

DASHBOARD

🏠

Dashboard

REPORT MANAGEMENT

- 📁

Reports
- ⚠️

Attack Profiles
- 🛡️

Victim Profiles

USERS

👤

User Management



Attack Profiles

6



Victim Profiles

3

Reports Overview



●

Published

●

Saved

Monthly Report Counts

2025



Select All

January	0
February	0
March	0
April	3
May	2
June	0
July	0
August	0
September	0
October	0
November	0
December	0

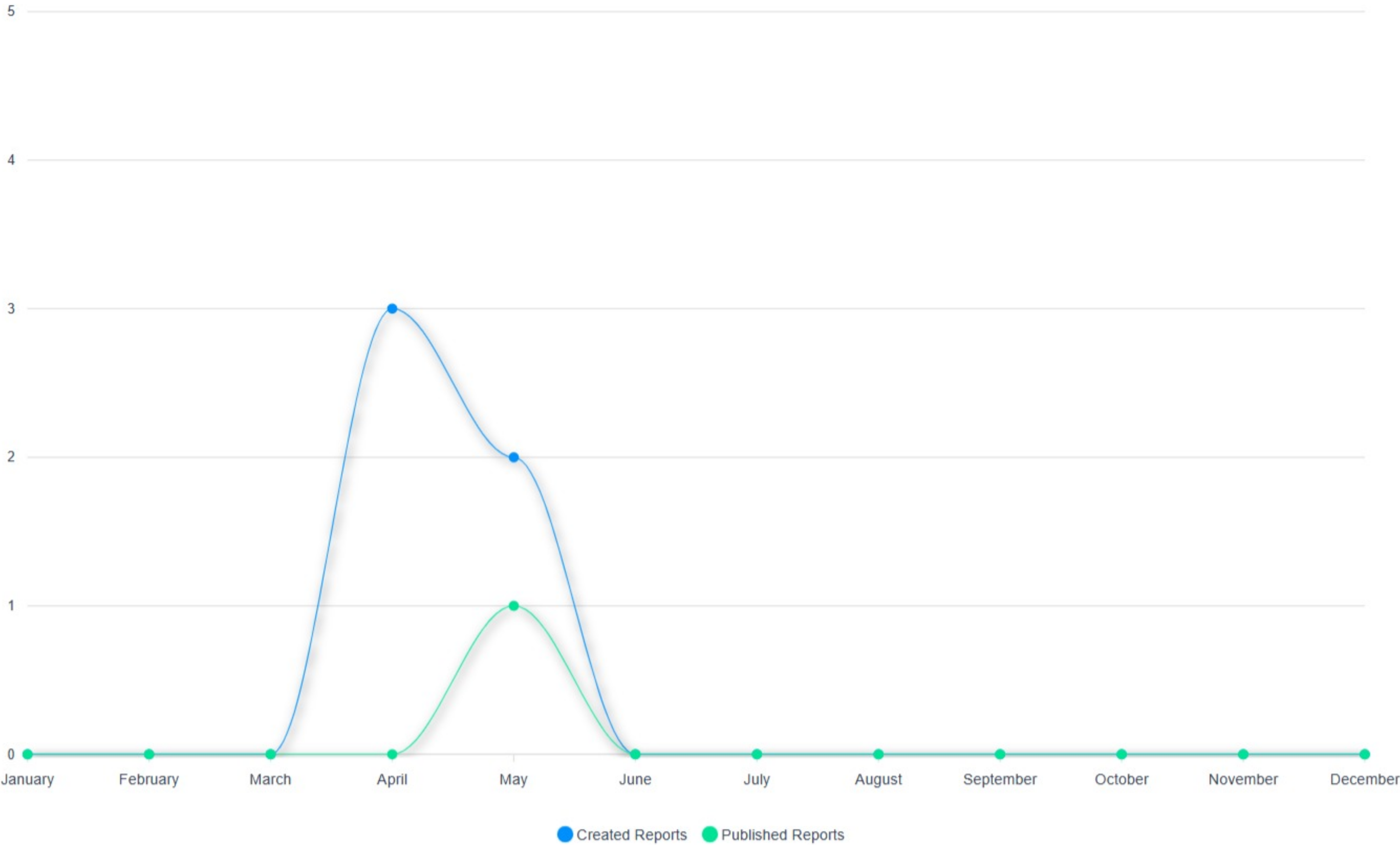
Reports Timeline

2025



Select All

Reports Timeline



DASHBOARD

[Dashboard](#)

REPORT MANAGEMENT

[Reports](#)

[Attack Profiles](#)



[Home](#) > [Report Management](#) > [Edit Report](#)



Reports

Please fill out the Title, Date and Identification of new report you want to opne. Otherwise the report will be discarded and WILL NOT saved!

1 Basic Information 2 Threat Context 3 Attack Profile 4 Victim Profile 5 Conclusion

Report Title ⓘ

BlackHat operation (DE,HU)

Report Date ⓘ

13/05/2025 10:36

Report Identification ⓘ

BHo-35 (DE,HU)

Analysts ⓘ

1: Analyst1

Add

Delete

Criticality ⓘ

Vital

TLP ⓘ

Amber

Sensitivity ⓘ



Next →

Reports

Please fill out the Title, Date and Identification of new report you want to opne. Otherwise the report will be discarded and WILL NOT saved!

- 1 Basic Information
- 2 Threat Context
- 3 Attack Profile
- 4 Victim Profile
- 5 Conclusion

Scope ⓘ

Tento report sa zaoberá dlhodobou kybernetickou kampaňou skupiny APT28 (Fancy Bear), napojenou na ruské vojenské spravodajstvo GRU, ktorá v období od marca 2022 do mája 2024 cieľila na e-mailové systémy a kritickú infraštruktúru v Českej republike, Nemecku a ďalších členských štátoch EÚ s cieľom získať strategické politické a vojenské informácie a oslabiť dôveru v demokratické inštitúcie pred voľbami do Európskeho parlamentu a národnými voľbami v USA.

Objectives ⓘ

- Získať dôverné e-maily, prihlasovacie údaje a sieťové informácie štátnych inštitúcií a politických subjektov prostredníctvom zero-day exploitov v Microsoft Outlook (CVE-2023-23397) a spear-phishingu.
- Anonymizovať svoju prítomnosť v sieti cieľ'a použitím botnetu kompromitovaných SOHO routerov, aby sa predĺžil čas nepozorovaného pobytu v sieti.
- Šíriť dezinformácie a podlamovať dôveru verejnosti v demokratické procesy pred nadchádzajúcimi voľbami či už v USA alebo v EU.

Impacted Sectors ⓘ

Vláda; Politika; Kritická infraštruktúra; Energetika; IT služby; Letecký a obranný priemysel

Impact ⓘ

Tieto útoky predstavujú priame ohrozenie národnej bezpečnosti, nakoľko kompromitácia e-mailových systémov vládnych a politických entít môže viesť k úniku strategických informácií. Zároveň znižujú dôveru občanov v demokratické inštitúcie a môžu vyvolať politickú nestabilitu počas volieb. Použitie anonymizačných botnetov zvyšuje riziko dlhodobého, neodhaleného prieskumu sietí, čo môže viesť k ďalším následným sabotážam kritickej infraštruktúry (energetika, doprava).

 Back

Next 

Reports

Please fill out the Title, Date and Identification of new report you want to opne. Otherwise the report will be discarded and WILL NOT saved!

- 1

Basic Information
- 2

Threat Context
- 3

Attack Profile
- 4

Victim Profile
- 5

Conclusion

Attack Profile

+ Choose an attacker's profile

Actor ⓘ

APT28 (Fancy Bear)

Location ⓘ

Russia

Motivations ⓘ

Cyber Warfare ⊗

Undermining Internationa

Affiliations ⓘ

State-Sponsored Hackers ⊗

Intelligence Ag

Capabilities ⓘ

APT28 disponuje schopnosťou využívať zero-day zraniteľnosti (CVE-2023-23397 v Outlooku), sofistikovaným spear-phishingom, orchestráciou botnetov kompromitovaných SOHO routerov, pohyb v cieľových sieťach a opatreniami na vymazanie stôp po extrakcii dát.

Operations ⓘ

- Exploit zero-day v Microsoft Outlook (marec 2023) na získanie Net-NTLMv2 hashov a následné relejové útoky na autentifikáciu.

- Spear-phishing cieleňý na e-mailové účty politických predstaviteľov a administrátorov vládnych sietí.

- Využitie botnetu stoviek kompromitovaných SOHO routerov pre anonymizáciu C2 komunikácie a predĺženie nepozorovaného prieskumu.

- Koordinovaná medzinárodná operácia "Dying Ember" (jan 2024) zameraná na rozbitie infraštruktúry APT28 pod vedením FBI, BfV, Europolu a partnerov.

← Back

Next →

Reports

Please fill out the Title, Date and Identification of new report you want to opne. Otherwise the report will be discarded and WILL NOT saved!

- 1 Basic Information
- 2 Threat Context
- 3 Attack Profile
- 4 Victim Profile
- 5 Conclusion

Victim Profile

+ Choose a victim's profile

Victim ⓘ

Politické subjekty, štátne inštitúcie a kritická infraštruktúra

Location ⓘ

Czech Republic

IOCs ⓘ

- CVE-2023-23397

- CVE-2022-38028

TTPs ⓘ

- Exploity zero-day v Microsoft Outlook (CVE-2023-23397) a Windows Print Spooler (CVE-2022-38028)

- Spear-phishing a credential harvesting

- Botnet-based anonymization (kompromitované SOHO routery)

- Lateral movement a extrakciadát z e-mailových serverov

- Vymazanie forenzných stôp a stôpo ponechaných po extrakcii dát zo systému

Targeted Sector ⓘ

Vláda; Politika; Kritická infraštruktúra; Energetika; IT služby; Letecký a obranný priemysel

Okrem Českej republiky boli zasiahnuté aj krajiny - Nemecko a USA

← Back

Next →



DASHBOARD

🏠 Dashboard

REPORT MANAGEMENT

📁 Reports

⚠️ Attack Profiles

🛡️ Victim Profiles

USERS

👤 User Management

Reports

Please fill out the Title, Date and Identification of new report you want to opne. Otherwise the report will be discarded and WILL NOT saved!

- 1 Basic Information 2 Threat Context 3 Attack Profile 4 Victim Profile 5 Conclusion

Findings ⓘ

- 1. APT28 zneužila zero-day zraniteľnosť v Microsoft Outlook z roku 2023 na kompromitáciu e-mailových systémov českých a nemeckých inštitúcií.
- 2. Útočníci používali botnet z kompromitovaných SOHO routerov pre anonymizáciu C2 komunikácie a predĺženie prieskumu bez odhalenia.
- 3. Identifikované metódy zodpovedajú profilu štátmi sponzorovanej skupiny APT28 (Fancy Bear), napojenej na GRU.
- 4. Postihnuté subjekty dostali technické odporúčania a zapojili sa do operácie "Dying Ember" na neutralizáciu infraštruktúry útočníkov.

Overview ⓘ

Kampaň APT28 trvala od marca 2022 do mája 2024. Útočníci cieľili na e-mailové systémy vládnych a politických subjektov v Česku, Nemecku a ďalších krajinách EÚ. Hlavnou metódou bol zero day exploit v Outlooku, podporený spear-phishingom a botnet anonymizáciou. Operácia Dying Ember potvrdila medzinárodnú spoluprácu na neutralizácii hrozby.

Sources ⓘ

- 1: https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html
- 2: <https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html>
- 3: <https://www.rewterz.com/threat-advisory/russias-apt28-abused-microsoft-outlook-vulnerability-to-target-german-and-czech-organ>
- 4: <https://thehackernews.com/2024/05/microsoft-outlook-flaw-exploited-by.html>
- 5: <https://www.rewterz.com/threat-advisory/russias-apt28-abused-microsoft-outlook-vulnerability-to-target-german-and-czech-organ>

Add

Delete

← Back

Publish







[Dashboard](#)

Reports

Attack Profiles

+ Add an attacker's profile

Search

Actor	Location	Actions
PshishingGroup	Brazil	
CyberWarfare	China	
Trojan	Estonia	
DDOS3	Andorra	
APT28 (Fancy Bear)	Russia	
BlackHatG5	Cocos (Keeling) Islands	

<<

<

1

>

>>

DASHBOARD

[Dashboard](#)

Add an attacker's profile

Actor ⓘ

Actor

Location ⓘ

Location

Motivations ⓘ

Motivations

Affiliations ⓘ

Affiliations

Capabilities ⓘ

Capabilities

Operations ⓘ

Operations

[← Return](#)[Save](#)

- ☐
- Nation-State Actors**
- ☐  Military Units
- ☐  Intelligence Agencies
- ☐  State-Sponsored Hackers
- ☐  Paramilitary Organizations

DASHBOARD

[Dashboard](#)

REPORT MANAGEMENT

[Reports](#)

[Attack Profiles](#)

[Victim Profiles](#)

USERS

[User Management](#)



[Home](#) > [Report Management](#) > [Victim Profiles](#)




Victim Profile

[+ Add Victim Profile](#)

Search

Victim	Location	Actions
Militantné organizácie	Nigeria	
Politické subjekty	Greenland	
Politické subjekty, štátne inštitúcie a kritická infraštruktúra	Czech Republic	
<div><< < 1 > >></div>		

DASHBOARD

 Dashboard

REPORT MANAGEMENT

 Reports



 > Report Management > Add Victim Profile



Add Victim Profile

Victim ⓘ

Victim

Location ⓘ

Location



Targeted Sector ⓘ

Targeted Sector



TTPs ⓘ

TTPs



IOCs ⓘ

IOCs



 Return

Save

DASHBOARD

Dashboard

REPORT MANAGEMENT

Reports

Attack Profiles

Victim Profiles

USERS

User Management



Home > Management > User Management



User Management

New Invitation

Add User

Search

Staff ID	First Name	Last Name	Email	Role	Department	Actions
221037	Martina	Molnarova	221037@vut.cz	ADMIN	FEKT	
12345	Guest	Guest	guest@guest.com	GUEST	Guest	
<div><< < 1 > >></div>						

DASHBOARD

Dashboard

REPORT MANAGEMENT

Reports

Attack Profiles

Victim Profiles

USERS

User Management



Management > Add User



Add User

Use this page to add a new user.

Role

Role

ADMIN

USER

GUEST

First Name

First Name

Last Name

Last Name

Staff ID

Staff ID

Department

Department

Email

Email

Password

Password

Create User

Clear

DASHBOARD

Dashboard

REPORT MANAGEMENT

Reports

Attack Profiles

Victim Profiles

USERS

User Management



Home > Management > Invitation



Token Management



Role	Token	Date of Creation	Date of Expiration	Actions
GUEST	58qdqxy8n	2025-05-12T19:14:52.522Z	2025-05-14T19:14:52.522Z	
USER	rw6yi32pl	2025-05-12T19:20:11.242Z	2025-05-14T19:20:11.242Z	

Navigation: << < 1 > >>

Generate Token



Generate

Send



Send