

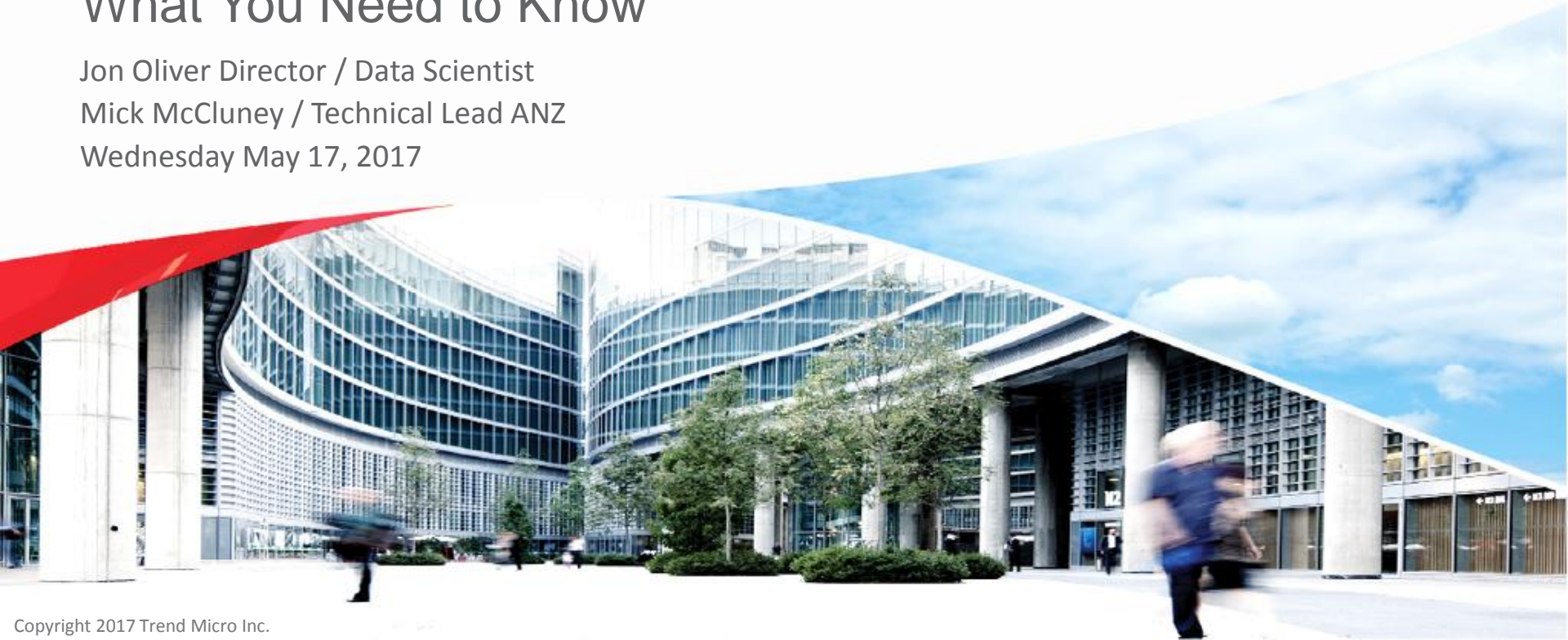
WannaCry/WCRY Ransomware

What You Need to Know

Jon Oliver Director / Data Scientist

Mick McCluney / Technical Lead ANZ

Wednesday May 17, 2017





**CYBER ATTACK TARGETS HOSPITAL
COMPUTER SYSTEMS ACROSS THE UK**

FOX NEWS ALERT

Abfahrt

Linie

Ziel

Gleis

Gleis

Zeit

Über

Nach

Olbernhau

8

11

10

8

9

5

14

11

22:10

RB81

22:30

RB30

22:31

RB30

22:36

RB80

22:36

RB45

22:44

RE6

22:45

RB89

23:30

RB30

Flöha - Pockau-Lengefeld

Flöha - Freiberg

- fährt heute

Hohenstein

Flöha - Zsch

fährt heute von

Geithain - B

Einsiedel - Thalheim (Erzgeb)

Flöha - Freiberg (Sachs) - Tharandt

fährt heute von Gleis 11

Hbf

(S) Hbf

g-B. Süd

Hbf

Aue (Sachs)

Dresden Hbf

Oops, your files have been encrypted!

Was geschah mit meinem Computer?

Ihre wichtigen Dateien sind verschlüsselt. Ihre Dokumente, Fotos, Videos, Datenbanken und andere Dateien sind nicht mehr zugänglich, weil sie verschlüsselt wurden. Versteht sich, Sie sind besorgt, wenn Sie Ihre Dateien nicht wiederherstellen können, aber wir verstehen Sie.

Können ich meine Dateien wiederherstellen?

Klar, wir garantieren, dass Sie alle Ihre Dateien sicher und einfach wiederherstellen können. Aber Sie haben noch ein Problem. Versuchen Sie jetzt, indem Sie auf "Decrypt" klicken.

Wie bezahlt ich?

Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf "Bitcoin".

Send \$200 worth of bitcoin to this address:

1B8YDQp... (Bitcoin address)

Check Payment Decrypt

06 - 12.09.2017

BMG | MIS

Worldwide Outbreak



192 Countries
300K Windows
machines

The screenshot shows the Trend Micro Security Intelligence Blog interface. At the top, the Trend Micro logo and 'TrendLabs SECURITY INTELLIGENCE Blog' are visible, along with a search bar and social media icons. The main article is titled 'Massive WannaCry/Wcry Ransomware Attack Hits Various Countries' and is categorized under 'Malware'. The article text states: 'Earlier this year, two separate security risks were brought to light: CVE-2017-0144, a vulnerability in the SMB Server that could allow remote code execution that was fixed in March, and WannaCry/Wcry, a relatively new ransomware family that was found in late April. Previously WannaCry was spread via Dropbox URLs embedded in emails, but new variants are now spreading via this previously found SMB vulnerability. This has resulted in one of the most serious ransomware attacks to hit'. To the right of the article is a red icon of a shopping bag with a dollar sign. On the right side of the page, there are sections for 'Featured Stories' and 'Business Process Compromise'.



TLP: WHITE

FBI *FLASH*

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION



13 May 2017

Alert Number

MC-000081-MW

WE NEED YOUR HELP!

Indicators Associated With WannaCry Ransomware

This is a joint product with the Department of Homeland Security.

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

Timeline



Shadow Brokers Leaks Hacking Tools: What it Means for Enterprises

April 18, 2017

On April 14, several hacking tools and exploits targeting systems and servers running Microsoft Windows were leaked by hacking group Shadow Brokers. Several of these were reportedly tools targeting financial organizations worldwide. The hacking group initially put these troves of stolen malware up for sale last year but failed, and has incrementally released them since.



Microsoft Patch March 14, 2017

WannaCry/WCRY 1.0 April 14, 2017



WannaCry/WCRY 2.0 May 12, 2017



Shadow Brokers Leak Tools April 14, 2017

MS17-010



Microsoft Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144)

Published date: March 15, 2017



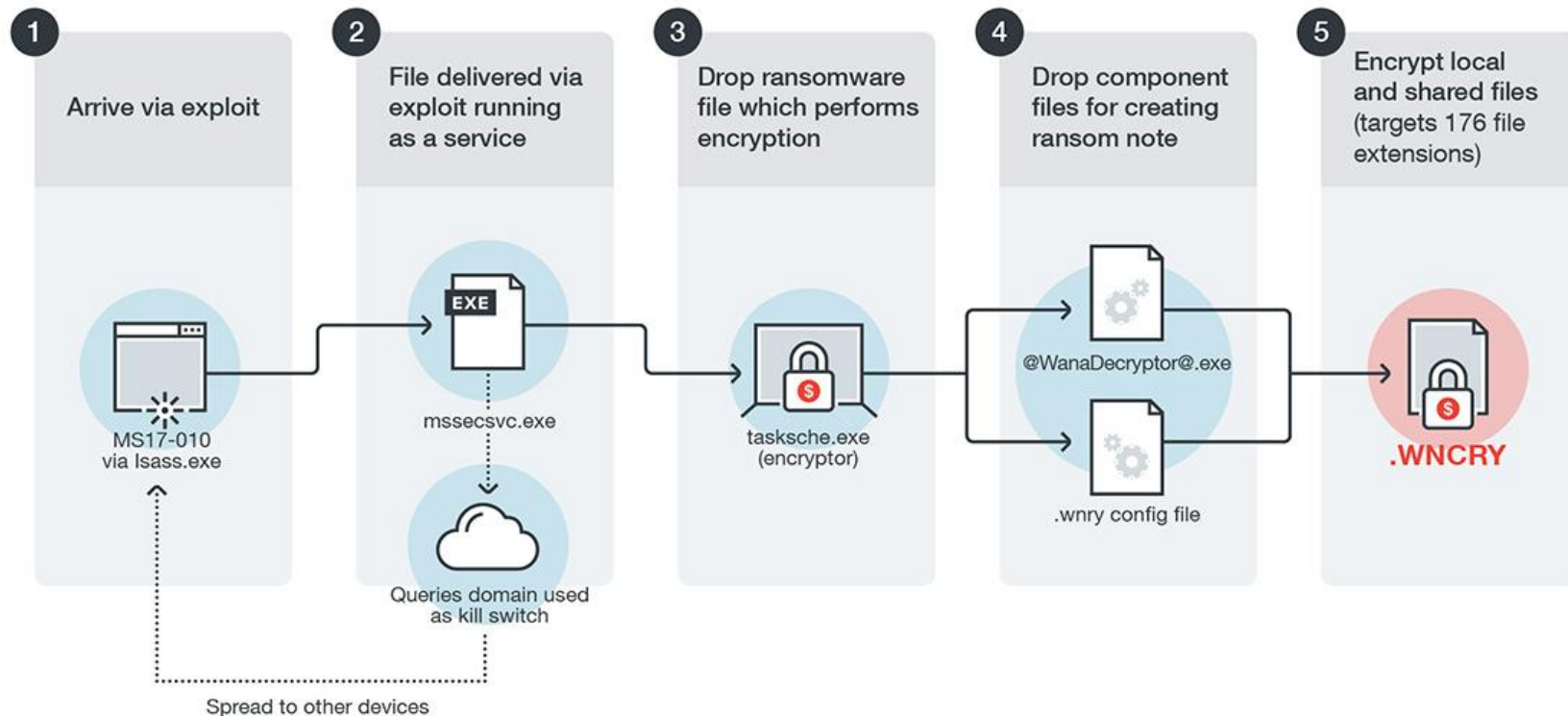
Severity: CRITICAL
CVE Identifier: CVE-2017-0144

Ransomware Infection Popup



- Demands payment in Bitcoin or files will be deleted
- Ransom notes observed in 27 languages
- Encrypts shared and local files (176 file types)

Infection Chain





WIKIPEDIA
The Free Encyclopedia

EternalBlue

From Wikipedia, the free encyclopedia

EternalBlue, sometimes stylized as **ETERNALBLUE**,^[1] is an [exploit](#) which some believe to have been developed by the U.S. [National Security Agency](#) (NSA). It was released by the [Shadow Brokers](#) hacker group on April 14, 2017.^{[2][1][3][4][5]}

MS17-010, Port 445, SMBv1

March 14, 2017

 TechNet 

United States (English) [Sign in](#)

Security TechCenter

[Home](#) [Security Updates](#) [Tools](#) [Learn](#) [Library](#) [Support](#)

Security Advisories and Bulletins > Security Bulletins > 2017 ▾

...
MS17-013
MS17-012
MS17-011
MS17-010
MS17-009
MS17-008
MS17-007
MS17-006
MS17-005
MS17-004

Microsoft Security Bulletin MS17-010 – Critical

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see [Microsoft Knowledge Base Article 4013389](#).

 Print
 Share

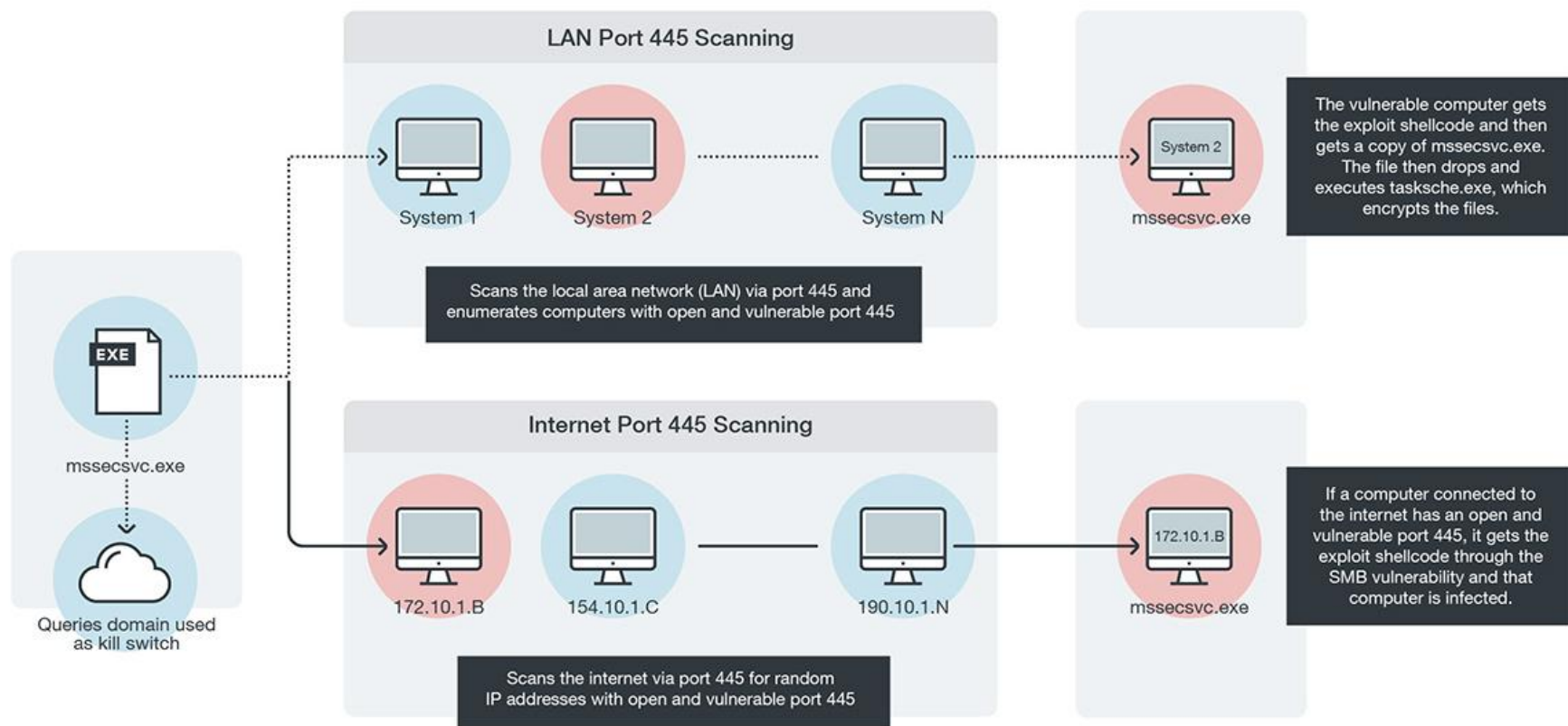
IN THIS ARTICLE

- Executive Summary**
- Affected Software and Vulnerability Severity Ratings
- Vulnerability Information
- Security Update Deployment
- Acknowledgments
- Disclaimer
- Revisions

On this page

- [Executive Summary](#)
- [Affected Software and Vulnerability Severity Ratings](#)
- [Vulnerability Information](#)
- [Security Update Deployment](#)
- [Acknowledgments](#)
- [Disclaimer](#)
- [Revisions](#)

Propagation via SMB v1



User interaction is not necessary for the malware to propagate



- *Exposed devices
- *External devices
- *Devices that re-enter the network
- *Devices connected by VPN



port:445 os:windows 'SMB version: 1'

Exploits

Maps

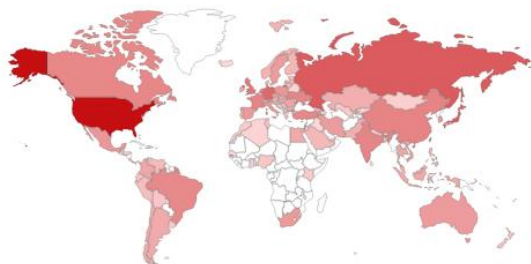
Share Search

Download

TOTAL RESULTS

287,925

TOP COUNTRIES



United States	113,781
Russian Federation	19,089
Taiwan, Province of China	17,007
Japan	15,917
Germany	13,096

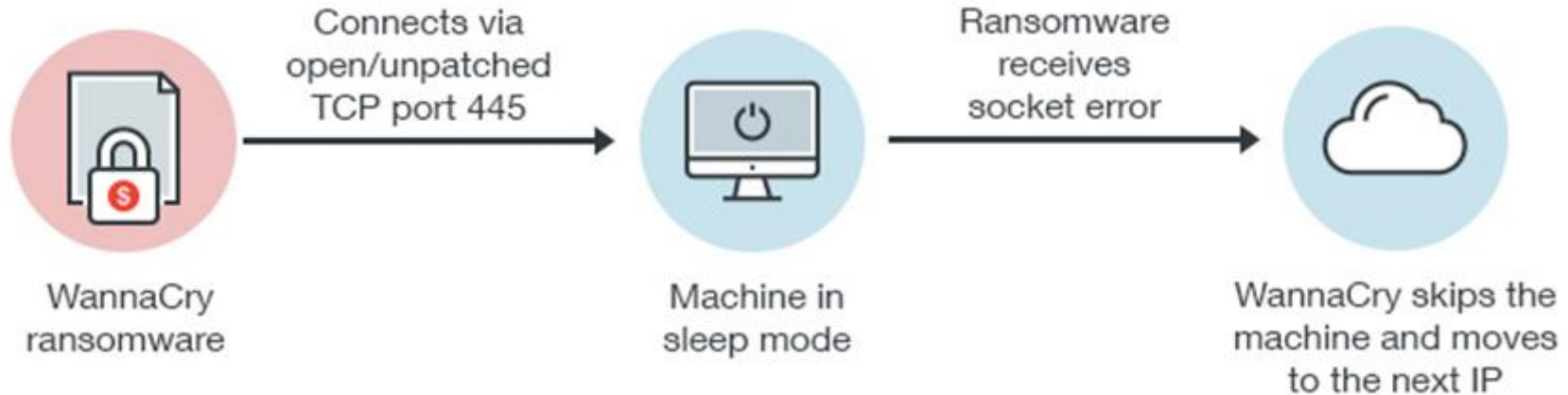
TOP OPERATING SYSTEMS

Windows Server 2008 R2 E...	54,461
Windows Server 2012 R2 S...	47,686
Windows Server 2008 R2 S...	32,065
Windows 6.1	16,723
Windows Server 2012 R2 D...	15,235

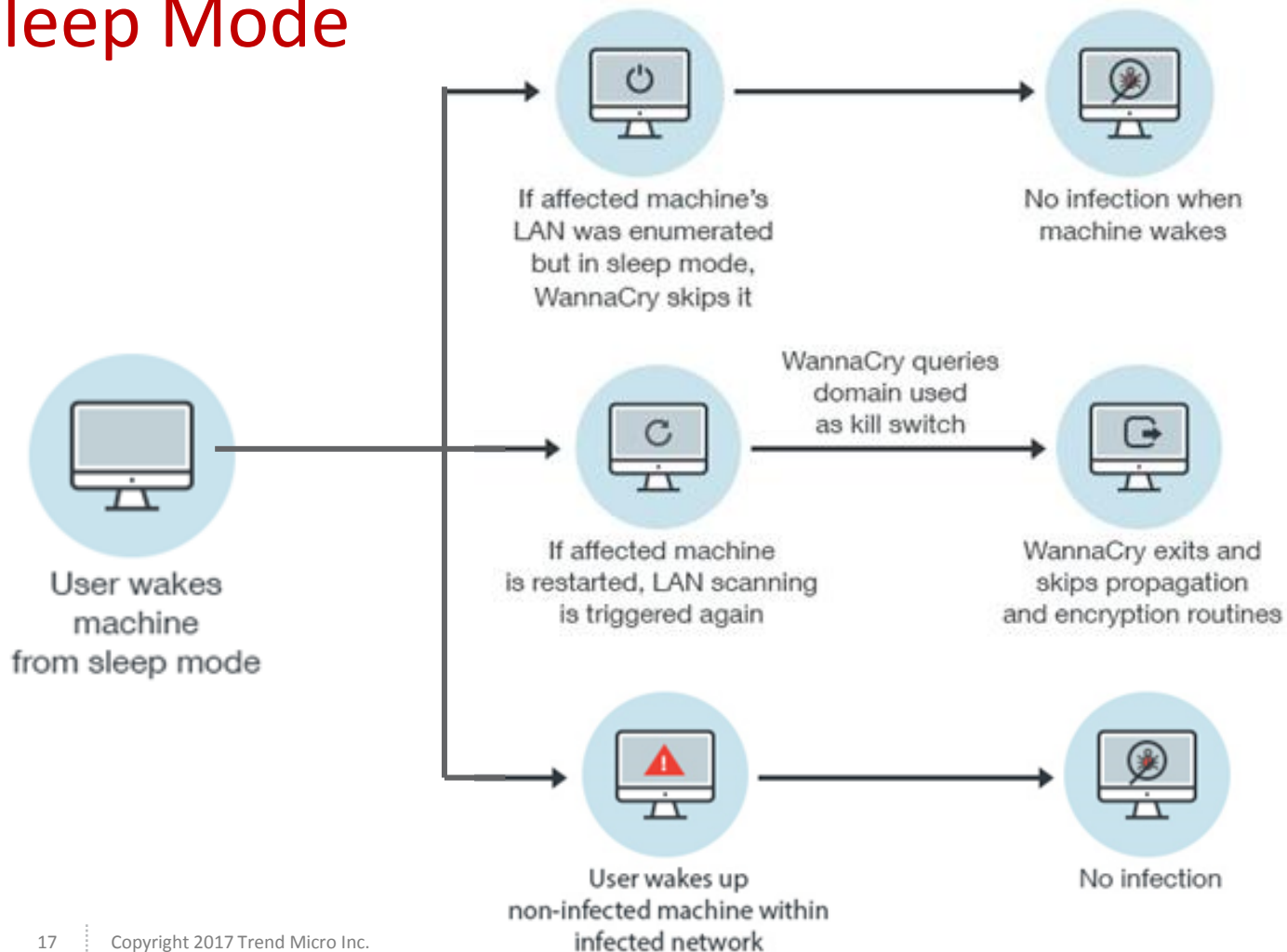
WANNACRY Kill Switch

```
v4 = InternetOpenA(0, 1u, 0, 0, 0);  
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...  
if ( v5 )  
{  
    InternetCloseHandle(v4);  
    InternetCloseHandle(v5);  
    result = 0;  
}  
else  
{  
    InternetCloseHandle(v4);  
    InternetCloseHandle(0);  
    sub_408090();  
    result = 0;  
}  
return result;
```

Sleep Mode



Sleep Mode



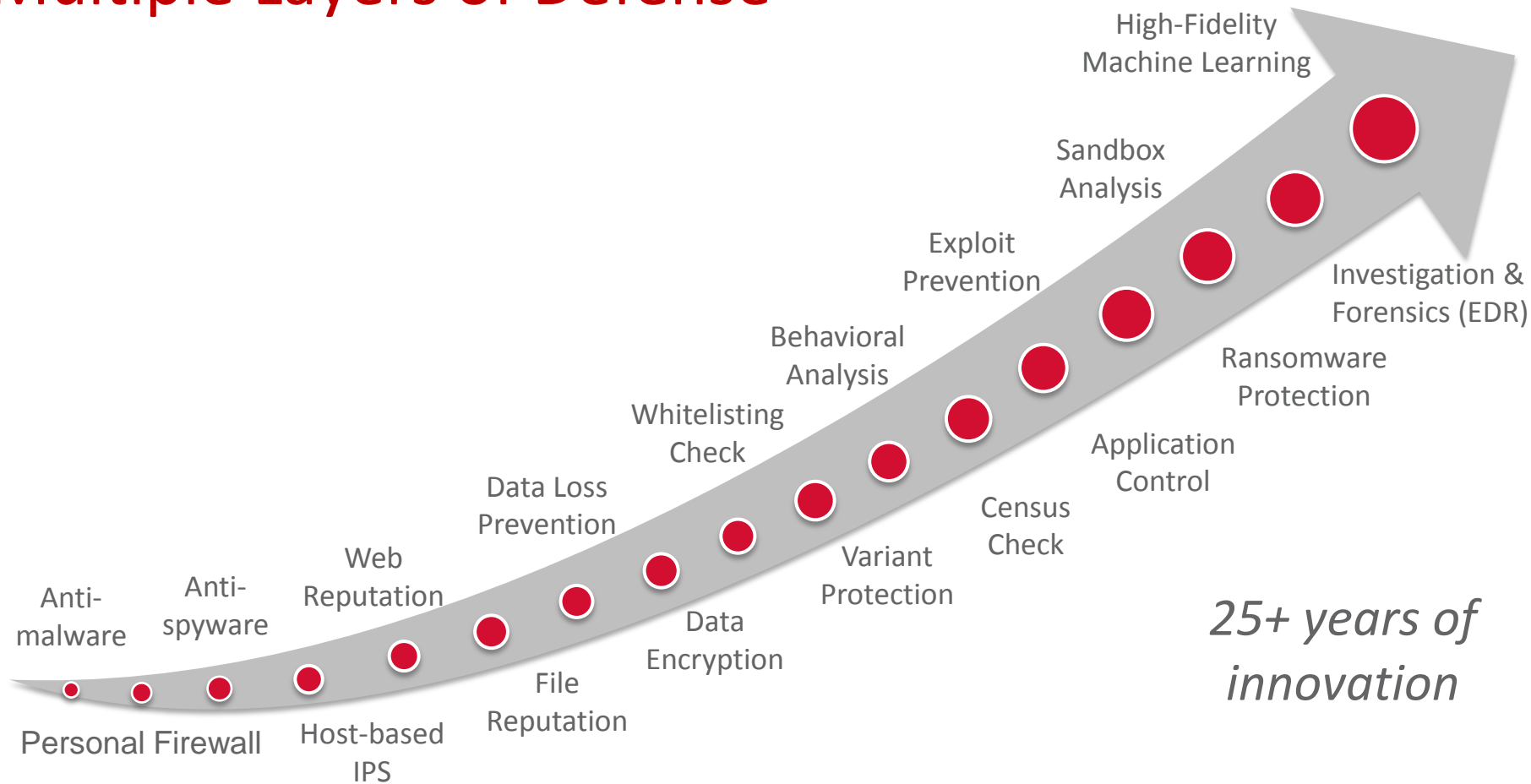
The background is a solid red color with a series of overlapping, curved, and flowing lines in various shades of red and dark red, creating a sense of movement and depth. The lines originate from the right side and sweep across the frame towards the left.

Minimize Risk of Threats

Recommended Critical Actions - General

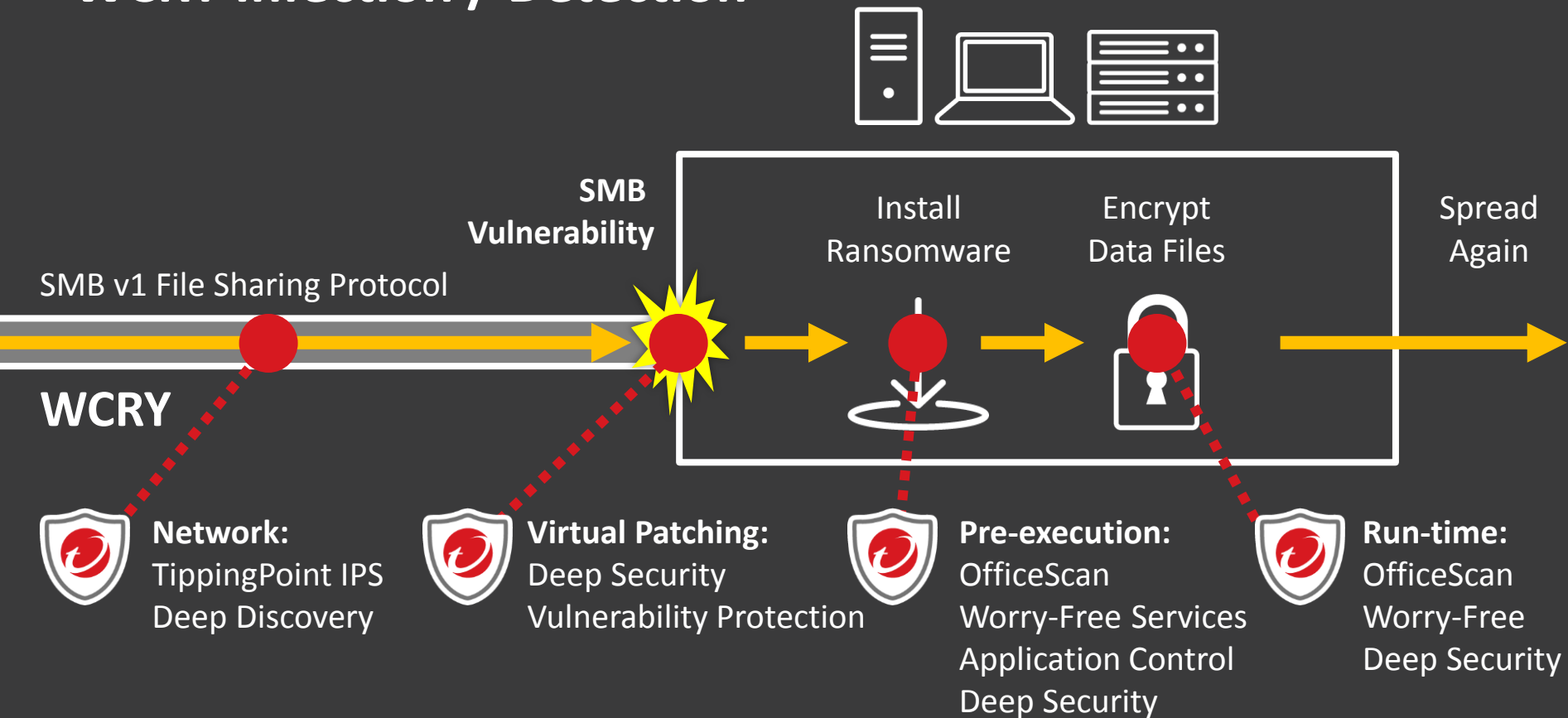
- ✓ **Backup.**
- ✓ **Patch Immediately** - all Windows-based machines (servers and workstations) should be updated to protect against MS17-010
- ✓ Disable SMBv1 on non-essential servers and systems
- ✓ Ensure all security solutions have updated patterns/signatures and optimal configuration settings
- ✓ Deploy firewalls and intrusion prevention systems (IPS) where practical
- ✓ Check integrity of critical data periodic backups
- ✓ Remind end users to be diligent and promptly report any suspicious activity to your internal InfoSec team

Multiple Layers of Defense



*25+ years of
innovation*

WCRY Infection / Detection





Policies



Common Objects



Rules



Firewall Rules



Intrusion Prevention Rules



Integrity Monitoring Rules



Log Inspection Rules



Application Control Rulesets



Lists



Other



Contexts



Firewall Stateful Configuration



Malware Scan Configuration

IPS Rules

All ▾

By Application Type ▾



New ▾



Delete...



Properties...



Duplicate



Export ▾



Application Types...



C

NAME

PRIORI...

SEVERI...

▼ DCERPC Services (6)



1008327 - Identified Server Suspicious SMB Session

2 - Normal



Critical



1008306 - Microsoft Windows SMB Remote Code Execution Vulnerability (MS17-010)

2 - Normal



Critical



1008227 - Microsoft Windows SMB Remote Code Execution Vulnerability (CVE-2017-01...

2 - Normal



Critical



1008228 - Microsoft Windows SMB Remote Code Execution Vulnerability (CVE-2017-01...

2 - Normal



Critical



1008225 - Microsoft Windows SMB Remote Code Execution Vulnerability (CVE-2017-01...

2 - Normal



Critical



1008224 - Microsoft Windows SMB Remote Code Execution Vulnerabilities (CVE-2017-0...

2 - Normal



Critical

▼ DCERPC Services - Client (1)



1008328 - Identified Client Suspicious SMB Session

2 - Normal



Critical

- **Trend Micro Deep Security and Vulnerability Protection** (formerly the IDF plug-in for OfficeScan) customers with the latest rules have an updated layer of protection for multiple Windows operating systems, including some that have reached end-of-support (XP, 2000, 2003). Specifically, Trend Micro released the following rule for proactive protection:
 - **IPS Rules 1008224, 1008228, 1008225, 1008227** - Includes coverage for MS17-010 and some specific protection against Windows SMB remote code execution vulnerabilities
- **Trend Micro Deep Discovery Inspector** customers with the latest rules also have an additional layer of protection against the vulnerabilities associated with the exploit. Specifically, Trend Micro has released the following official rule for proactive protection:
 - **DDI Rule 2383: CVE-2017-0144 - Remote Code Execution - SMB (Request)**
- **Trend Micro TippingPoint** customers with the following filters have updated protection:
 - **Filters 5614, 27433, 27711, 27935, 27928** - Includes coverage for MS17-010 and some specific protection against Windows SMB remote code execution vulnerabilities and attacks
 - **ThreatDV Filter 30623** - helps to mitigate outbound C2 communication
 - **Policy Filter 11403** - provides additional protection against suspicious SMB fragmentation

Does this mean...
If I update my systems
with MS17-010...
We are protected?

Yes, I would be protected...

- Against this version of attack
- Of the auto propagation method
- Future attacks that exploit this vulnerability



Not protected from...

- New attacks that utilize vulnerabilities published from ShadowBrokers
- New attacks that utilize new vulnerabilities



Additional Reference Links

- Trend Micro Simply Security Blog: [WannaCry & The Reality of Patching](#)
- Trend Micro SimplySecurity Blog: [WannaCry and the Executive Order](#)
- Virus Encyclopedia: [Ransom_Wana.A](#)
- Virus Encyclopedia: [Ransom_WCRY.I](#)
- Defense Strategies Blog: [Defending against WannaCry/Wcry Ransomware](#)
- Support Article: [Latest Trend Micro Protection Against Shadow Brokers Tools](#) (including "Eternalblue")