

# TALOS

Cisco Security Research



## Fighting the Good Fight

# Who Am I?

## Edmund Brumaghin

- Threat Researcher at Cisco Talos.
- I <3 Malware.
- Spent over a decade protecting critical infrastructure.
- Embedded Systems/IoT Research



@b4n1shed

# Threat Intelligence



We are an elite group of security experts devoted to providing superior protection to customers with our products and service.

Cisco Talos' core mission is to provide verifiable and customizable defensive technologies and techniques that help customers quickly protect their assets from cloud to core.

**Our job is protecting your network.**

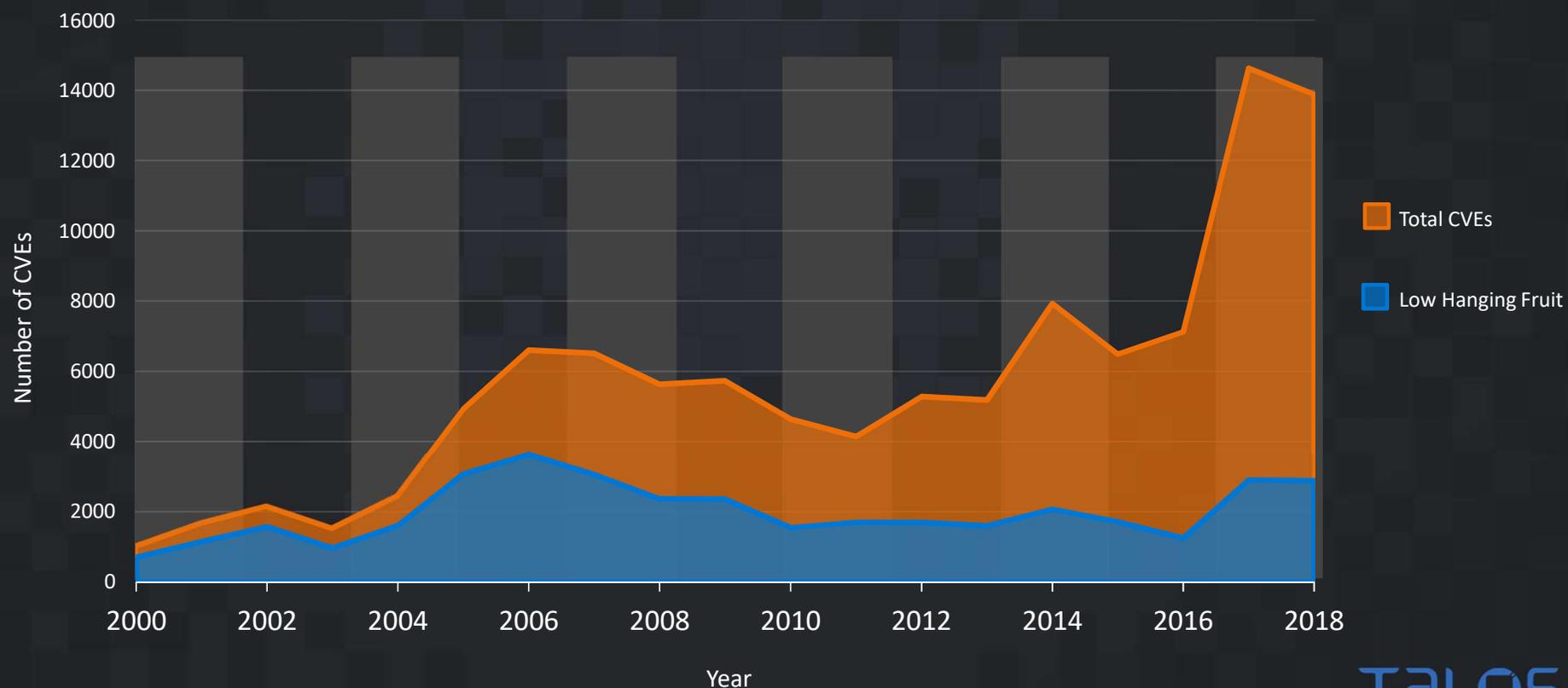


**Talos encompasses six key areas:**

Threat Intelligence & Interdiction, Detection Research, Engine Development, Vulnerability Research & Discovery, Open Source & Education, and Global Outreach.

# Threat Landscape

Vulnerabilities – Low hanging fruit is on the decline



# Windows 10 Mitigations

Pwn2Own@CanSecWest 2018:  
(fully patched OS, not hardened)

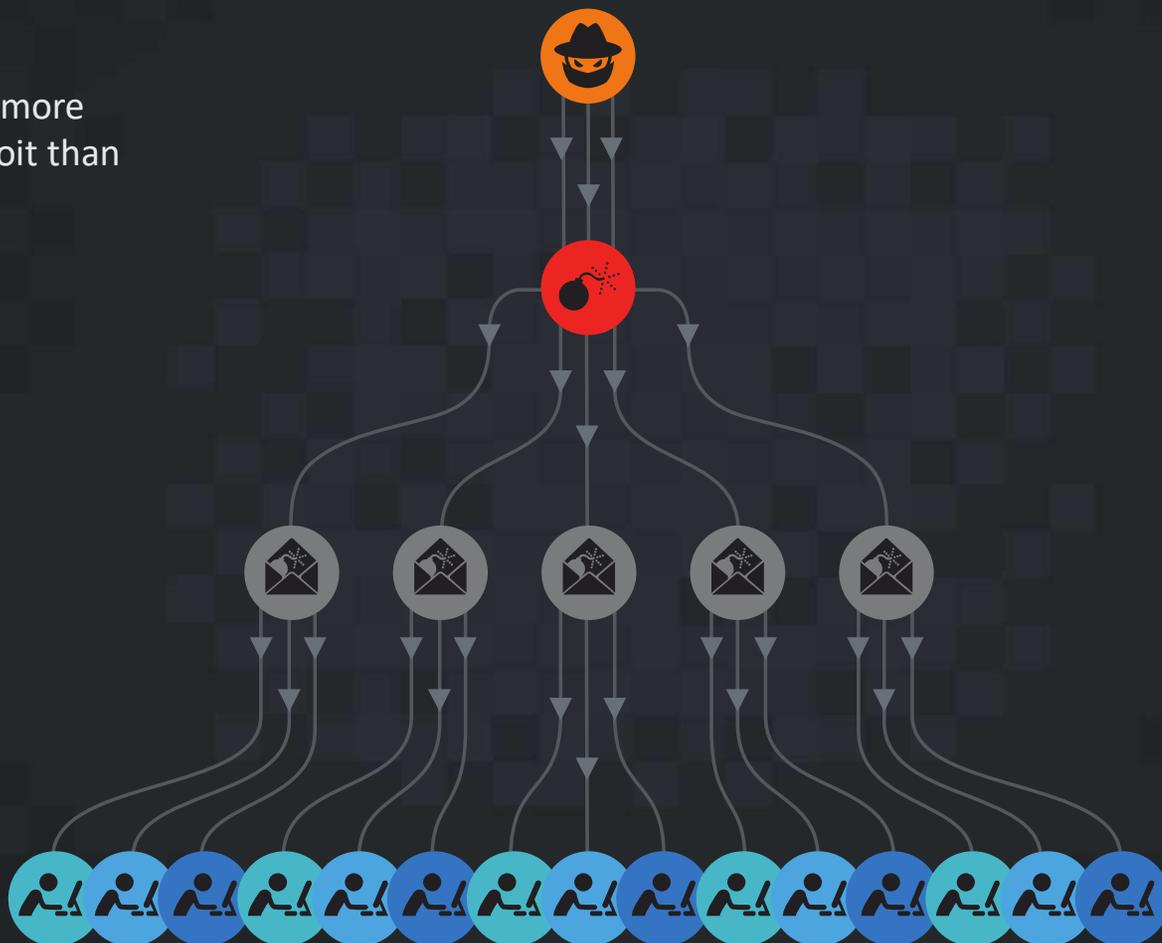
“... targeted the [Edge] browser with a **pair of use-after-free bugs** and an **integer overflow in the kernel** to run code with elevated privileges”

“...It's the second year in a row that Chrome has **emerged unscathed from the competition.**”

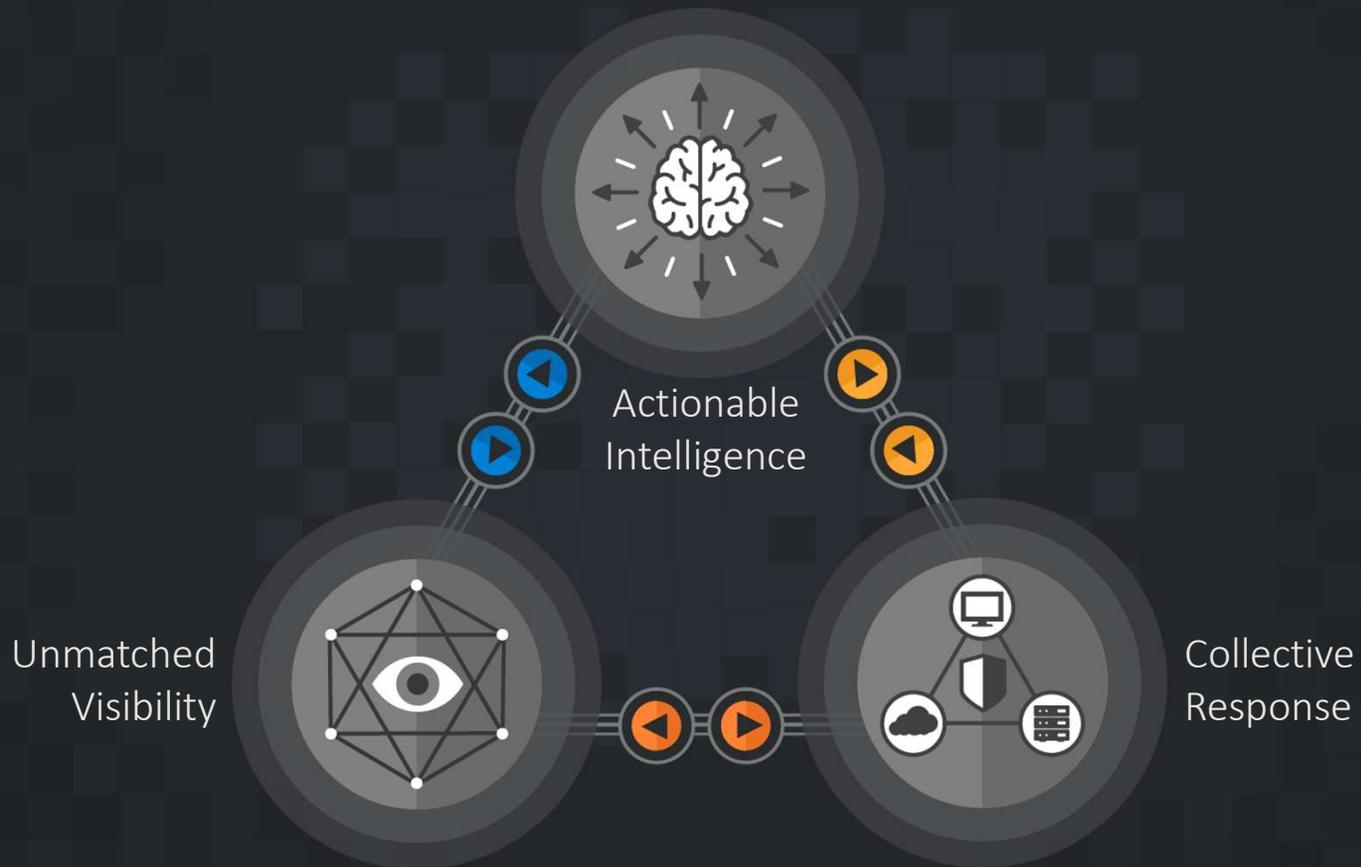
- Control flow guard (CFG)
- Data Execution Prevention (DEP)
- Mandatory Address Space Layout Randomization (ASLR)
- Bottom-up Mandatory Address Space Layout Randomization (ASLR)
- Validate exception chains (SEHOP)
- Validate heap integrity
- Arbitrary code guard (ACG)
- Block low integrity images
- Block remote images
- Block untrusted fonts
- Code integrity guard
- Disable extension points
- Disable Win32k system calls
- Do not allow child processes
- Export address filtering (EAF)
- Import address filtering (IAF)
- Simulate execution (SimExec)
- Validate API invocation (CallerCheck)
- Validate handle usage
- Validate image dependency integrity
- Validate stack integrity (StackPivot)
- ....
- Applocker, Device Guard, Patch Guard, Browser Sandbox, Security Development Lifecycle (SDL)...

# Threat Landscape

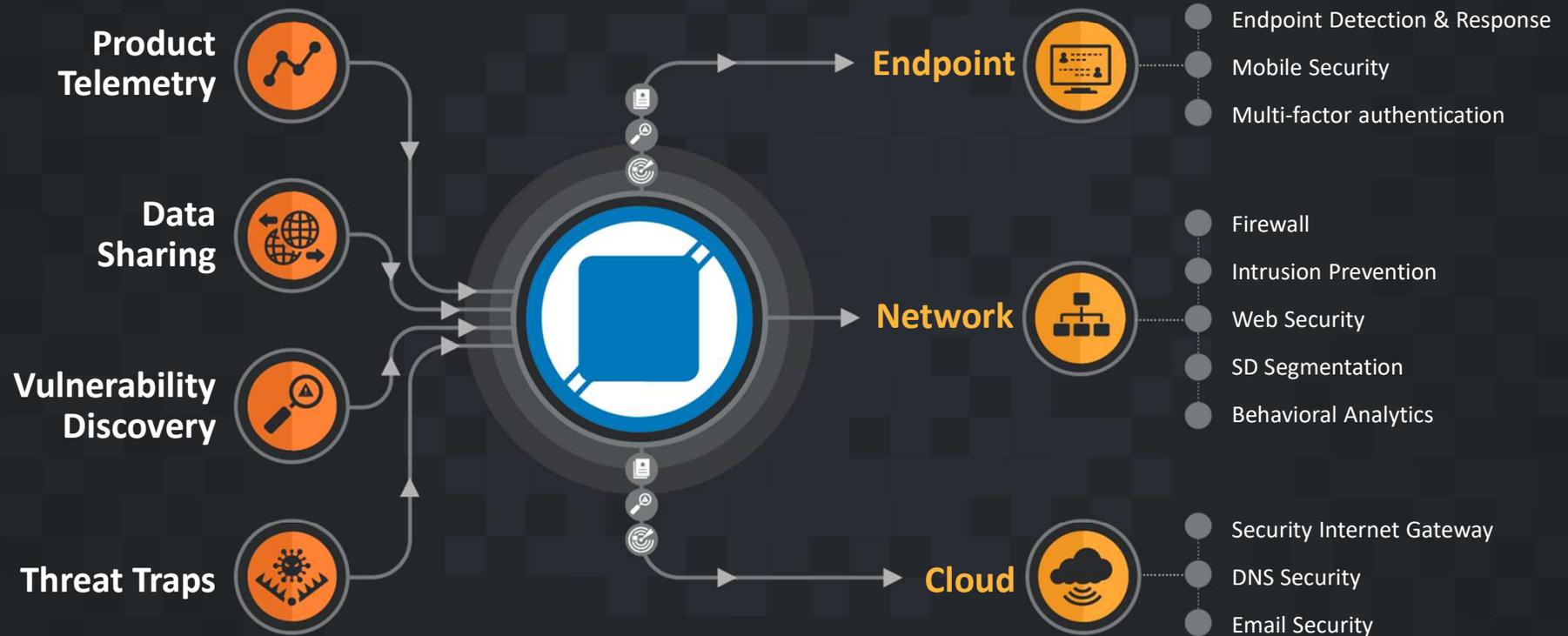
- People are much more economic to exploit than software.



# Why trust Talos?



# From Unknown to Understood

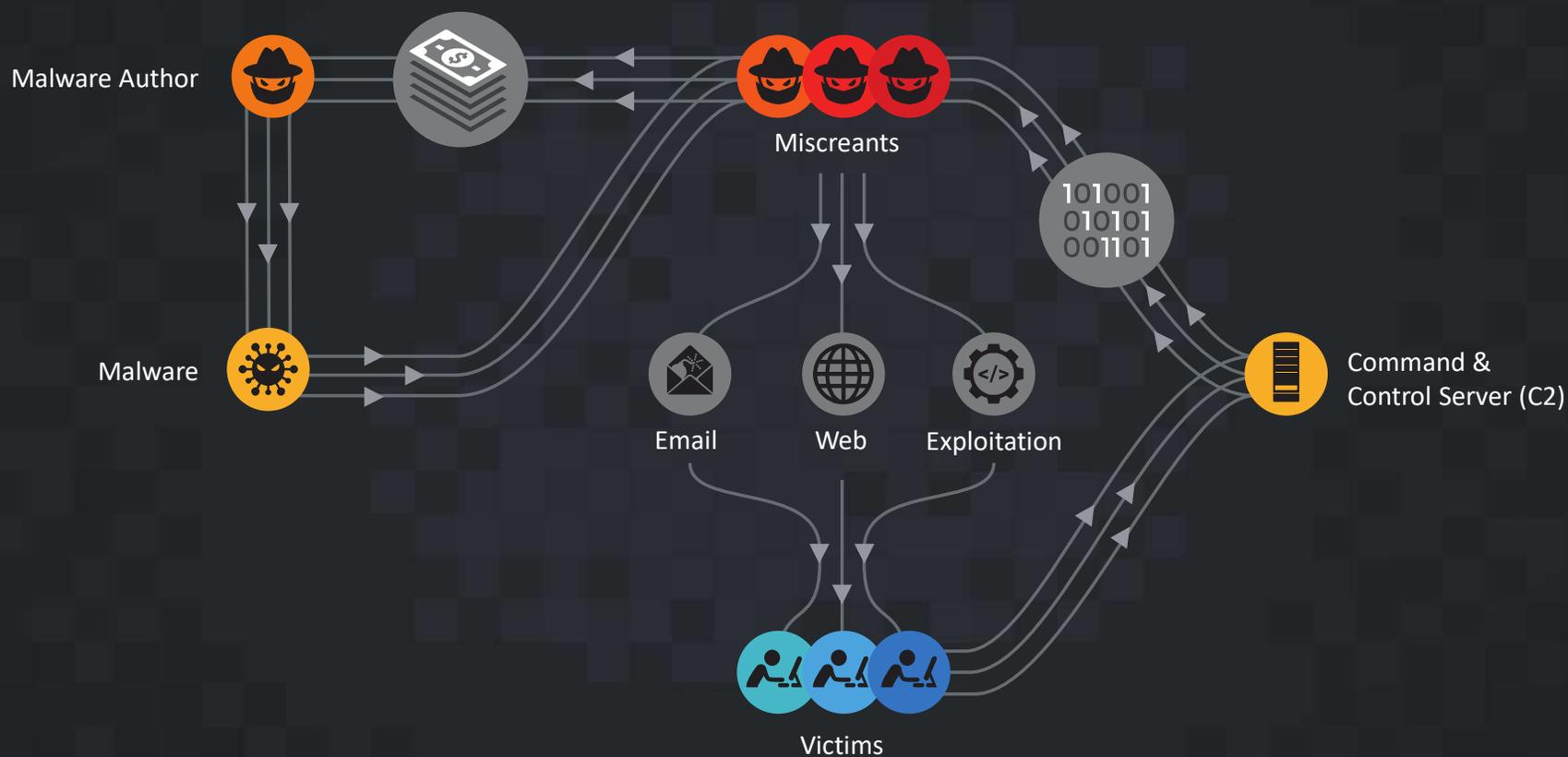


# Common Threats

# Threats Facing Enterprises Today



# Commodity Malware Lifecycle



# Malicious Crypto Mining



## **i** Description

- Utilizes spare CPU to make money
- Wide and Common
- Low bar like Ransomware

## **🔧** Tools

- Macros, Docs, PDFs, and EXEs
- Also compiled for IoT devices
- Mimikatz and Credential stealers

## **🕒** Tactics

- Default passwords
- Spam, Link Spam, and Phishing
- Coin Hive and other embedded miners

## **⚙️** Processes

- Steals CPU time
- Doesn't cause problems, so users don't report it.

# Cryptomining Profits

Worker ID	Average Hash Rate	Potential Profit
4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGApbF5vWtANQpR48NWyTgLF8daDK	450 KH/s	\$330,000.00
4AQe5sAFWZKECiaeNTt59LG7kVtqRoSRJMjrmQ6GiMFaeUvoL3MFeTE6zwwHkFPrAyNw2JHDxUSWL82RiZThPpk4SEg7Vqe	350 KH/s	\$257,000.00
4875jA3AmHFaiYMxSCqnw39viv7NcqJUcbW3kR1kwpQ1stxLKhHM75DDqFBqpMsfzPkqKxJEHokjXP8m3uwzXz38EX4C	325 KH/s	\$238,000.00
43rfEtGjJdFaXDJRYvo7wJ9Cmq1vWjMdkZzaKEkp4aQBHKkZ7Rp6oB1QMBPFJUKGGWc9AeAbr9V6gYVSM8XwbXBYZXBss	245 KH/s	\$180,000.00
46xzbEFicggME8PBfwPnuwHbtk2UQU6xmMjAs3MHvLEmSyTnBv3BQTdYZ5Nfw5qLGbZmvTH4rZMXZF6rYNjgfAABSm9FaYT	240 KH/s	\$176,000.00
<b>Total</b>	<b>1.6 MH/s</b>	<b>\$1,181,000.00</b>

# Commercial RATs



## **i** Description

- Commercial Remote Access Trojan
- Sold / supported on various forums
- Costs less than 300 USD

## **🔧** Tools

- C++
- Anti-Analysis
- RC4 encoded C2

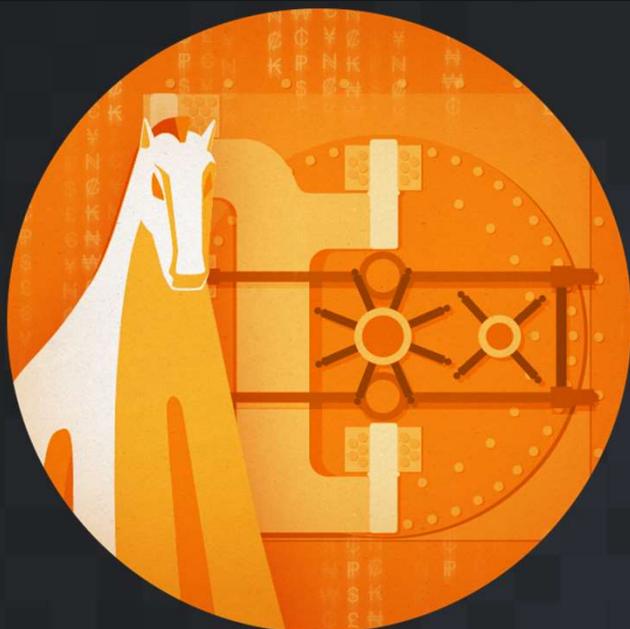
## **🕒** Tactics

- Spear Phishing
- RePacking
- Delivery is actor choice

## **⚙️** Processes

- Capture Password, and Screenshots
- Resell to more sophisticated actor

# Banking Trojans



## **i** Description

- Multiple Variants at Any Given Time
- Designed to Steal Banking Credentials
- Examples: Trickbot, Emotet, Zeus

## **🔧** Tools

- C++
- Anti-Analysis
- RC4 encoded C2

## **🕒** Tactics

- Email Delivery Common
- Malware Downloaders Common (.DOCX, .XLSX, etc)
- Delivery is actor choice

## **⚙️** Processes

- Capture Banking Credentials, and Screenshots
- Banking Credentials Used for Significant Financial Theft

# Sextortion Scams



## **i** Description

- Leveraged Open Source Breach Data
- Crafted Emails w/ Username/Password
- Generated ~\$150K in crypto currency

## **🔧** Tools

- Leveraged Old Data Breach Information
- Threatening Sextortion Emails
- Bitcoin for Payout

## **🎯** Tactics

- Take Advantage of Old Data
- Provide Username/Password to Scare Users
- Threaten with Exposure, Profit

## **⚙️** Processes

- Used Freely Available Data
- Played on Peoples Fear
- Generated Significant Profits

# Original Attack

● Kimberly

Yesterday at 5:33 PM



randy55

To: randy55

I am well aware randy55 one of your password. Lets get right to point. You do not know me and you are most likely thinking why you are getting this e-mail? Not one person has paid me to investigate you.

actually, I actually setup a software on the xxx video clips (adult porn) web-site and you know what, you visited this website to experience fun (you know what I mean). While you were viewing videos, your internet browser started working as a RDP with a key logger which provided me accessibility to your display screen and cam. after that, my software program obtained your complete contacts from your Messenger, Facebook, as well as email . And then I created a double video. First part shows the video you were viewing (you have a good taste lol . . .), and 2nd part displays the view of your web cam, & its u.

You do have a pair of possibilities. We are going to go through the solutions in details:

First alternative is to dismiss this email message. In such a case, I will send your actual video to each one of your contacts and also just consider about the awkwardness you feel. Do not forget should you be in an intimate relationship, precisely how it will certainly affect?

Next choice will be to give me \$5000. We are going to describe it as a donation. In this scenario, I will straightaway delete your video footage. You will continue on your daily life like this never occurred and you are never going to hear back again from me.

You'll make the payment via Bitcoin (if you don't know this, search "how to buy bitcoin" in Google).

BTC Address: 14Hi644NfDiE1ZXXwjndApiqVxAXKjqbzs  
[CASE sensitive, copy and paste it]

In case you are curious about going to the law enforcement officials, very well, this e mail cannot be traced back to me. I have taken care of my steps. I am not looking to ask you for so much, I simply prefer to be rewarded.

You have one day to pay. I have a specific pixel within this mail, and right now I know that you have read this e mail. If I don't receive the BitCoins, I will, no doubt send your video recording to all of your contacts including close relatives, coworkers, and so on. Nonetheless, if I receive the payment, I will destroy the video immediately. If you want proof. reply with Yes! then I will certainly send out your video to your 5 friends. This is

# Attacker's Evolve

**Hoax bomb threat cyber extortion emails similar to sex video threats**

**Extortion emails carrying bomb threats cause panic across the US**

Police in New York, Chicago, Detroit, San Francisco, and Washington tell Americans to stay calm.

**'Spam' bomb threats at schools and businesses nationwide demand Bitcoin ransom payments**

**Sandy Hook Elementary School evacuated over bomb threat on sixth anniversary of shooting**

**A series of email bomb threats shock the US, criminals want Bitcoin**

# Ransomware

## A Crash Course

# What Is Ransomware?

## What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA\\_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

## What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

## How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

## What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.

If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

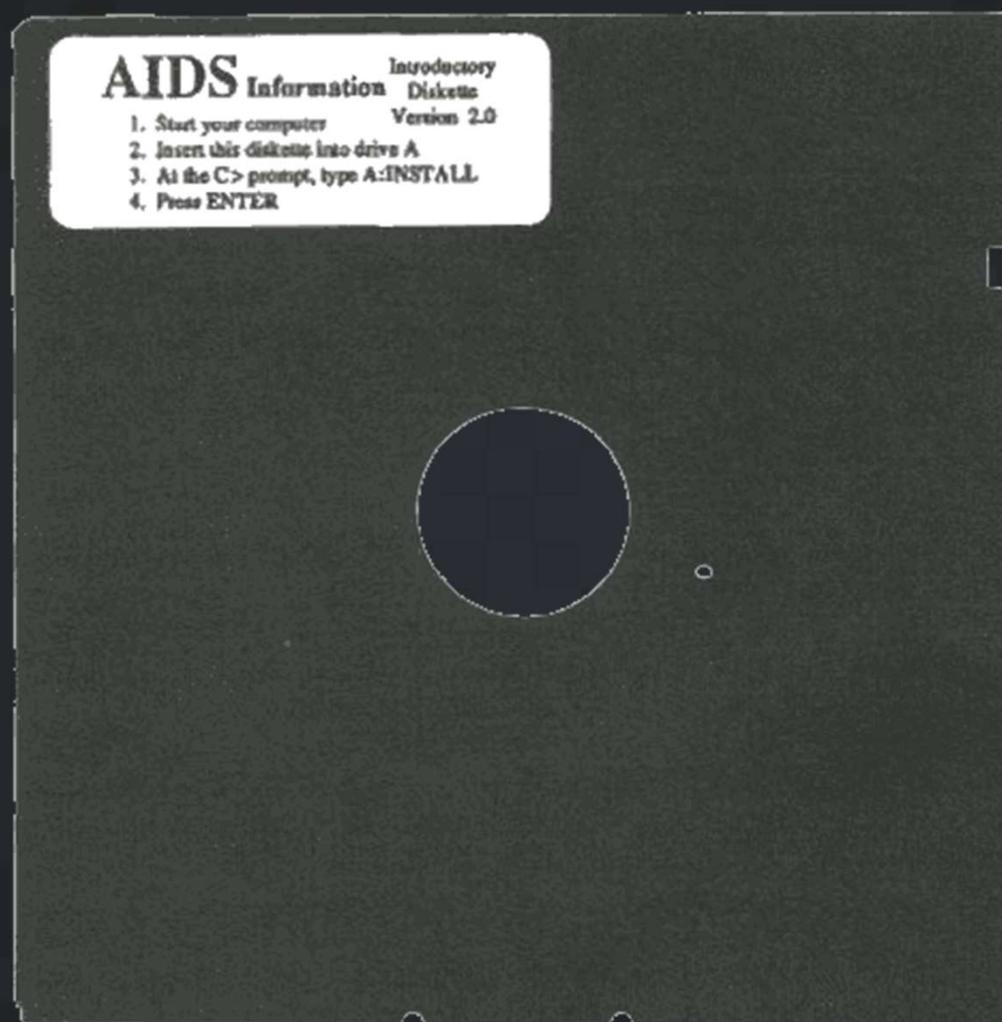
1. [REDACTED].com/1L6N5x9
2. [REDACTED]/1L6N5x9
3. [REDACTED]om/1L6N5x9
4. [REDACTED]

If for some reasons the addresses are not available, follow these steps:

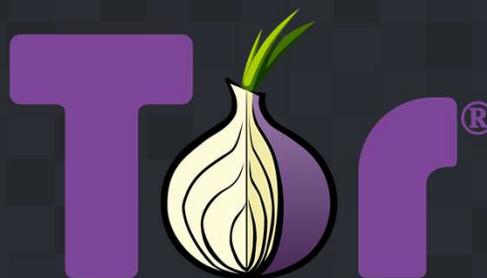
1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. [REDACTED] Type in the address bar
4. Follow the instructions on the site.

**IMPORTANT INFORMATION:**

# AIDS Trojan - 1989



# Game Changers



TorProject.org



# Where Are We Now?

## YOUR COMPUTER AND FILES ARE ENCRYPTED

YOU MUST PAY 0.2 BITCOINS TO UNLOCK YOUR COMPUTER

YOUR FILES HAVE  
ESSENTIAL INFORMATION  
AND YOUR

ONCE YOUR  
FILES

Your computer files have been encrypted. Your photos, videos, documents, etc....  
But, don't worry! I have not deleted them, yet.  
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.  
Every hour files will be deleted. Increasing in amount every time.  
After 72 hours all that are left will be deleted.

If you do not have bitcoin  
Purchase 150 American Dollars  
Send to the Bitcoin address  
Within two minutes of receipt  
Try anything funny and the  
As soon as the payment is

Thank you

1GB

IF YOU DO NOT  
IF YOU HAVE MADE

59:59

1 file will be deleted.

View encrypted files

Please, send \$150 worth of

15fyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ

I made a payment, now give me back my

## YOUR COMPUTER AND FILES ARE ENCRYPTED

**\$125 WITHIN 24 HOURS. \$199 AFTER 24 HOURS**  
**OPERATING SYSTEM AND FILES DELETED AFTER 72 HOURS**

-----WRITE THIS INFORMATION DOWN-----

Email: [supportfile@yandex.com](mailto:supportfile@yandex.com)

The same information is on your desktop called  
Payment\_Instructions  
Ransom Id:

BTC Address: 1HxkJ3vz2tvpchGdt9yyY4XivdY9jKkcZH

IF YOU LOOSE THIS INFO YOU WILL NOT BE ABLE TO CONTACT US

Your computer files have been encrypted and moved to a hidden  
encrypted partition on your computer.

Without the decryption password you will not get them back.  
No matter what you do the files will not re-appear and be  
decrypted until you pay.

Once payment is received you will get the decryption password  
and simple instructions to restore all your files and computer  
to normal instantly. Email us if you need assistance or have paid.

Email: [supportfile@yandex.com](mailto:supportfile@yandex.com)

DO NOT LOOSE THE CONTACT INFO

Emotet, Trickbot, Ryuk... Oh My!

# What is Emotet?



One of the most widely distributed and actively developed malware families used by cybercriminals today.



Started as a banking trojan, but now also functions as a dropper for other payloads.



Can cause persistent infections, credential theft, account lockouts, email hijacking, and fraudulent bank account transfers and withdrawals.

# Why do we care?



US-CERT estimates that Emotet is one of the most costly and destructive malware families affecting public and private sectors.



Emotet poses a serious threat to businesses, and individual users, with the number of Emotet-related cases remaining consistently high.

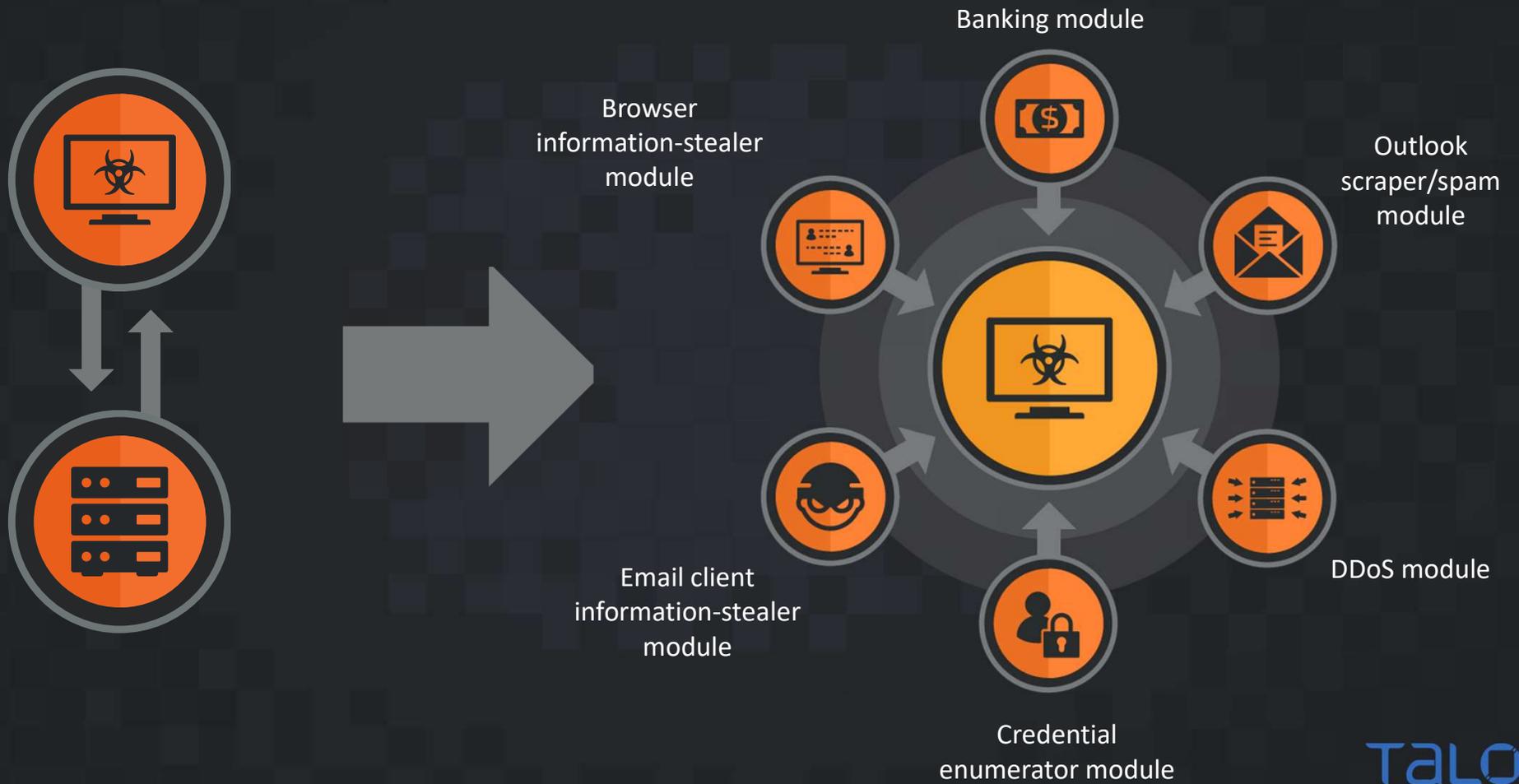


Infections cause loss of sensitive or proprietary data, financial damages, reputational harm, and operational downtime.

# Distribution



# Modules



# Network Propagation

## Brute Forcing Passwords

- Downloads spreader module that contains a password list
- Uses list to brute force access to other machines on the same network
- Can cause unauthorized access, operational downtime, and loss in productivity

# Network Propagation

## Brute Forcing Passwords

- Downloads spreader module that contains a password list
- Uses list to brute force access to other machines on the same network
- Can cause unauthorized access, operational downtime, and loss in productivity

## Malspam

- Installs a spam module to move laterally across the network
- Scrapes email accounts and sends malicious messages to addresses in those contact lists
- Harder to block by anti-spam systems since they come from the victim's legitimate infrastructure

# Network Propagation

## Brute Forcing Passwords

- Downloads spreader module that contains a password list
- Uses list to brute force access to other machines on the same network
- Can cause unauthorized access, operational downtime, and loss in productivity

## Malspam

- Installs a spam module to move laterally across the network
- Scrapes email accounts and sends malicious messages to addresses in those contact lists
- Harder to block by anti-spam systems since they come from the victim's legitimate infrastructure

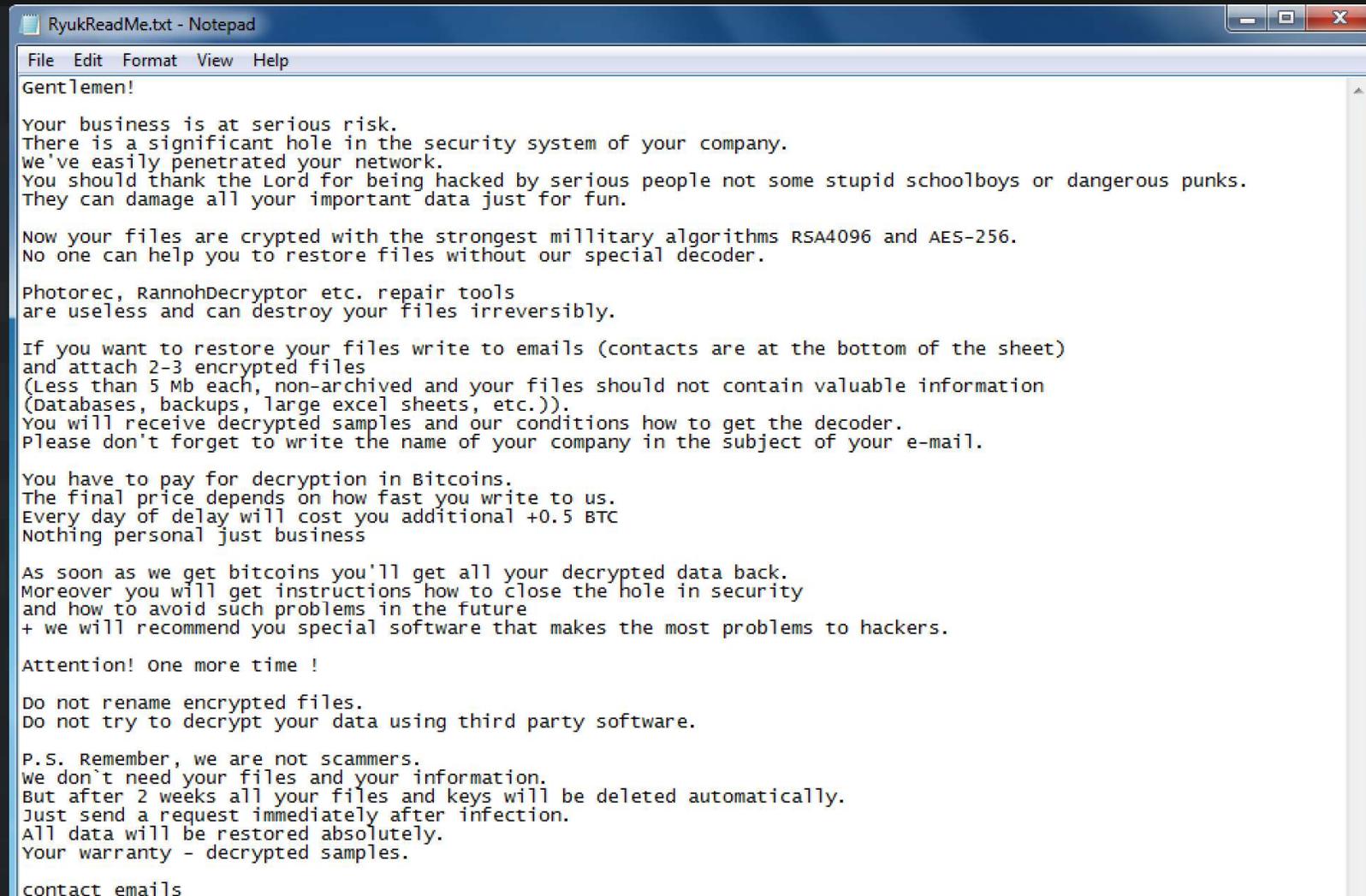
## EternalBlue

- Emotet uses EternalBlue to attack unpatched systems by exploiting a Windows vulnerability in the SMB protocol.

# Delivery of Different Payloads



# Ryuk Ransom Note



RyukReadMe.txt - Notepad

File Edit Format View Help

Gentlemen!

Your business is at serious risk.  
There is a significant hole in the security system of your company.  
We've easily penetrated your network.  
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.  
They can damage all your important data just for fun.

Now your files are crypted with the strongest military algorithms RSA4096 and AES-256.  
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools  
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)  
and attach 2-3 encrypted files  
(Less than 5 Mb each, non-archived and your files should not contain valuable information  
(Databases, backups, large excel sheets, etc.)).  
You will receive decrypted samples and our conditions how to get the decoder.  
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.  
The final price depends on how fast you write to us.  
Every day of delay will cost you additional +0.5 BTC  
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.  
Moreover you will get instructions how to close the hole in security  
and how to avoid such problems in the future  
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.  
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.  
We don't need your files and your information.  
But after 2 weeks all your files and keys will be deleted automatically.  
Just send a request immediately after infection.  
All data will be restored absolutely.  
Your warranty - decrypted samples.

contact emails

# Recent Events



In June 2019, the Emotet botnet went offline, with C2 infrastructure no longer operational.



New Emotet activity ceased during a period of inactivity for several months.

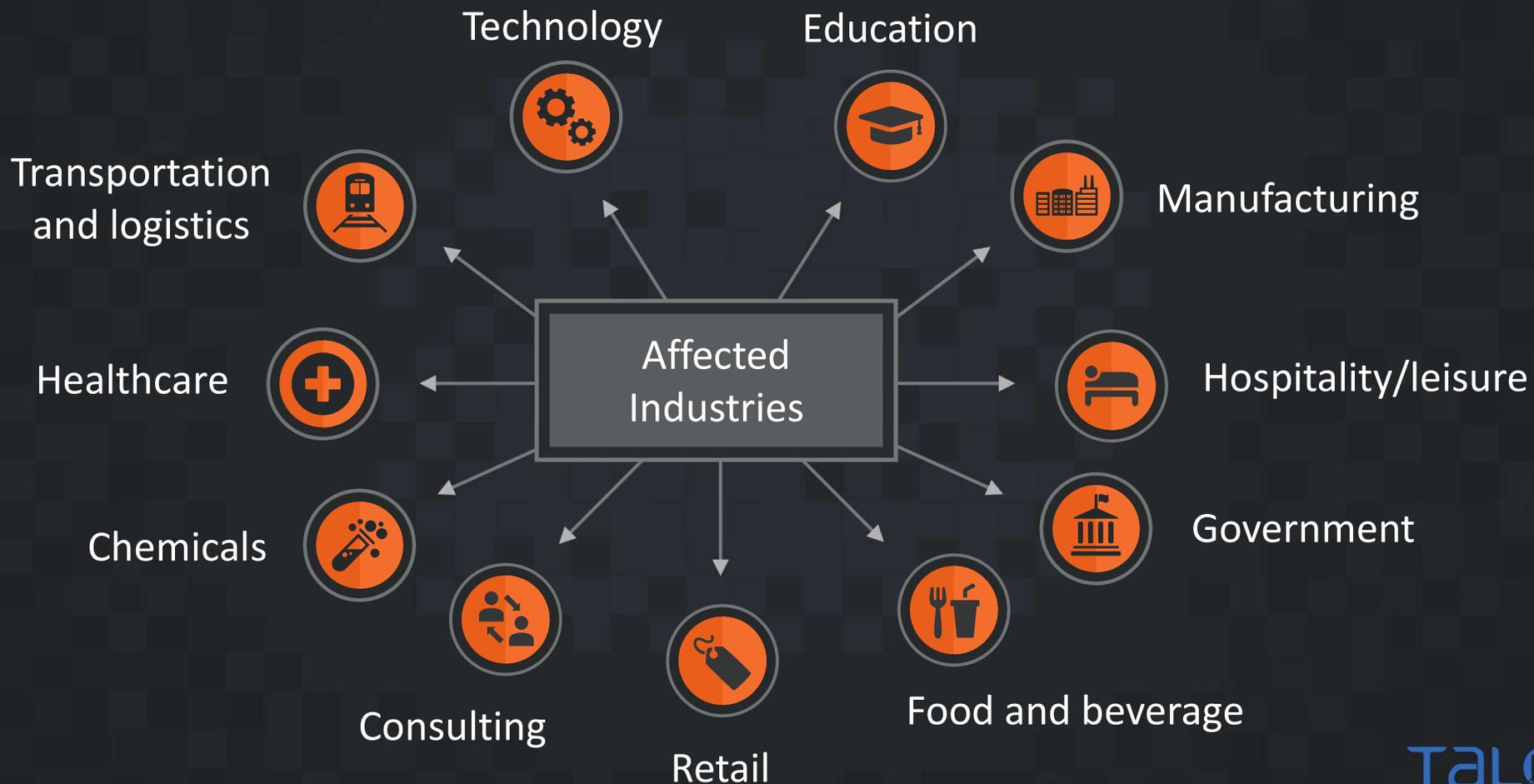


In September, the Emotet botnet came back online and distribution activity resumed in high volumes.

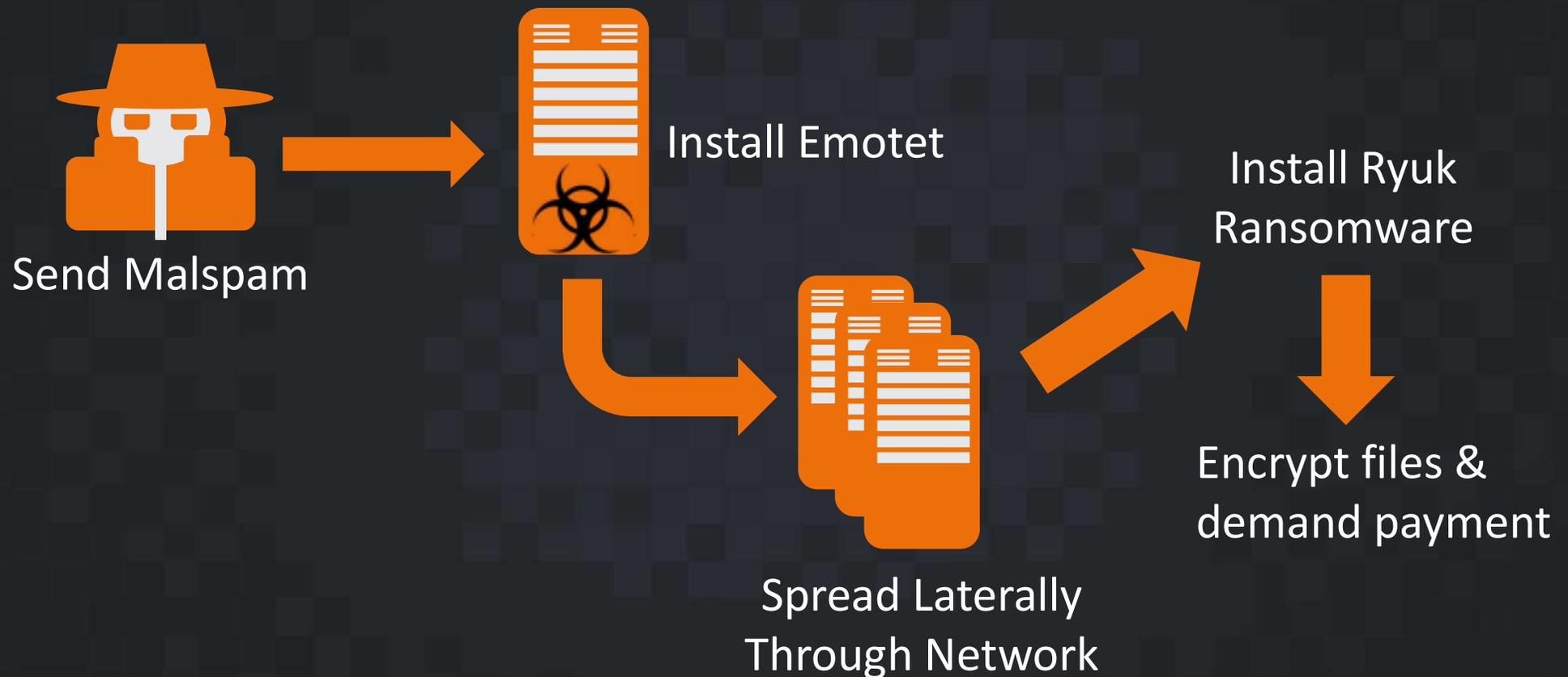


Emotet is currently active with new campaigns being observed very frequently.

# Targeting and Victimology



# 2019 – The Year Of “Big Game Hunting”



# Big Game Hunting Is Profitable



# Ryuk – Profitability Analysis

~400 Ryuk Samples

12vs0ry1XrPjPCaH8gWzDJeYT7dhTmpcjL  
1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY  
1FtQnqvjxEK5GJD9PthHM4MtdmkAeTeoRt  
14aJo5L9PTZhv8XX6qRf  
1E4f0qzCvS8wgqy5T7n  
1GXgngwDMSJZ1Vahmf6  
1Cyh35KqhhDewmXy63yp  
15LsUgfnuGc1PsHJPcf

Summary	
Address	<a href="#">1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY</a>
Hash 160	<a href="#">cfe033645641e20c5df91a091014fe5d8b90be9f</a>
Transactions	
No. Transactions	16
Total Received	182.9999668 BTC
Final Balance	0 BTC



# Ryuk Profits

Bitcoin Wallet Address	Bitcoins Received	Value in USD
1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY	182.9999668	\$1,462,484.49
12vsQry1XrPjPCaH8gWzDJeYT7dhTmcpjL	55	\$439,544.60
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj	50.41	\$402,862.61
1FtQnqvjxEK5GJD9PthHM4MtdmkAeTeoRt	48.25	\$385,600.49
1L9fYHJJxeLMD2yyhh1cMFU2EWF5ihgAmJ	40.035	\$319,948.51
1FRNVupsCyTjUvF36GxHZrvLaPtY6hgkTm	38.9999859	\$311,676.97
1Jq3WwsaPA7LXwRNYsfySsd8aojdmkFnW	35	\$279,710.20
1C8n86EEttnDjNKM9Tjm7QNVgwGBncQhDs	30.00821708	\$239,817.27
1GXgngwDMSJZ1Vahmf6iexKVePPxsxGS6H	30.00217032	\$239,768.94
1ChnbV4Rt7nsb5acw5YfYvBFDj1RXcVQu	28	\$223,768.16
14aJo5L9PTZhv8XX6qRPncbTXecb8Qohqb	25.00016544	\$199,794.32
19AE1YN6Jo8ognKdJQ3xeQQL1mSZyX16op	25	\$199,793.00
1CW4kTqeoedinSmZiPYH7kvn4qP3mDJQVa	24.077	\$192,416.64
18eu6KrFgzv8yTMVvKJkRM3YBAyHLonk5G	30	\$159,834.40
1CbP3cgi1Bcjuz6g2Fvwk4tVhqohqAVpDQ	13	\$103,892.36
1KUbXkjDZL6HC3Er34HwJiQUAE9H81Wcsr	10	\$79,917.20
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk	10	\$79,917.20
1NuMXQMUXcngJ7MNQ276KdaXQgGjpfPhK	10	\$79,917.20
129L4gRSYgVJTRCgbPDtvYPabnk2QnY9sq	6.4995167	\$51,942.32
1ET85GTps8eFbgF1MvVhFVZQeNp2a6LeGw	3.325	\$26,572.47
1Cyh35KqhhDewmXy63yp9ZMqBnAWE4oJRr	2.79993008	\$22,376.26
1K6MBjz79QqfLBN7XBnwxCJb8DYUmmDWAt	1.70004113	\$13,586.25
1E4fQqzCvS8wgqy5T7n1DW8JMNMaUbeFAS	0.001	\$7.99
<b>Total</b>	<b>700.1079935</b>	<b>\$5,515,149.85</b>

# Protection



Routinely update and patch software and operating systems



Disable macros



Perform system hardening



Implement a data backup and recovery plan



Enable advanced event logging and monitoring



Exercise anti-phishing best practices



Actively whitelist and blacklist applications



Create long, complex passwords and use multi-factor authentication

# Remediation Steps

- 1** Disconnect and reimage the infected machine
- 2** In extreme cases, disconnect the network from the internet
- 3** Quarantine infected systems on VLAN
- 4** Prevent logins from domain or shared local administrator accounts
- 5** Reformat file systems and reinstall operating systems and applications
- 6** Move hosts to a staging VLAN for monitoring and patching
- 7** Restore critical data
- 8** Change all passwords
- 9** Review infected users' log files and Outlook mailbox rules

# Forcing the Bad Guys to Innovate

Spreading security news, updates, and other information to the public.



Talos publicly shares security information through numerous channels to help make the internet safer for everyone.



TALOSINTELLIGENCE.COM



@talossecurity



blog.talosintelligence.com

TALOS  
Cisco Security Research