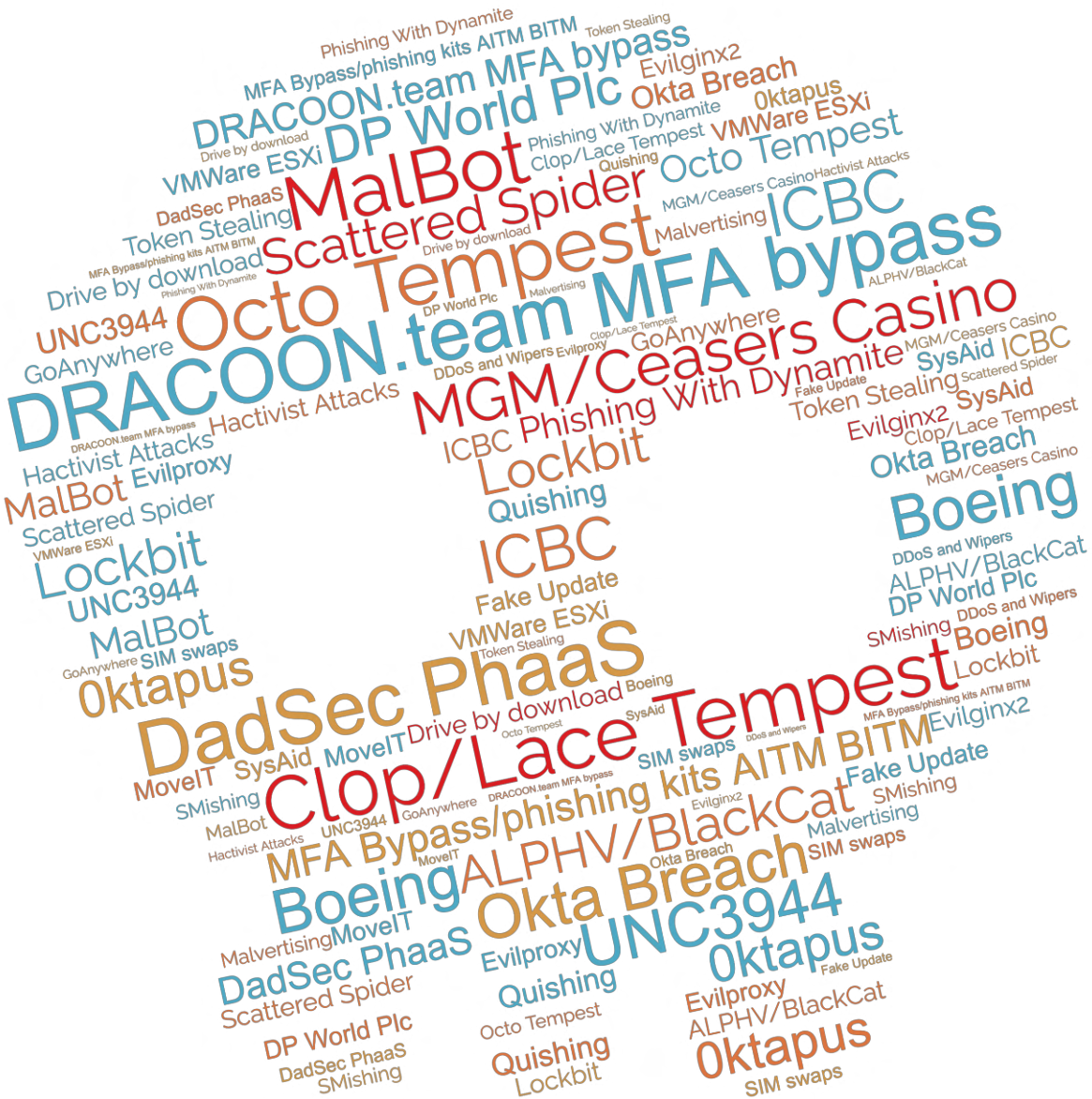
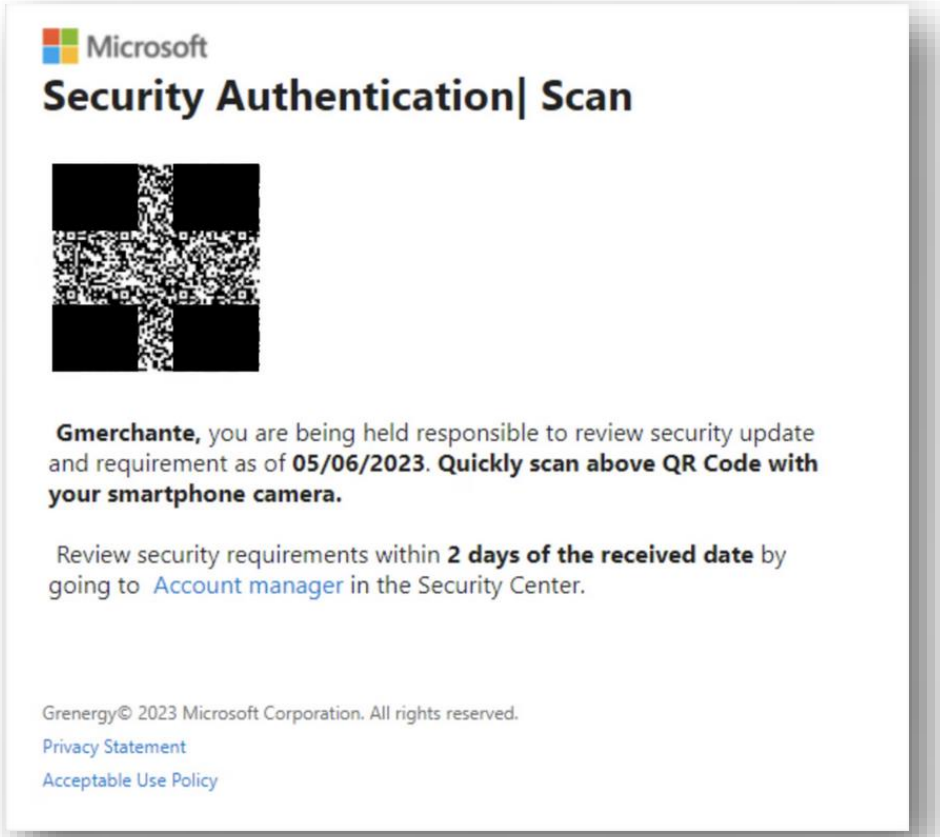

# CYBEREKSPRESS

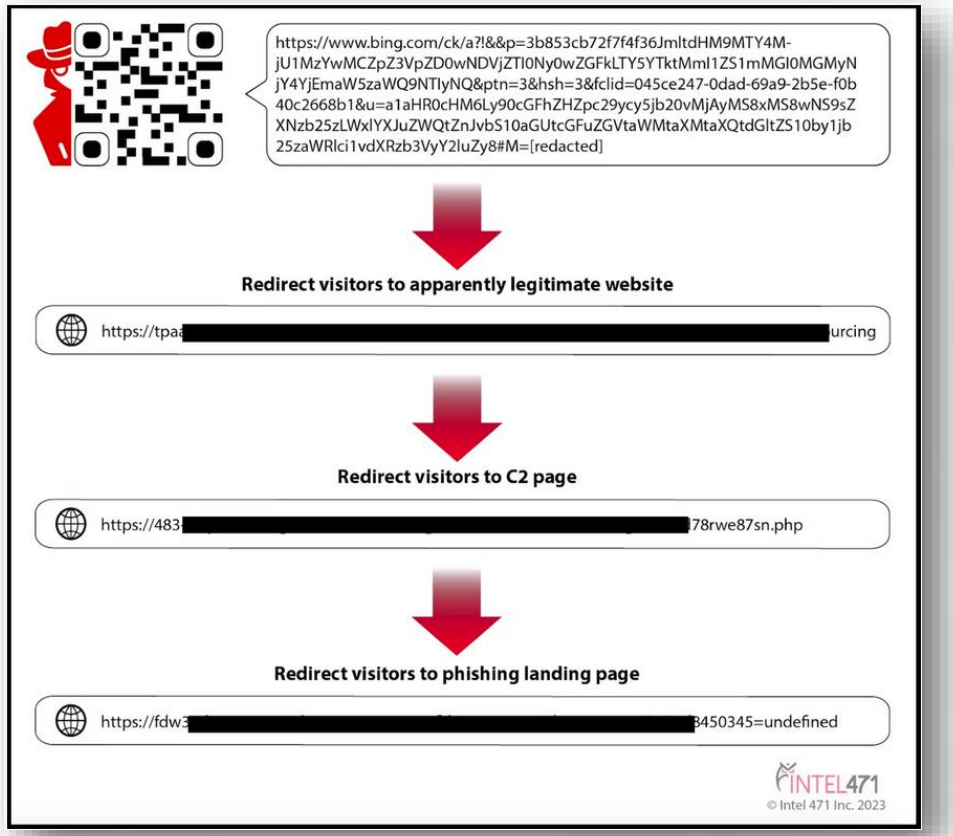
**Marcin Święty**
**Chief Security Officer @ Relativity**

# Działo się dużo



# QR Code Phishing (Quishing) | SMishing




Ref:

- https://intel471.com/blog/phishing-emails-abusing-qr-codes-surge
- https://www.reliaquest.com/blog/qr-code-phishing/
- https://www.proofpoint.com/us/blog/email-and-cloud-threats/cybersecurity-stop-month-qr-code-phishing

# Rapid and Mass exploitation of vulnerabilities

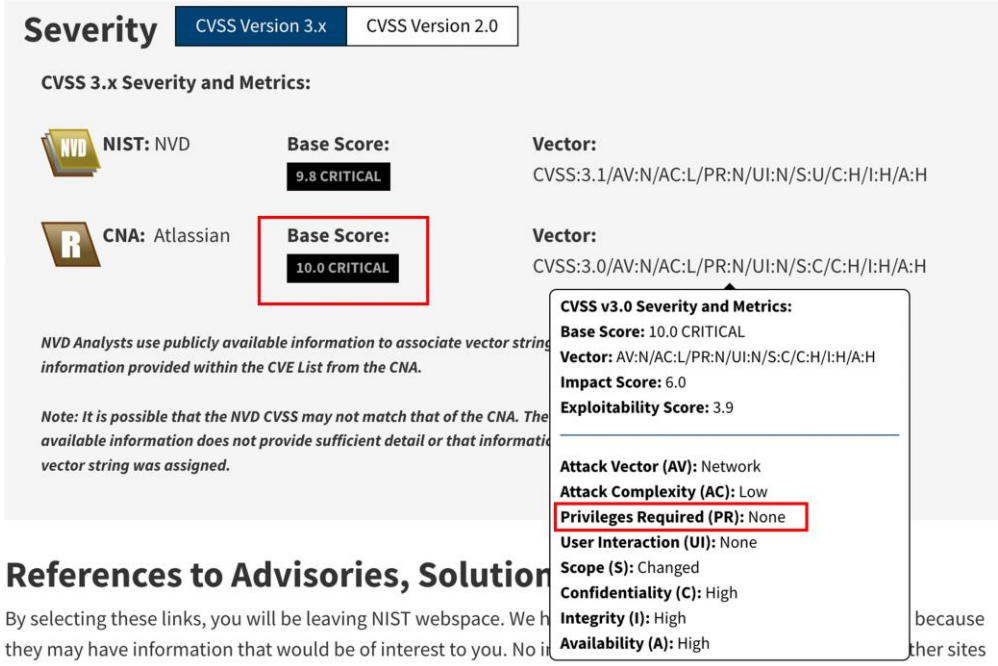
- Lace Tempest aka Storm-0950
  - SysAid CVE-2023-47246
    - Użycie SysAid by załadować loader
      - Archiwum WAR z web shellem na Tomcat
      - Powershell z loaderem Gracewire
      - Drugi Powershell by zatrzeć ślady
      - Przypadki użycia MeshCentral Agent oraz Cobalt Strike
    - Dalej już ręcznie wykorzystanie infrastruktury
  - Znani z masowych ataków
    - MOVEit Transfer
    - PaperCut
    - Zwykle monetyzacja przez Cl0p Ransomware

Ref:

- https://thehackernews.com/2023/11/zero-day-alert-lace-tempest-exploits.html
- https://www.kaspersky.com/blog/confluence-data-center-server-vulnerability/49404/
- https://confluence.atlassian.com/kb/faq-for-cve-2023-22515-1295682188.html
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-289a

- Atlassian Confluence CVE-2023-22515

  Broken Access Control Vulnerability in Confluence Data Center and Server



# Atlassian Confluence CVE-2023-22518

## Improper Authorization Vulnerability In Confluence Data Center and Server

- 2023-10-31
  - CVSS 9.1
  - AV:N/AC:L/PR:N/UI:N/S:U/C:**N**/I:H/A:H
  - *„There is no impact to confidentiality as an attacker cannot exfiltrate any instance data”*
- 2023-11-03 (+4d)
  - Atlassian powiadomiony przez klienta o aktywnym eksploicie
- 2023-11-06 (+7d)
  - CVSS 10
  - AV:N/AC:L/PR:N/UI:N/S:C/C:**H**/I:H/A:H
  - *„Attacker can then perform all administrative actions that are available to Confluence instance administrator leading to - but not limited to - **full loss of confidentiality**, integrity and availability.”*
- 2023-11-07 (+9d)
  - Attlassian informuje o aktywności w instancjach Data Center wskazujących na **wykorzystanie podatności**, pomimo upgrade’u
- 2023-11-08 (+10d)
  - Atlassian **wycofuje się** z poprzedniej wiadomości

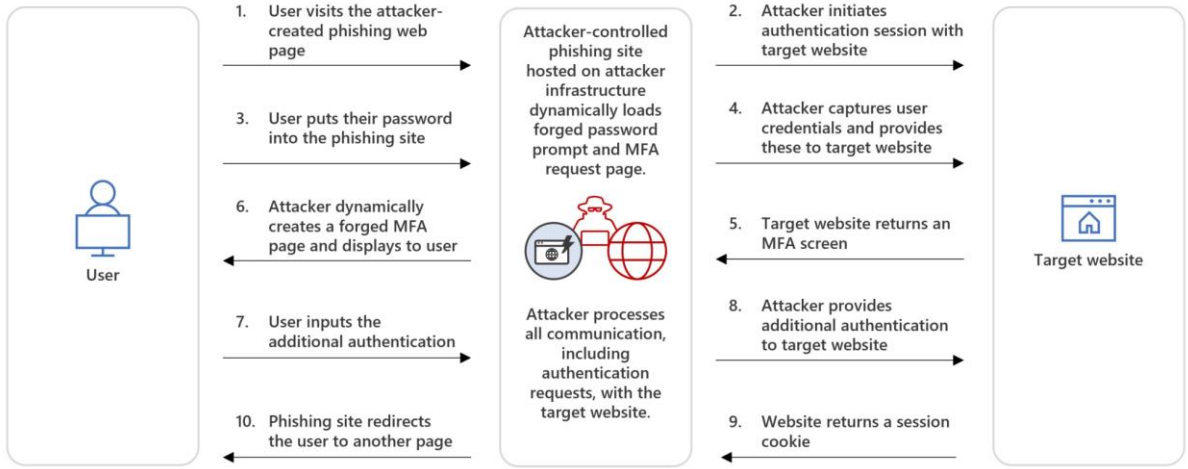
- *„As part of Atlassian's ongoing monitoring of this CVE, we observed **publicly posted critical information about the vulnerability** which increases risk of exploitation. There are still no reports of an active exploit, though customers must take immediate action to protect their instances. If you already applied the patch, no further action is required.”*
- *„At this time we are **unable to disclose** the details you’ve requested without putting added risk on instances that have not yet been patched”*
- *„We **detected a malicious plugin** that matches confirmed threat actor activity. This malicious plugin has been known to encrypt backup copies of Confluence instances and execute a ransomware attack. The CVE has been increased from CVSS 9.1 to 10.”*
- *„**Previous message sent in error**: We have no reason to believe that your Confluence DC instance has been compromised. It has come to our attention that the previous message was sent in error.”*

- https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html
- https://www.rapid7.com/blog/post/2023/11/06/etr-rapid7-observed-exploitation-of-atlassian-confluence-cve-2023-22518/

# MFA Bypass/phishing kits AITM BITM

Ze wzrostem adopcji MFA, pojawił się wzrost i zapotrzebowanie na metody obejścia MFA (*nie działa na thin-client z cert-pinning, lub np. FIDO*)

- **AITM: Adversary-in-the-Middle (**e.g. DadSec PhaaS, Evilginx2, Evilproxy**)**




https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

**BITM: Browser-in-the-Middle (**e.g. Cuddlephish**)**


- *Krok 1: Wysyłaj strumień video przeglądarki do przeglądarki ofiary*
- *Krok 2: Odbieraj interakcję ofiary ze stroną (myszka, klawiatura)*
- *Krok 3: Wykonaj te same czynności na swojej przeglądarce*
- *Krok 4: Ciesz się zdobytymi danymi uwierzytelniającymi, ale co ważniejsze – tokenem sesji by pomijać MFA na czas życia tokena.*

# Octo Tempest, Oktapus, Scattered Spider, oraz UNC3944 + LockBit + ALPHV/BlackCat,

- **Octo Tempest:**
  - aka Group-IB, Scattered Spider, UNC3944, Oktapus
  - Umotywowana finansowo
  - Angielsko języczna
  - Duże kampanie, nie koniecznie dużo
  - Phishing, SIM swapping, AiTM i inne
  - Afiliacja z ALPHV/BlackCat
  - Sukcesy: Coinbase, MGM Casino

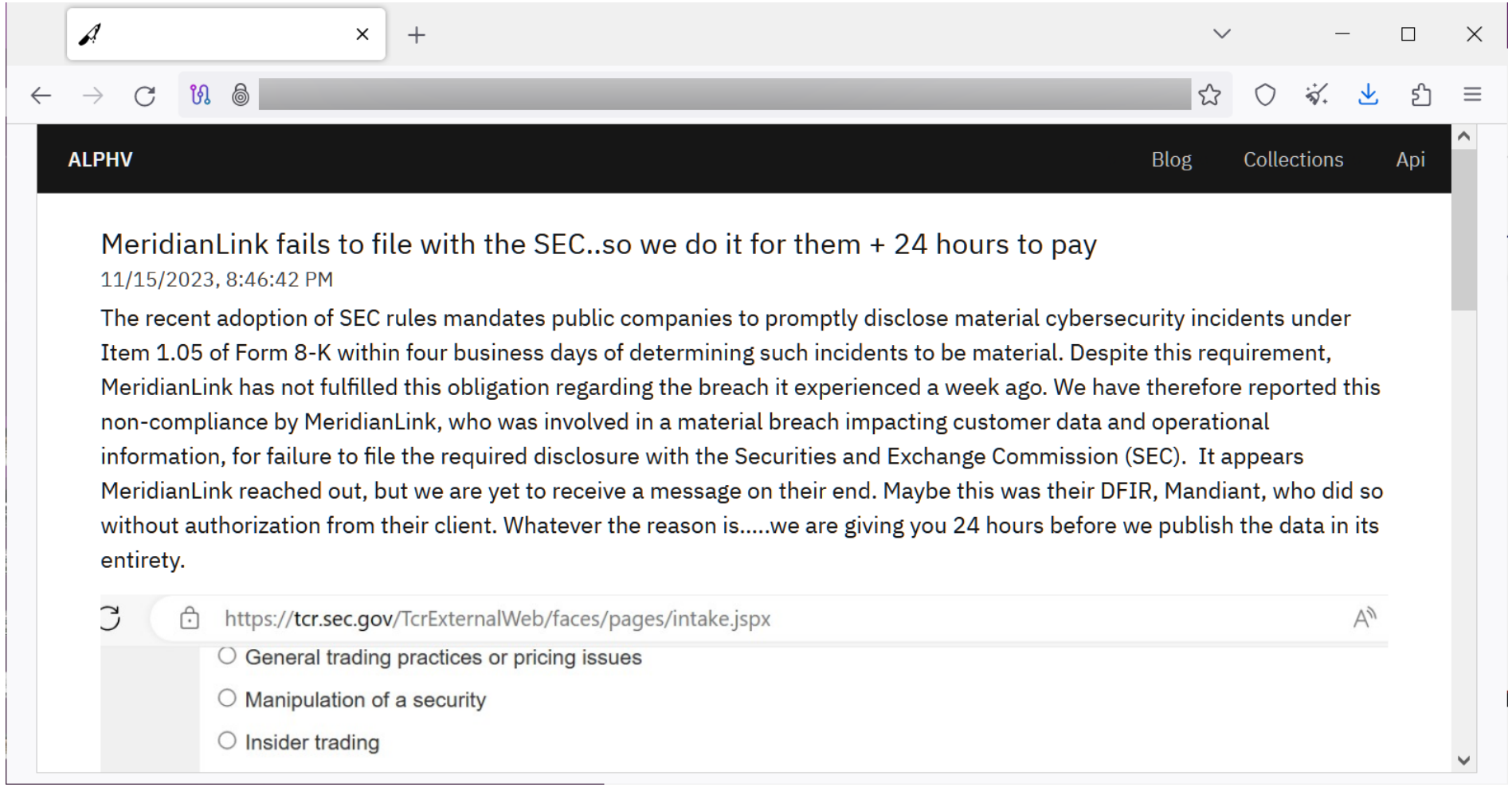

Figure 1. *The evolution of Octo Tempest's targeting, actions, outcomes, and monetization*

- **LockBit**
  - RaaS – Ransomware as a Service
  - Pewne podobieństwa z Alphv, BlackMatter i Conti

  - Boeing – Citrix Bleed, 50 GB danych pomimo negocjacji
  - ICBC – Citrix Bleed, okup opłacony, sprawa zamknięta
  - DP World Plc

- **ALPHV/BlackCat**
  - RaaS Ransomware-as-a-Service
  - Wykorzystuje reklamy Google Search oraz Bing
  - Wykorzystanie exploita Nirtogen do obfuskacji i loadera
  - Tradycyjnie podwójne wymuszenie, czasem potrójne
  - Listopad przyniósł kolejny ciekawy pomysł na wywarcie dodatkowej presji – zgłoszenie wycieku do SEC by wywrzeć presję.

# ALPHV/BlackCat oraz nowy pomysł na presje



# Działo się dużo