# The Rise of Ransomware Is Prevention Possible?

Patrick Reischl, CISSP

*Specialist System Engineer – Traps – Nordics, Baltics and Eastern Europe*


Abfahrt
Linie
Ooops, your importa
HD Webcam
FAKE
NEWS
Cyber Attack
sunrise
8.15
HACKERS PARA
BMG | MIS

# *The Impact of Ransomware*

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

38% Global Rise in
Cyber Insurance Demand

Bitcoin nearly 2x in
3 months


**Over $1 Billion Dollars in 2016 on ransom alone**

# The Impact of Ransomware

## How did it impact your business?

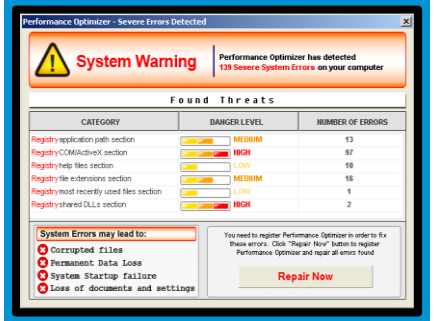
- Honda, Renault, and Nissan had to stop production
- UK National Health Service forced to run on emergency-only basis during attack
- Public Transit systems affected gave free ridership until the issue was resolved

## 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?*

# Evolution path

## MISLEADING APP




## FAKE AV


## LOCKER RANSOMWARE

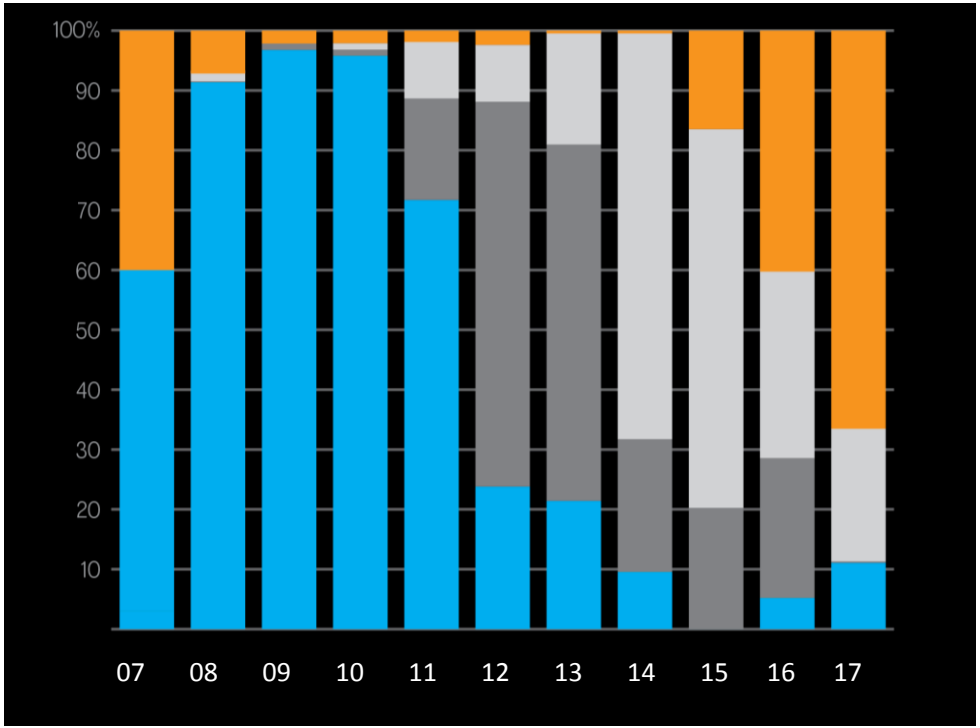

## CRYPTO RANSOMWARE

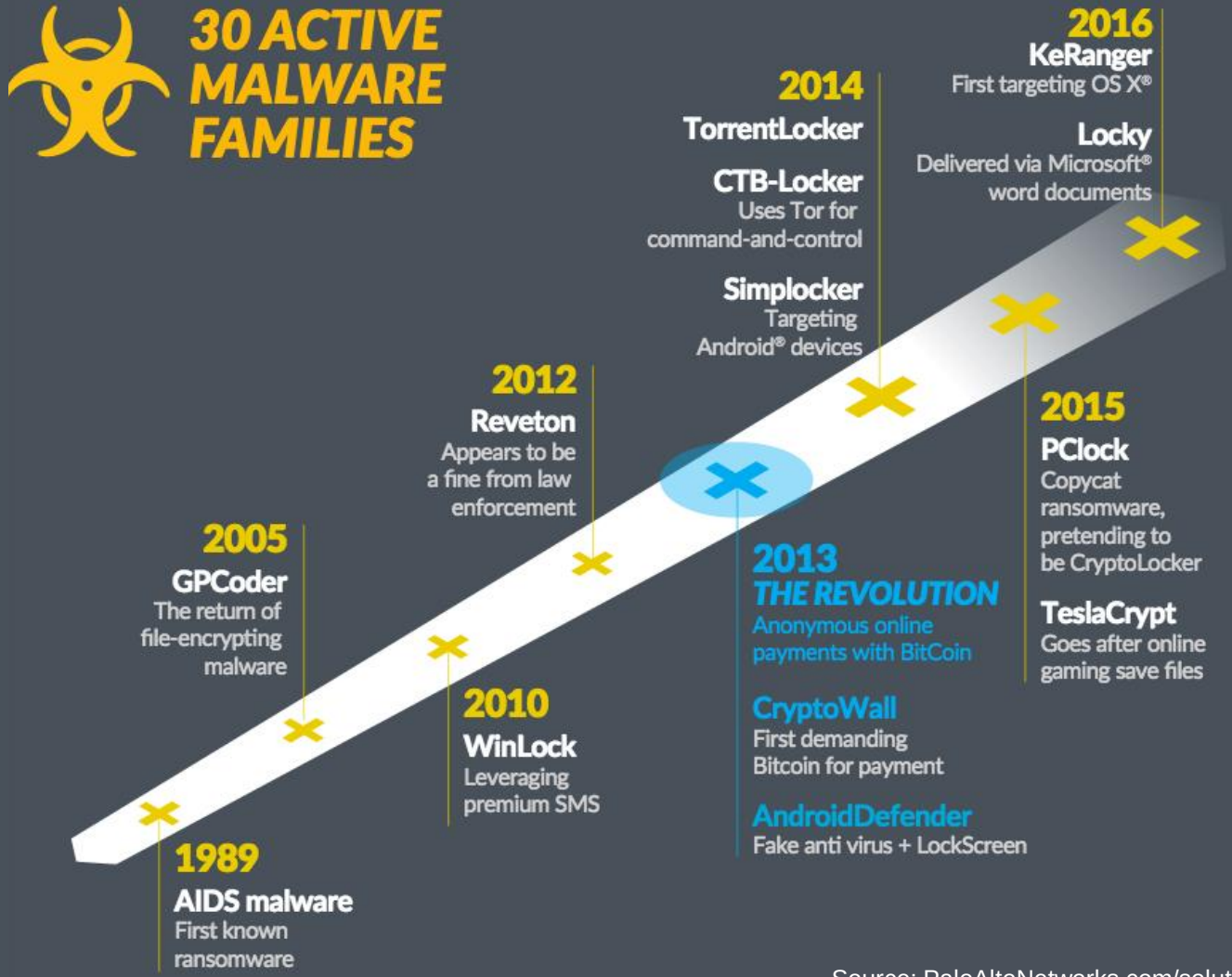

**2005-2009** → **2010-2011** → **2012-2013** → **2014 -->**

**"FIX"** | **"CLEAN"** | **"FINE"** | **"FEE"**

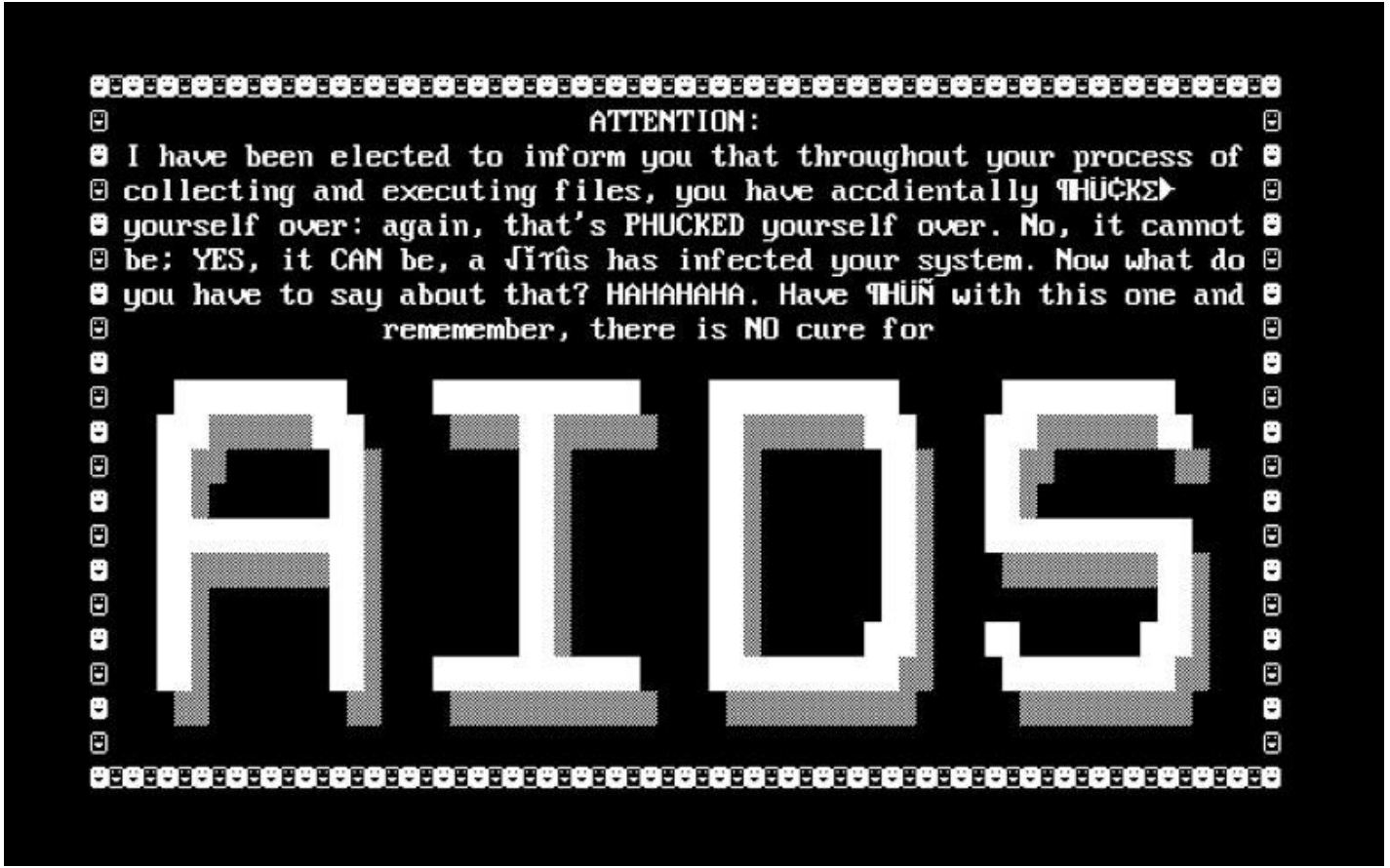
# Growing Dominance of Crypto-Ransomware

MISLEADING APP | FAKE AV | LOCKER RANSOMWARE | CRYPTO RANSOMWARE

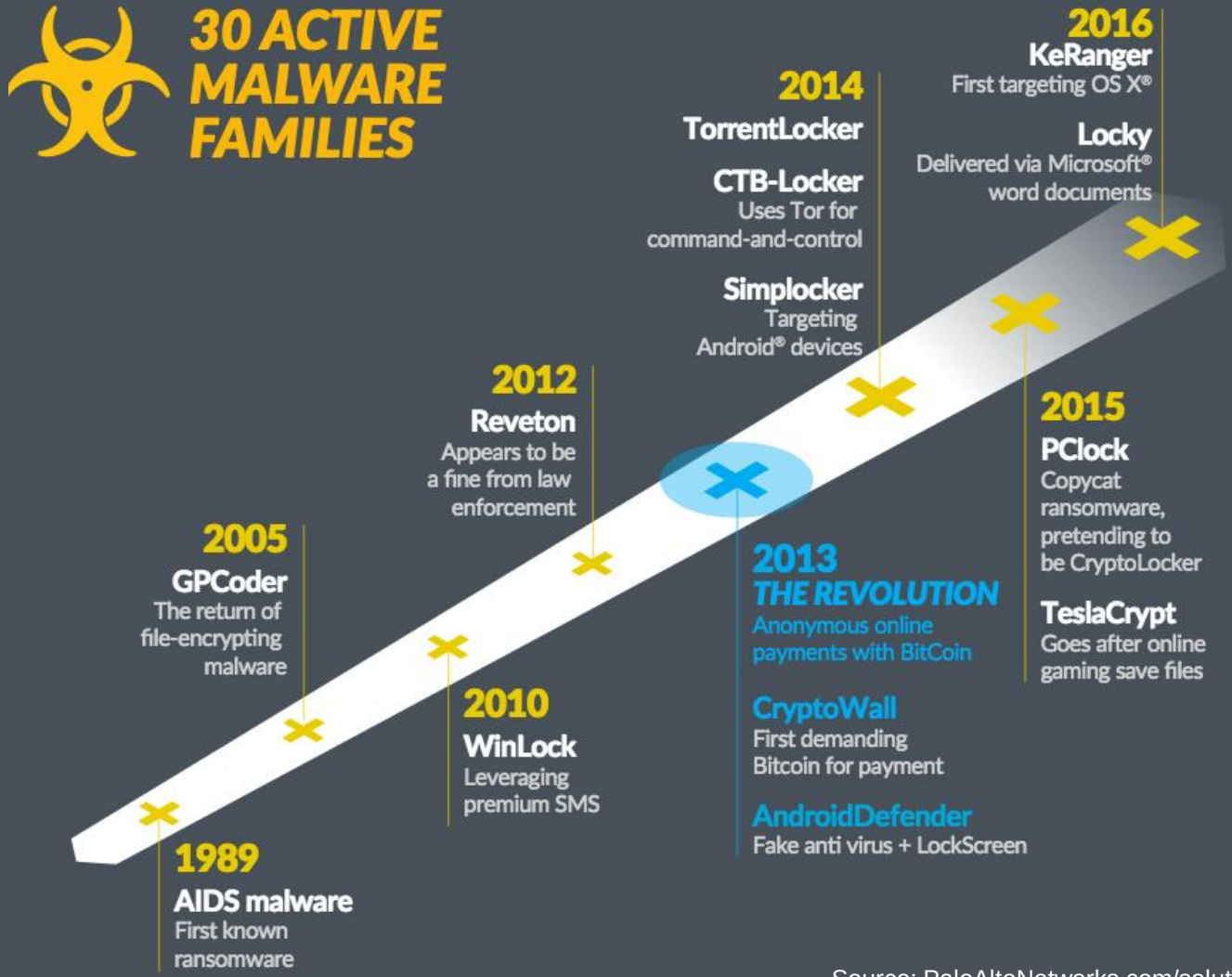





Source: PaloAltoNetworks.com/solutions/initiatives/ransomware

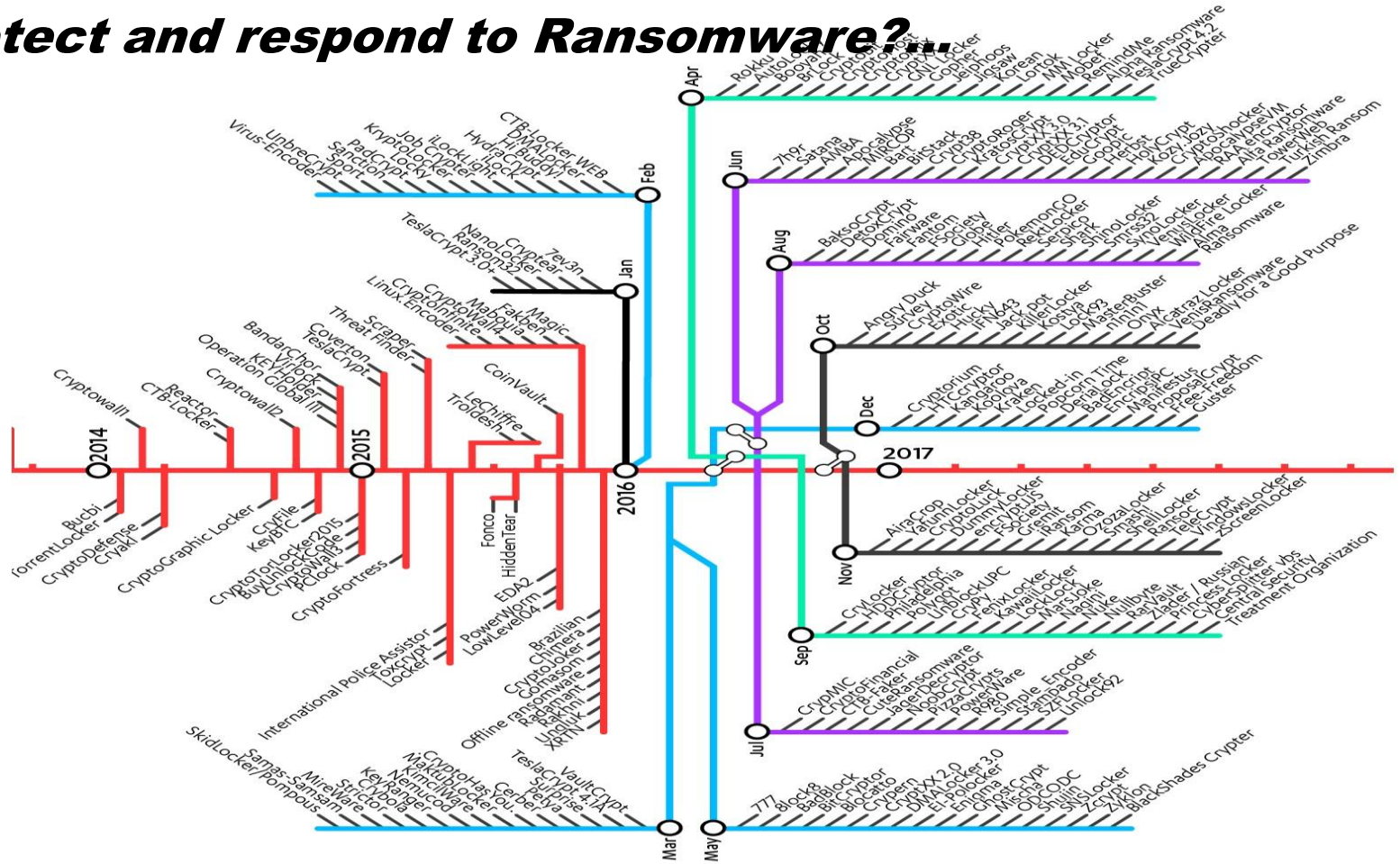


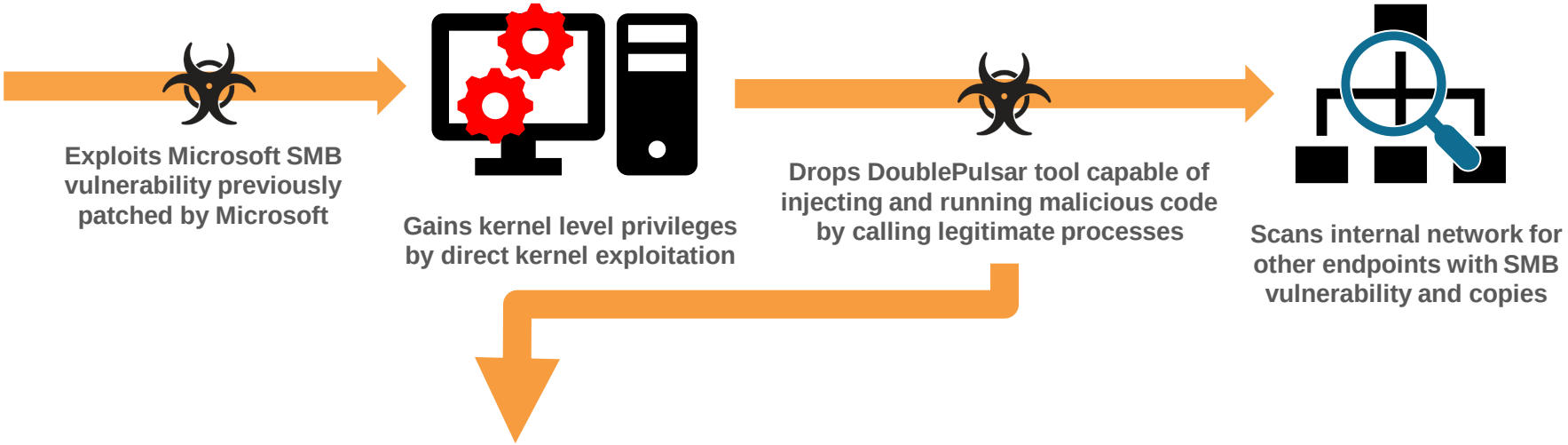



Source: PaloAltoNetworks.com/solutions/initiatives/ransomware

# Detect and respond to Ransomware?...



# ...Prevent the Ransomware?



Exploits Microsoft SMB vulnerability previously patched by Microsoft

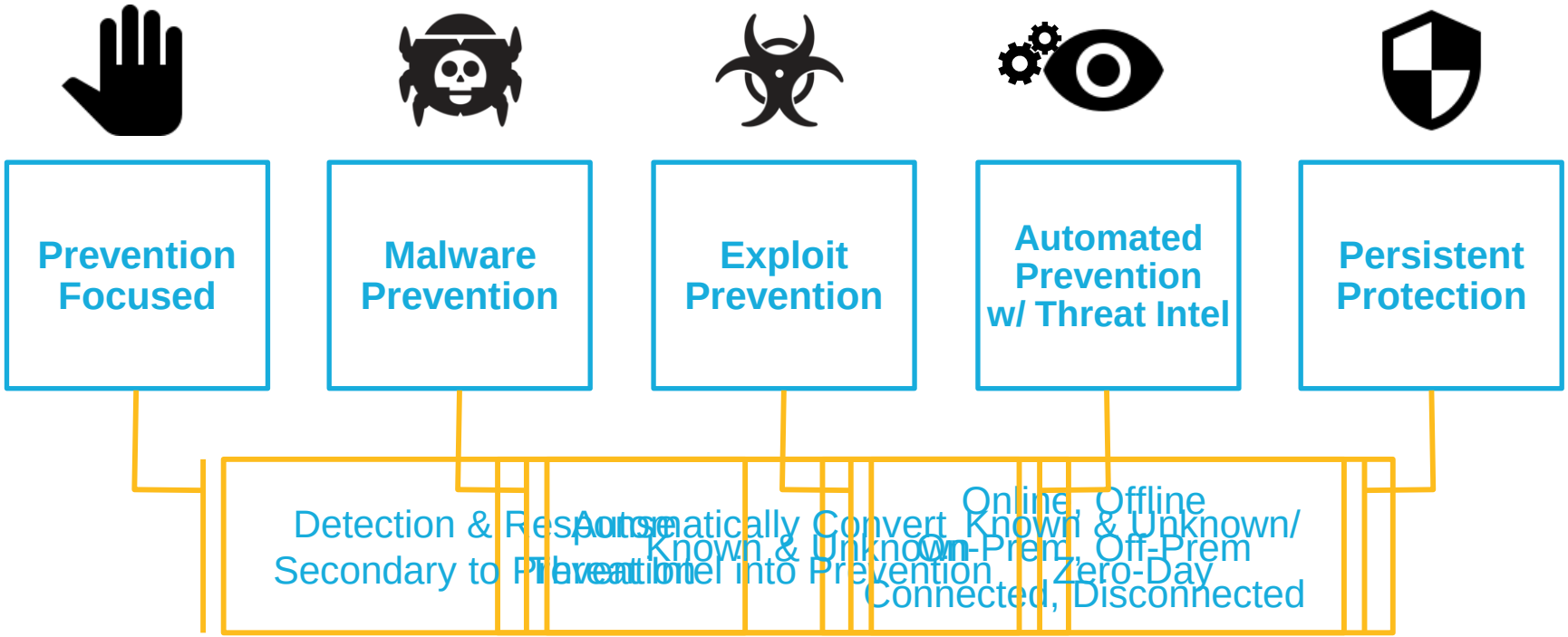
Gains kernel level privileges by direct kernel exploitation

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

# *Five Fundamental Capabilities of Any Endpoint Product*



***Is Real-Time, Automatic Prevention of Attacks that use Unknowns and Zero-Days Possible?***

**To Prevent Ransomware:**

1. **The Payload**
2. **Delivery Methods**

# The Attack Sequence

Attack Sequence

Conduct Reconnaissance

Compromise Endpoint

Establish Control Channel

Pursue Objectives

Exploit Software Vulnerabilities

- Weaponized Data Files/Content
- Subvert Existing Applications

Execute Malicious Programs

- Self-Contained, Malicious Program
- Contain Necessary Executable Code

paloalto NETWORKS

# The Attack Sequence

Attack Sequence

Conduct Reconnaissance

Compromise Endpoint

Establish Control Channel

Pursue Objectives

**Delivery**

- Exploit Kits
- Drive by Download
- Email Attachments

**Malicious Action**

# Exploit Kits

User visits a compromised website

Malicious code or ad redirects to exploit kit landing page

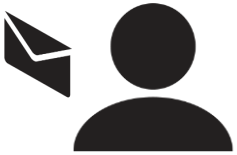
Exploit kit page loads; determines best way to compromise user endpoint

Exploit kit compromises user endpoint

Exploit kit delivers ransomware

Ransomware encrypts data and holds it for ransom

# Email Attachments



User receives targeted email with infected file


User opens file, thinking it is a legitimate document


Office runs macro, downloads ransomware from URL embedded in doc

Ransomware encrypts data and holds it for ransom

# Drive-by Download

User visits a compromised website

Website serves exploit to compromises user endpoint

Exploit downloads ransomware

Ransomware encrypts data and holds it for ransom

# The Attack Sequence

Attack Sequence

Conduct Reconnaissance

Compromise Endpoint

Establish Control Channel

Pursue Objectives

**Delivery**

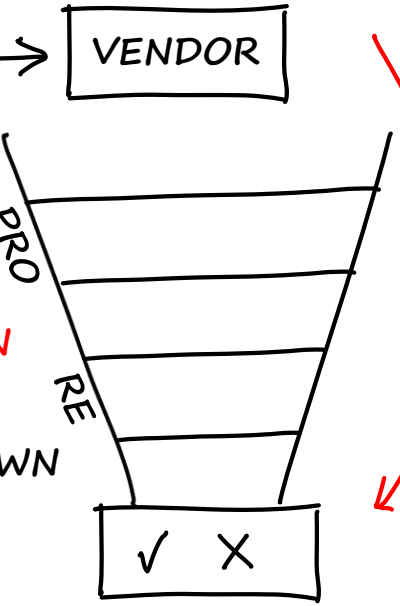
- Web-Based Exploitation
- Malware Download
- Email Attachments

**Malicious Action**

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

paloalto NETWORKS

< 1 DAY




✓ X =FP

UNKNOWN

KNOWN

3 SEC
RANSOM

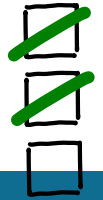
EP

? NETWK

? CLOUD

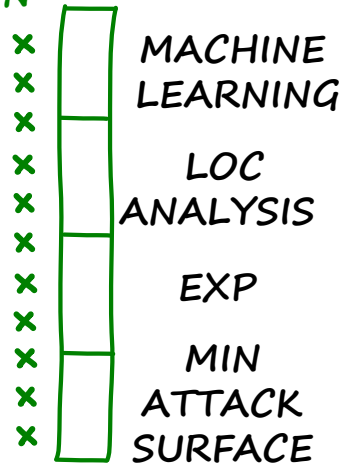
PREVENT

RESPOND

$ 750M
Wanacrypt


UNKNOWN




KNOWN++

paloalto NETWORKS

# Q&A