Talos

Cisco Security Research

DNS

Warren Mercer & Paul Rascagneres

About Me

Paul Rascagneres

- prascagn@cisco.com // @r00tbsd
- Security researcher at Cisco Talos
- Worked on several Talos investigations:
  - Wannacry
  - Nyetya / MEDoc
  - BadRabbit
  - CCleaner
  - Group123 / ROKRAT
  - Olympic Destroyer
  - DNSpionage
  - …
- Malware & APT hunter for too many years…

When I reverse Delphi
Or VB

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

Agenda – We do have one!

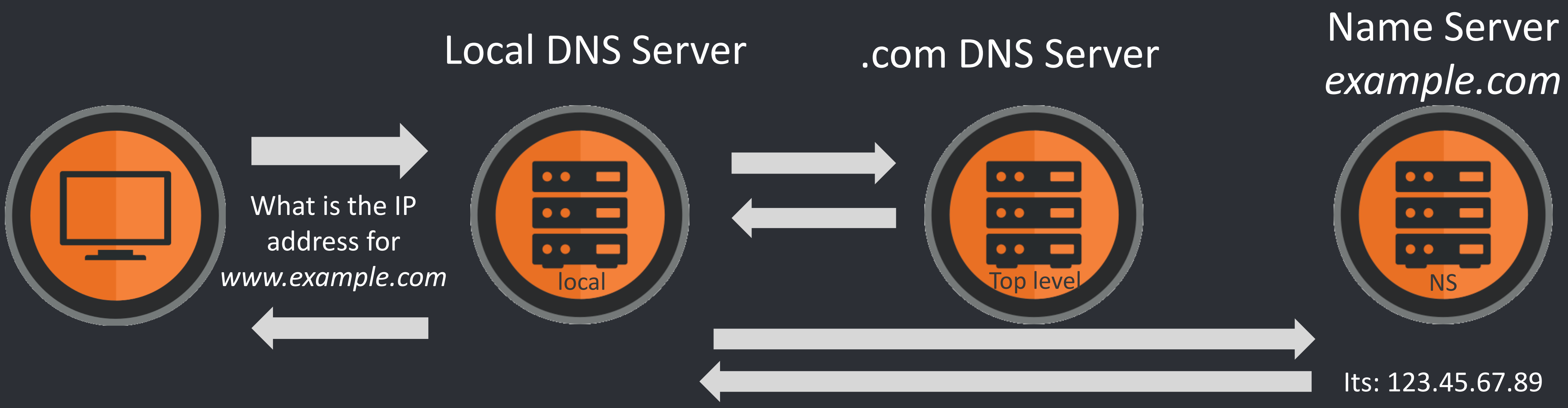
- Brief DNS introduction
  DNS Protocol & Hijacking
- DNSpionage (Event 1)
- SeaTurtle (Event 2)
- Protection/Mitigations
- Q&A – no hard questions allowed!

DNS Protocol

&

DNS Hijacking

Brief Introduction to DNS



Local DNS Server

.com DNS Server

Name Server
example.com

What is the IP
address for
www.example.com

local

Top level

NS

Its: 123.45.67.89

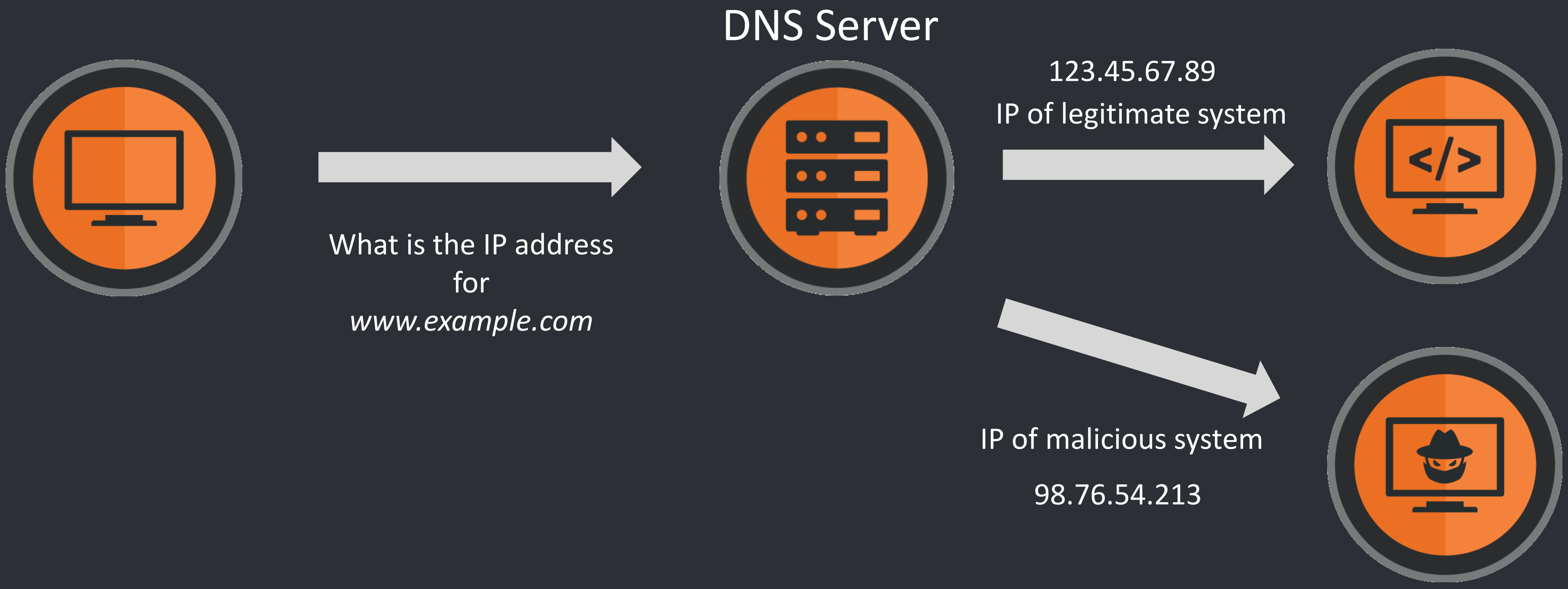
“I don’t know,
I’ll ask
someone else”

“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

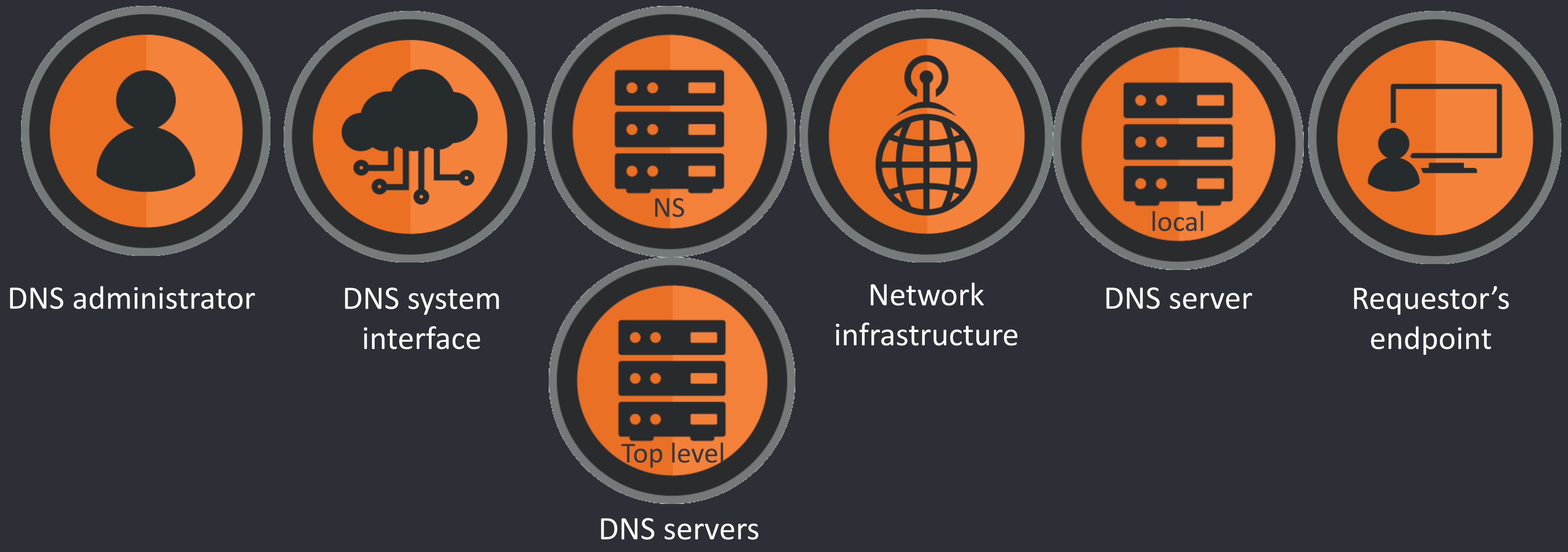
IP of legitimate system

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

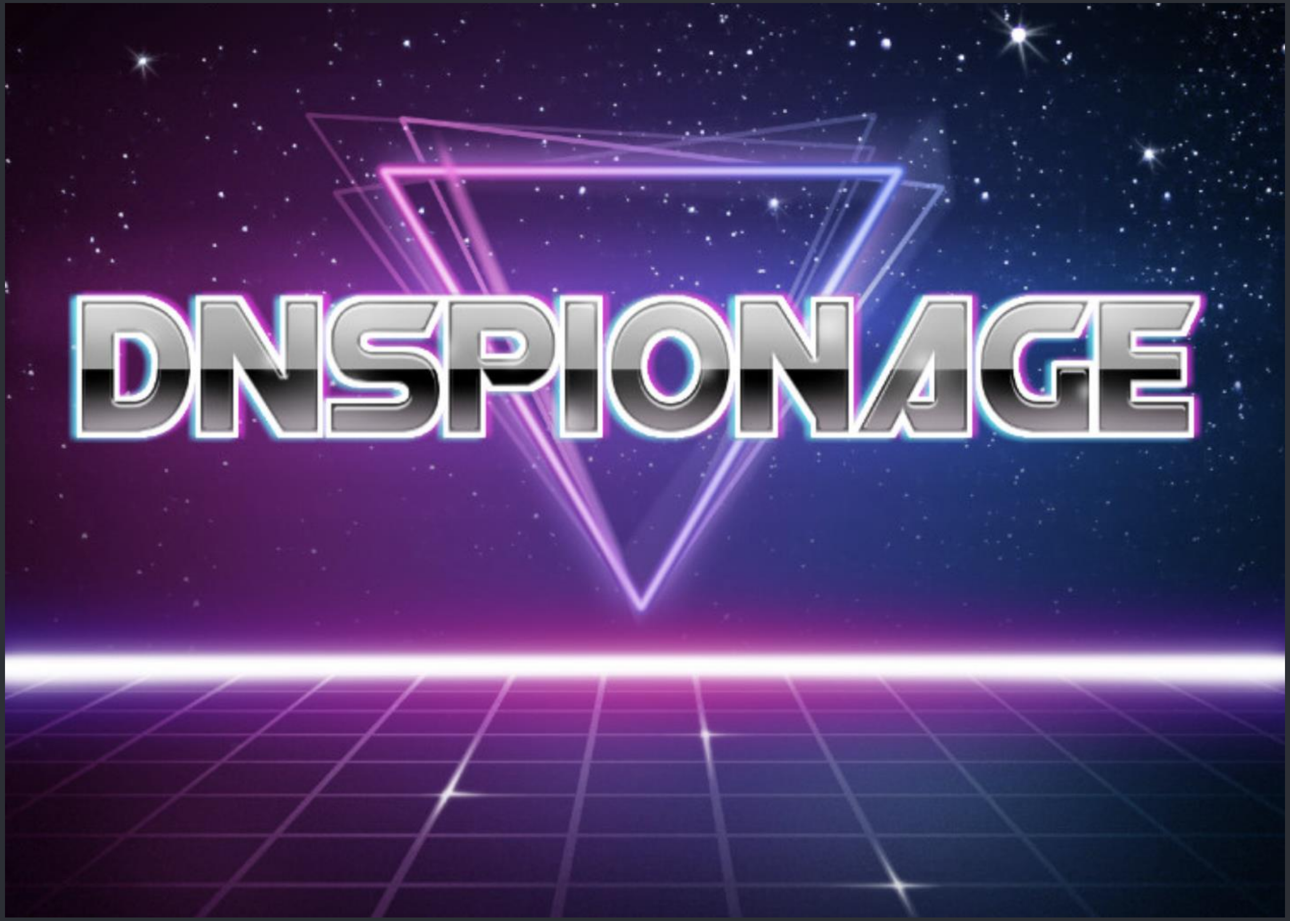
DNS Redirection Attacks

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…

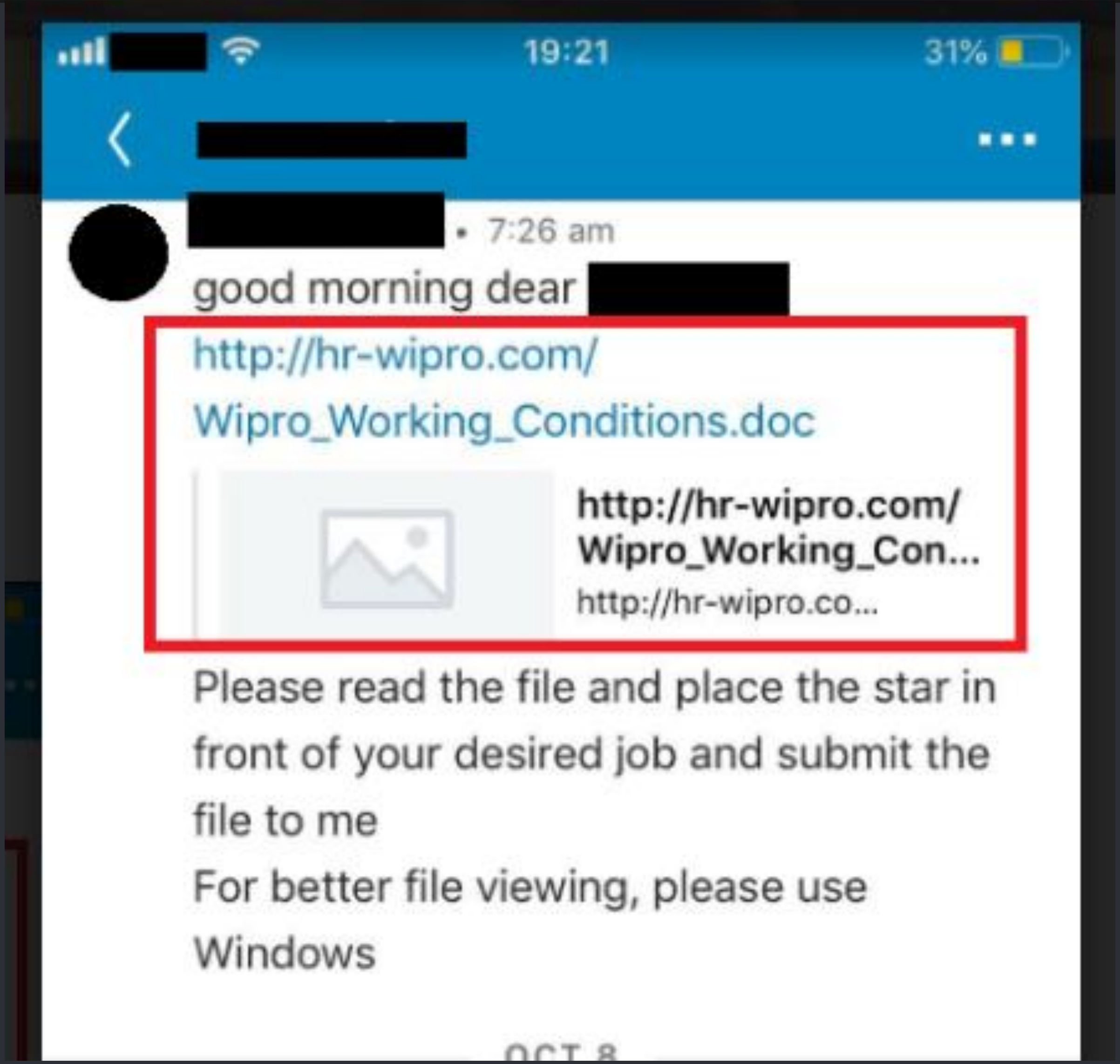
Event #1



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]

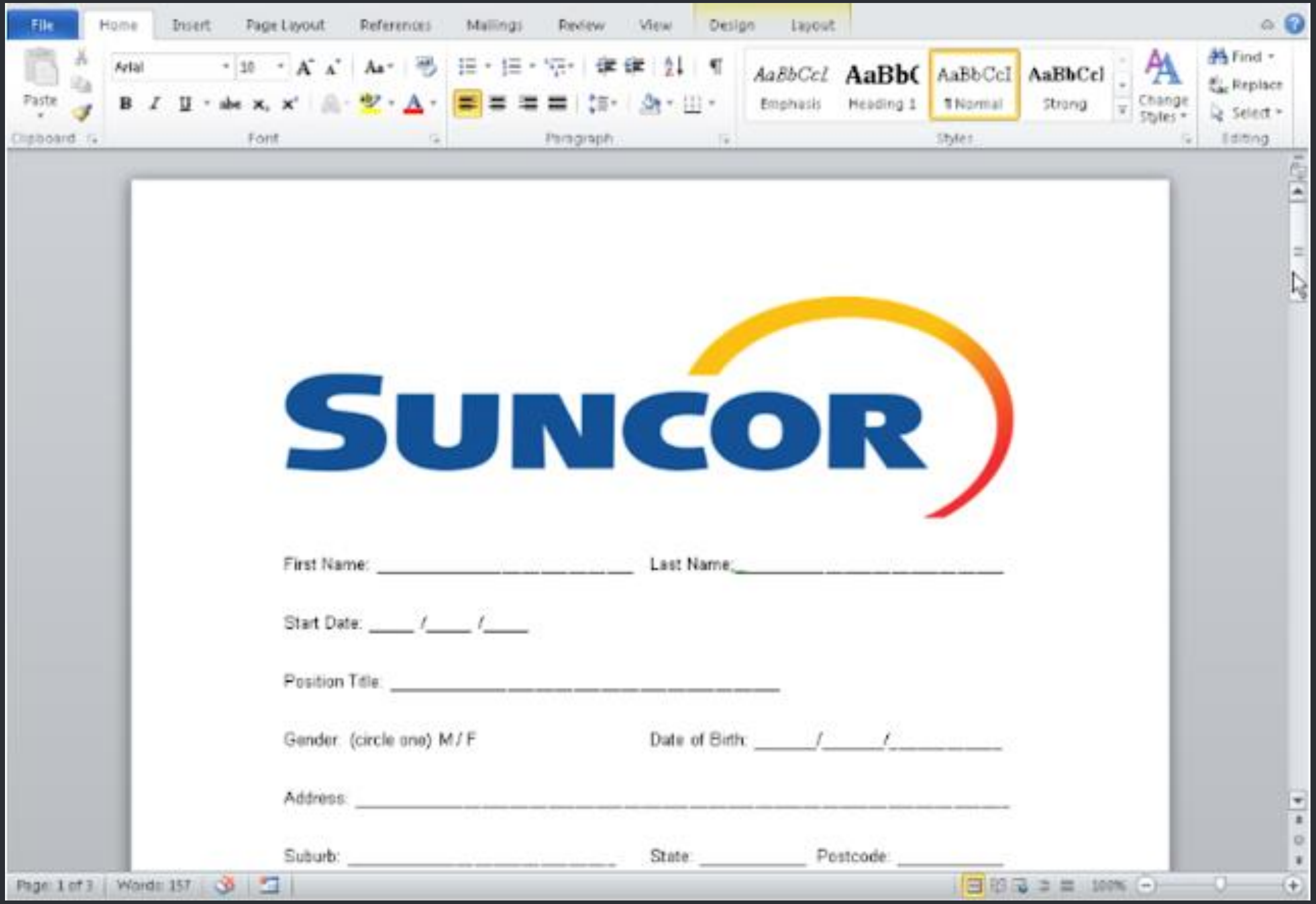
http://hr-wipro.com/Wipro_Working_Conditions.doc

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

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

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

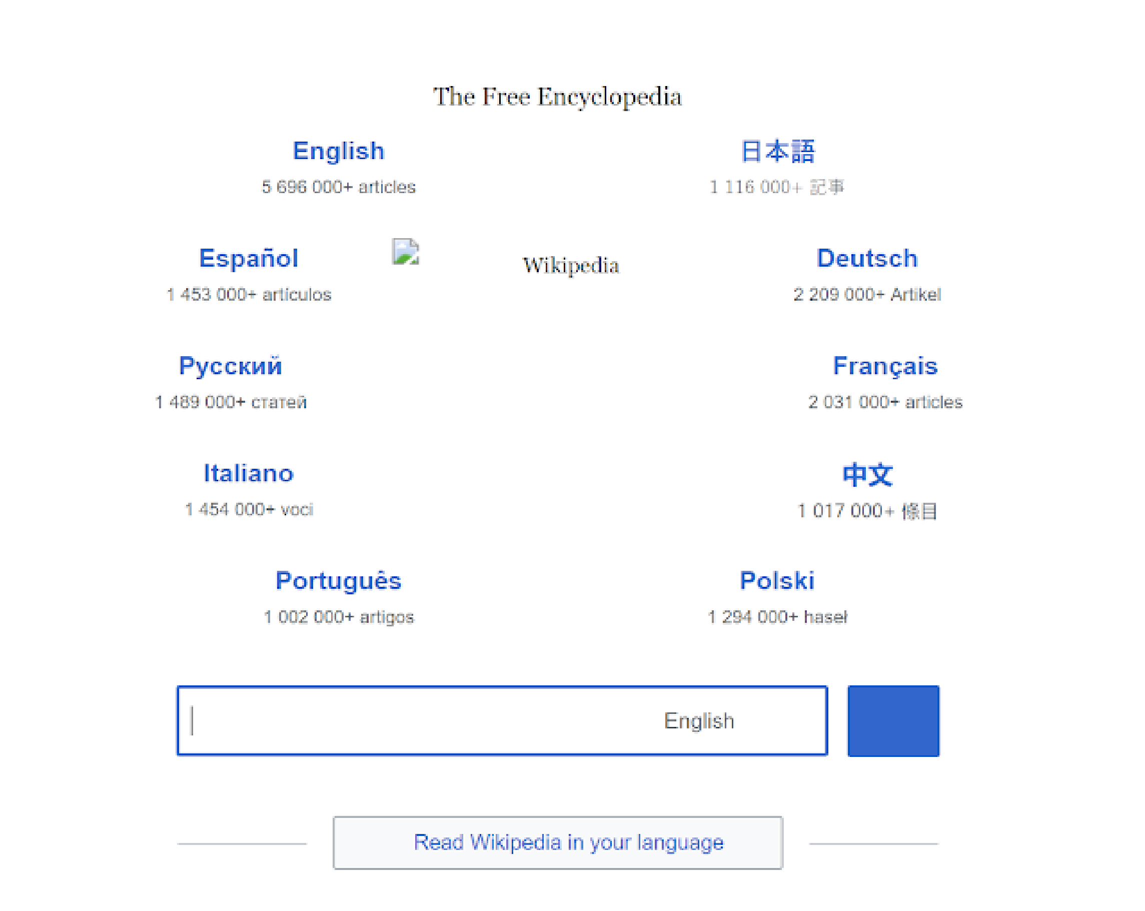
A very handy file that contains plaintext logging info.

Configure.txt

A text file containing configuration information.

DNSpionage

HTTP Mode



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

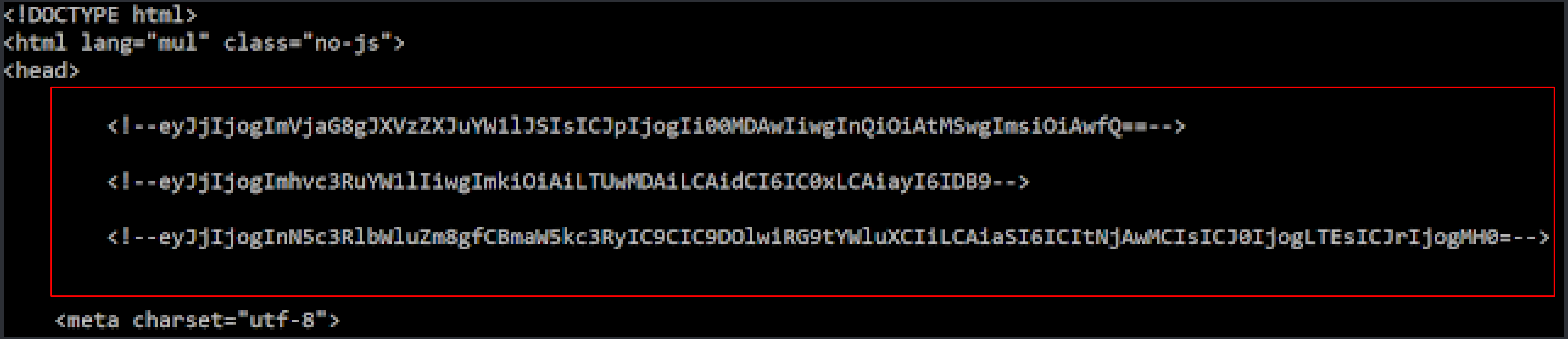
Polski
1 294 000+ haseł

- 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.

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">
```

DNSpionage

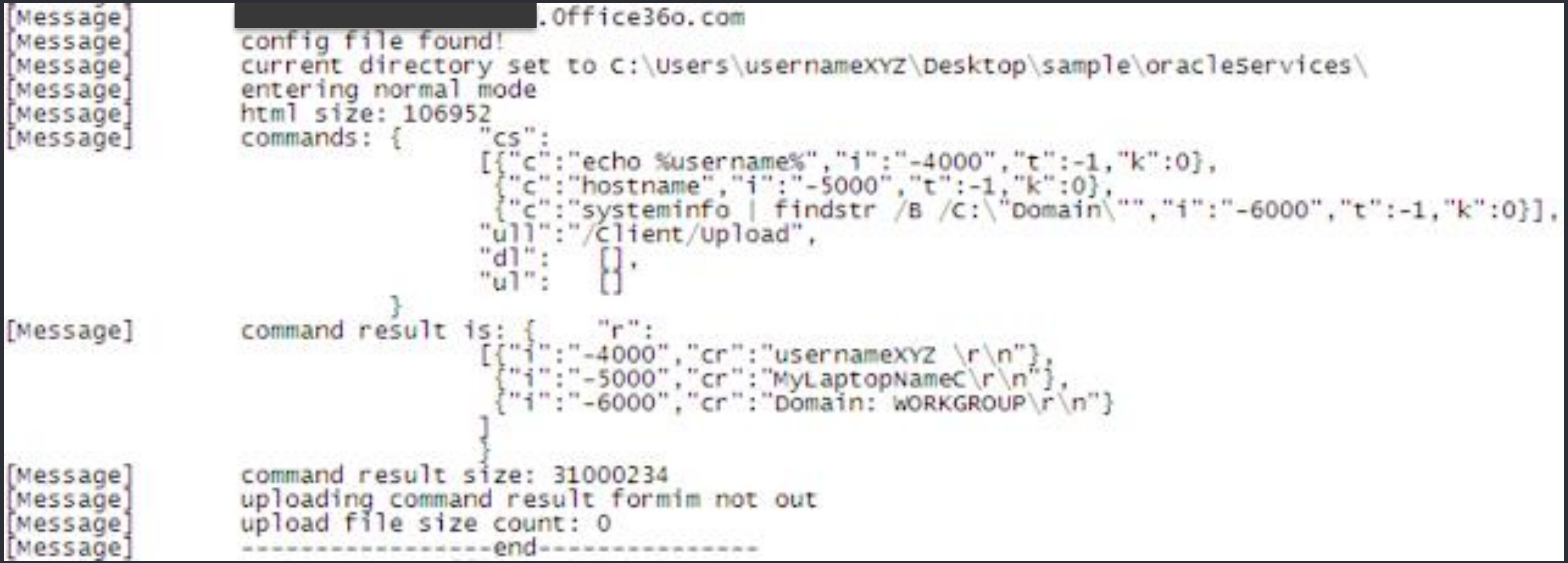
HTTP Mode

- 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].Office36o.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---------------
```

DNSpionage

DNS Mode

- 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 execute.

DNSpionage

DNS Mode

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

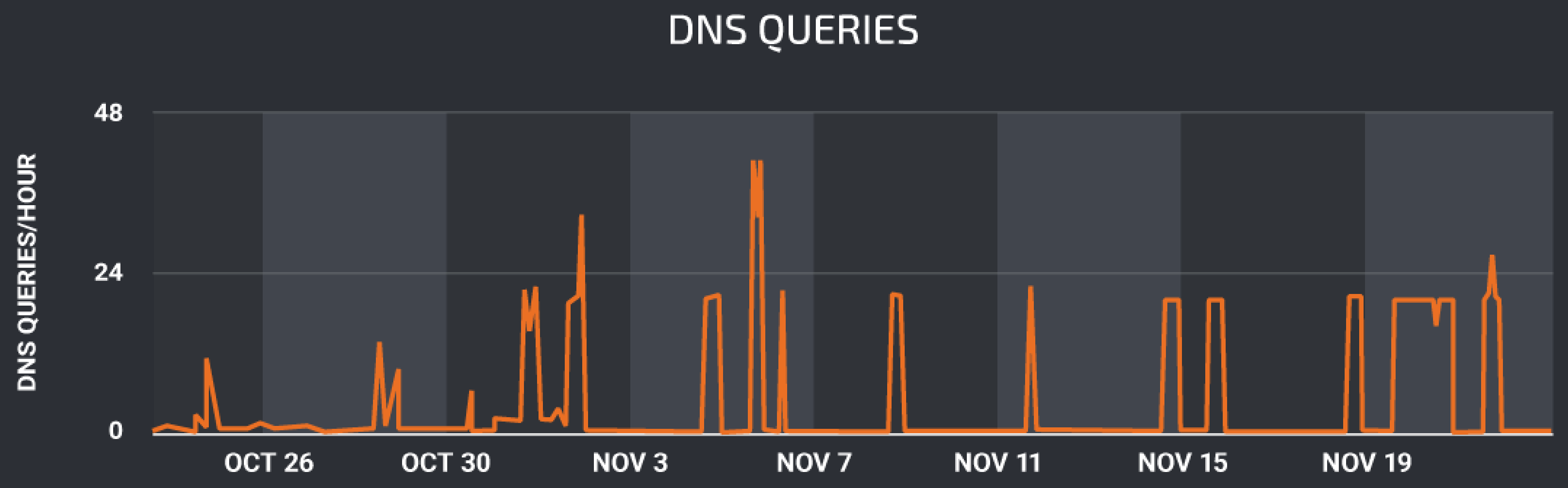
- gLtAGJDVIAJAKZXWY000.0ffice36o[.]com ->
  GJDVIAJAKZXWY000 -> "2GT\x01 Vol”
- TwGHGJDVIATVNVSSA000.0ffice36o[.]com ->
  GJDVIATVNVSSA000 -> "2GT\x02ume”
- 1QMUGJDVIA3JNYQGI000.0ffice36o[.]com ->
  GJDVIA3JNYQGI000 -> "2GT\x03in d”
- iucCGJDVIBDSNF3GK000.0ffice36o[.]com ->
  GJDVIBDSNF3GK000 -> "2GT\x04rive”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



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

DNS Redirection

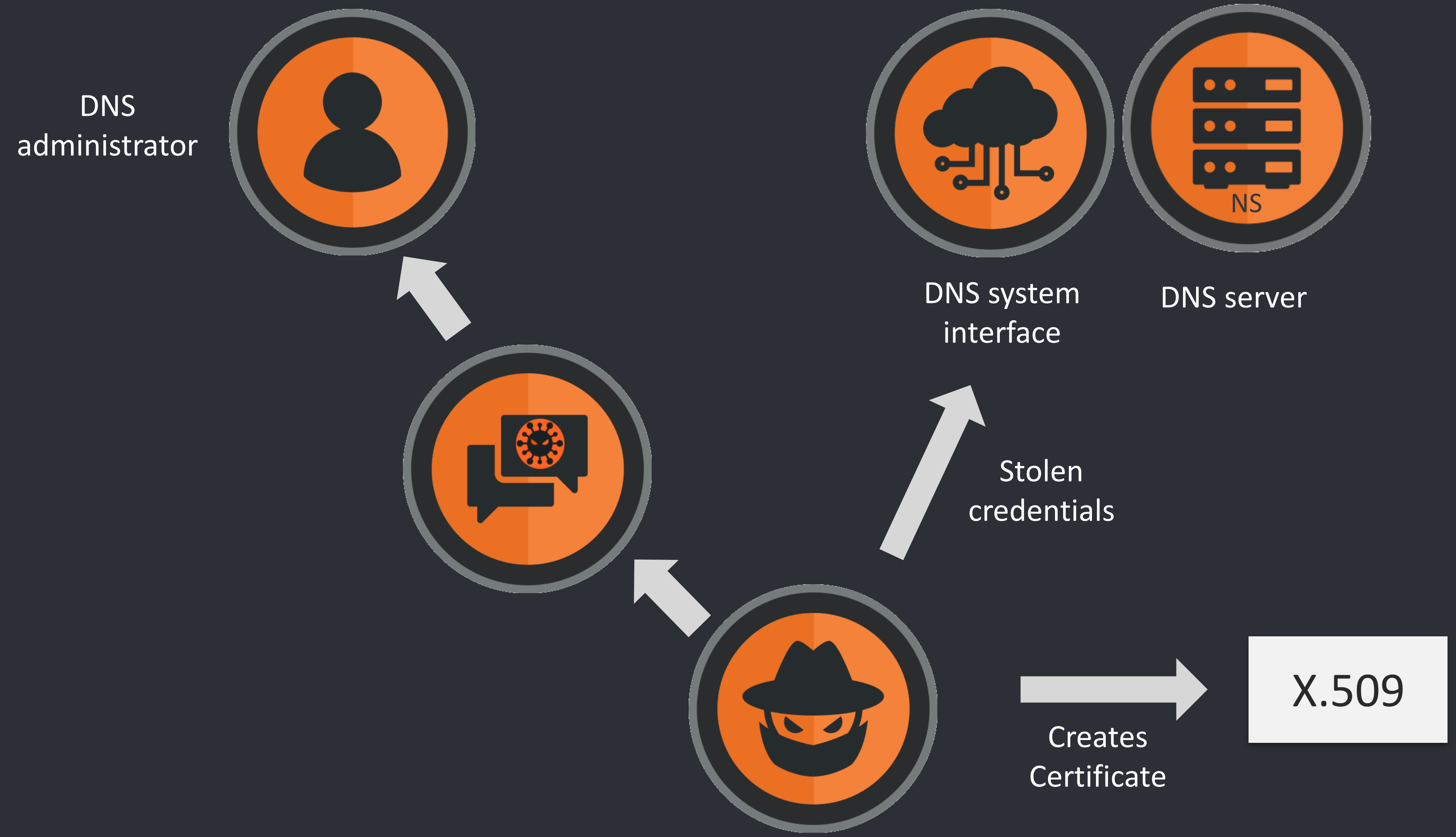
- Within the DNSpionage attack lies DNS redirection:
    - 185.20.184.138
    - 185.161.211.72
    - 185.20.187.8

- 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.

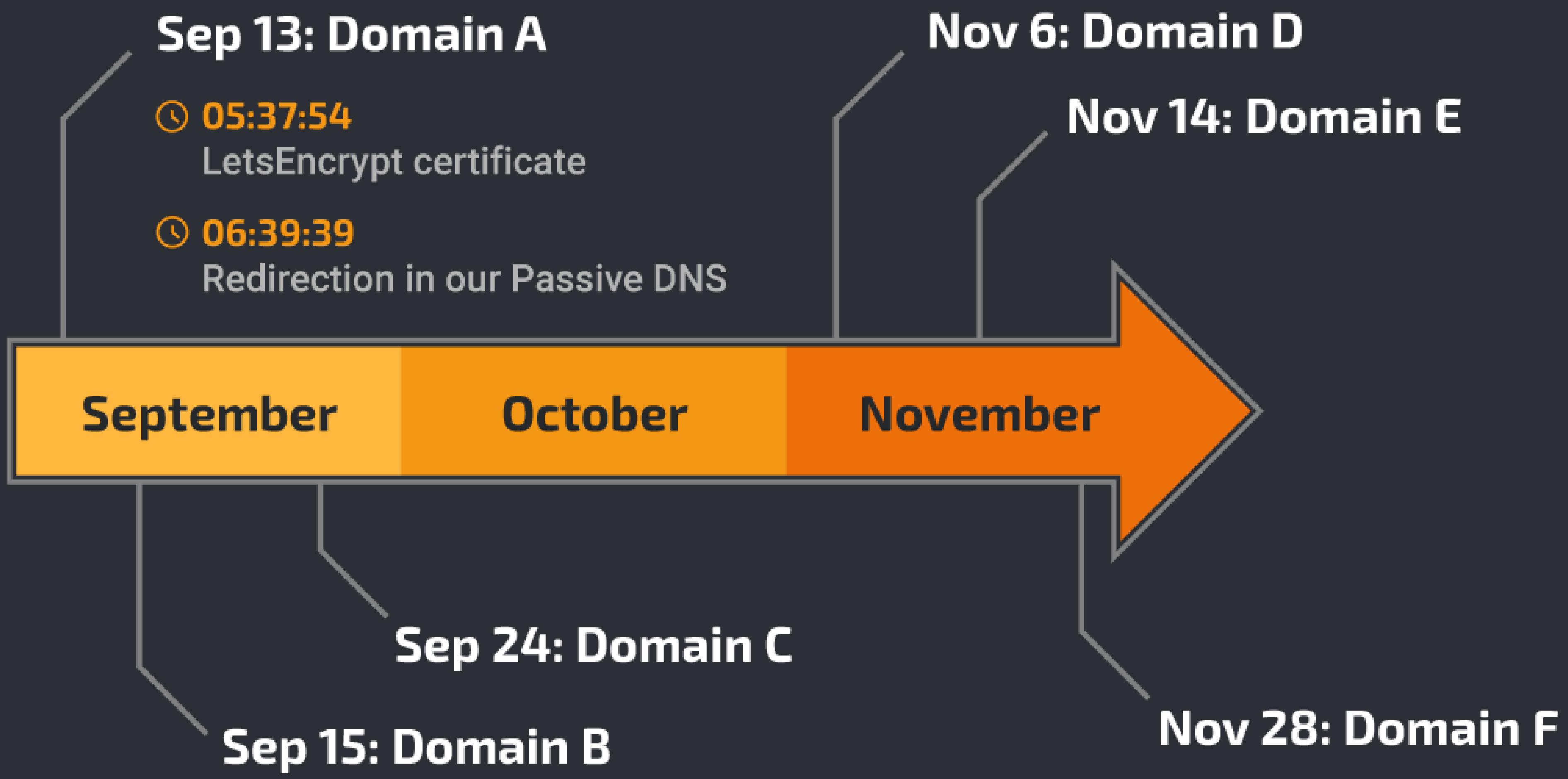
DNSpionage Methodology

Stealing Credentials to Change DNS Records



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

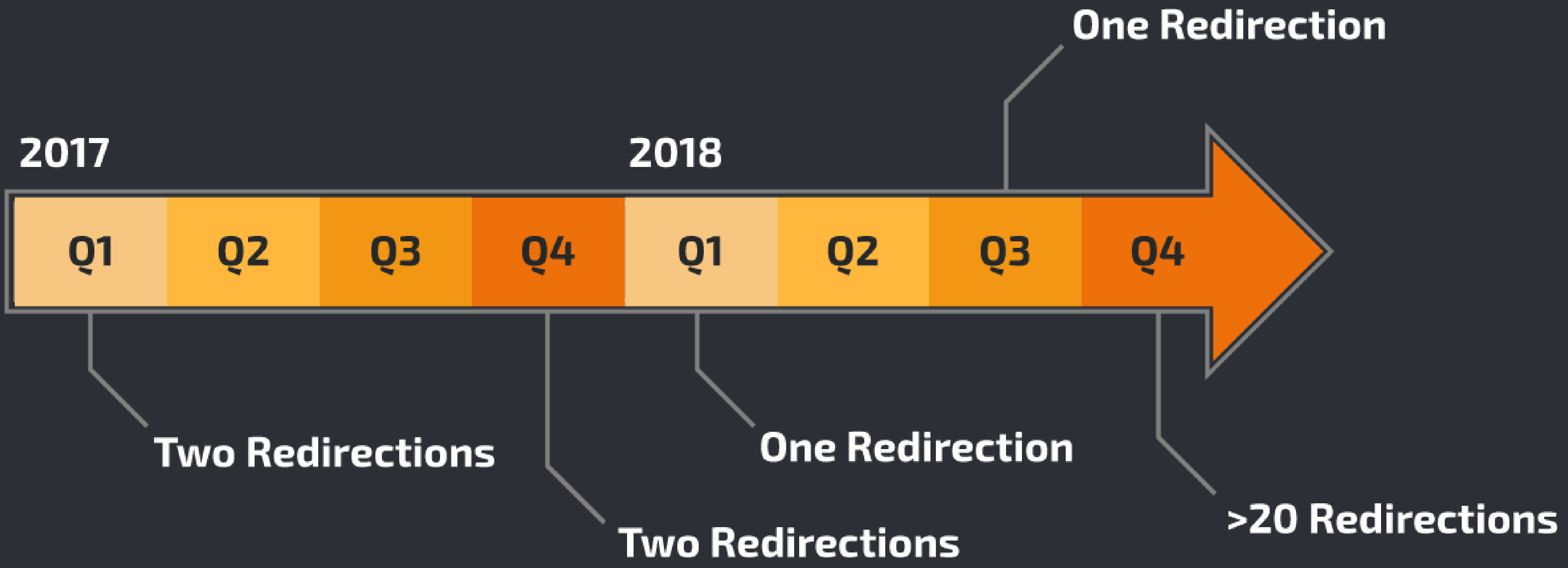
Nov 6: Domain D

Nov 14: Domain E

Nov 28: Domain F

DNS Redirection

2 years of activities



DNS Redirection

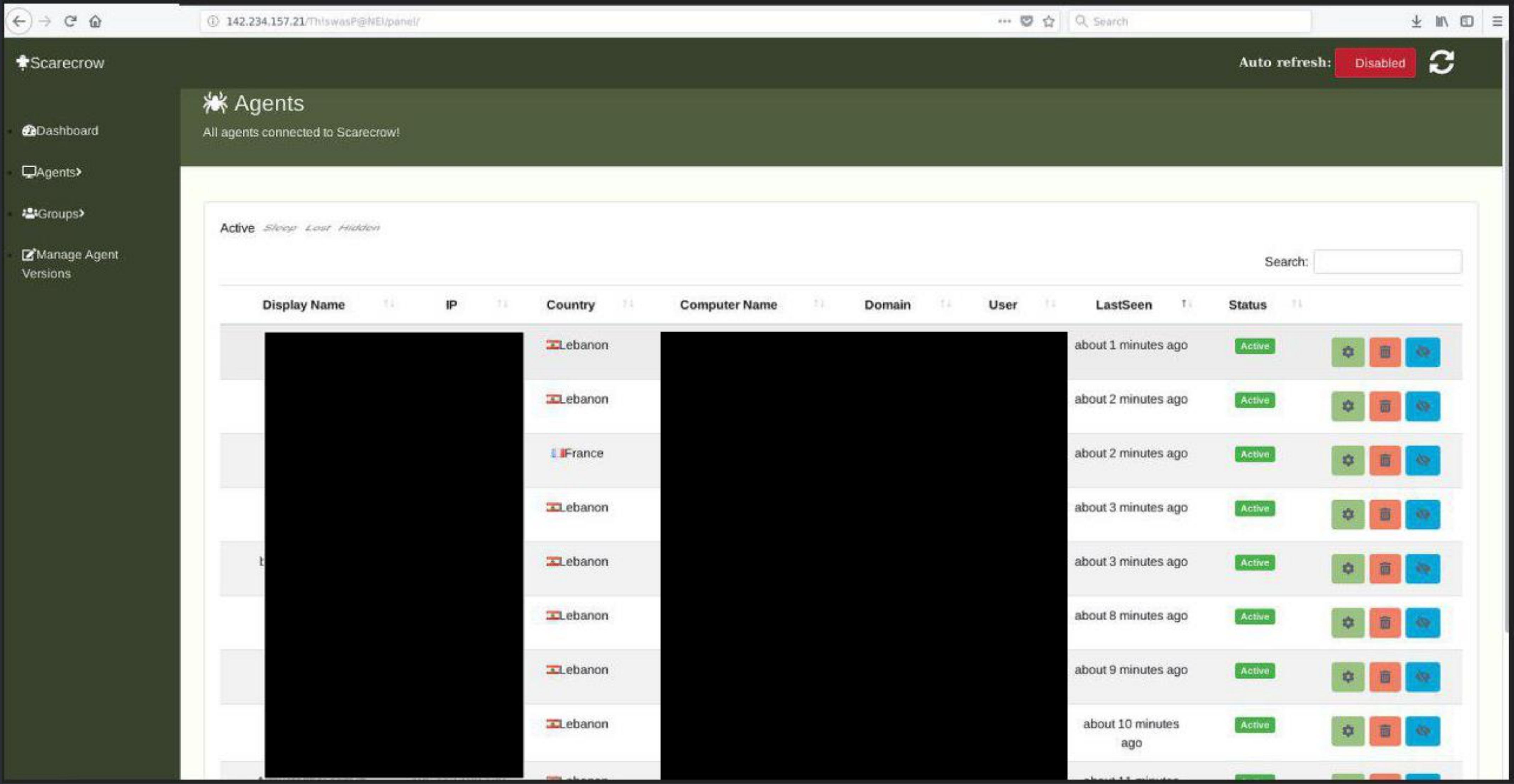
- Few statistics
  - More than 25 identified redirections
  - 2 years of activities
  - A peak during 2018 Q4
  - More than 10 countries
  - Public & private sectors
  - Mainly in Middle-East … few in EU/USA

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….

Oilrig leak



142.234.157.21/Th!swasP@NEl/panel/

Scarecrow

Auto refresh: Disabled

Agents

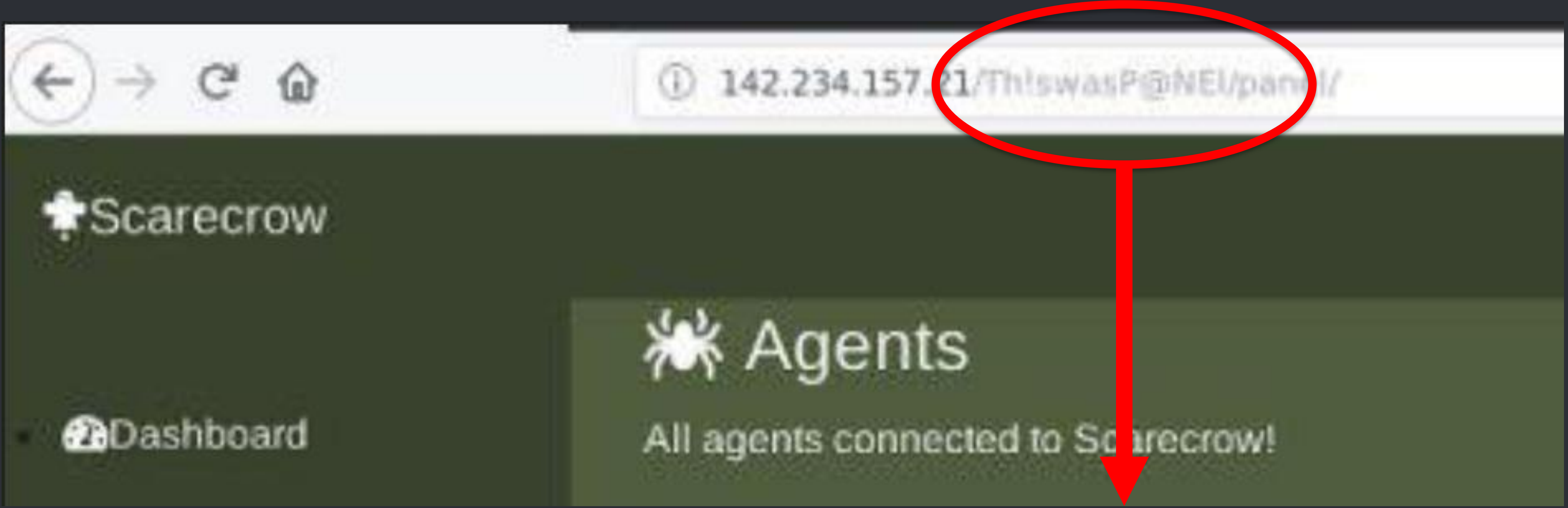
All agents connected to Scarecrow!

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@NEl/panel/

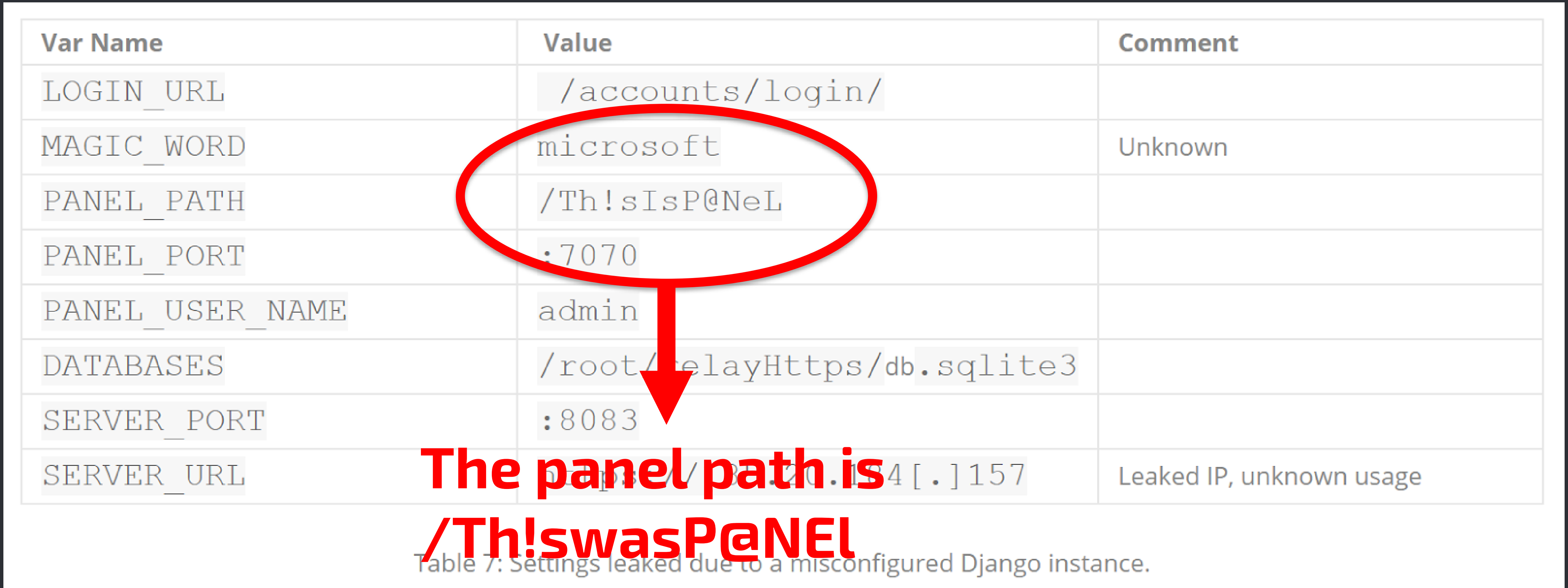
Agents

All agents connected to Scarecrow!

The panel path is /Th!swasP@NEl

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://[illegible]8.20.1[illegible]4[.]157	Leaked IP, unknown usage

The panel path is /Th!swasP@NEl

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

*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

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

Oilrig leak

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

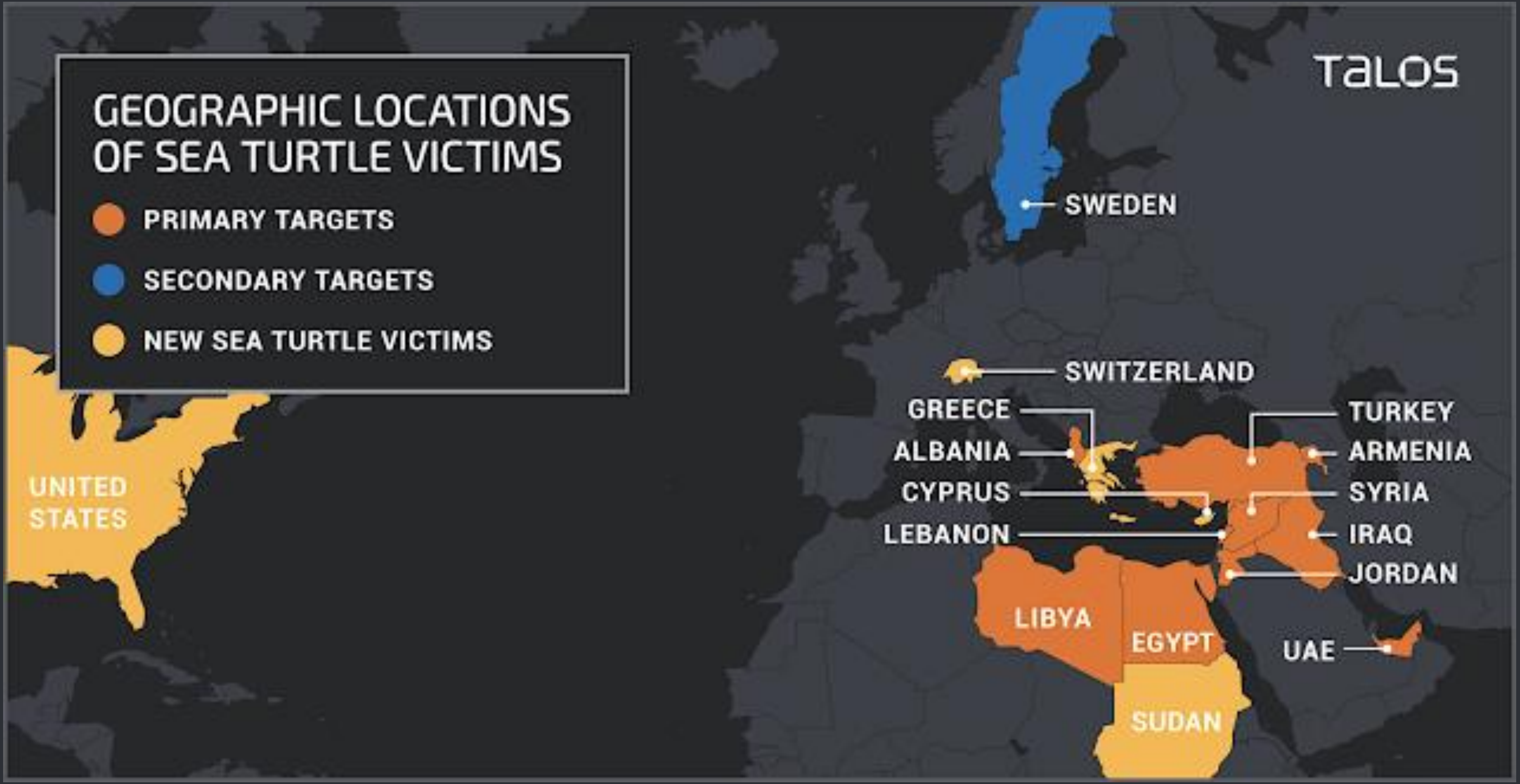
Event #2

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

Victimology Mapping (July 2019)



Registrar vs Registry vs Registrant

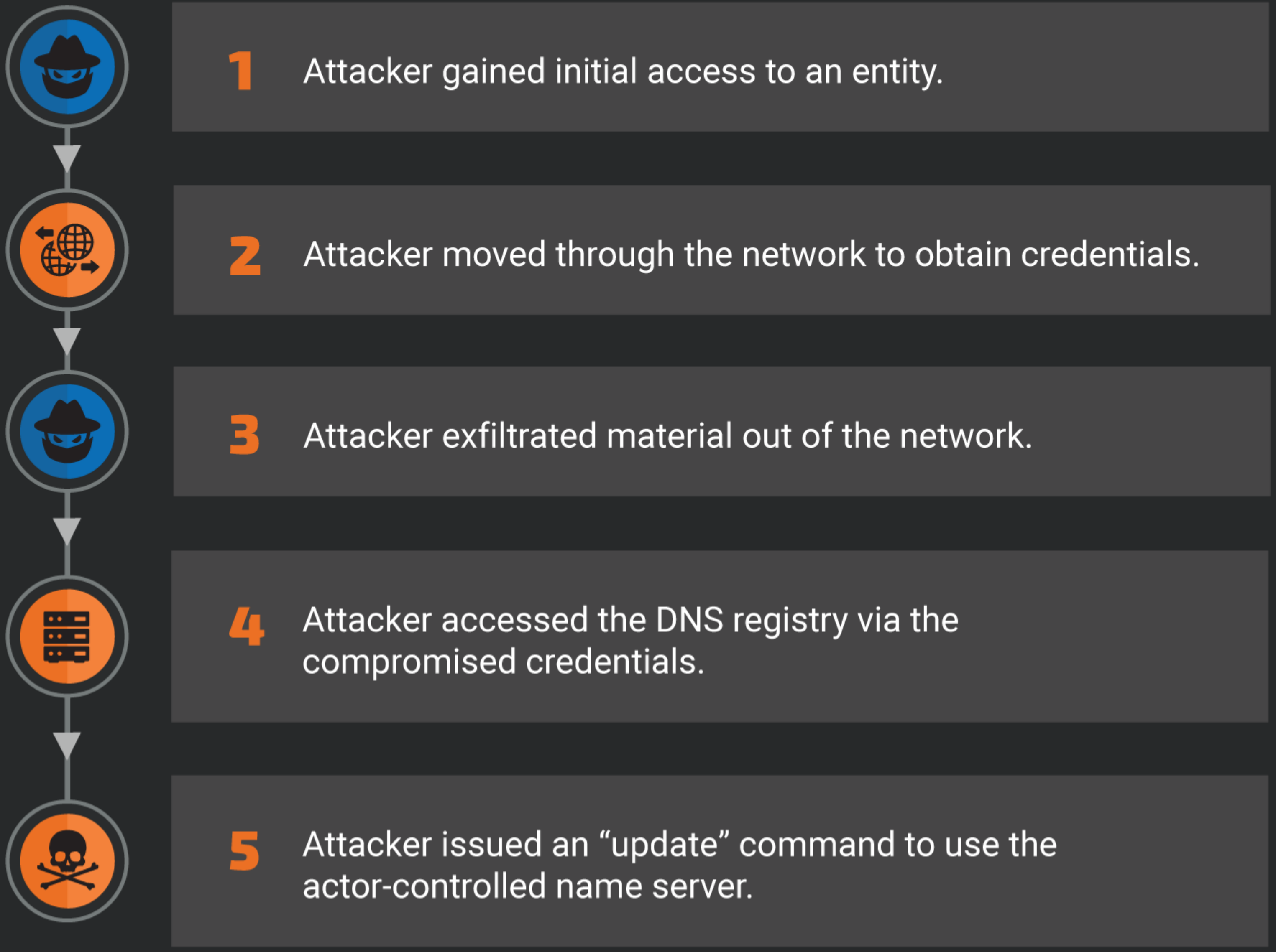
- Sea Turtle attacked both a Registrar & Registary…
  - So, what’s the difference? Quickly…

- 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 ;)

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.

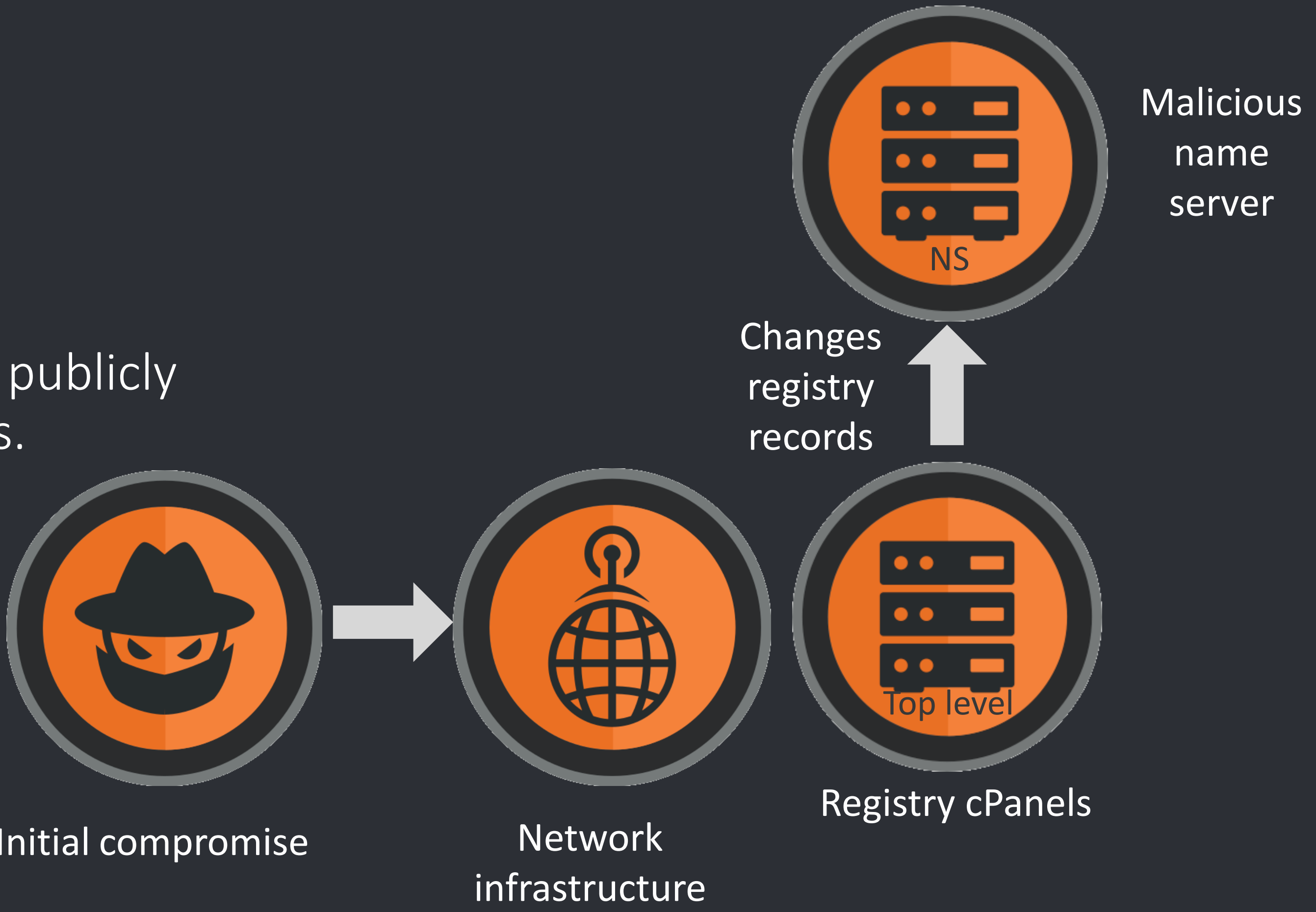
4 Attacker accessed the DNS registry via the compromised credentials.

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

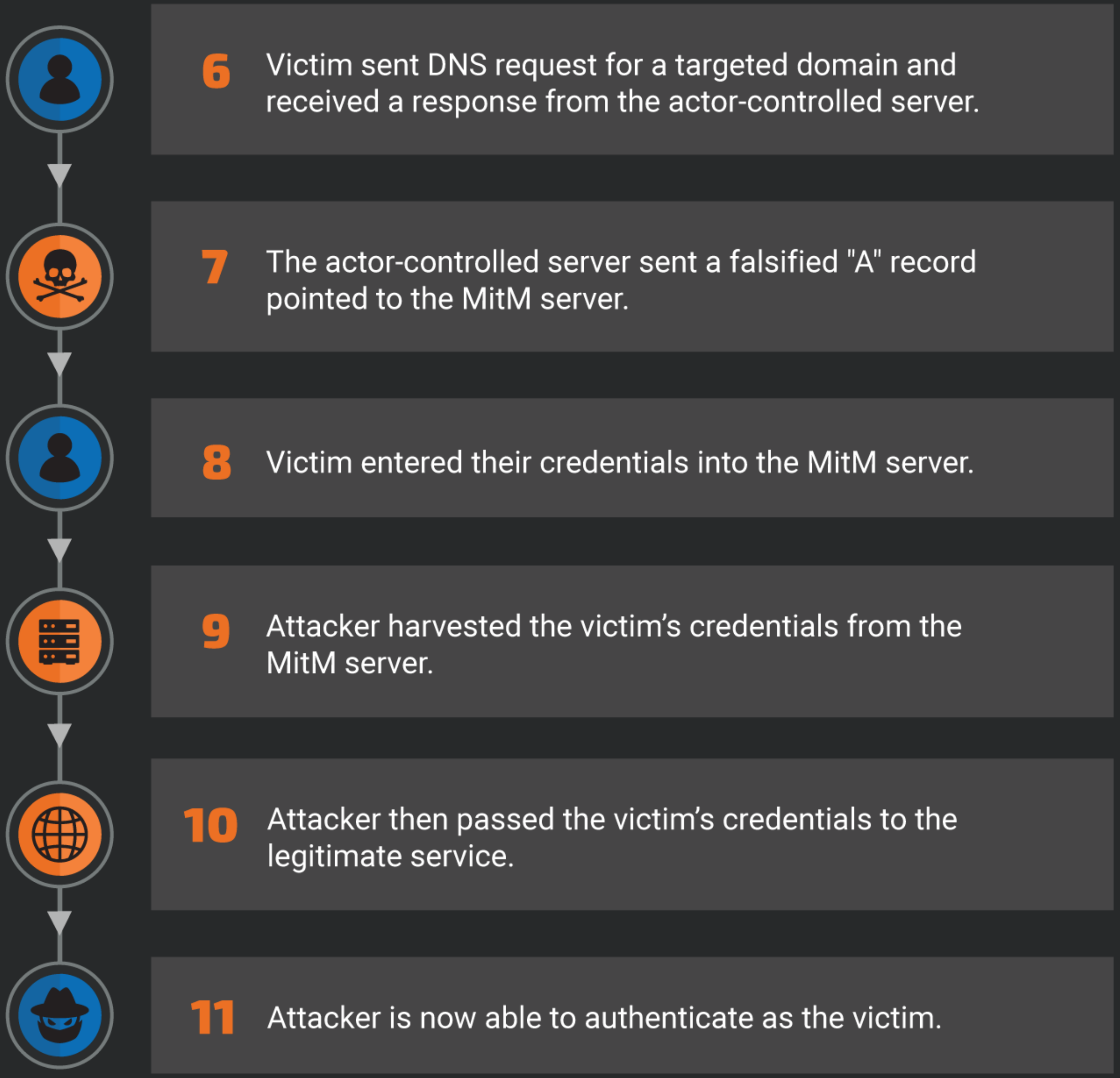
Sea Turtle Methodology

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.

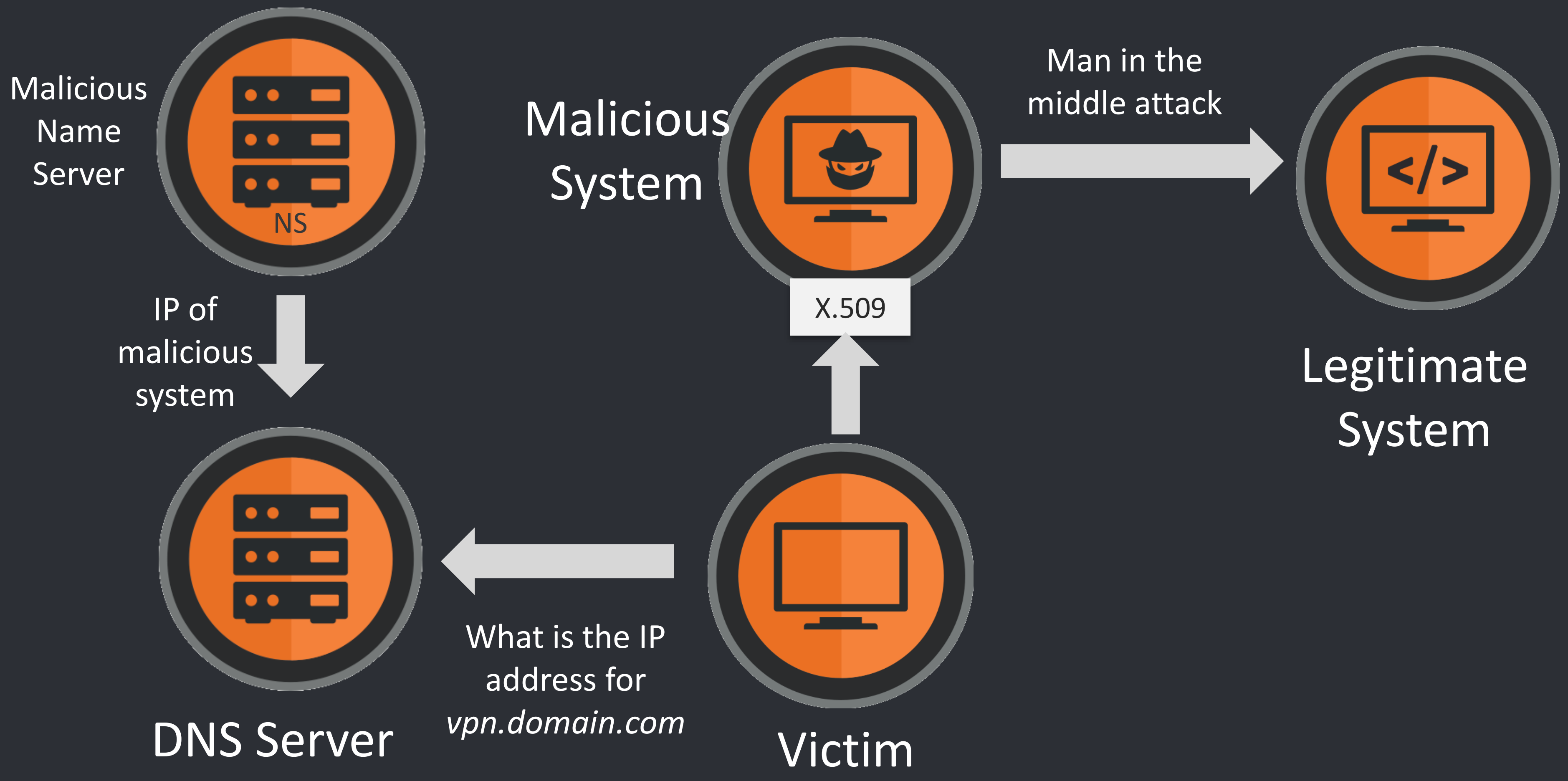
9 Attacker harvested the victim’s credentials from the MitM server.

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

11 Attacker is now able to authenticate as the victim.

Sea Turtle Man-in-the-Middle

Intercepting connections to harvest data



Talos

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 Disrupt and we say Bye Bye to Sea Turtle

July 2019 Techniques

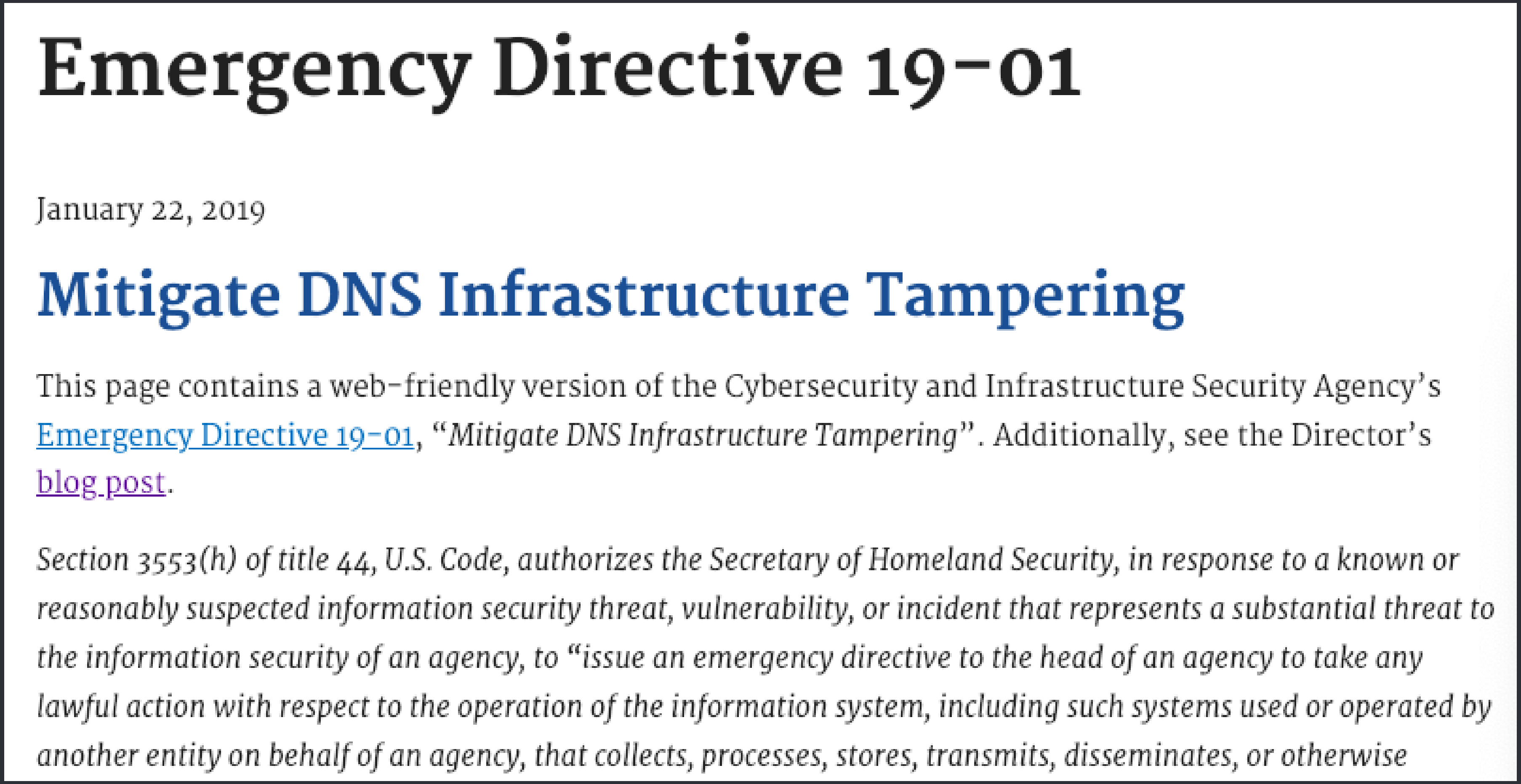
- Sea Turtle continues to compromise entities throughout the world using a new technique which has single use name-servers.
- This makes tracking difficult and also further detection difficult.
- Multiple observed cases they were “live” for <24 hours.
- Gov orgs in Middle East and North Africa

They swim on…

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

Conclusion

Q&A

TALOSINTELLIGENCE.COM

@talossecurity

blog.talosintelligence.com

@securitybeard
@r00tbsd

Talos

www.talosintelligence.com

blog.talosintel.com

@talossecurity

cisco