Title

Ransomware

Presenter

Bill Wright

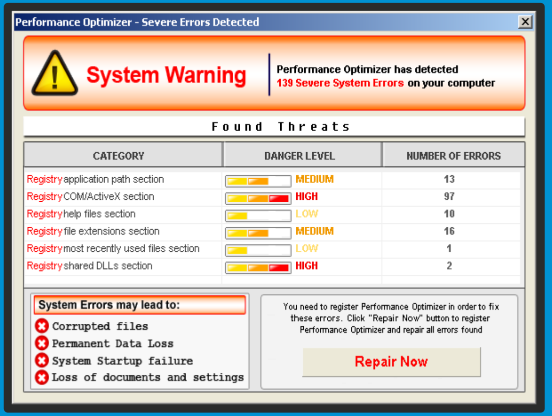
Government Affairs

Date

6/29/2017

Evolution path

MISLEADING APP



Performance Optimizer - Severe Errors Detected

System Warning

Performance Optimizer has detected **139 Severe System Errors** on your computer

Found Threats

CATEGORY	DANGER LEVEL	NUMBER OF ERRORS
Registry application path section	MEDIUM	13
Registry COM/ActiveX section	HIGH	97
Registry help files section	LOW	10
Registry file extensions section	MEDIUM	16
Registry most recently used files section	LOW	1
Registry shared DLLs section	HIGH	2

System Errors may lead to:

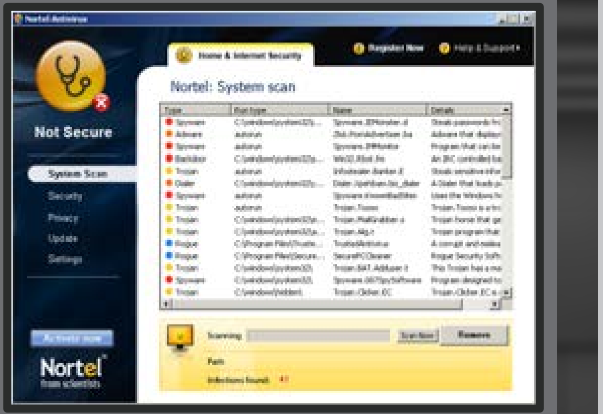
- ☒ Corrupted files
- ☒ Permanent Data Loss
- ☒ System Startup failure
- ☒ Loss of documents and settings

You need to register Performance Optimizer in order to fix these errors. Click "Repair Now" button to register Performance Optimizer and repair all errors found

2005-2009

"FIX"

FAKE AV



Nortel: System scan

Type	Run type	Name	Details
Spyware	C:\windows\system32\...	Spyware.IEMonitor.d	Steals passwords fr
Adware	autorun	Zlob.PornAdvertiser.ba	Adware that display
Spyware	autorun	Spyware.IEMonitor	Program that can be
Backdoor	C:\windows\system32\...	Win32.Rbot.fm	An IRC controlled ba
Trojan	autorun	Infostealer.Banker.E	Steals sensitive info
Dialer	C:\windows\system32\...	Dialer.Xpehbam.biz_dialer	A Dialer that leads p
Spyware	autorun	Spyware.KnownBadSites	Uses the Windows ho
Trojan	autorun	Trojan.Tooso	Trojan.Tooso is a tro
Trojan	C:\windows\system32\...	Trojan.PhatGrabber.a	Trojan horse that ge
Trojan	C:\windows\system32\...	Trojan.Alg.r	Trojan program that
Rogue	C:\Program Files\Truste...	TrustedAntivirus	A corrupt and malicio
Rogue	C:\Program Files\Secure...	SecurePCCleaner	Rogue Security Soft
Trojan	C:\windows\system32\	Trojan.BAT.Adduser.t	This Trojan has a ma
Spyware	C:\windows\system32\	Spyware.007SpySoftware	Program designed to
Trojan	C:\windows\hidden\	Trojan-Clicker.EC	Trojan-Clicker.EC a

Scanning:

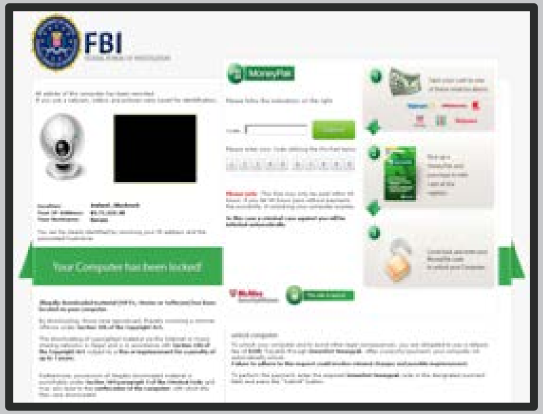
Path:

Infections found: 43

2010-2011

"CLEAN"

LOCKER RANSOMWARE

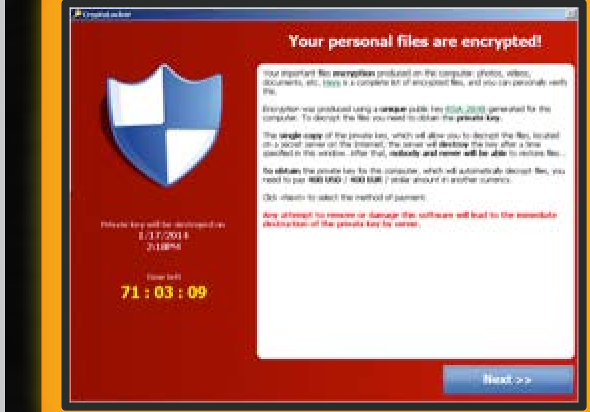


FBI
Federal Bureau of Investigation
MoneyPak
Your Computer has been locked!
McAfee

2012-2013

"FINE"

CRYPTO RANSOMWARE



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To **obtain** the private key for this computer, which will automatically decrypt files, you need to pay **400 USD** / **400 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
1/17/2014
2:18PM

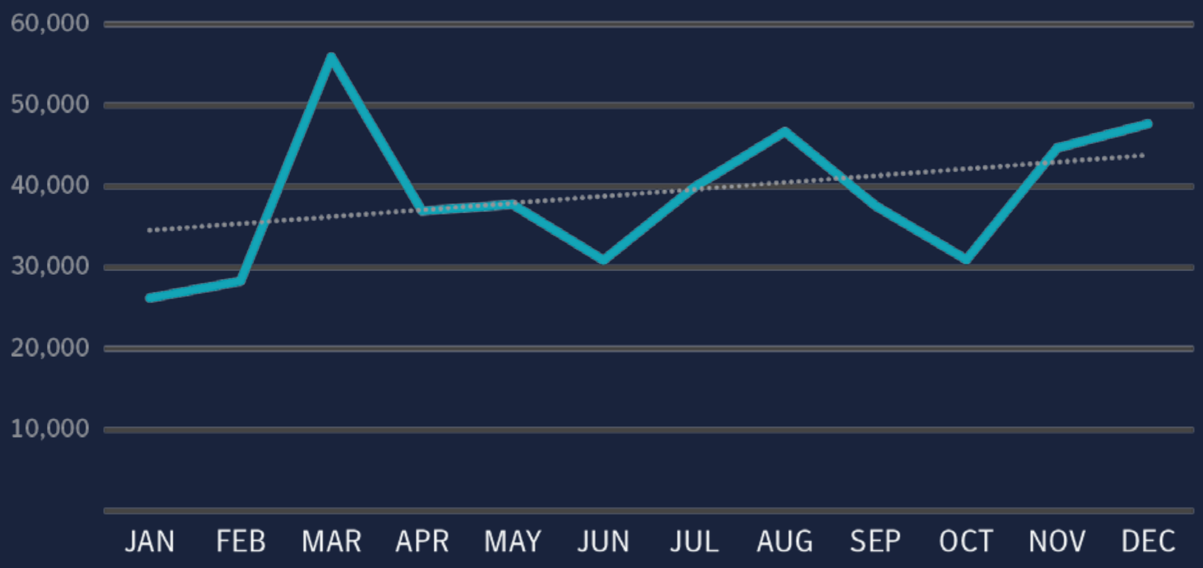
Time left
71 : 03 : 09

2014-2017

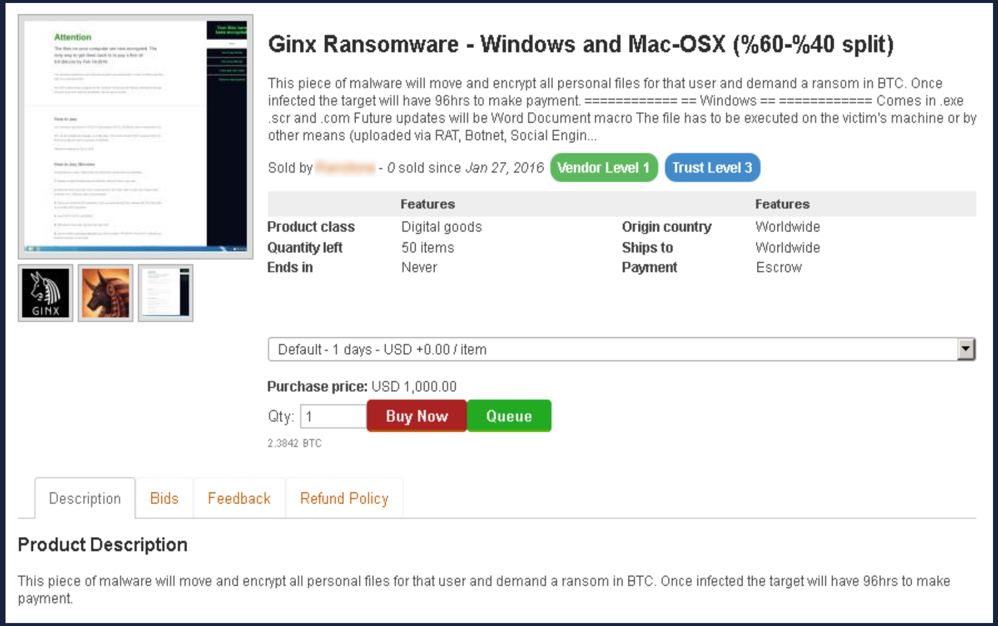
"FEE"

2016 Internet Security Threat Report
Volume 21

36% Increase in Ransomware Attacks



- Highly profitable
- Low Barrier to Entry
  - Multiple Software as a Service offerings available



Ginx Ransomware - Windows and Mac-OSX (%60-%40 split)

This piece of malware will move and encrypt all personal files for that user and demand a ransom in BTC. Once infected the target will have 96hrs to make payment. ============ == Windows == ============ Comes in .exe .scr and .com Future updates will be Word Document macro The file has to be executed on the victim's machine or by other means (uploaded via RAT, Botnet, Social Engin...

Sold by [redacted] - *0* sold since *Jan 27, 2016* Vendor Level 1 Trust Level 3

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	50 items	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 1,000.00

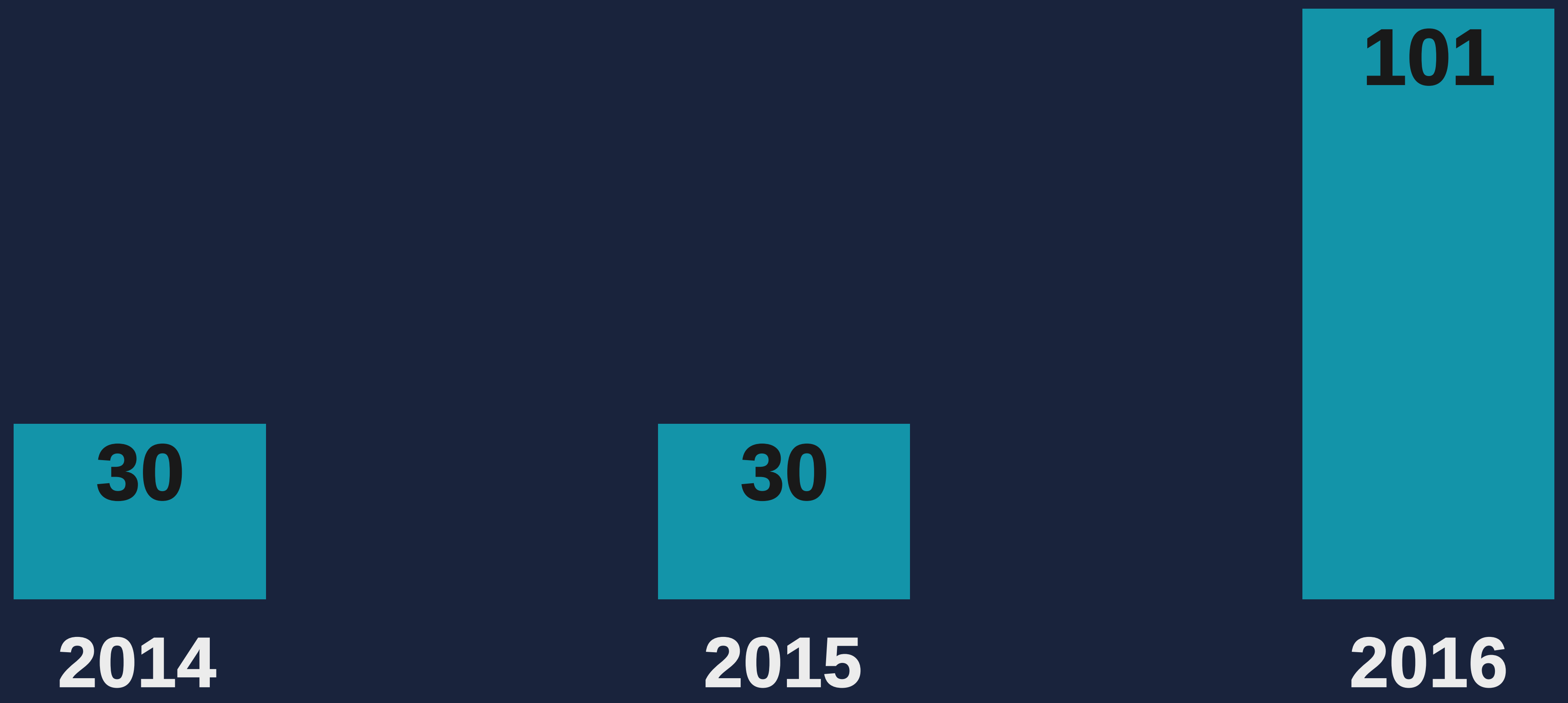
Qty: 1 Buy Now Queue

2.3842 BTC

Product Description

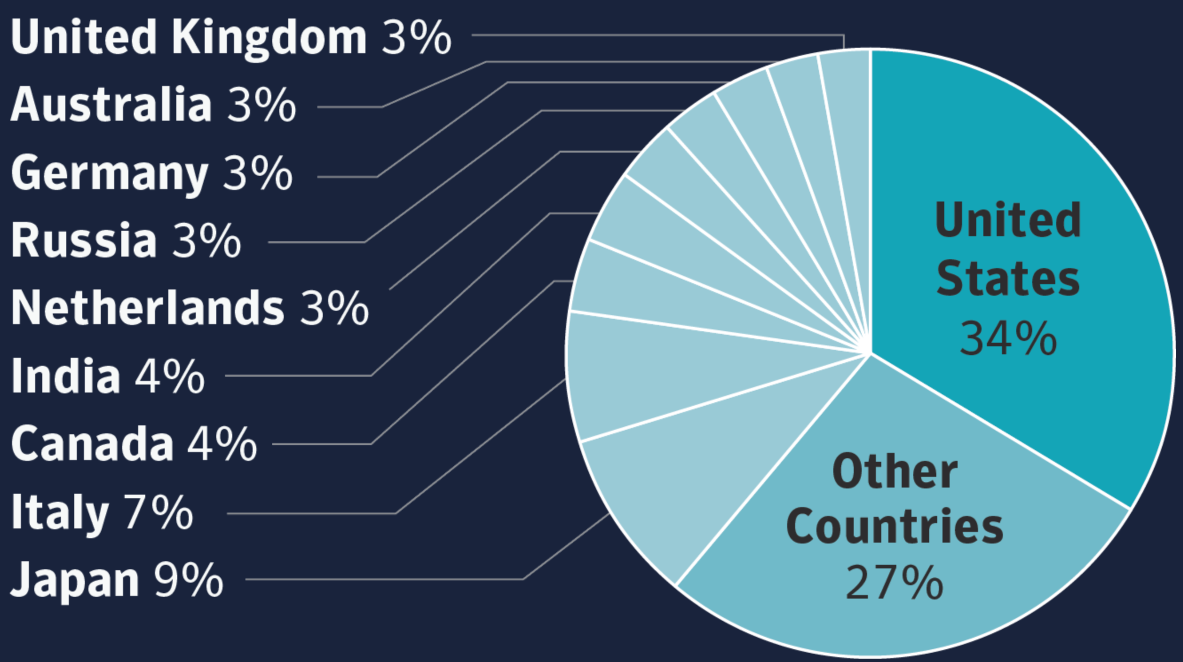
This piece of malware will move and encrypt all personal files for that user and demand a ransom in BTC. Once infected the target will have 96hrs to make payment.

3x as many new ransomware families in 2016



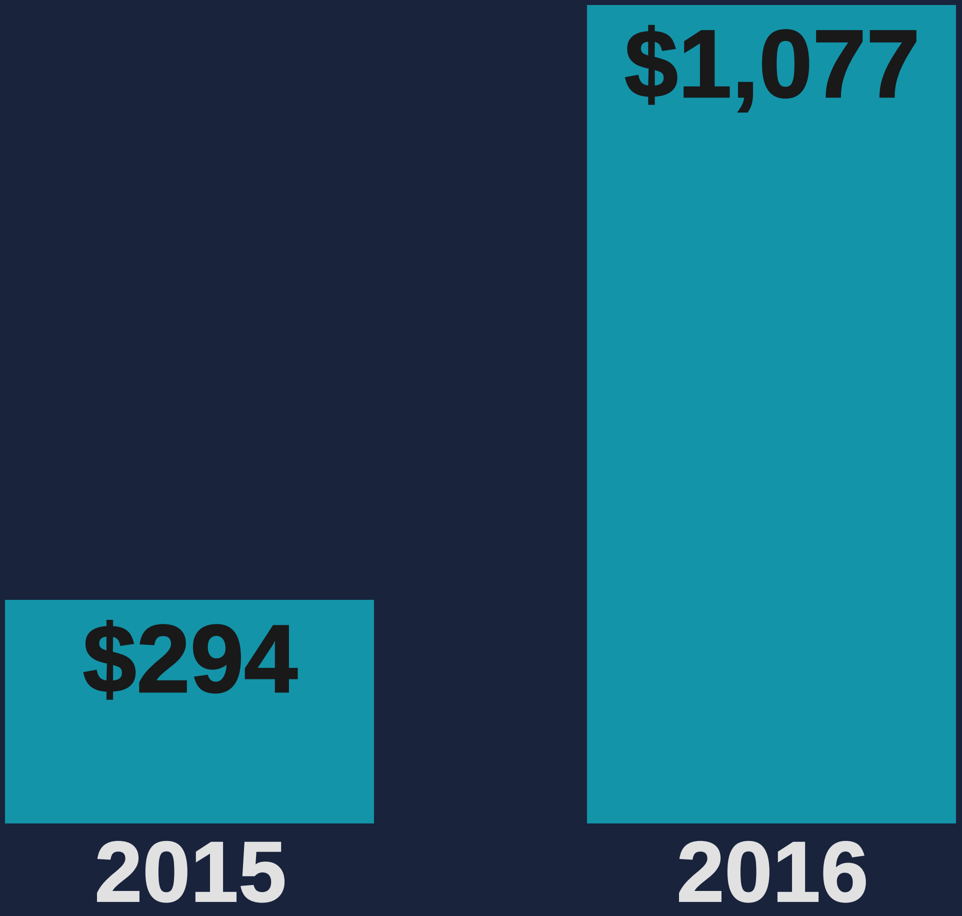
4

Ransomware Detections by Country



- With 34% of all attacks, US the region most affected by Ransomware
- Attackers target countries that can pay the largest ransom
- Number of internet connected computers also effect the numbers
- But US also has characteristic that is driving up the cost of the ransom

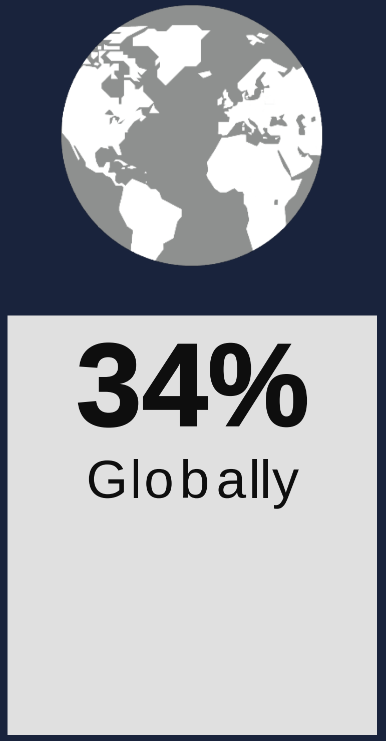
Average Ransom Demand



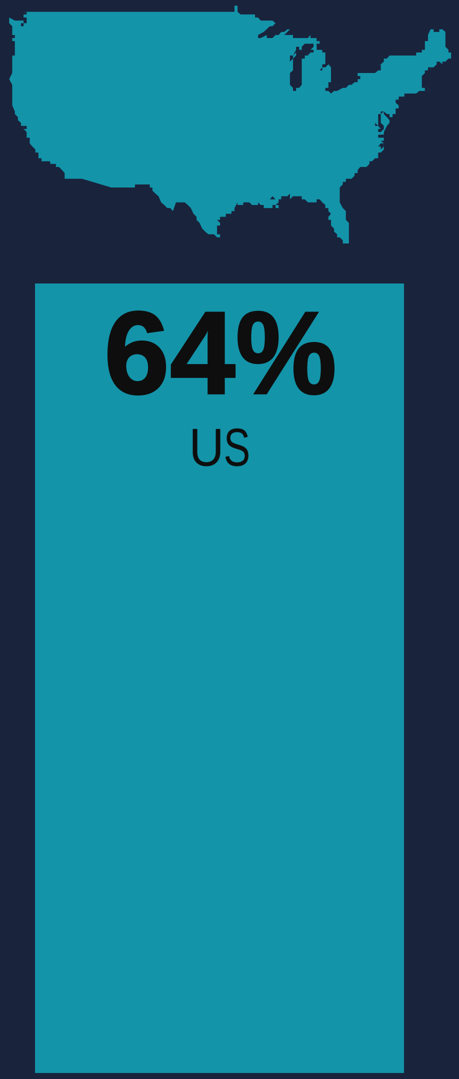
- The average starting ransom demand soared in 2016.
- Once infected many threats raise price if ransom not paid by deadline
- Some criminals will negotiate
- Targeted businesses will see higher demands
- Highest ransom demand for single machine seen in 2016 - $28,730 (Ransom.Mircop)

What is Driving Up the Ransom Demand?

Percentage of Consumers Who Pay Ransom

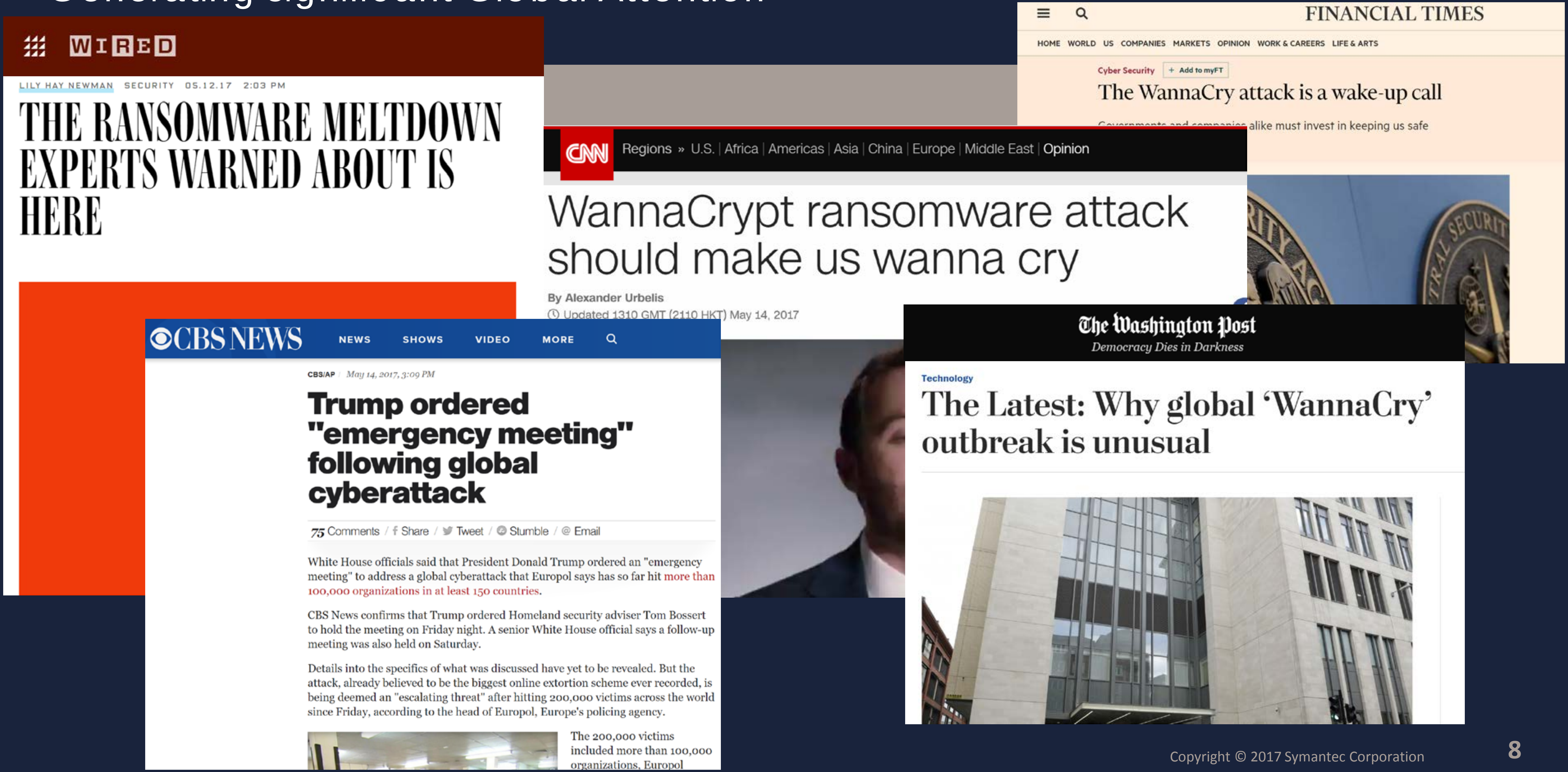


- There does not appear to be price sensitivity among victims, especially in the US
  - As long as victims willing to pay, criminals can raise the price



WannaCry Ransomware

Generating Significant Global Attention



WIRED

LILY HAY NEWMAN SECURITY 05.12.17 2:03 PM

THE RANSOMWARE MELTDOWN EXPERTS WARNED ABOUT IS HERE

FINANCIAL TIMES

HOME WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Cyber Security + Add to myFT

The WannaCry attack is a wake-up call

Governments and companies alike must invest in keeping us safe

CNN Regions » U.S. | Africa | Americas | Asia | China | Europe | Middle East | Opinion

WannaCrypt ransomware attack should make us wanna cry

By Alexander Urbelis

Updated 1310 GMT (2110 HKT) May 14, 2017

CBS NEWS NEWS SHOWS VIDEO MORE

CBS/AP / May 14, 2017, 3:09 PM

Trump ordered "emergency meeting" following global cyberattack

75 Comments / Share / Tweet / Stumble / Email

White House officials said that President Donald Trump ordered an "emergency meeting" to address a global cyberattack that Europol says has so far hit more than 100,000 organizations in at least 150 countries.

CBS News confirms that Trump ordered Homeland security adviser Tom Bossert to hold the meeting on Friday night. A senior White House official says a follow-up meeting was also held on Saturday.

Details into the specifics of what was discussed have yet to be revealed. But the attack, already believed to be the biggest online extortion scheme ever recorded, is being deemed an "escalating threat" after hitting 200,000 victims across the world since Friday, according to the head of Europol, Europe's policing agency.

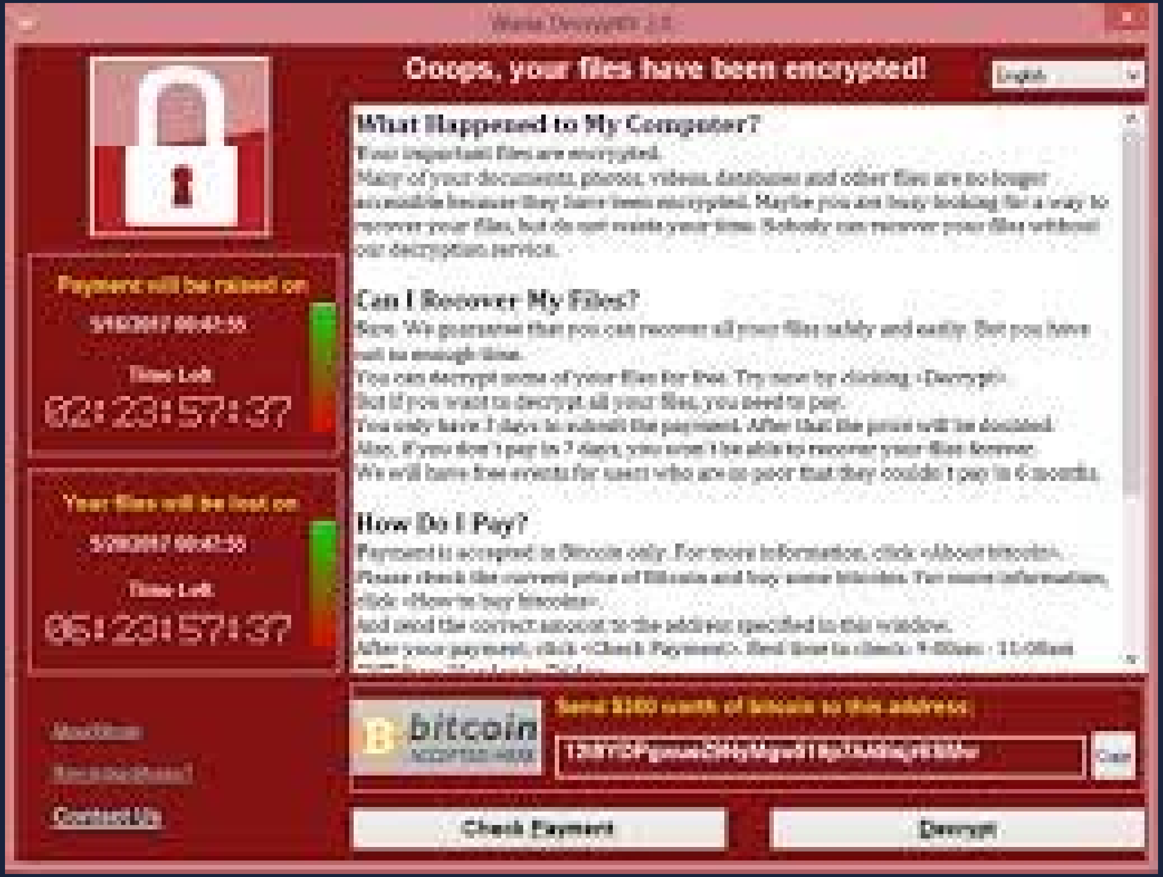
The 200,000 victims included more than 100,000 organizations, Europol

The Washington Post

Democracy Dies in Darkness

Technology

The Latest: Why global 'WannaCry' outbreak is unusual



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

About bitcoin

How to buy bitcoins?

Contact Us

Send $300 worth of bitcoin to this address:

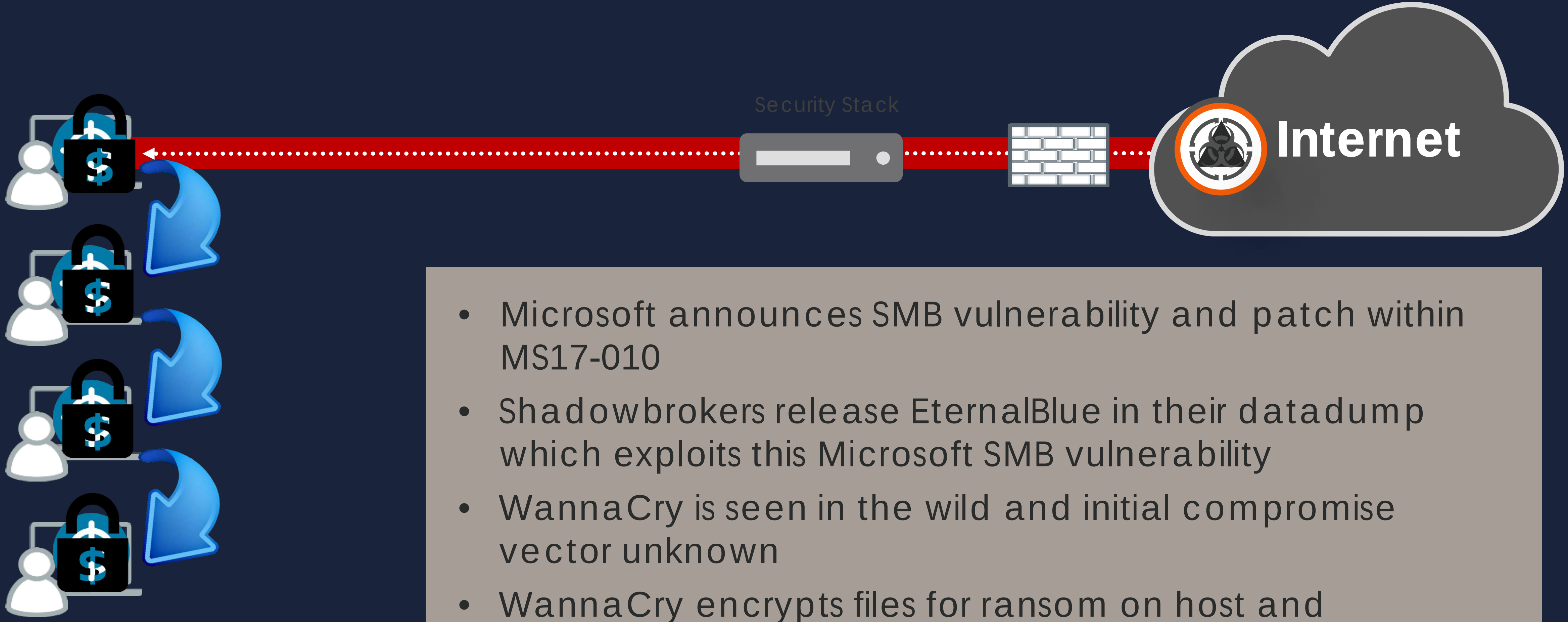
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

WannaCry Ransomware: Basics of the Attack



- Microsoft announces SMB vulnerability and patch within MS17-010
- Shadowbrokers release EternalBlue in their datadump which exploits this Microsoft SMB vulnerability
- WannaCry is seen in the wild and initial compromise vector unknown
- WannaCry encrypts files for ransom on host and propagates to other unpatched/unprotected hosts

YOU WOULDN'T
DOWNLOAD A BEAR
Fancy
Hurley

Attribution: Possibly Lazarus Group

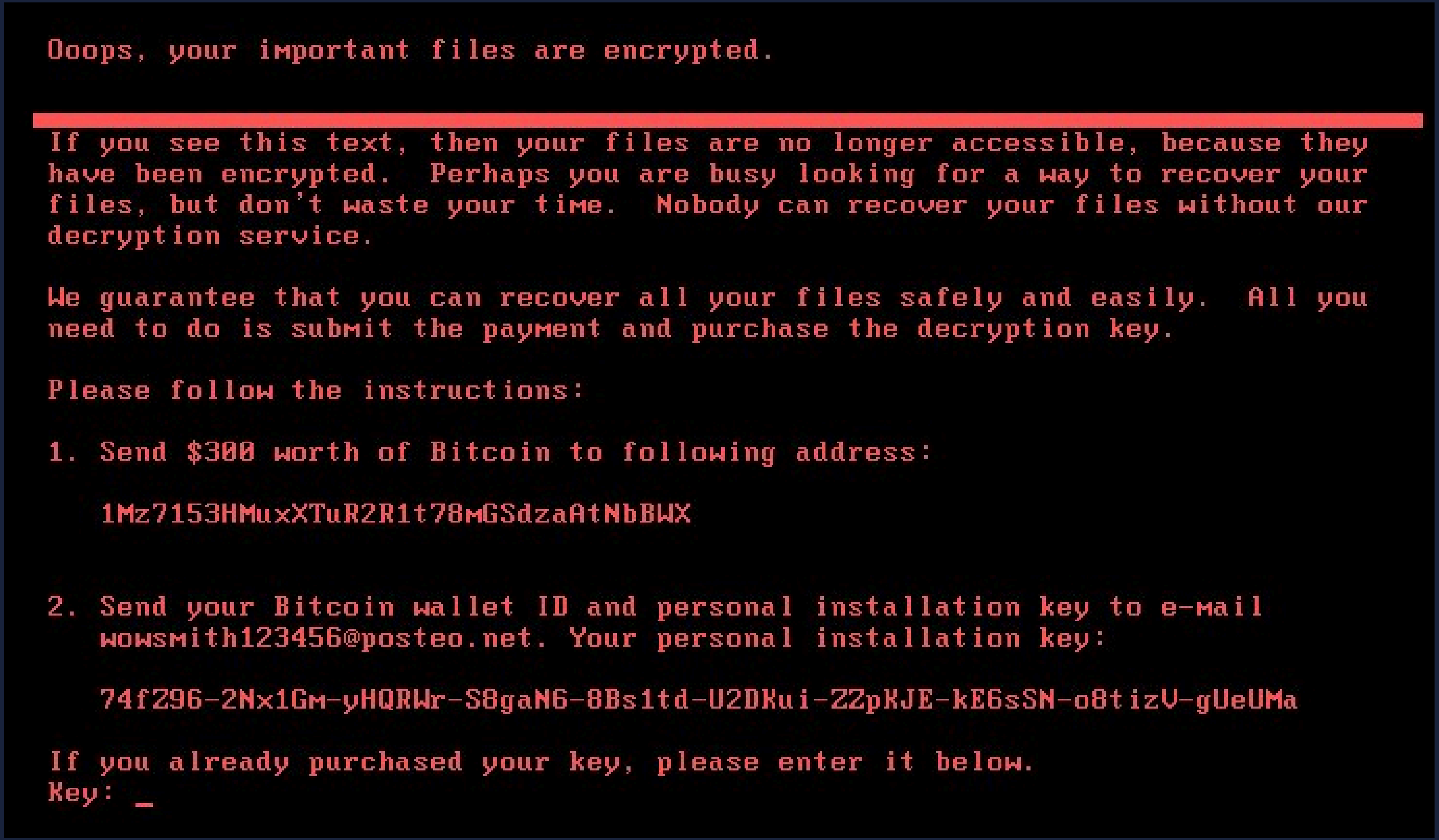
- Code used/borrowed from other Lazarus attacks
- Earlier versions of WannaCry found on computers with Lazarus tools
- Precedence exists: SWIFT Attacks $81million

Public Private Partnership: WannaCry

DHS's National Cybersecurity and Communications Integration Center (NCCIC)

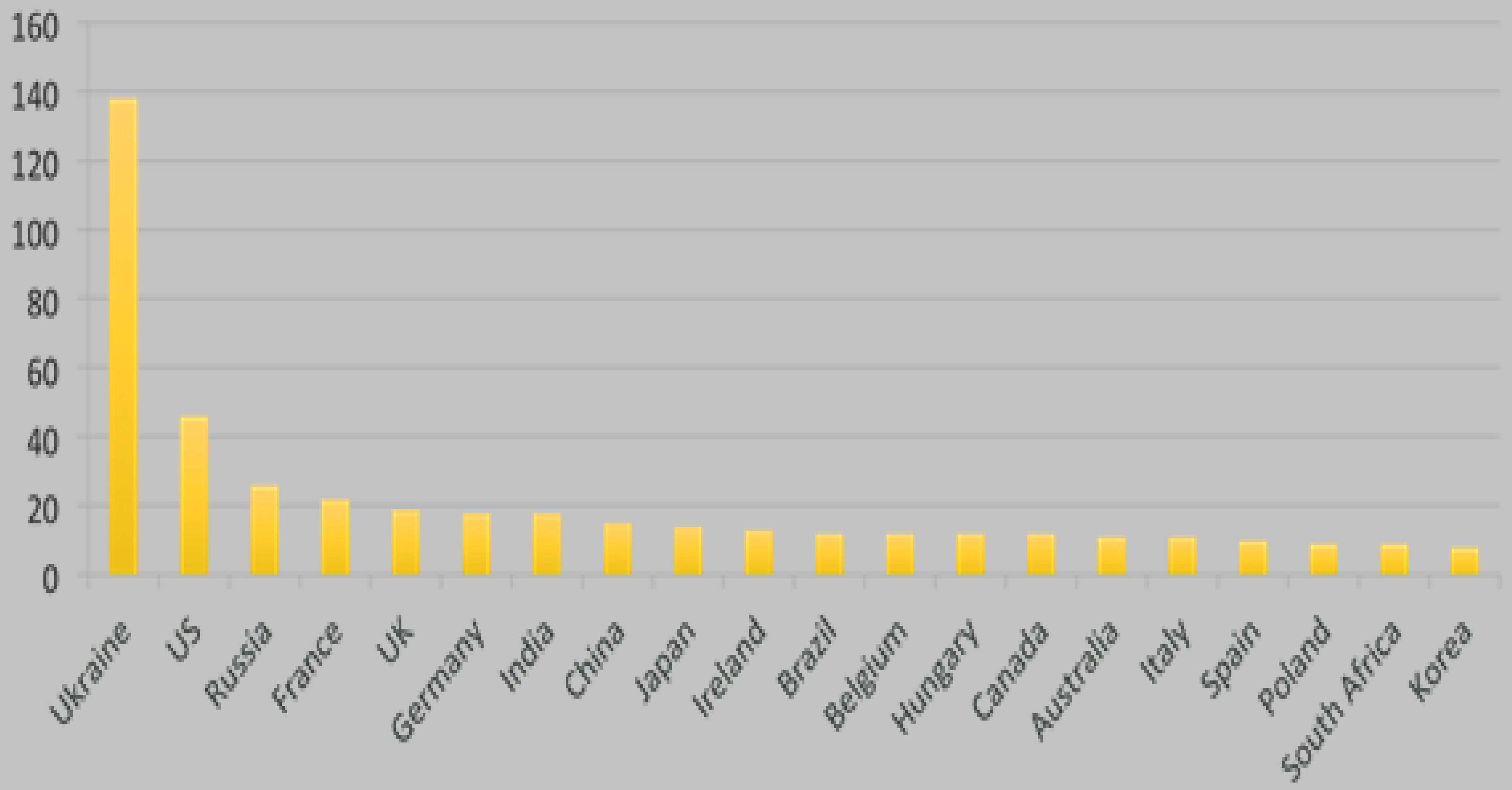
Cyber Threat Alliance

Petya Ransomware



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

Petya


160
140
120
100
80
60
40
20
0
Ukraine
US
Russia
France
UK
Germany
India
China
Japan
Ireland
Brazil
Belgium
Hungary
Canada
Australia
Italy
Spain
Poland
South Africa
Korea

Looking Ahead

Q&A

Ransomware

Thank You!

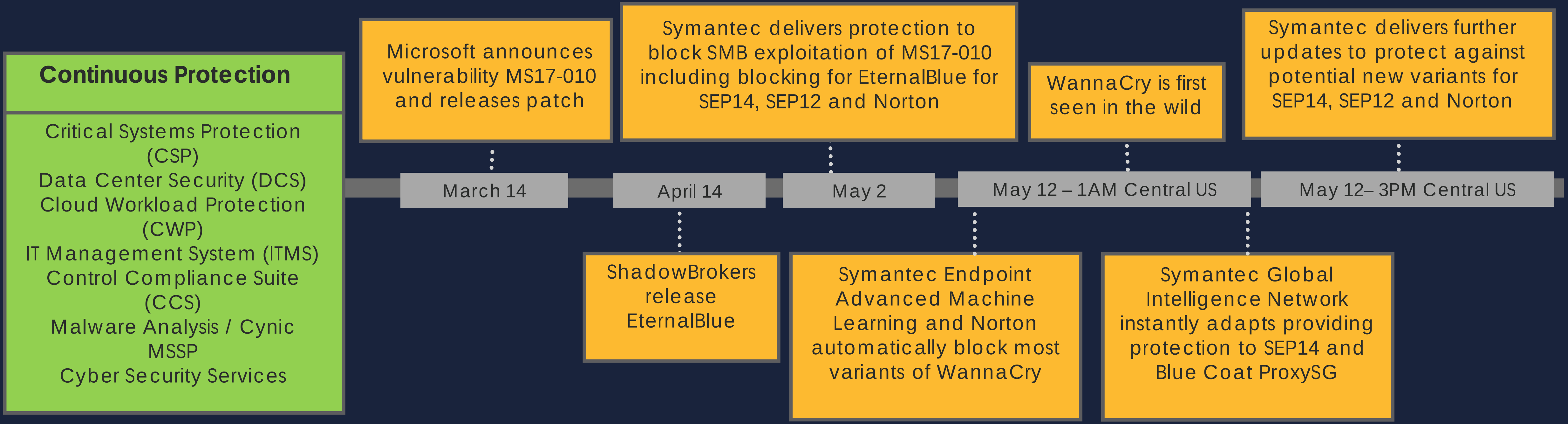
Symantec™

Volume

22

Symantec’s Timeline of WannaCry

Symantec Blocked 22M Attempted Attacks on Nearly 300,000 Endpoint Systems



Continuous Protection

Critical Systems Protection (CSP)
Data Center Security (DCS)
Cloud Workload Protection (CWP)
IT Management System (ITMS)
Control Compliance Suite (CCS)
Malware Analysis / Cynic
MSSP
Cyber Security Services

March 14

Microsoft announces vulnerability MS17-010 and releases patch

April 14

ShadowBrokers release EternalBlue

May 2

Symantec delivers protection to block SMB exploitation of MS17-010 including blocking for EternalBlue for SEP14, SEP12 and Norton

Symantec Endpoint Advanced Machine Learning and Norton automatically block most variants of WannaCry

May 12 – 1AM Central US

WannaCry is first seen in the wild

Symantec Global Intelligence Network instantly adapts providing protection to SEP14 and Blue Coat ProxySG

May 12– 3PM Central US

Symantec delivers further updates to protect against potential new variants for SEP14, SEP12 and Norton