protiviti®
Face the Future with Confidence

WANNACRY: A COMPLETE COMPROMISE WALKTHROUGH

October 2017

Protiviti Perspective provided by Roger Z., Houston

Internal Audit, Risk, Business & Technology Consulting

PRESENTERS

Presenter

Teddy Guzek
Security Consultant

Teddy is a senior consultant in Protiviti's Technology Consulting practice specializing in technical security assessments. He has performed dozens of network and application penetration tests, configuration reviews, phishing campaigns, and red team engagements.

Utilizing his OSCP certification, Teddy is excited to continue to identify security holes in complex networks around the world.

Presenter

Spencer Strausbaugh
Security Consultant

Spencer Strausbaugh received a B.S. in Digital Forensics, and a minor in Criminal Justice from Defiance College. He joined the Protiviti Chicago office Internal Audit practice in 2012 to focus in Cybersecurity.

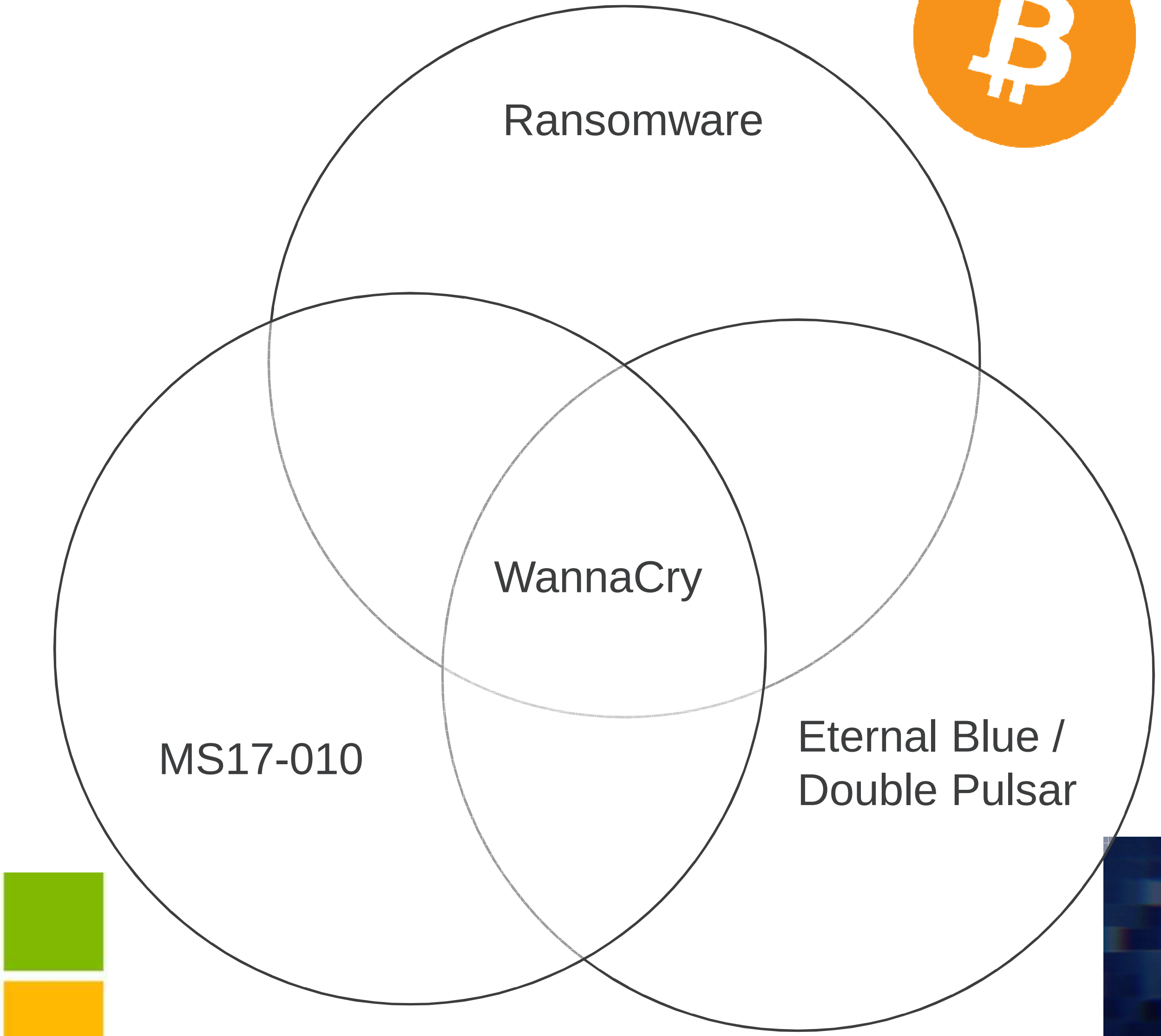
Spencer currently works in Chicago's cybersecurity center of excellence as a expert in internal penetration testing, external penetration testing, application penetration testing, social engineering, and security program reviews.

AGENDA

- **Goals, Expectations and Why**
- **WannaCry Exploit Overview**
- **Compromise Walkthrough/Demo**
- **Demo Recap**
- **What You Can Do**

GOALS EXPECTATIONS AND WHY?

- Presentation goal
  - Understanding how the WannaCry attack worked
  - Understanding how easy it is to go from an exploit of the MS17-010 vulnerability to gaining control of a domain
- Expectations
  - Give a (not too technical) overview of exploits and how they can affect a corporate environment
- Why does this matter?
  - To give context to risks, and to educate!



Ransomware

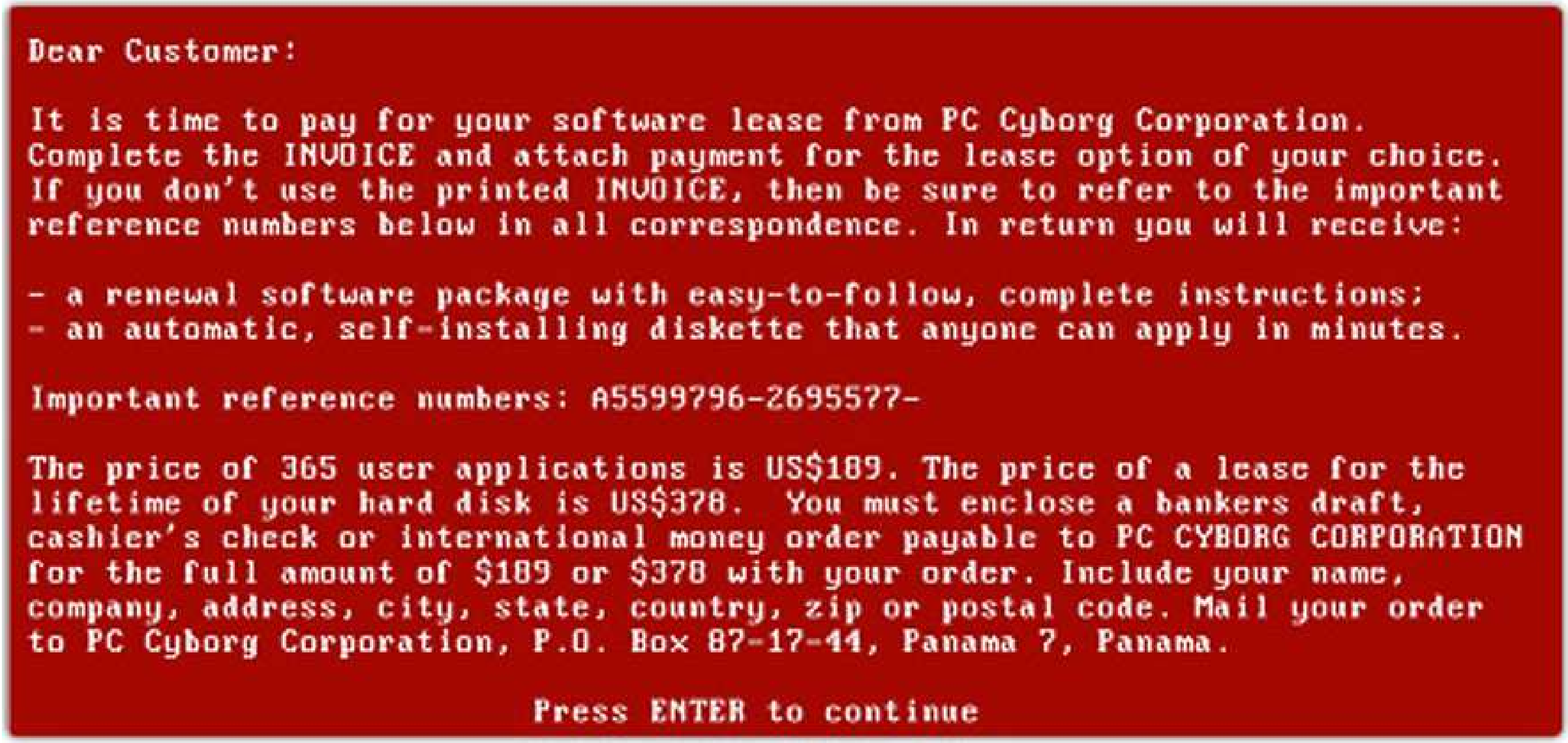
WannaCry

MS17-010

Eternal Blue /
Double Pulsar

HISTORY OF RANSOMWARE

- PC Cyborg (AIDS Trojans) - 1989
  - Dr. Joseph Popp
  - Affected the healthcare industry
  - Activation of malware was delayed to help keep the culprit anonymous
    - After 90x, the malware went active
  - Message demanded a payment of $189 for a year or $387 for the lifetime of computer
    - P.O. box in Panama
  - Poor encryption made the campaign ineffective



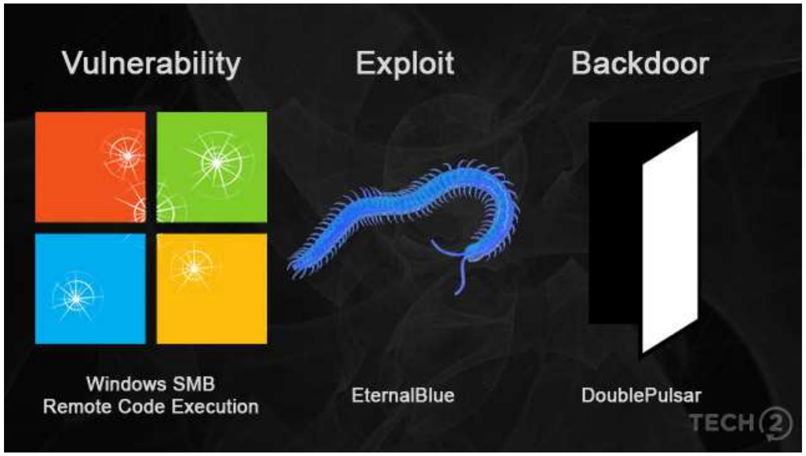
```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                          Press ENTER to continue
```

EVOLUTION OF RANSOMWARE

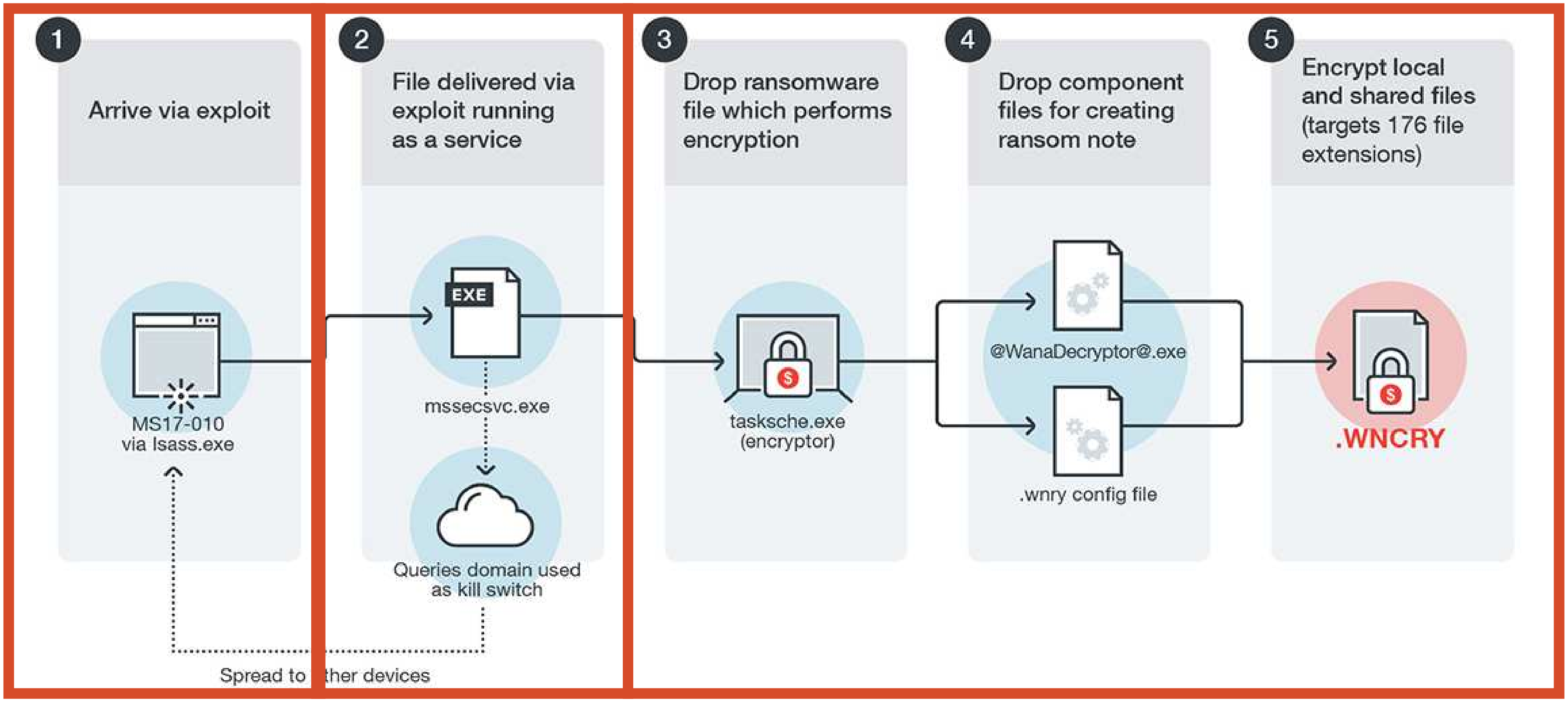
- Strength of Encryption
- Methods of transmission
  - Floppy disk to email to self-propagating
- Who’s capable of carrying out these attacks?
  - Used to just be sophisticated attackers and Nation States
  - Ransomware-as-a-Service (RaaS)
- Payment Options
  - Evolution of cryptocurrencies has made it much easier, allowing for the attacker to stay anonymous
- Increasing popularity of IoT will make these ransomware attacks even more detrimental
  - Wearables, household items, etc.

MS17-010

- Takes advantage a vulnerability in the SMB service
- Microsoft released the patch on March 14th, 2017
  - 10th vulnerability of 2017
- Shadow Brokers released exploit April 15, 2017
  - Eternal Blue - Exploit
  - Double Pulsar – Backdoor
- Mostly seen in internal environments but found externally
  - 40 examples externally
- Gives system privileges, ENDLESS POSSIBILITIES



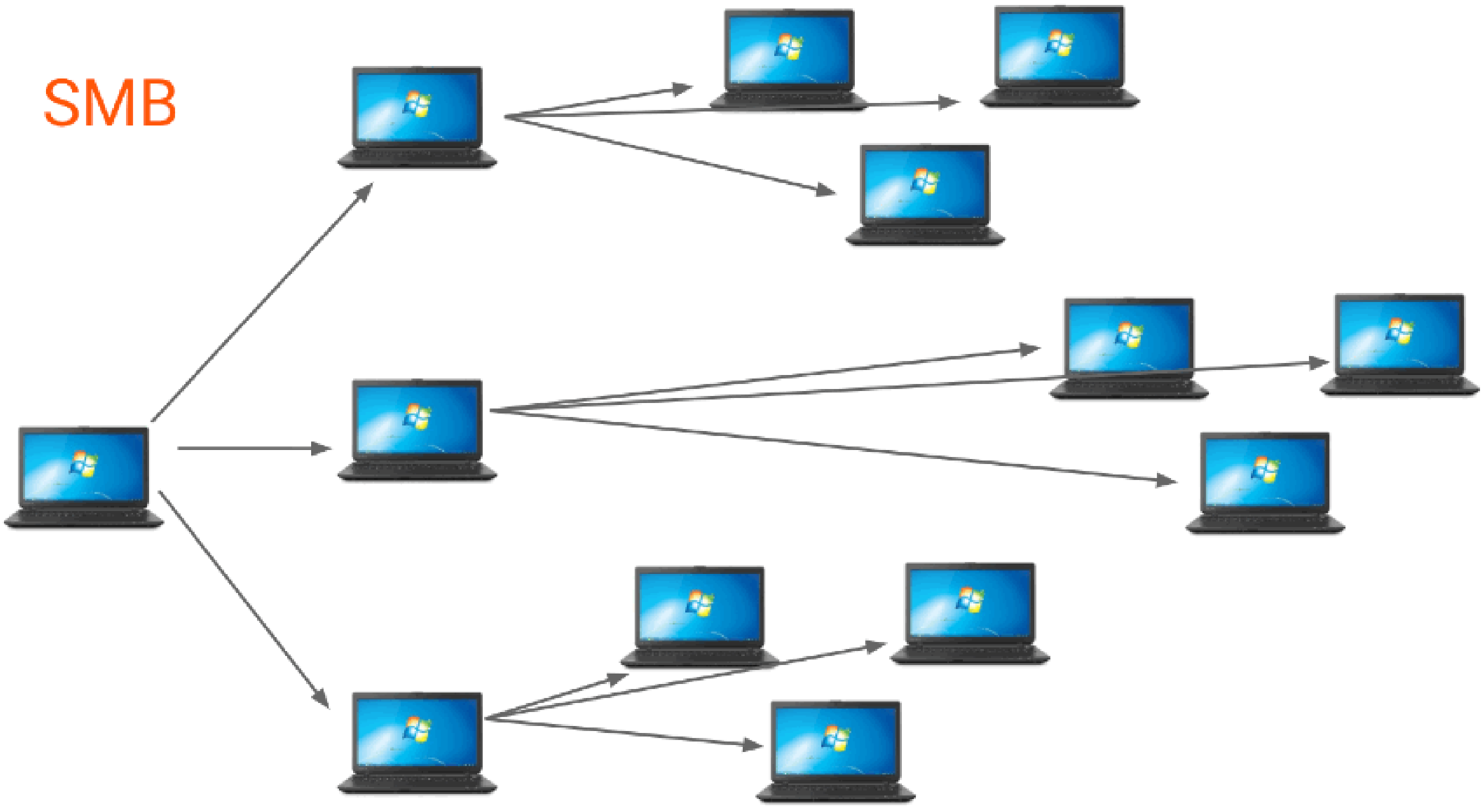
HOW WANNACRY WORKS



1
Arrive via exploit
MS17-010
via lsass.exe
2
File delivered via exploit running as a service
EXE
mssecsvc.exe
Queries domain used as kill switch
Spread to other devices
3
Drop ransomware file which performs encryption
taskche.exe
(encryptor)
4
Drop component files for creating ransom note
@WanaDecryptor@.exe
.wnry config file
5
Encrypt local and shared files (targets 176 file extensions)
.WNCRY

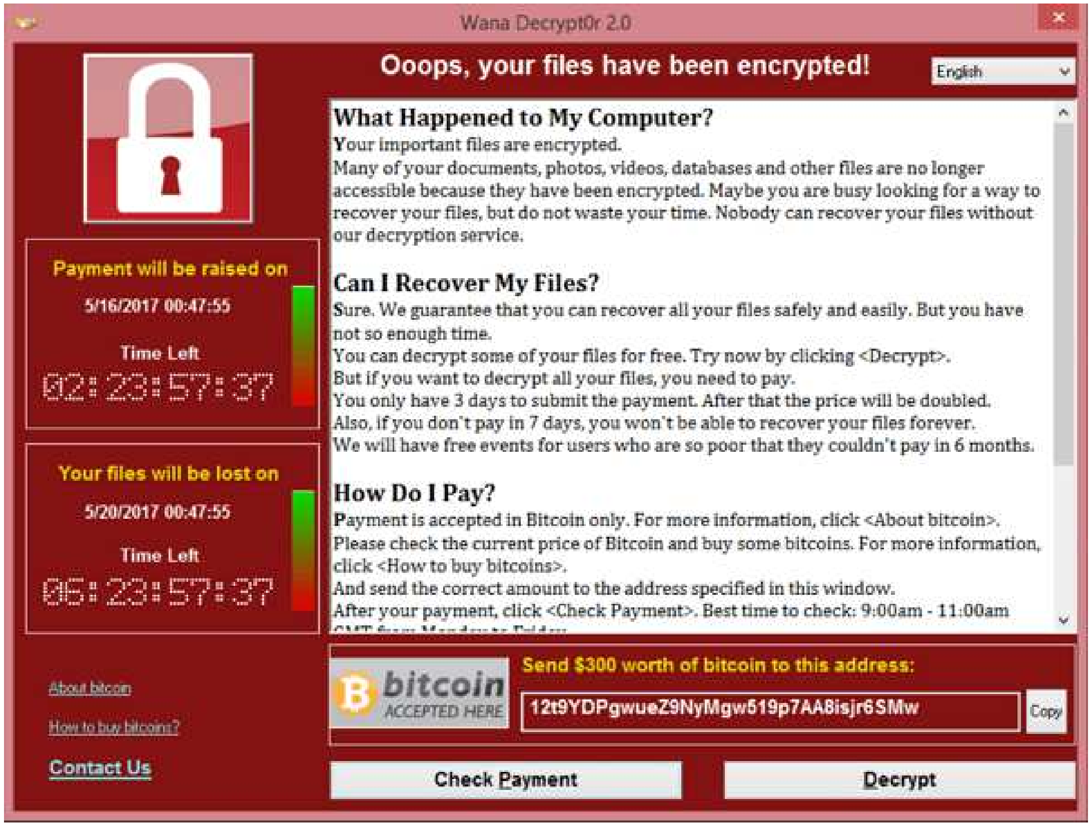
MS17-010 Eternal Blue Ransomware

HOW WANNACRY SPREAD



AFTERMATH OF WANNACRY RANSOMWARE

- Encrypted 176 different file types
- Over 200,000 victims and more than 300,000 computers affected
- Asked for $300 or $600
- 338 payments at $140,000
- Microsoft made patches for unsupported systems
- Many copycat crimes



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>.

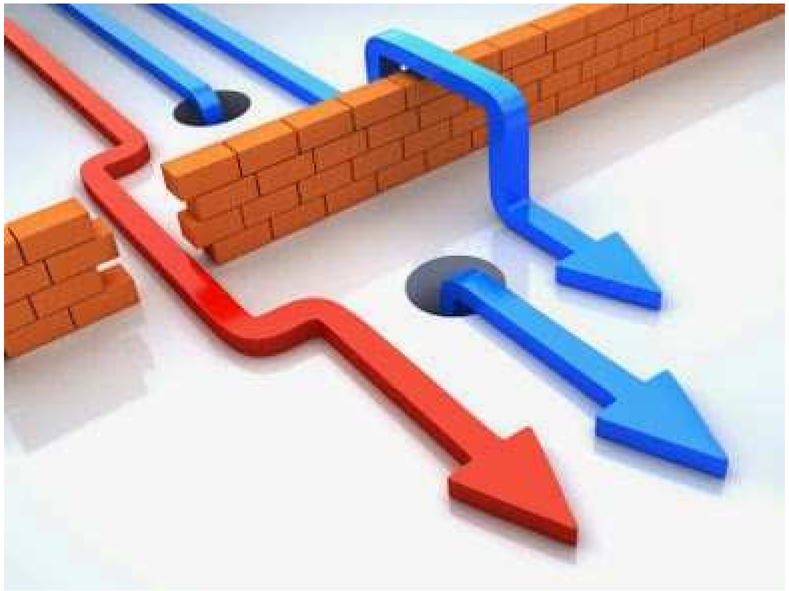
And send the correct amount to the address specified in this window.

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

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

LIVE DEMO



ACTIONS IN REVIEW – RECAP OF DEMO

- Ran a scan using one of the various tools to identify the MS17-010 vulnerability
- Loaded the attack for MS17-010 on my Linux computer, pointed the attack at the vulnerable machine and executed the attack
- Dumped the passwords and hashes from the domain
- Used the Domain Admin credentials to login to the vulnerable machine

WHAT YOU CAN DO

- How to stop identification of the vulnerability?
  - Don’t have the vulnerability!
  - Keep up to date with your patch management programs
- How do I stop the attacker from dumping passwords?
  - Use the Protected Users group in recent versions of Active Directory (Windows 2012 R2)
  - Limit the number of services running as system
- How do I stop a Domain Admin from logging into systems
  - You cant really
  - BUT you can limit the amount of people on your network with Domain Admin privileges.
  - If they don’t login to machines often, the credentials cannot be dumped
  - DO NOT use a local admin account
  - Try to keep your end users as aware as possible

Face the Future with Confidence

protiviti®