

# Report: APT28-22/24

## Basic Information

### Title:

Kybernetické útoky vykonané aktérom APT28 (CZ, DE, USA)

### Date:

30/04/2025, 15:30:44

### Analysts:

Martina Molnárová

## Threat Context

### Criticality:

Important

### TLP Level:

Clear

### 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 cieľa použitím botnetu kompromitovaných SOHO routerov, aby sa predĺžil čas nepozorovaného pobytu v sieti.
- Šíriť dezinformácie a podlamať dôveru verejnosti v demokratické procesy pred nadchádzajúcimi voľbami či už v USA alebo v EU.

### Targeted Sector:

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).

## Attack Profile

### Actor of the attack:

APT28 (Fancy Bear)

### Location:

Russia

### Motivations:

Cyber Warfare, Undermining International Alliances, Disinformation & Media Manipulation

### Affiliations:

State-Sponsored Hackers, Intelligence Agencies

### 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 cielený 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.

## Victim Profile

### Victim:

Politické subjekty, štátne inštitúcie a kritická infraštruktúra

### Location:

Czech Republic

### **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

### **Indicators (IOCs):**

- CVE-2023-23397
- CVE-2022-38028

### **Target Sector:**

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

Okrem Českej republiky boli zasiahnuté aj krajiny - Nemecko a USA

## **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 štátni 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**

[https://mzv.gov.cz/jnp/en/issues\\_and\\_press/press\\_releases/statement\\_of\\_the\\_mfa\\_on\\_the\\_cyberattacks.html](https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html)  
<https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html>  
<https://www.rewterz.com/threat-advisory/russias-apt28-abused-microsoft-outlook-vulnerability-to-target-german-and-czech-organizations>  
<https://thehackernews.com/2024/05/microsoft-outlook-flaw-exploited-by.html>  
<https://www.rewterz.com/threat-advisory/russias-apt28-abused-microsoft-outlook-vulnerability-to-target-german-and-czech-organizations>

