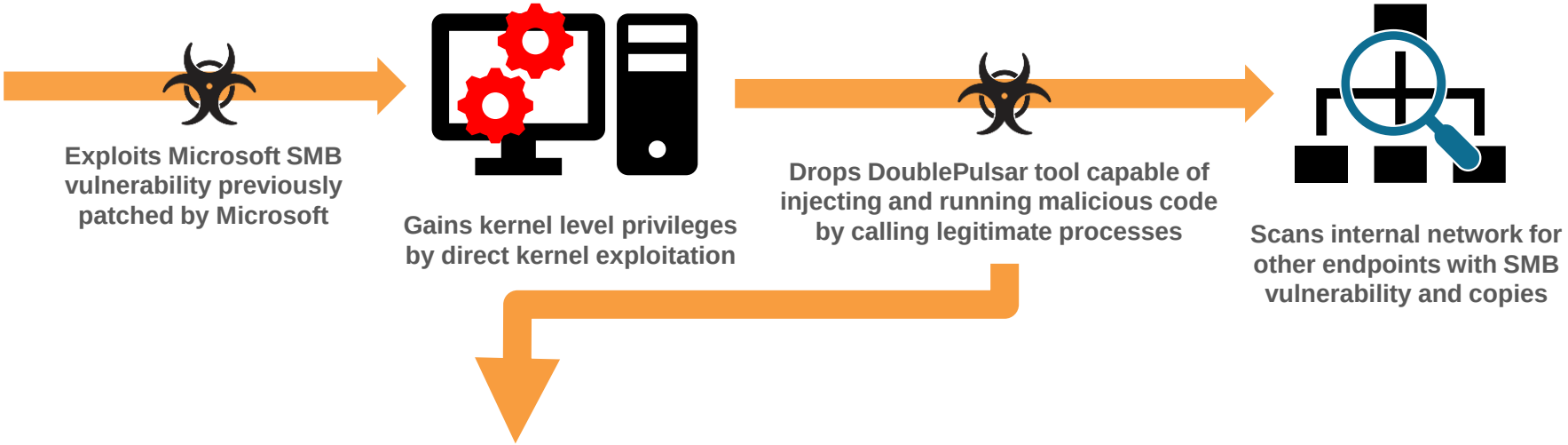
Behavior-Based Ransomware Protection

- An additional layer of prevention to pre-existing malware and exploit prevention capabilities
- Not reliant on signatures or known samples
- Able to discern between good and malicious encryption

Traps Malware Prevention Flow

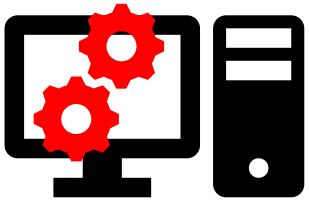


Traps vs. WannaCry



Traps vs. WannaCry

Exploits Microsoft SMB vulnerability previously patched by Microsoft



Gains kernel level privileges by direct kernel exploitation

Drops Doubl… capable of injecting and ru… malicious code by calling legitimate processes

Kernel Exploit Prevention

Child Process Protection

Scans internal network for other endpoints with SMB vulnerability and copies

Blocks processes from accessing infected shellcode

Blocks executables from spawning malicious processes necessary for propagation

Local Analysis

Malicious EXE Detected

Dynamic Analysis

Threat Intelligence

Known Threat Prevented

Behavior-Based Ransomware Protection

Ransomware behavior detected and stopped

annaCry Ran… ypting users mach…

Traps Delivers Flexible Platform Coverage

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)
- macOS 10.13 (High 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.

Flexible and Scalable, With Minimal Footprint

Flexible

- Supports physical & virtual systems
- Supports Windows & Mac
- Up to 150,000 endpoints/ESM DB

Minimal Footprint

- 0.1% CPU Load
- 50 MB RAM
- 200 MB HD
- No scanning
- No virus-signature databases