CISCO
SECURE

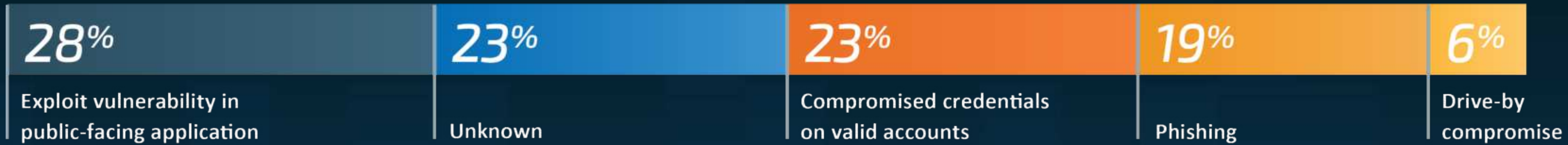
A jó, a rossz és az unknown

Top initial access vectors

According to Talos Incident Response data

Exploits in public-facing applications and compromised credentials/valid accounts accounted for half of initial access vectors in 2023.

Phishing rounds out the top 3 of known initial access vectors.



Note: Initial access vector is often hard to determine due to a variety of reasons — including insufficient logging or lack of visibility into the affected environment — resulting in "unknown" being highly represented.

CISCO TALOS

Goals may be different, but methodologies are similar

Cyber crime

- Financially motivated
- Phishing
- Big-game hunting
- Social engineering

Different motivations

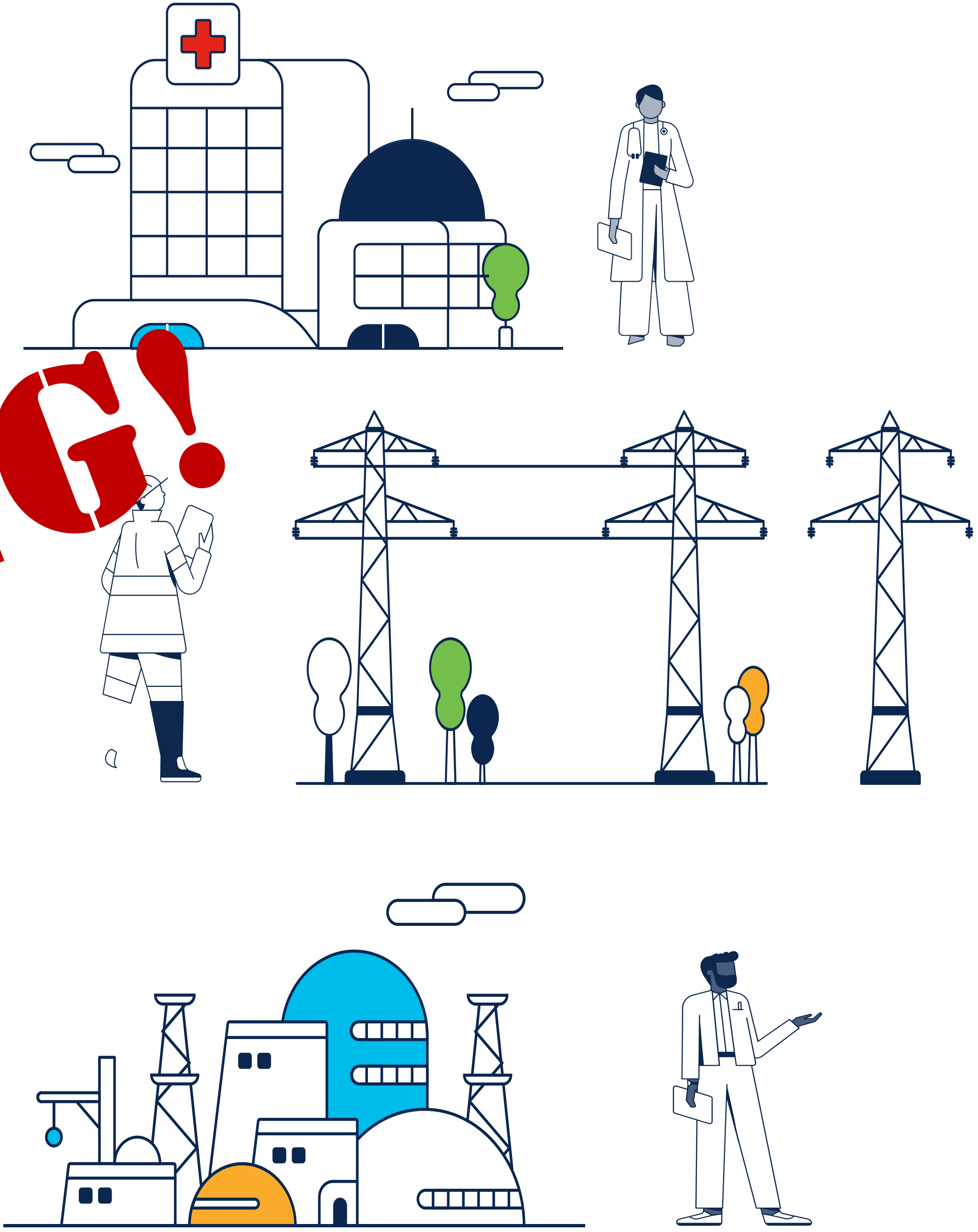
State-sponsored

- Data and espionage
- Havoc and chaos
- Supply chain attacks
- Partner abuse

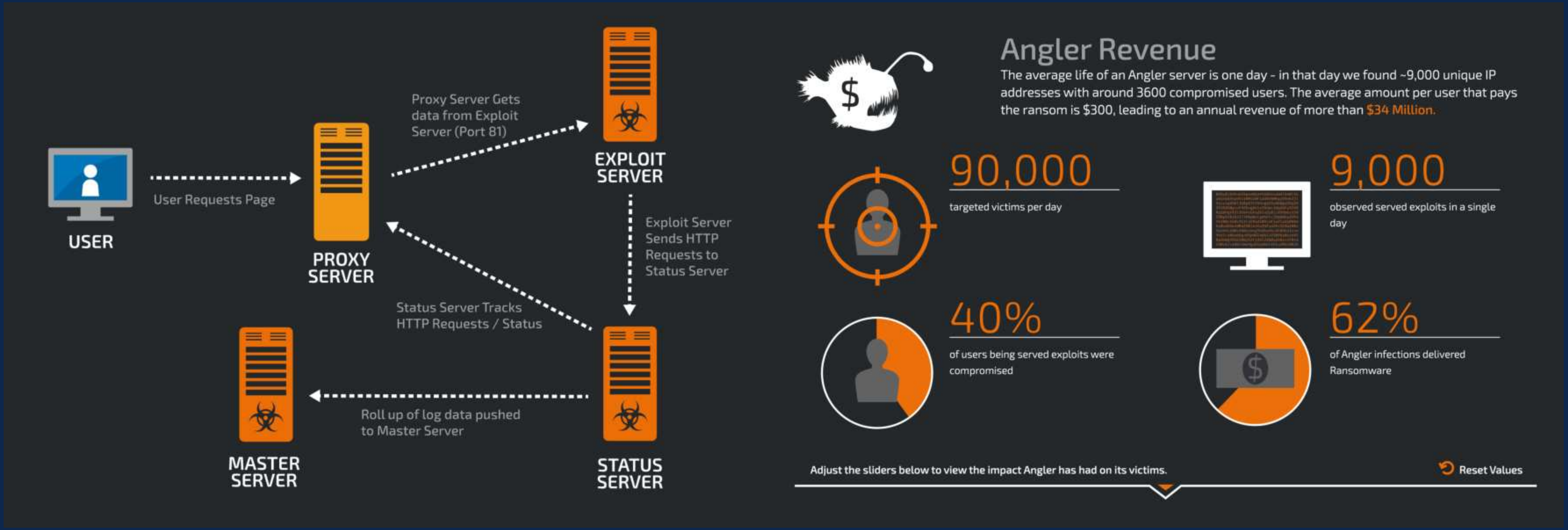
A vált$ágdíj az új drog

- 1.7 millió ransomware támadást indítanak naponta (ez 19 másodpercenként egy)
- 2022 első fele: közel 236.7 millió ransomware támadás
- Előrejelzés 2031-re: $265 milliárd költség évente

BORING!



Cyber Corleone


USER
User Requests Page
PROXY SERVER
Proxy Server Gets data from Exploit Server (Port 81)
EXPLOIT SERVER
Exploit Server Sends HTTP Requests to Status Server
Status Server Tracks HTTP Requests / Status
STATUS SERVER
Roll up of log data pushed to Master Server
MASTER SERVER
$
$

Angler Revenue

The average life of an Angler server is one day - in that day we found ~9,000 unique IP addresses with around 3600 compromised users. The average amount per user that pays the ransom is $300, leading to an annual revenue of more than $34 Million.

90,000 targeted victims per day

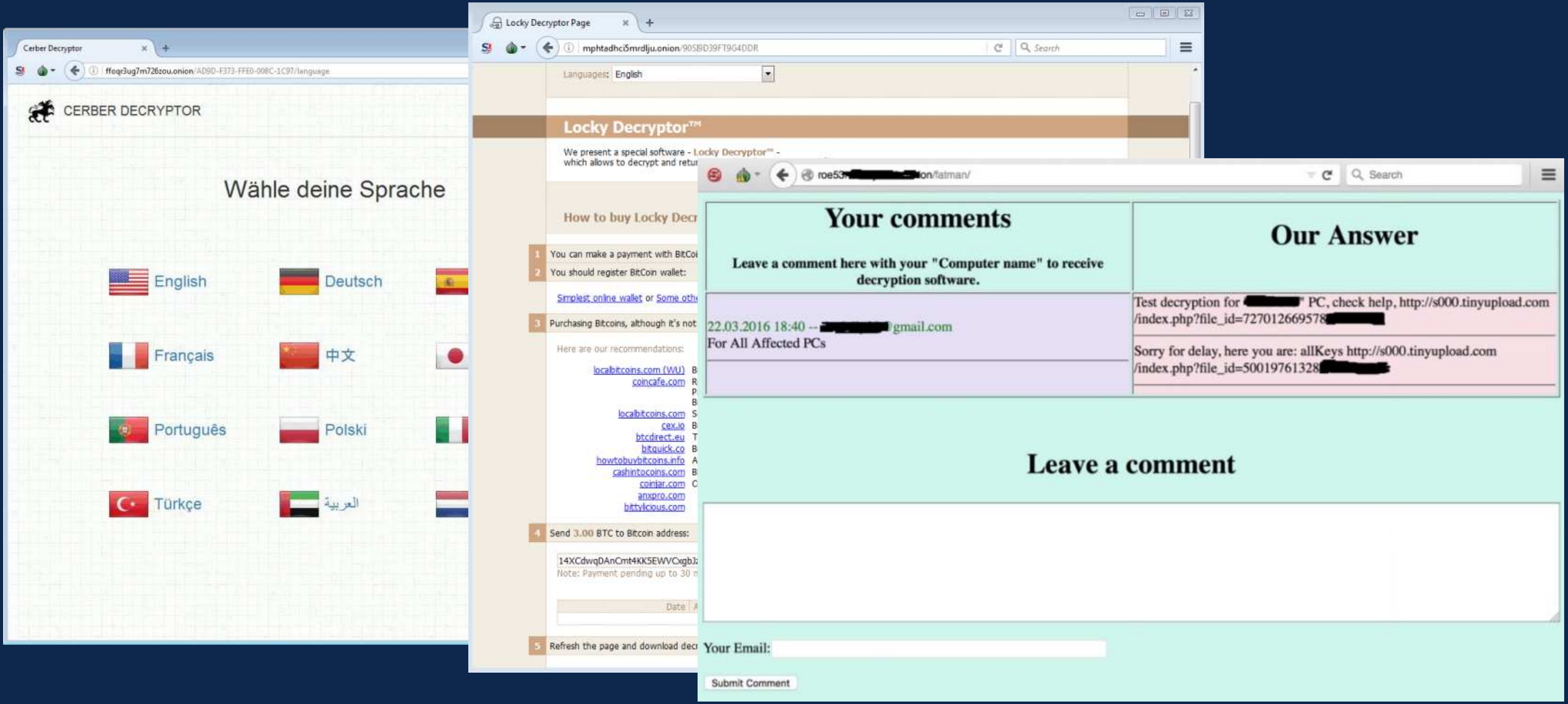
9,000 observed served exploits in a single day

40% of users being served exploits were compromised

62% of Angler infections delivered Ransomware

Adjust the sliders below to view the impact Angler has had on its victims.

Kibertámadás Zrt.



ffoqr3ug7m726zou.onion/AD9D-F373-FFE0-008C-1C97/language

CERBER DECRYPTOR

Wähle deine Sprache

mphtadhci5mrdlju.onion/90SBD39FT9G4DDR

Languages: English

Locky Decryptor™

We present a special software - Locky Decryptor™ -
which allows to decrypt and retur

How to buy Locky Decr

1 You can make a payment with BitCoi
2 You should register BitCoin wallet:

Simplest online wallet or Some othe

3 Purchasing Bitcoins, although it's not

Here are our recommendations:

localbitcoins.com (WU) B
coincafe.com R
P
B
localbitcoins.com S
cex.io B
btcdirect.eu T
bitquick.co B
howtobuybitcoins.info A
cashintocoins.com B
coinjar.com C
anxpro.com
bittylicious.com

4 Send 3.00 BTC to Bitcoin address:

14XCdwqDAnCmt4KK5EWVCxgbJ
Note: Payment pending up to 30 m

Date | A

5 Refresh the page and download decr

roe53[redacted]on/fatman/

Your comments Leave a comment here with your "Computer name" to receive decryption software.	Our Answer
22.03.2016 18:40 -- [redacted]gmail.com For All Affected PCs	Test decryption for [redacted]" PC, check help, http://s000.tinyupload.com/index.php?file_id=727012669578[redacted] Sorry for delay, here you are: allKeys http://s000.tinyupload.com/index.php?file_id=50019761328[redacted]

Leave a comment

Your Email:

Kibertámadás Zrt. - Conti group

- Képzési lehetőségek
- Jutalék a tárgyaló kollégáknak a befizetések után
- Teljesítményértékelések
- Ajánló program
- Hónap dolgozója díj
- Meglepetés a pozícióban

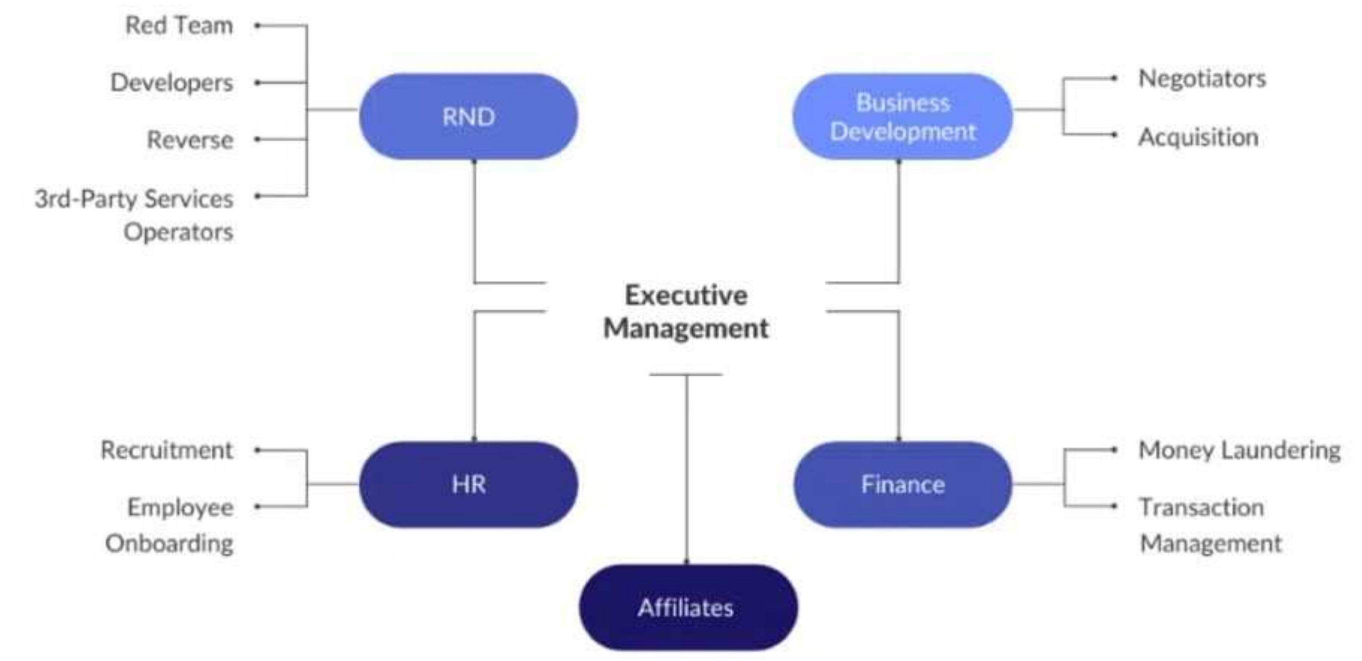
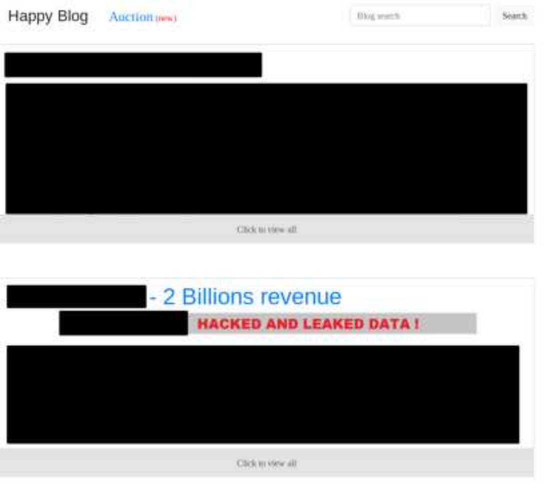


Figure 8: Conti's organization chart concluded from the leaks

Proliferation of Data Leak Sites



Happy Blog Auction (new) Blog search Search

[redacted]

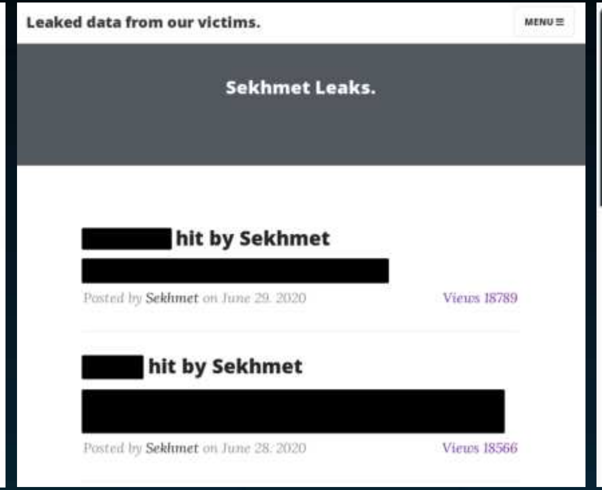
Click to view all

[redacted] - 2 Billions revenue

[redacted] HACKED AND LEAKED DATA !

[redacted]

Click to view all



Leaked data from our victims. MENU ☰

Sekhmet Leaks.

[redacted] **hit by Sekhmet**

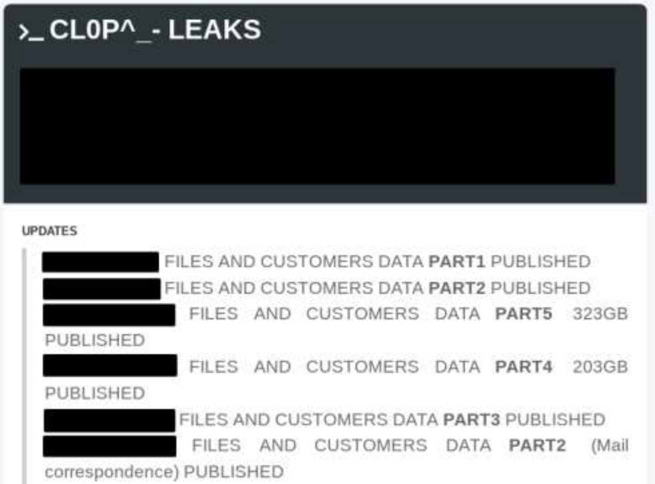
[redacted]

Posted by Sekhmet on June 29, 2020 Views 18789

[redacted] **hit by Sekhmet**

[redacted]

Posted by Sekhmet on June 28, 2020 Views 18566



>_ CL0P^_- LEAKS

[redacted]

UPDATES

[redacted] FILES AND CUSTOMERS DATA **PART1** PUBLISHED

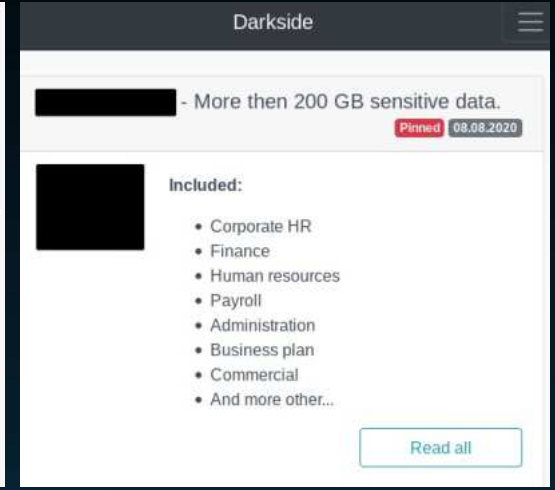
[redacted] FILES AND CUSTOMERS DATA **PART2** PUBLISHED

[redacted] FILES AND CUSTOMERS DATA **PART5** 323GB PUBLISHED

[redacted] FILES AND CUSTOMERS DATA **PART4** 203GB PUBLISHED

[redacted] FILES AND CUSTOMERS DATA **PART3** PUBLISHED

[redacted] FILES AND CUSTOMERS DATA **PART2** (Mail correspondence) PUBLISHED



Darkside

[redacted] - More then 200 GB sensitive data.

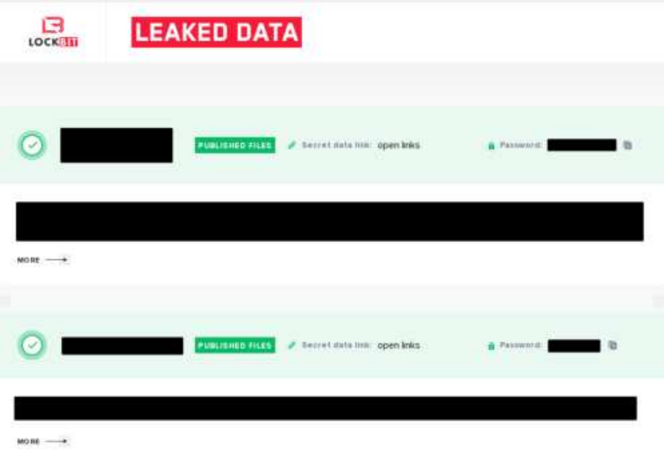
Pinned 08.08.2020

[redacted]

Included:

- Corporate HR
- Finance
- Human resources
- Payroll
- Administration
- Business plan
- Commercial
- And more other...

Read all



LOCKBIT **LEAKED DATA**

[redacted] PUBLISHED FILES Secret data link: open links Password: [redacted]

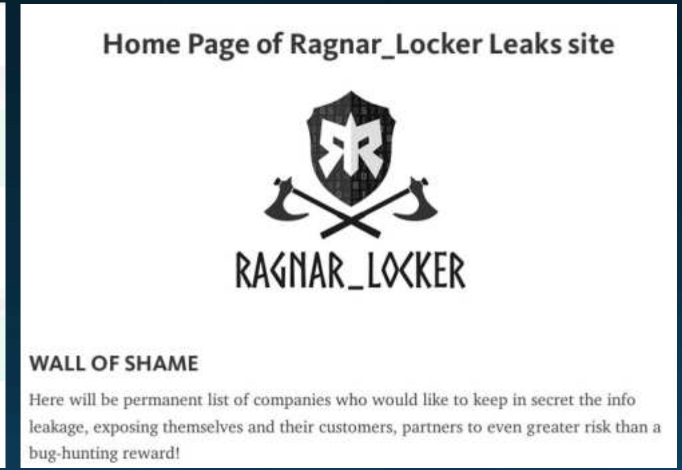
[redacted]

MORE →

[redacted] PUBLISHED FILES Secret data link: open links Password: [redacted]

[redacted]

MORE →

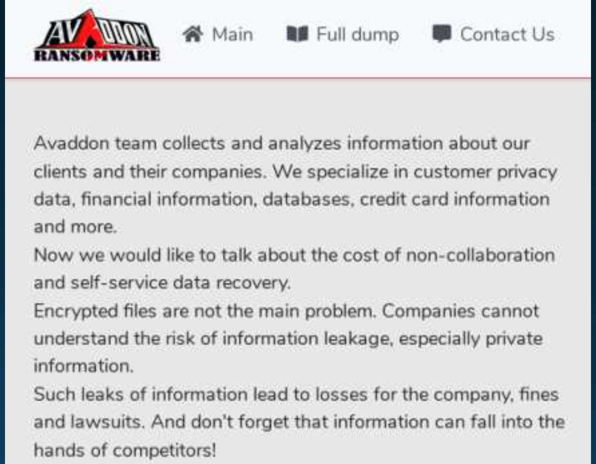


Home Page of Ragnar_Locker Leaks site

RAGNAR_LOCKER

WALL OF SHAME

Here will be permanent list of companies who would like to keep in secret the info leakage, exposing themselves and their customers, partners to even greater risk than a bug-hunting reward!



AVADDON RANSOMWARE Main Full dump Contact Us

Avaddon team collects and analyzes information about our clients and their companies. We specialize in customer privacy data, financial information, databases, credit card information and more.

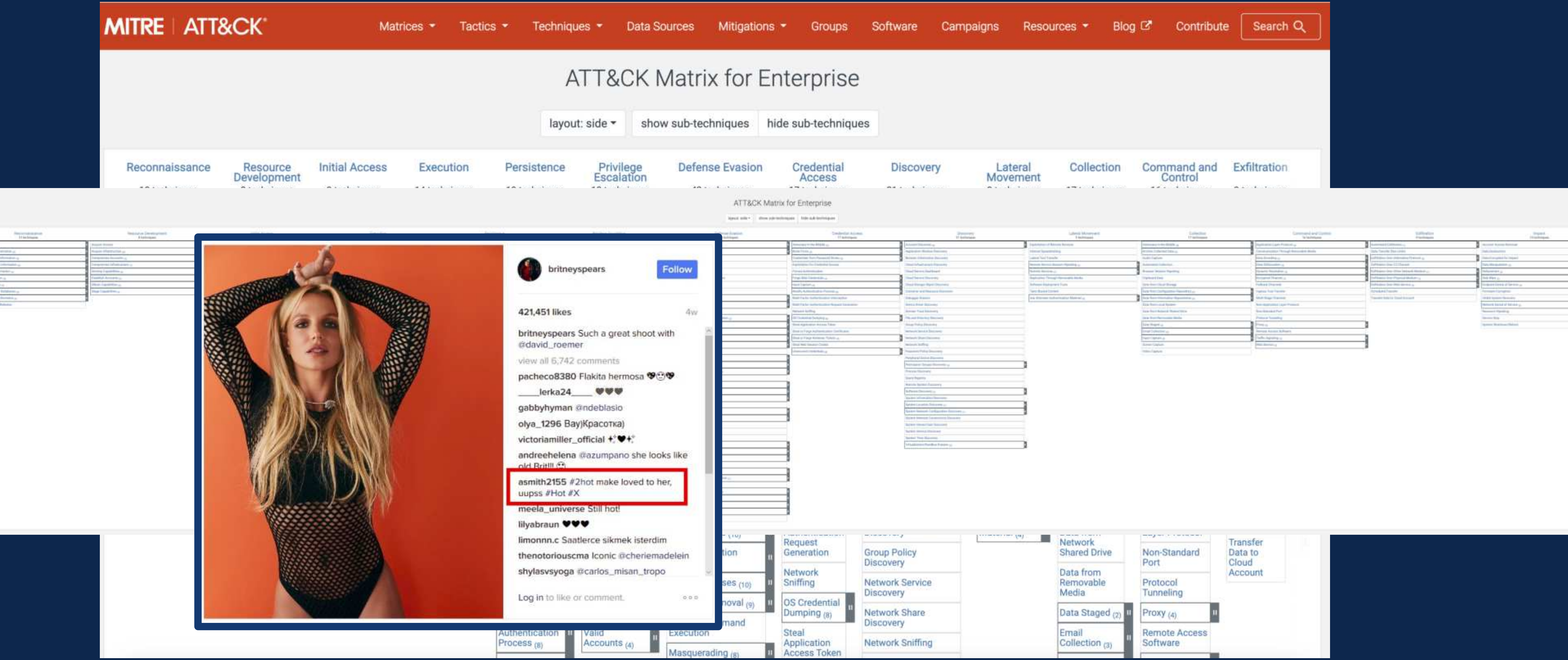
Now we would like to talk about the cost of non-collaboration and self-service data recovery.

Encrypted files are not the main problem. Companies cannot understand the risk of information leakage, especially private information.

Such leaks of information lead to losses for the company, fines and lawsuits. And don't forget that information can fall into the hands of competitors!

CISCO TALOS

Taktikák, technikák… és trükkök



MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Data Sources Mitigations ▾ Groups Software Campaigns Resources ▾ Blog Contribute Search

ATT&CK Matrix for Enterprise

layout: side ▾ | show sub-techniques | hide sub-techniques

Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration

britneyspears Follow

421,451 likes 4w

britneyspears Such a great shoot with @david_roemer

view all 6,742 comments

pacheco8380 Flakita hermosa 💖😍💖

____lerka24____ 🖤🖤🖤

gabbyhyman @ndeblasio

olya_1296 Вау)Красотка)

victoriamiller_official ✨🖤✨

andreehelena @azumpano she looks like old Brit!!! 😍

asmith2155 #2hot make loved to her, uupss #Hot #X

meela_universe Still hot!

lilyabraun 🖤🖤🖤

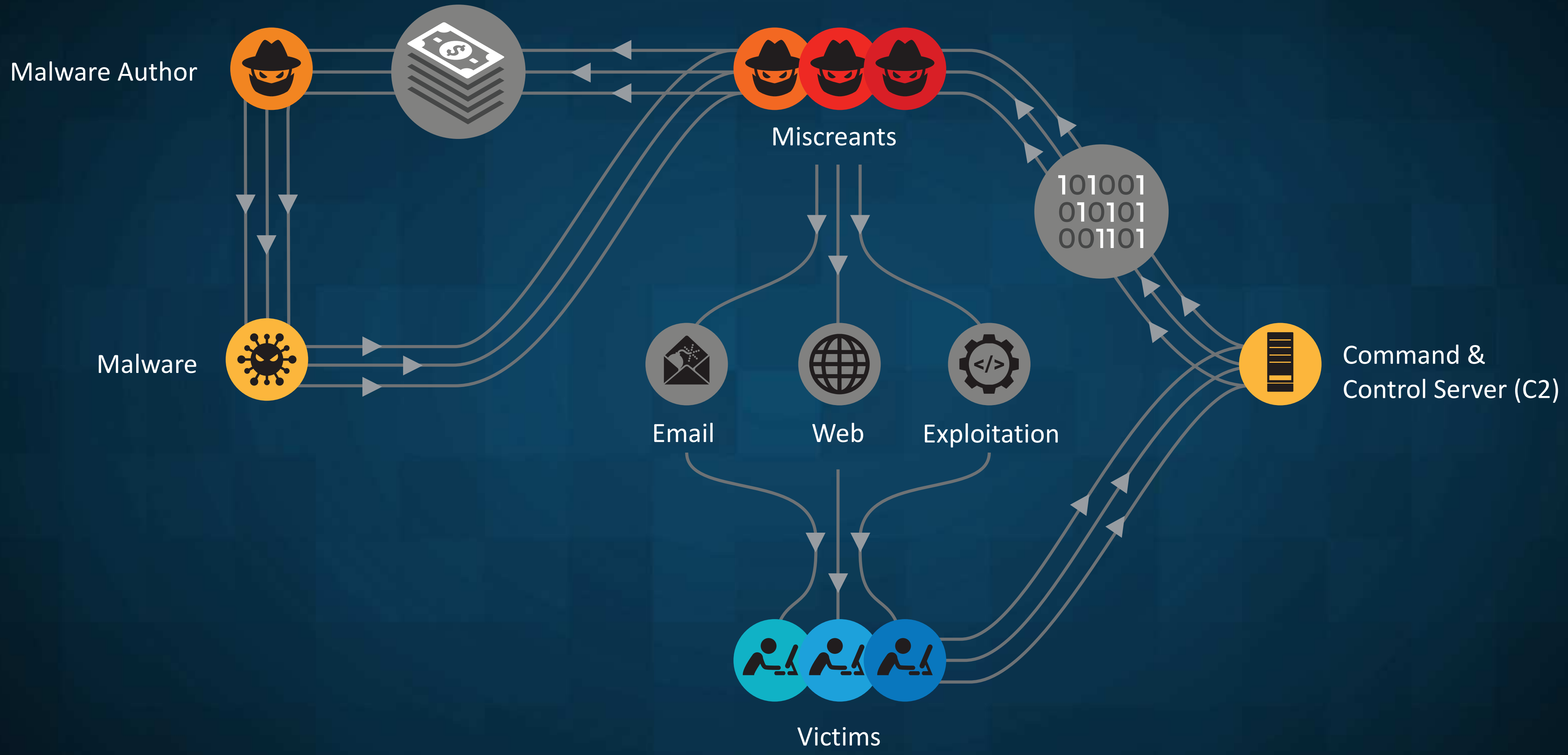
limonnn.c Saatlerce sikmek isterdim

thenotoriouscma Iconic @cheriemadelein

shylasvsyoga @carlos_misan_tropo

Log in to like or comment.

Commodity Malware Lifecycle

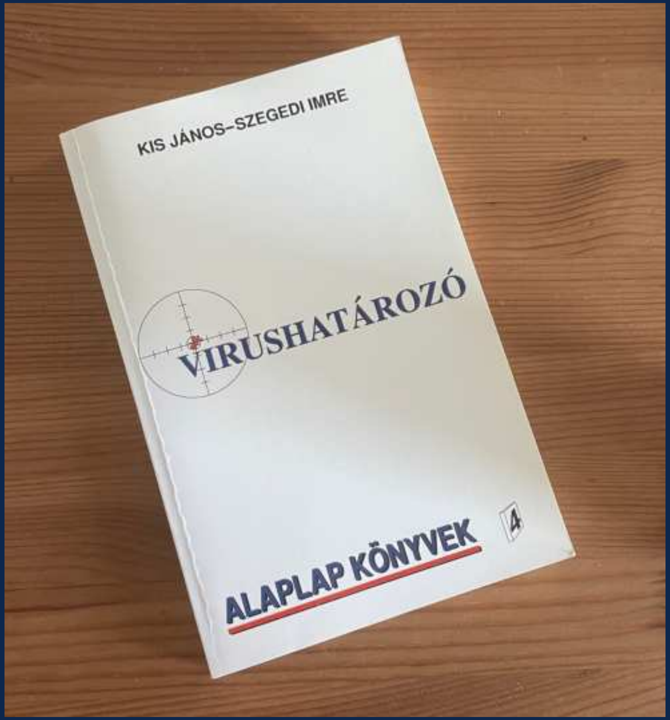


Talos
Cisco Security Research

Sziszüphosz szignatúrákat írna

- 1992

1263 (534 + 729) vírus SZUMMA


KIS JÁNOS–SZEGEDI IMRE

VIRUSHATÁROZÓ

ALAPLAP KÖNYVEK

- 2022

1.4 M új malware minta naponta

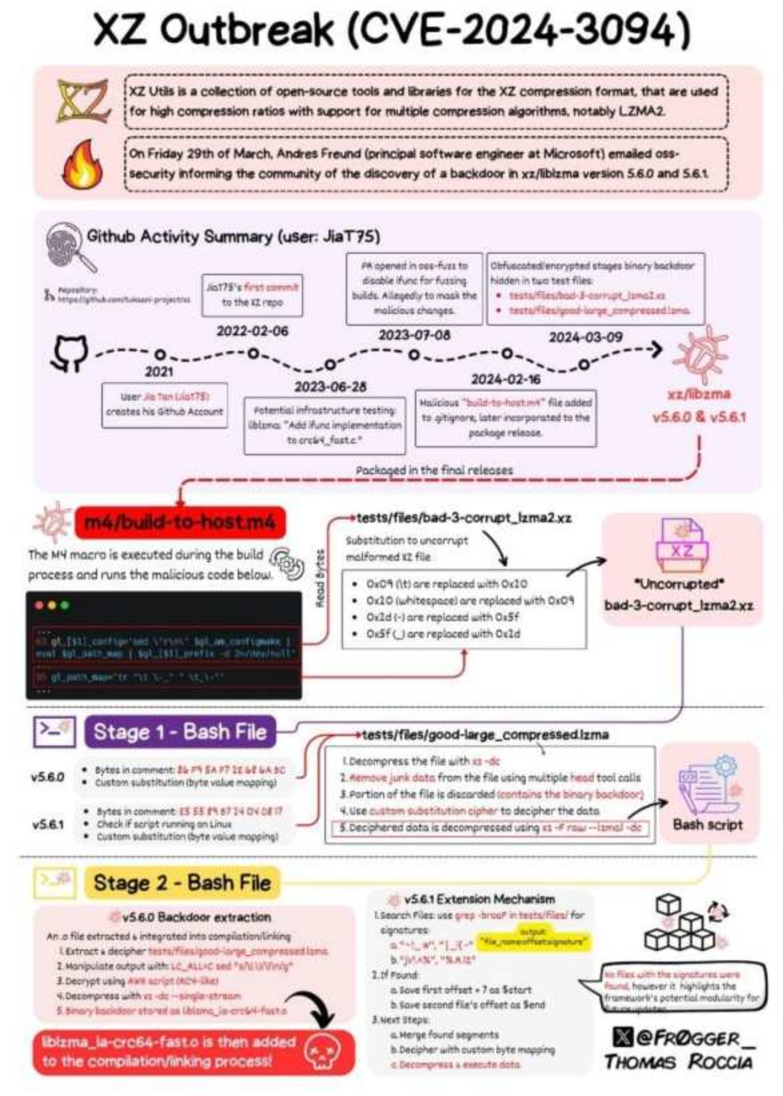
TALOS
A DOUBLE-EDGED SWORD
THE THREAT OF DUAL-USE TOOLS

Native Functionality

- How is it abused by attackers?
- Common Examples
  - PowerShell
  - WinRM/PS Remoting
  - VBScript
  - JScript
  - WMI

Supply chain, cyberweapons, etc.

- XZ-UTILS, CVSS: 10/10
  - Linux, SSH backdoor, CVE-2024-3094, opensource project
  - https://cert.europa.eu/publications/security-advisories/2024-032/



XZ Outbreak (CVE-2024-3094)

XZ Utils is a collection of open-source tools and libraries for the XZ compression format, that are used for high compression ratios with support for multiple compression algorithms, notably LZMA2.

On Friday 29th of March, Andres Freund (principal software engineer at Microsoft) emailed oss-security informing the community of the discovery of a backdoor in xz/liblzma version 5.6.0 and 5.6.1.

Github Activity Summary (user: JiaT75)

Repository: https://github.com/tukaani-project/xz

2021 – User Jia Tan (JiaT75) creates his Github Account

2022-02-06 – JiaT75's first commit to the XZ repo

2023-06-28 – Potential infrastructure testing: liblzma: "Add ifunc implementation to crc64_fast.c"

2023-07-08 – PR opened in oss-fuzz to disable ifunc for fuzzing builds. Allegedly to mask the malicious changes.

2024-02-16 – Malicious "build-to-host.m4" file added to .gitignore, later incorporated to the package release.

2024-03-09 – Obfuscated/encrypted stages binary backdoor hidden in two test files:
- tests/files/bad-3-corrupt_lzma2.xz
- tests/files/good-large_compressed.lzma

xz/liblzma v5.6.0 & v5.6.1

Packaged in the final releases

m4/build-to-host.m4

The M4 macro is executed during the build process and runs the malicious code below.

```
...
gl_[$1]_config='sed \"r\n\" $gl_am_configmake | eval $gl_path_map | $gl_[$1]_prefix -d 2>/dev/null'
...
gl_path_map='tr "\t \-_" " \t_\-"'
...
```

Read Bytes

→tests/files/bad-3-corrupt_lzma2.xz

Substitution to uncorrupt malformed XZ file
- 0x09 (\t) are replaced with 0x20
- 0x20 (whitespace) are replaced with 0x09
- 0x2d (-) are replaced with 0x5f
- 0x5f (_) are replaced with 0x2d

"Uncorrupted" bad-3-corrupt_lzma2.xz

Stage 1 - Bash File

v5.6.0
- Bytes in comment: 86 F9 5A F7 2E 68 6A BC
- Custom substitution (byte value mapping)

v5.6.1
- Bytes in comment: E5 55 89 B7 24 04 D8 17
- Check if script running on Linux
- Custom substitution (byte value mapping)

→tests/files/good-large_compressed.lzma

1. Decompress the file with xz -dc
2. Remove junk data from the file using multiple head tool calls
3. Portion of the file is discarded (contains the binary backdoor)
4. Use custom substitution cipher to decipher the data
5. Deciphered data is decompressed using xz -F raw --lzma1 -dc

Bash script

Stage 2 - Bash File

v5.6.0 Backdoor extraction

An .o file extracted & integrated into compilation/linking
1. Extract & decipher tests/files/good-large_compressed.lzma
2. Manipulate output with: LC_ALL=C sed "s/\(.\)/\1\n/g"
3. Decrypt using AWK script (RC4-like)
4. Decompress with xz -dc --single-stream
5. Binary backdoor stored as liblzma_la-crc64-fast.o

liblzma_la-crc64-fast.o is then added to the compilation/linking process!

v5.6.1 Extension Mechanism

1. Search Files: use grep -broaF in tests/files/ for signatures:
   a. "~!:_ W", "|_!{ -"
   b. "jV!.^%", "%.R.1Z"

   output: "file_name:offset:signature"
2. If Found:
   a. Save first offset + 7 as $start
   b. Save second file's offset as $end
3. Next Steps:
   a. Merge found segments
   b. Decipher with custom byte mapping
   c. Decompress & execute data

No files with the signatures were found, however it highlights the framework's potential modularity for future updates.

@FR0GGER_ Thomas Roccia

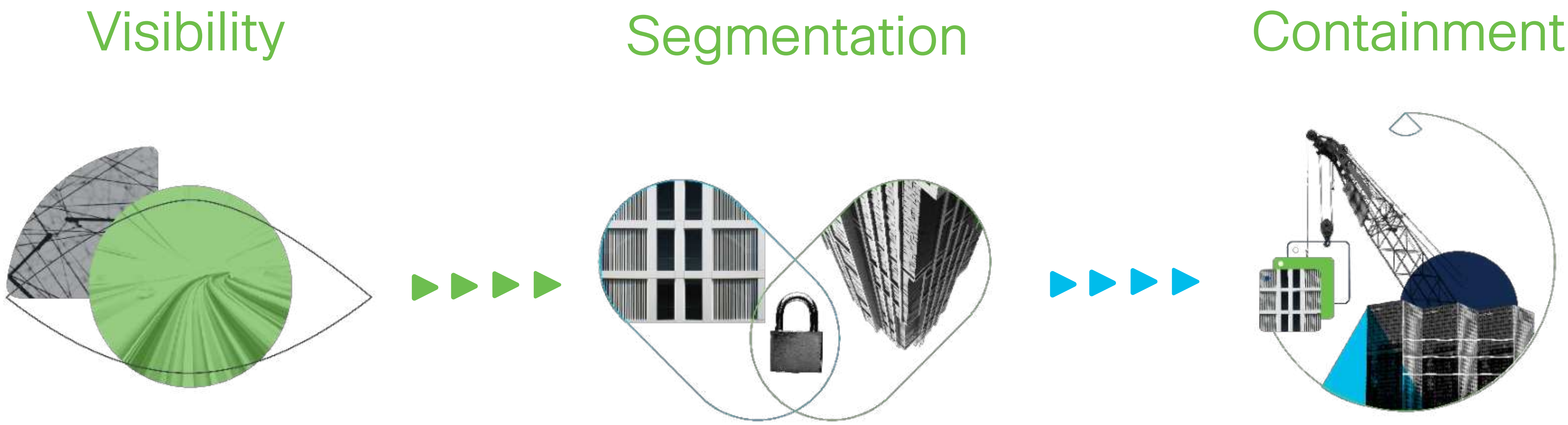
NIS2

Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as

- zero-trust principles,
- software updates,
- device configuration,
- network segmentation,
- identity and access management
- user awareness
- …

Zero trust

The Foundations of Zero Trust in Your Workplace



Visibility

Grant the right level of network access to users across domains

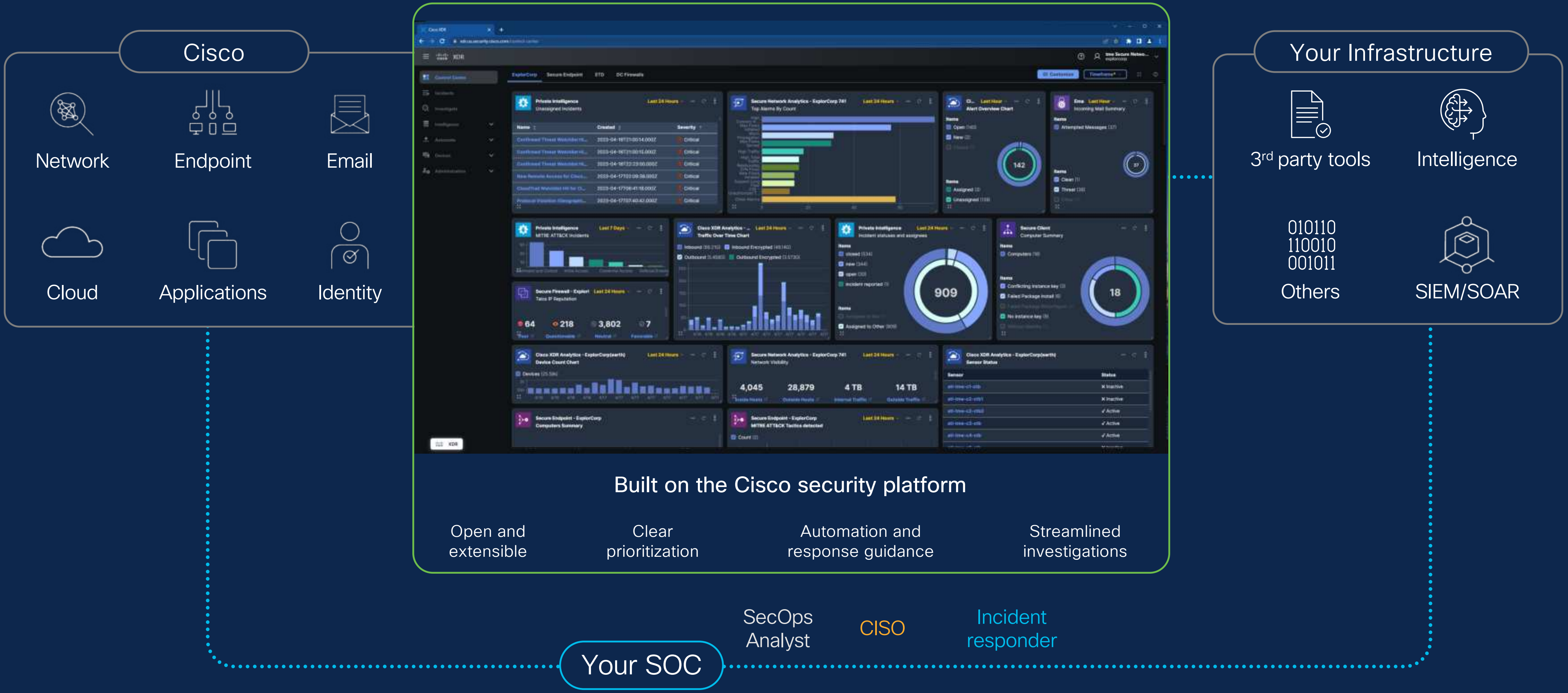
Segmentation

Shrink zones of trust and grant access based on least privilege

Containment

Automate containment of infected endpoints and revoke network access

XDR



Cisco

Network

Endpoint

Email

Cloud

Applications

Identity

Built on the Cisco security platform

Open and extensible

Clear prioritization

Automation and response guidance

Streamlined investigations

Your Infrastructure

3rd party tools

Intelligence

010110
110010
001011

Others

SIEM/SOAR

SecOps Analyst

CISO

Incident responder

Your SOC

Interview with a LockBit ransomware operator

By Azim Khodjibaev,
Dmytro Korzhevin and Kendall McKay

> If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Bruce Schneier

cisco

The bridge to possible