

Cheers to Chaos

**Ransomware, Hacktivism, and a
Cold Beer in Hand**

Diana Selck-Paulsson

Today's itinerary (travel time ~30 mins)

1 Introduction

Speaker bio

3 Crossovers

The five families & a little bit of ransom

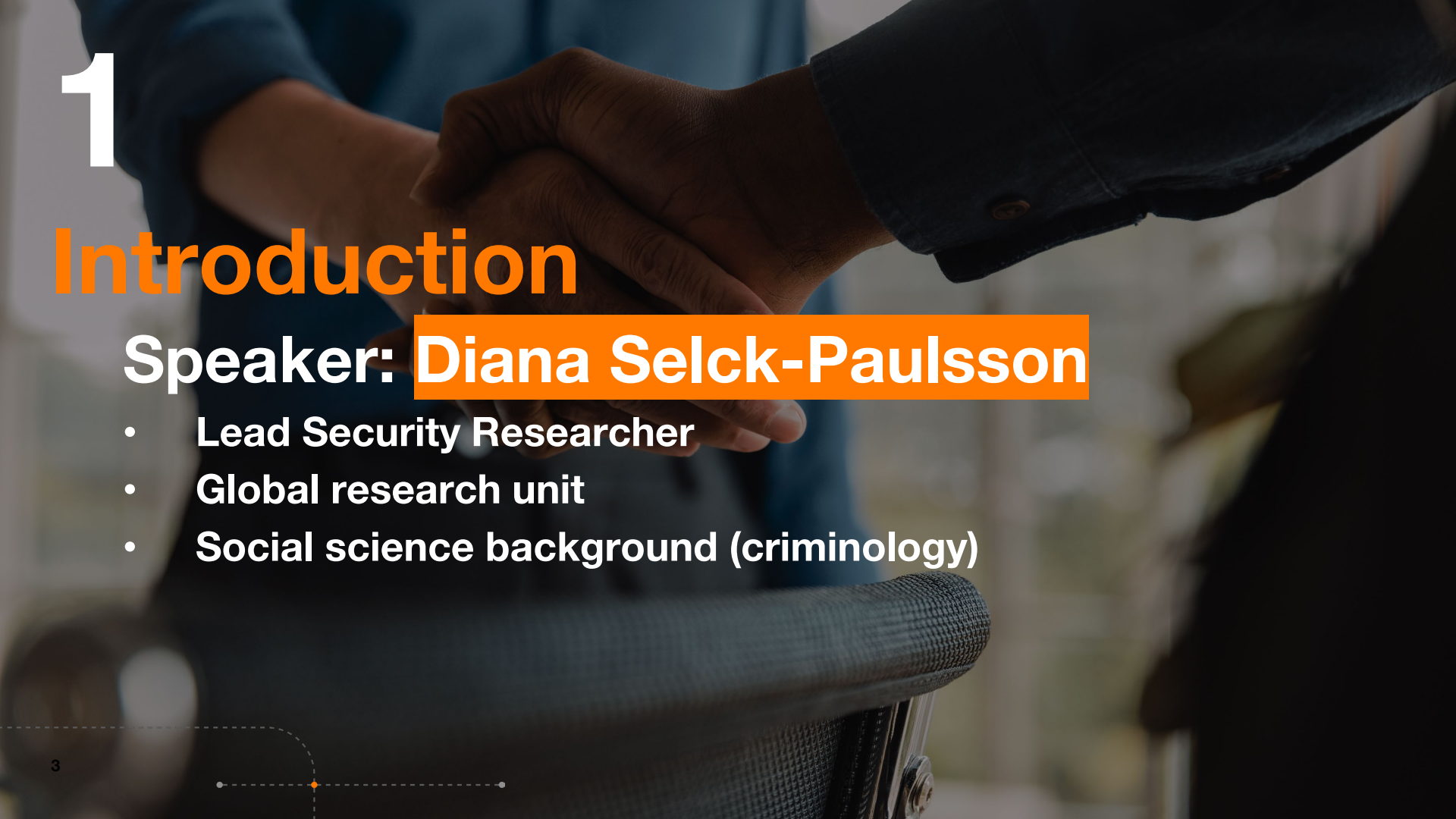
2 A storm in Belgium

Ransomware /
Hacktivism

4 Current threat landscape

Global & local





1

Introduction

Speaker: Diana Selck-Paulsson

- Lead Security Researcher
- Global research unit
- Social science background (criminology)

A dark, moody photograph showing two hands in business suits. One hand is holding a thick stack of US dollar bills, and the other hand is reaching out to receive them. The background is dark and out of focus, suggesting an indoor setting with wooden paneling.

2

A Storm in Belgium

Cyber extortion & Hacktivism
(ransomware)

The commonality of beer and coffee

The Record.
Recorded Future News



IMAGE: BRETT JORDAN VIA PEXELS

Jonathan Greig

March 7th, 2024

Stormous ransomware gang takes credit for attack on Belgian brewer Duvel



De_Roymeester • 3mo ago

I think this should be classified under National Emergency



21



Reply



Belgium's largest coffee roaster falls victim to cyber attack

“The Belgian village of Breendonk — home to Duvel Moortgat Brewery, which was hit by a cyberattack last week — is now facing a second incident affecting local coffee roasters Koffie Beyers.”



A photograph showing two men in suits. The man on the right is handing a thick stack of US dollar bills to the man on the left. They are positioned under a wooden shelf. The image is dimly lit, with the focus on the hands and the money.

3

Crossovers

The five families & a little bit of
ransom

A Storm hits Belgium

Stormous

Active since 2015

Political & financially motivated

Part of **The Five Families** collective

- **ThreatSec**
- **GhostSec**
- **Stormous**
- ~~**SiegedSec**~~
- ~~**Black Forums**~~

RaaS in collaboration with **GhostSec**

Crossovers between RaaS & Hacktivism



The screenshot shows the Stormous X/GhostLocker website interface. At the top, there are navigation tabs: "Stormous X/GhostLocker", "Today's leaks", "Number of victims '2021/2024'", and "largest ransom". Below these is a search bar and a "Last victims" section. The main content is a table listing various victims, including their name, country, size, site, date, and status. The table is color-coded: red for active or ongoing ransomware attacks, and green for completed or finished attacks. The status column also includes a progress indicator (a circle with a percentage or a checkmark).

Name	Country	size	site	Date	Data
 casio india	India	200GB+	casio.co.in	05/04/2024	66 h 13m 55s 0%
 berjayaclubs	Malaysia	?	www.berjayaclubs.com	20/03/2024	FINISHED 100%
 paginesi	Italy	170GB	www.paginesi.it	17/03/2024	FINISHED 100%
 education.eeb-lost	Lebanon	?	www.education.eeb-lost.org	14/03/2024	FINISHED 100%
 lostfb	Lebanon	?	www.lostfb.org	14/03/2024	FINISHED 100%
 mioa.gov	?	?	www.mioa.gov.mk	14/03/2024	FINISHED 100%
 www.duvel.com	Belgium	88GB	www.duvel.com	07/03/2024	NEGOTIATION 0%
 www.loghmanpharma.com	Iran	?	www.loghmanpharma.com	06/03/2024	FINISHED 100%
 viadirectmarketing	Spain	2.7GB	www.viadirectmarketing.com	06/03/2024	FINISHED 100%
 airbogo	?	10TB	www.airbogo.com	05/03/2024	FINISHED 100%
 tox.chat	?	?	www.tox.chat	05/03/2024	FINISHED 100%
 everplast	Brazil	57 GB	www.everplast.com.br	04/03/2024	IN NEGOTIATION 0%
 bombaygrills	India	12 GB	www.bombaygrills.com	15/02/2024	EXPIRED 0%
 pcmarket	Uzbekistan	1 GB	www.pcmarket.uz	31/01/2024	FINISHED 100%
 KAI	Indonesia	1 TB	www.kai.id	22/01/2024	FINISHED 100%
 della.pt	Poland	64 GB	www.della.pt	16/02/2024	FINISHED 100%
 calcomp	Thailand	12 GB	www.calcomp.co.th	14/02/2024	FINISHED 100%
 Abelsantosyasoc	Argentina	26 GB	www.Abelsantosyasoc.com.ar	14/02/2024	FINISHED 100%

Hacktivism

Blurry li

-
-
-
-
-
-

Hacked

←  **The Five Families**
5.8K subscribers

The Five Families May 15

Forwarded from

 **GhostSec**

We'd like to announce GhostSec's leave from the "CyberCrime" Scene. We as Ghosts have obtained enough funding through our times to continue funding our operations for a while we deem the cybercrime and ransomware we once promoted no longer necessary and will shift back to pure hacktivism what does this mean?

All this means is that we will not be providing services anymore therefore the Ghostsec services channel and services once provided will be closed, The ransomware Ghostlocker will be closed Though we will provide the entire code of V3 to Stormous and shift all buyers from GL to the new Stormous locker making it a clean exit without any exit scam. Five families will be taken over and Stormous will be in charge with the new associates involved in that organization resulting in our complete retirement from the "cybercrime" and ransomware scene!

ware & vice versa

lds.

new
em
an tr
A Di
arytl

מלון גורדון עלהם מל-אביב
גורדון עלהם מל-אביב
גורדון עלהם מל-אביב
גורדון עלהם מל-אביב

Part of The Five Families collective

- ~~ThreatSec~~
- ~~GhostSec~~
- ~~Stormous~~
- ~~SleekSec~~
- ~~BlackFarms~~

Trigona is Gone!

Trigona ransomware gang has been exfiltrated and wiped out

to the world you created for others

Hacked by
Ukrainian Cyber Alliance,
disrupting russian criminal enterprises (both public and private)
since 2014

October 8

Channel created

GhostLocker
New generation of RaaS

ionary,
are which
ess
make
ates as
success
attempt to
means ✓

AND

Contact: @GhostSecSR (For purchase or any questions relating to the product)

What am I seeing as a researcher?



Impact?

C - Confidentiality
I - Integrity
A - Availability

Basta News

duvel.com | boulevard.com

ESTD 1871

Duvel

Duvel Moortgat Brewery (Brouwerij Duvel Moortgat) is a Flemish family-controlled brewery founded in 1871 in Antwerp Province, Belgium. Its strong golden pale ale, Duvel, is exported to more than forty countries. Duvel is Brabantian, Ghent and Antwerp dialect for devil, the standard Dutch word being duivel. Other popular beers include Maredsous and Vedett.

SITE: www.duvel.com

ADDRESS:
Brewendok Dapp 58
2870 Puurs-Sint-Amands
Belgium

Founded in 1989, Boulevard Brewing Company has grown to become the largest specialty brewer in the Midwest. Our mission is simple: to produce fresh, flavorful beers using the finest ingredients and the best of both old and new brewing techniques. Click the link to learn what drove Boulevard founder John McDonald, and how we got where we are today.

SITE: www.boulevard.com

ADDRESS:
2501 Southwest Boulevard
Kansas City, MO 64108
USA

List of domain trusts:
1: DUVEL duvel.inta (NT S) (Direct Outbound) (Attr: 0x48)
2: BOULEVARD BeeNet.local (NT S) (Forest Tree Root) (Primary Domain) (Native)

ALL DATA SIZE: ~1.0GB
1. Accounting
2. HR
3. Home users folders
4 etc...

MountLocal

100



4

Current threat landscape

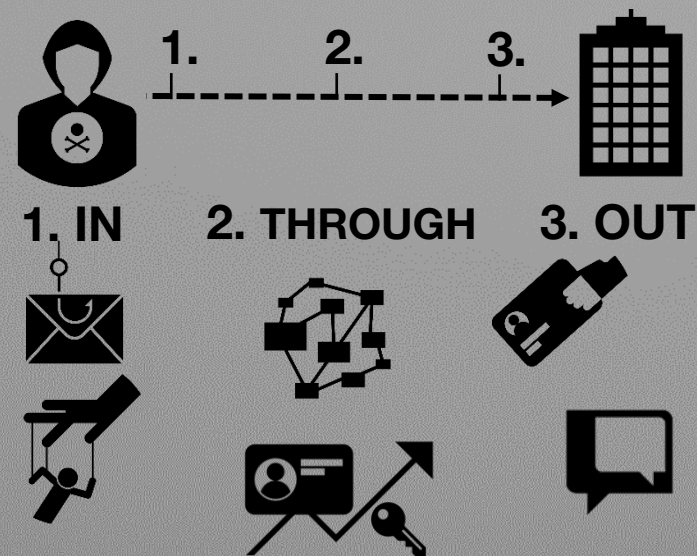
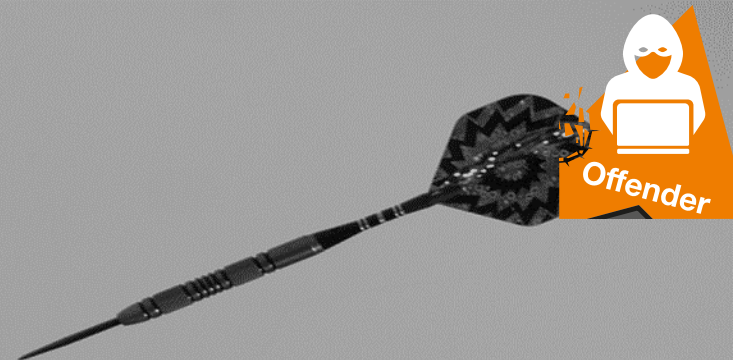
Global & local

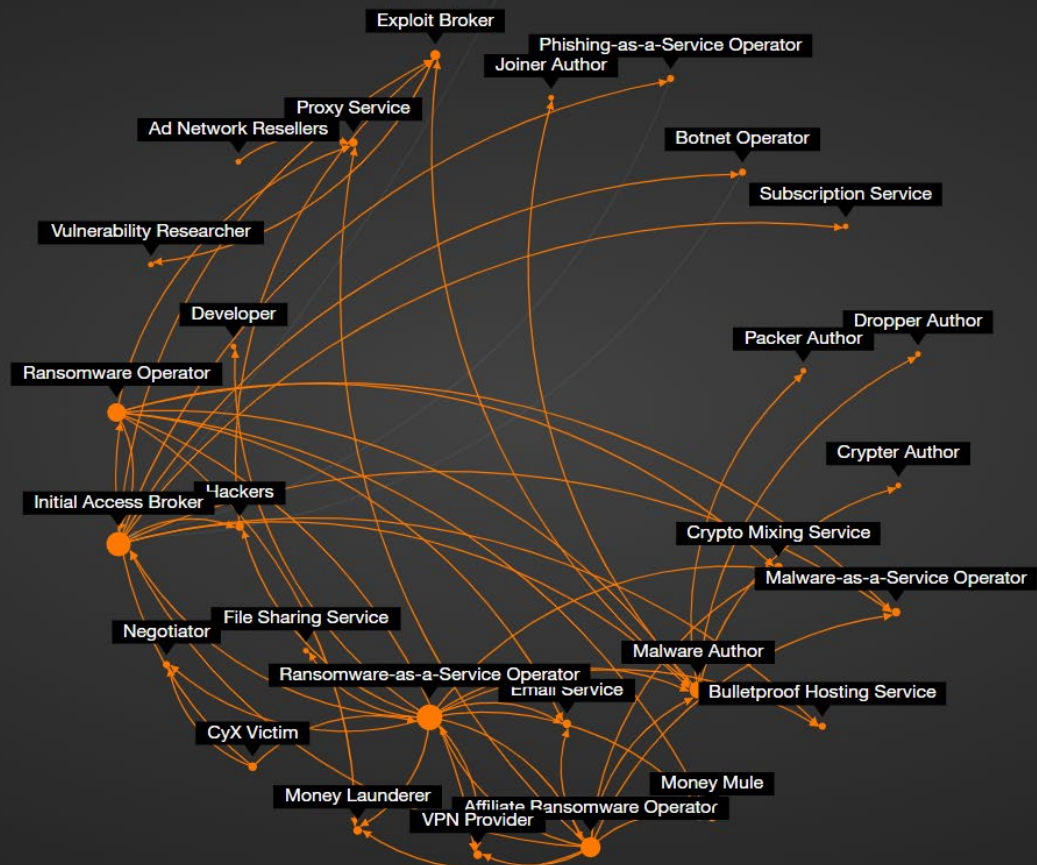


Ransomware

Criminal evolution

Towards a striving & resilient ecosystem

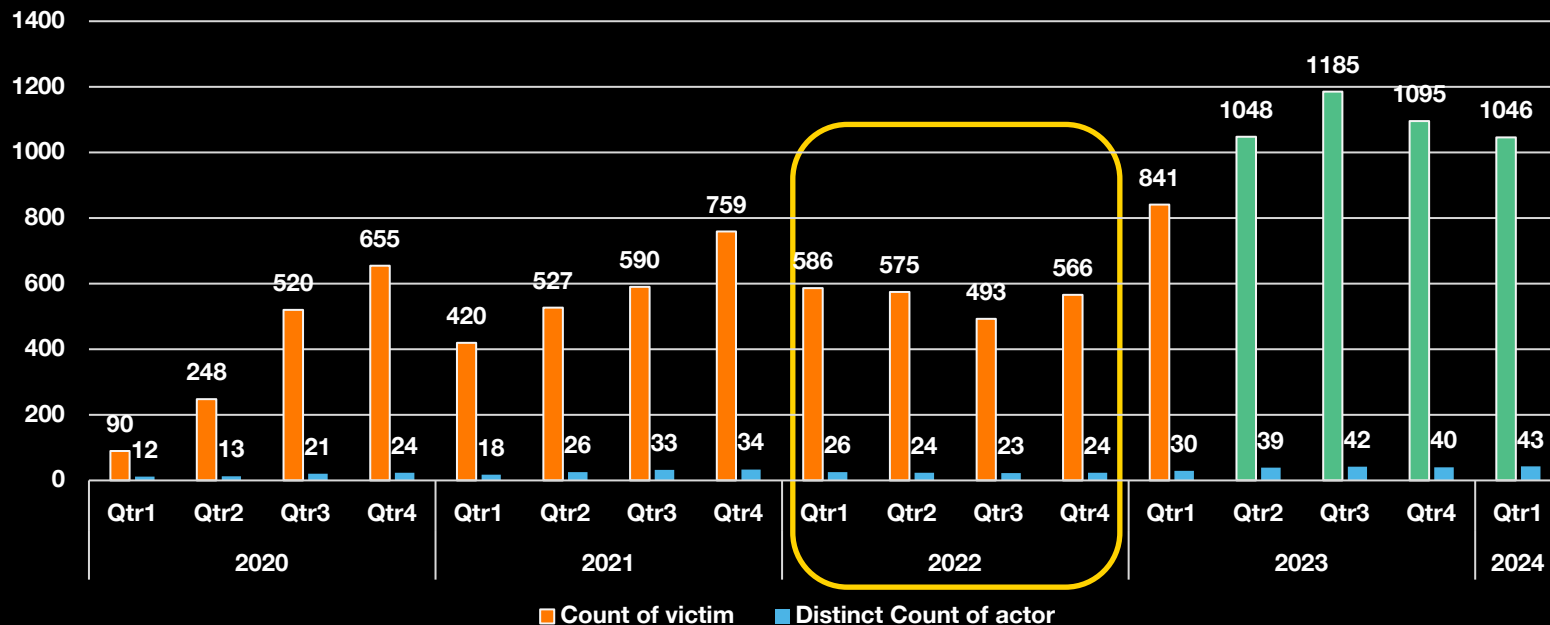




Threats and actors observed

Distinct threats and distinct actors over time

Cy-X victims over time



n=11,244

What we've seen

Hacking groups are taking positions in the conflict

"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022

272

0 [0.00 B]

Conti ransomware group announcing their support to Russia on February 25, 2022.

Leading to disclosures

Greetings,

Here is a friendly heads-up that the Conti gang has just lost all their shit. Please know this is true.
<https://twitter.com/ContiLeaks/status/1498830708736073734>

The link will take you to download an 1.tgz file that can be unpacked running tar -xvzf 1.tgz command in your terminal. The contents of the first dump contain the chat communications (current, as of today and going to the past) of the Conti Ransomware gang. We promise it is very interesting.

There are more dumps coming, stay tuned.
You can help the world by writing this as your top story.

It is not malware or a joke.
This is being sent to many journalists and researchers.

Thank you for your support

Glory to Ukraine!



GROUP	SUPPORTING	ATTACKS	COMMS	LOC	Date started
AgainstTheWest (ATW)	Ukraine	Data Breach & ransomware	Twitter	West Europe	2021
Belarusian Cyber Partisans	Ukraine/Free Belarus	Ransomware	Twitter	Belarus	2020
Anonymous	Ukraine	DDoS	Twitter	Global	FEB 2022
GhostSec	Ukraine	Hack	Telegram	UNK	FEB 2022
IT Army of Ukraine	Ukraine	DDoS	Telegram	Ukraine	FEB 2022
KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK	FEB 2022
BlackHawk	Ukraine	DDoS	Twitter	Georgia	FEB 2022
Anonymous Liberland & the PWN-BAR hack team	Ukraine	DDoS	Twitter	Global	FEB 2022
Raidforums Admin	Ukraine	Sanction	Raidforums	UNK	FEB 2022
Netsec	UNK	Hack	Twitter	UNK	FEB 2022
Free Civilian	Russia	Data Breach	Onion	UNK	JAN 2022
Cooming Project	Russia	Data Breach	Onion	UNK	2021
Conti Ransomware	Russia	Ransomware	Onion	Russia	2019
The Red Bandits	Russia	Data Breach	Twitter	Russia	2021
CyberGhost	Russia	Hack	UNK	Belarus	UNK
SandWorm	Russia	Hack & DDoS	UNK	Russia	UNK
28 FEB	----	-----	-----	-----	-----
GNG	Ukraine	DDoS	Twitter	Georgia	2022
NB65	Ukraine	Hack	Twitter	UNK	2022
ECO	UNK	UNK	Twitter	UNK	2022
Raidforums2	Ukraine	DDoS	Twitter	UNK	2022
ContiLeaks	Ukraine	Data Breach	Twitter	UNK	2022
SHDWSec	Ukraine	Hacks/Activism	Twitter	Global	2022
GhostClan	Ukraine	Hacks/DDoS	Telegram	Global	2022
Eye of the Storm	Ukraine/Free Belarus	Hacks	Twitter	Global	2022

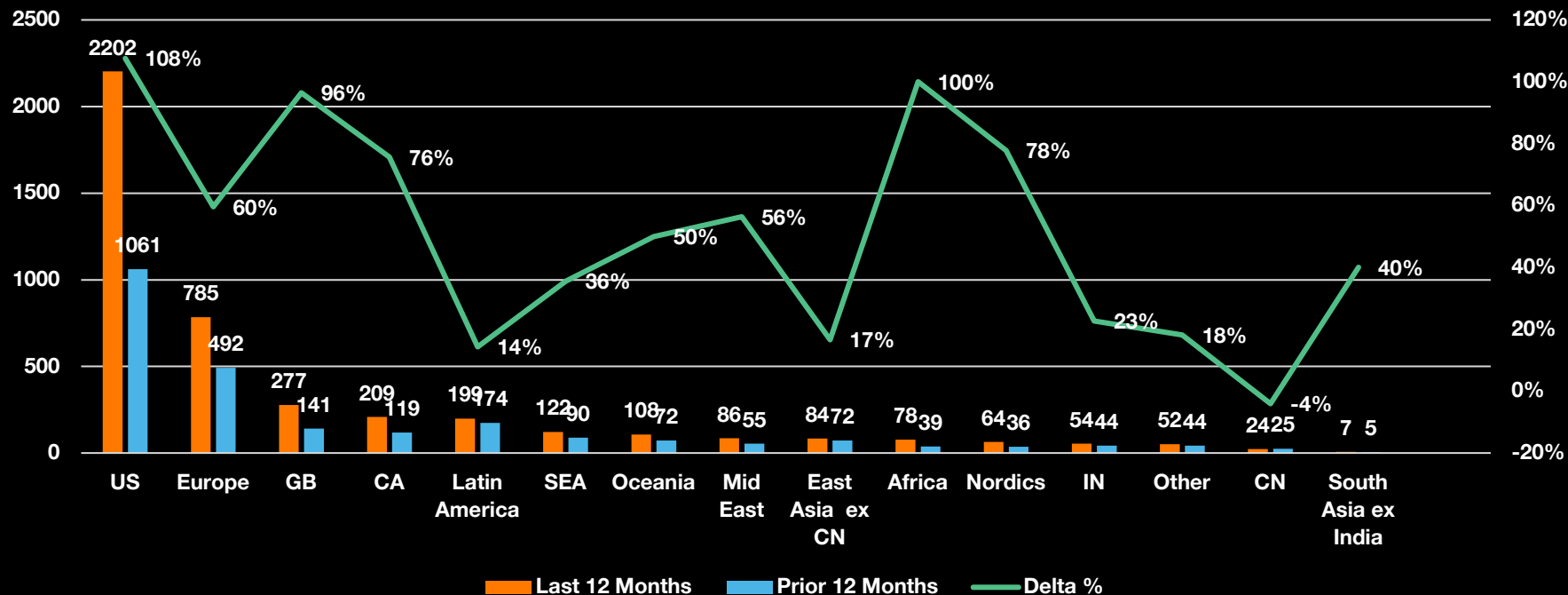
Cyber group tracking by @CyberKnow, visit: <https://cyberknow.medium.com/2022-russia-ukraine-war-cyber-group-tracker-update-1-ee3834fb03c>

Regional analysis

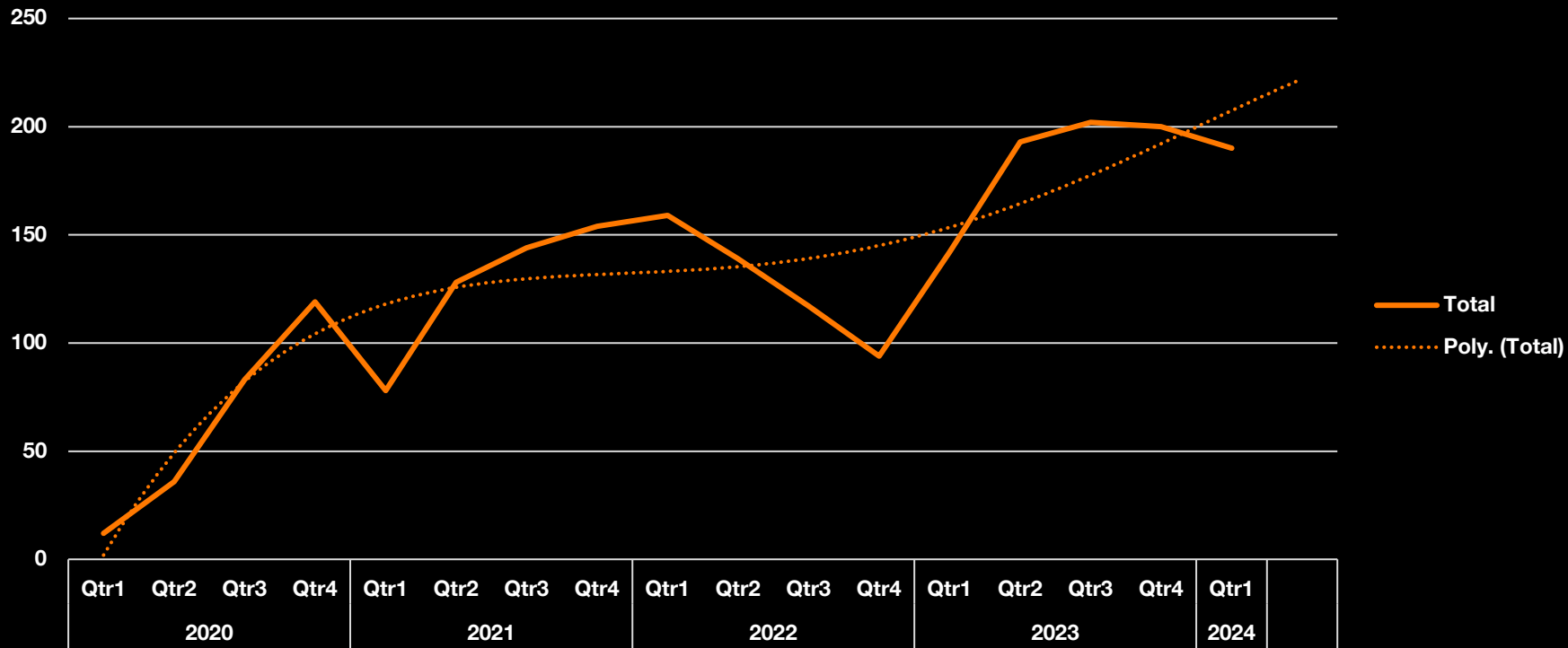
Distinct victims per country past 12 months vs. prior 12 months comparison



Victim

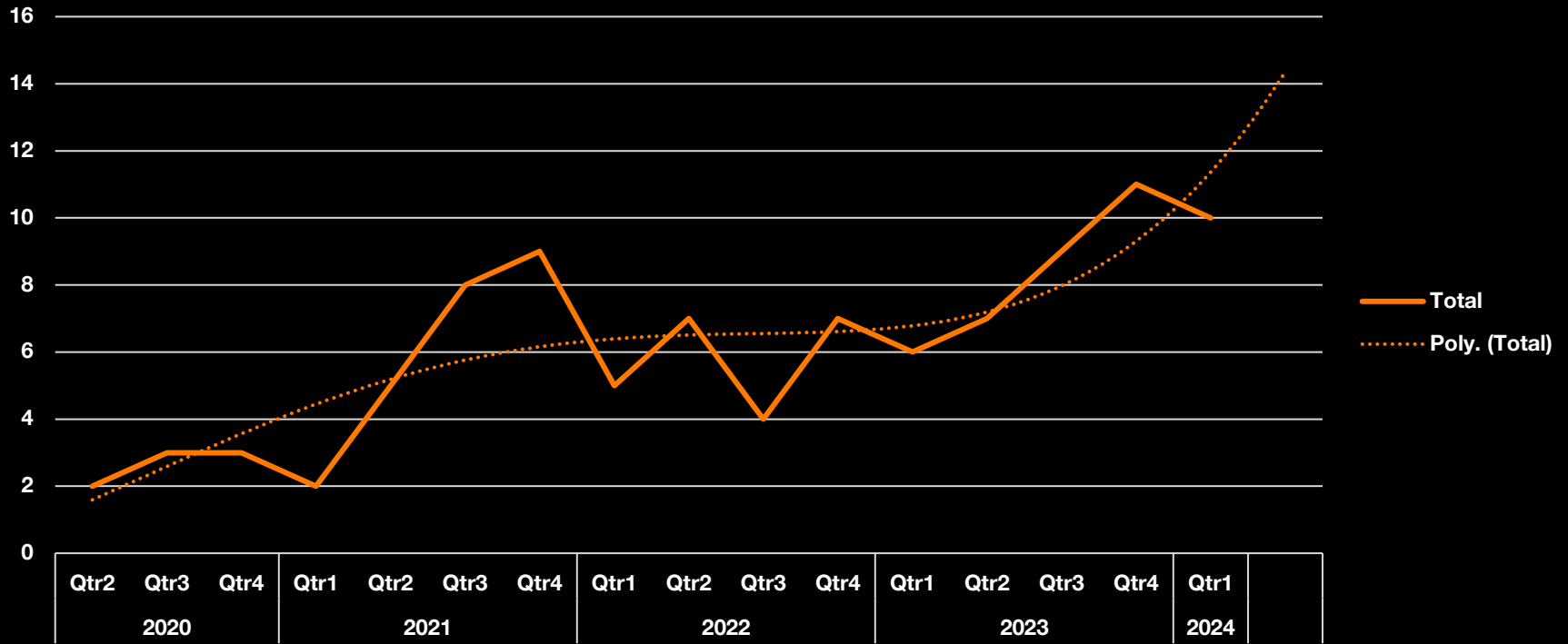


Europe

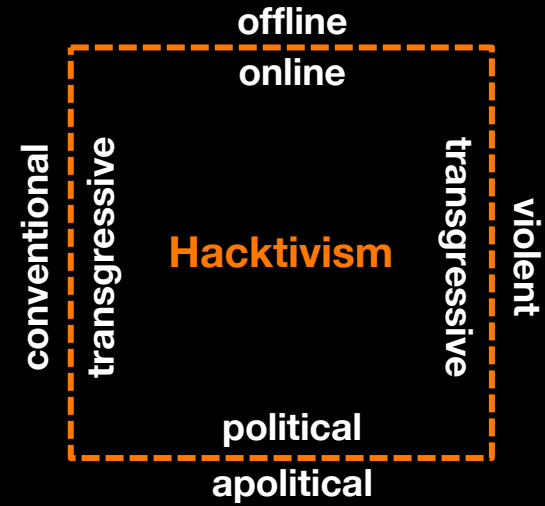




Belgium



Hacktivism



<https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf>

Hacktivism | Ukraine war

'It's Our Home Turf.' The Man On
Ukraine's Digital Frontline



Source: Time magazine (2022)

“Ukraine’s cyber response plan was carefully crafted by its Minister of Digital Transformation – Mykhailo Albertovych Fedorov – who coordinated one of the most successful, multifaceted information operations campaigns ever witnessed in history.”

- Darkowl whitepaper (2023)



Hacktivism | Ongoing geopolitical conflicts

02 NOV2023 Israel-Palestine CyberTracker #5 – 137 Groups

Pro-Israel - 19 Groups

- Team UCC Operations – DDoS
- Garuna Ops – DDoS
- Indian Cyber Force – Hack/DDoS
- SilentOne – DDoS
- Kerala Cyber Xtractors – DDoS
- Gaza Parking Lot Crew – Hack
- AnonyMiss – DDoS
- Termux Israel – DDoS/Hack
- Silencers of Evil – Hack
- Israel Cyber Defence – DDoS
- Predatory Sparrow – Hack
- Glorysec – Hack
- Dark Cyber Warrior – DDoS
- Anonymous India – DDoS
- Red Evils – DDoS/Hack
- Ares – Data Leak
- Op Iran – DDoS/Hack
- NEW ADDITIONS**
- Kerala Cyber Thunders – DDoS/Deface
- Black Dragon Sec – DDoS/Deface

Pro-Palestine/Anti-Israel – 118 Groups

- Mysterious Team Bangladesh – DDoS
- Team HeroX – DDoS
- Ghosts of Palestine – DDoS
- AnonGhost – DDoS
- Blackshieldcrew MY – DDoS
- Ghost Clan – DDoS
- Anonymous Sudan – DDoS
- Team Insane Pakistan – DDoS
- Ganosec team – DDoS
- Team Azrael Angel of Death – DDoS
- Garnesia Team – DDoS
- Moroccan Black Cyber Army – DDoS
- Hacktivist Indonesia – DDoS
- 4 Exploitation – DDoS
- Gb Anon 17 – DDoS
- Team 170 – DDoS
- Electronic Tigers Unit – DDoS
- YourAnonTDX – DDoS
- Stuxx Team – DDoS
- Hizbulish Cyber Team – DDoS
- StarsX Team – DDoS
- Cscrew – DDoS
- SyniaCyberCrimeMY – DDoS
- TYG Team – DDoS
- Eagle Cyber Crew – DDoS
- Ghost Clan Malaysia – DDoS
- 1st10 team – DDoS
- Killinet – DDoS – Pro Russian
- Purple team – DDoS
- Sylhet Gang SG – DDoS
- Muslim Cyber Army – DDoS
- Anonymous Morocco – DDoS
- Pakistani Left Hackers – DDoS
- Cyber Avengers – Hack
- Chaos – Hack
- Weedsec – Hack
- Dragonforce Malaysia – DDoS/Deface
- Storm.1133 – Hack
- Cyber Drag0nz – DDoS
- End Sodoma – DDoS/Hack
- Usersec – DDoS/Deface – Pro Russian
- Tengkorakcyber – DDoS
- Khalifah Cyber Crew – DDoS/Deface
- SkyNet – DDoS
- ACEH – DDoS/Hack
- Boom Security – DDoS
- DevilAttacks – DDoS
- Moses Staff – Hack
- PMOI – DDoS/Hack
- Kap Team – DDoS
- Islamic Hacker Army – DDoS/Deface
- Arab Anonymous Team – DDoS
- Garuda Security – DDoS
- Anonymous BD – DDoS
- Stuxx Team – DDoS/Dox
- Mysterious Silent Force – DDoS
- Ghost Princess of Palestine – DDoS
- Moroccan Ghosts – DDoS
- R4gn4r0k Gh0st – DDoS
- karawang cyber team – DDoS
- Komandan Hansip – DDoS
- Black Security Team – DDoS
- Tunisian Cyber Army – DDoS
- Cyber System Error – DDoS
- Ox Web Moroccan – DDoS/Deface
- Night Raid Cyber – DDoS/Hack
- ThreatMility – DDoS
- Cyber Army Palestine – DDoS
- C.O.A Agency – DDoS
- Esteem Restoration Eagle – DDoS
- Ketapang Grey Hat Team – DDoS
- Lulz Security Agency – DDoS
- 313 team – DDoS
- HostKillCrew – DDoS
- cyber soderhana team – DDoS
- kuningan Exploiter – DDoS
- Xecatsha – Hack
- Infinite Insight.ID – DDoS/Hack
- Anony_M0us – DDoS
- Vulzsec – DDoS/Hack
- Haghjoyan – DDoS
- Ben M'Tildi 54 – DDoS/Hack
- Anonghost Indonesian – DDoS
- US Nexus Networks – DDoS/Hack
- Soldiers of Solomon – Ransomware
- RuBit – DDoS – Pro Russian
- The Returnees – DDoS/Deface
- The Cyber Watchers – DDoS/Hack
- Xv888 – DDoS
- Blacksec – DDoS/Hack – Pro Russian
- IRoX Team – DDoS/Hack
- Darkseek Hacking Group – DDoS/Deface – Pro Russian
- Fallaga Team – DDoS
- Dark Strom Team – DDoS/Hack
- NEW ADDITIONS**
- Anonymous X – DDoS
- iEthesia – Hack
- Dark Olympuzt Crew – DDoS/Hack
- Kuwait Hackers – Deface
- Sul4wes1 teng4h bl4ckh4t – DDoS
- H4xor Umbrella Corp – DDoS/Deface
- The Camp 22 – DDoS/Deface
- Deadlink – DDoS/Hack
- 1 teng4h bl4ckh4t – DDoS
- IXP666secteam – DDoS/Deface
- JRex As7 – DDoS
- The Ddosser Garuda – DDoS
- Padang System Error – DDoS/Hack
- Agem Massive – Deface
- Esteem Restoration Evil – DDoS/Deface
- Team 1956 – DDoS/Deface
- Nixon Cyber Team – DDoS/Deface
- Brave Redstorm Eagle – DDoS/Deface
- Indonesia Anonymous – DDoS/Deface
- Fr13nds – DDoS
- 177 Members Team – Deface/DDoS
- Nothwh0me – Deface/DDoS
- Anonymous Collective – DDoS
- Malaysia Cyber Defacer – Deface

Faketivism

INTRODUCED IN THE CROWDSTRIKE 2016 GLOBAL THREAT REPORT, FAKETIVISM REFERS TO ACTIVITY BY ENTITIES THAT CHARACTERIZE THEMSELVES AS HACKTIVIST GROUPS BUT MORE LIKELY REPRESENT A FRONT FOR A GOVERNMENT OR OTHERWISE PROFESSIONAL ENTITY.

IN AN EFFORT TO APPEAR GENUINE, FAKETIVISTS – AKA INAUTHENTIC PERSONAS – OFTEN ADOPT THE EXISTING IMAGERY, RHETORIC, TTPS AND SOMETIMES NAMES OF ESTABLISHED HACKTIVISTS. THEY OFTEN SURFACE IN DIRECT RESPONSE TO GEOPOLITICAL EVENTS, OFTEN HAVE LITTLE OR NO ESTABLISHED ACTIVITY HISTORY, AND ALMOST ALWAYS OPERATE IN DIRECT ALIGNMENT WITH STATE GOVERNMENT INTERESTS. THESE PERSONAS PROVIDE STATE BACKERS WITH A LAYER OF DENIABILITY BUT CAN ALSO SERVE INFORMATION OPERATIONS GOALS.

SNCB website again online after 'large-scale cyber attack'



The image BELGA

The website of railway company SNCB is online again. Since this morning, the website could not be consulted due to a cyber attack, reports spokesman Bart Crols.

The news The Hackers

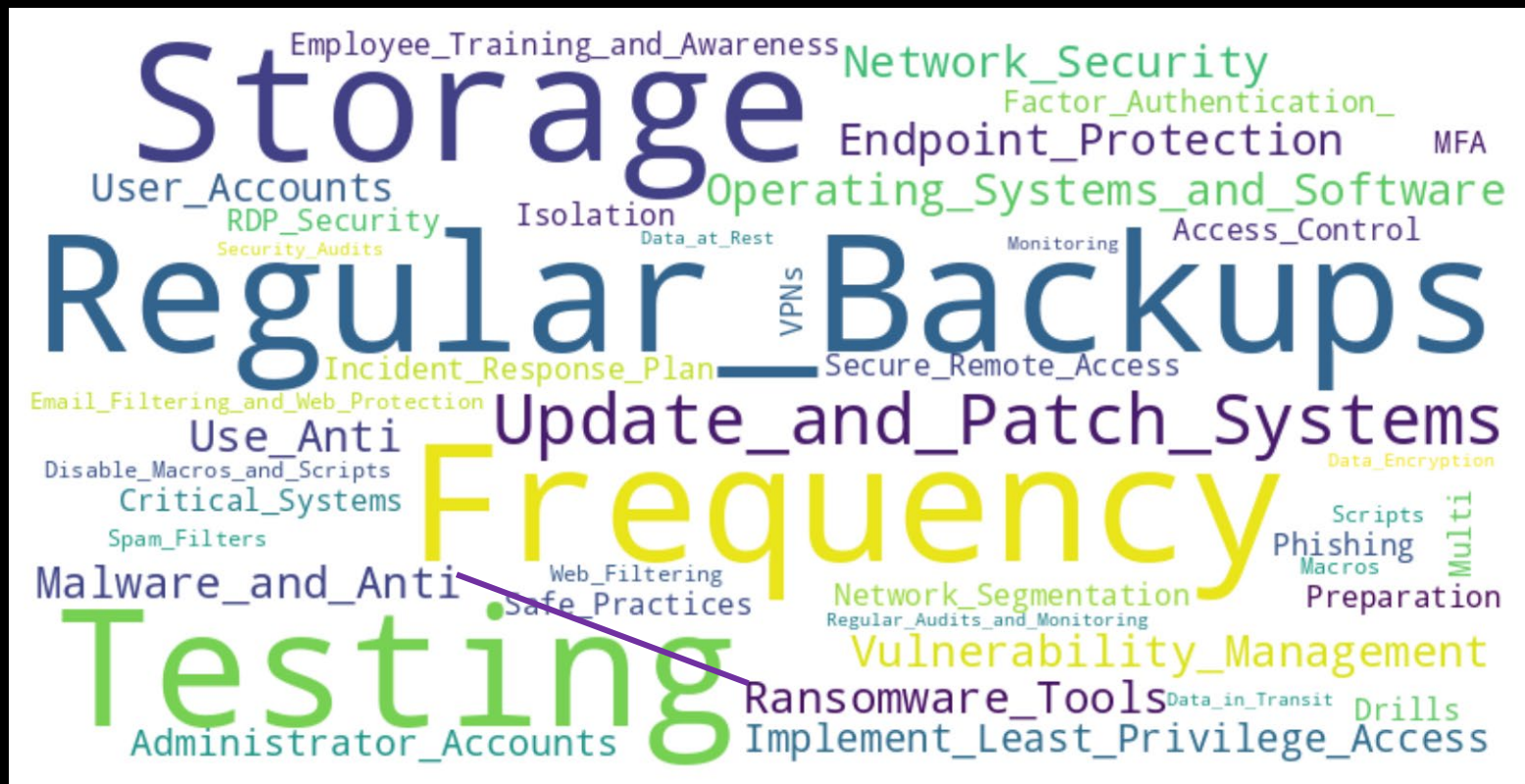
Cybercriminals attack website Room: 'Parliament has far too long Waiting to take action.'



The House's website was unreachable for some citizens and parliamentarians. Image HLN / Photo News

In recent days, the website of the House of Representatives has been re-eating by cyber criminals. Just like the previous times, it is a so-called DDoS attack in which the site is overwhelmed with internet traffic so that it is unreachable.

What do we do?



**Meet me & my colleagues
for a beer or coffee**

Orang Cyberdefense Live

Register as an early bird to seize
your chance to **win** one of **5**
Shokz headphones.

Register as an early bird

