

Bezpieczeństwo kodu

... z bezpłatnych źródeł (cybersec a korzystanie z różnorodnych bibliotek i komponentów)

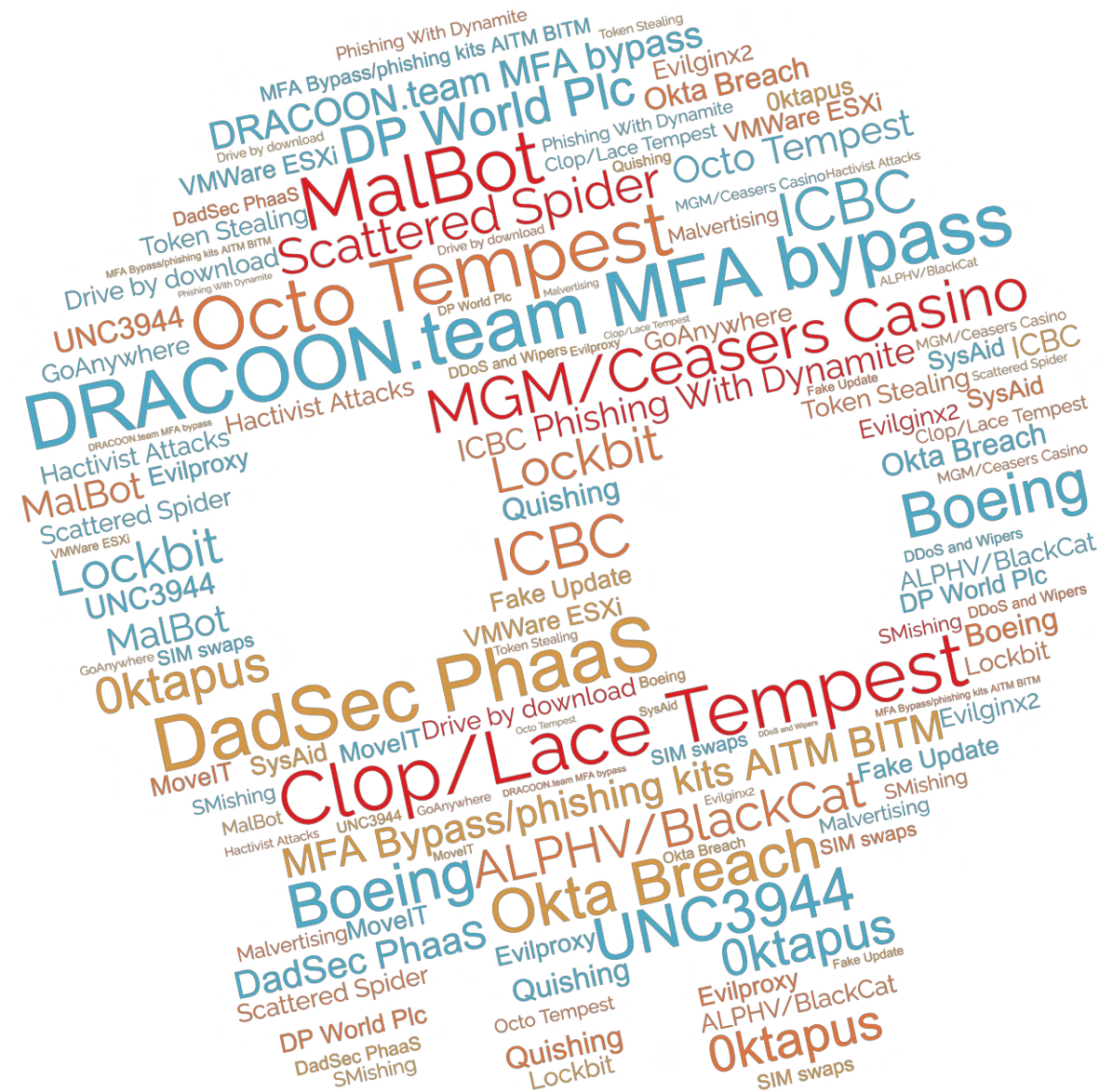
SPOTKANIE ONSITE

CYBEREKSPRESS

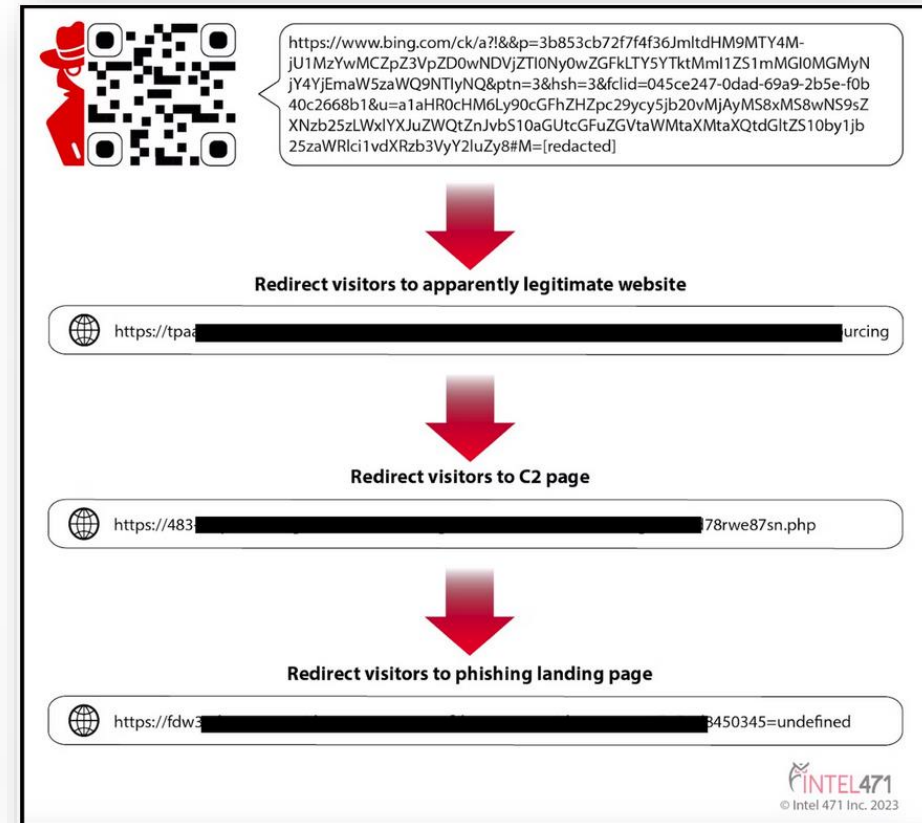
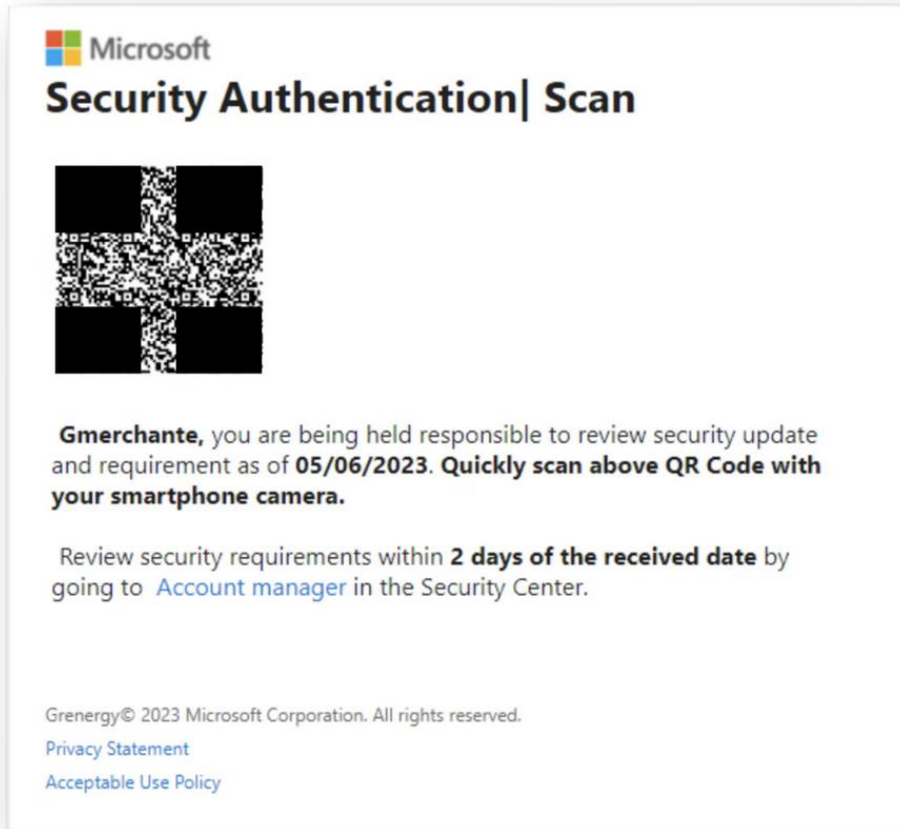


Marcin Święty
Chief Security Officer @ Relativity

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 ClOp 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

The screenshot shows the NIST NVD entry for CVE-2023-22515. It displays two severity metrics: CVSS 3.0 (10.0 CRITICAL) and CVSS 2.0 (9.8 CRITICAL). The CVSS 3.0 metrics are highlighted with a red box. Below the metrics, there is a section for 'References to Advisories, Solution' and a note about the NVD CVSS not matching the CNA CVSS. A tooltip is visible over the CVSS 3.0 metrics, showing the following details:

CVSS v3.0 Severity and Metrics:
Base Score: 10.0 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Impact Score: 6.0
Exploitability Score: 3.9
Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed
Confidentiality (C): High
Integrity (I): High
Availability (A): High

References to Advisories, Solution

By selecting these links, you will be leaving NIST webspace. We hope they may have information that would be of interest to you. No information is provided because other sites

Atlassian Confluence CVE-2023-22518

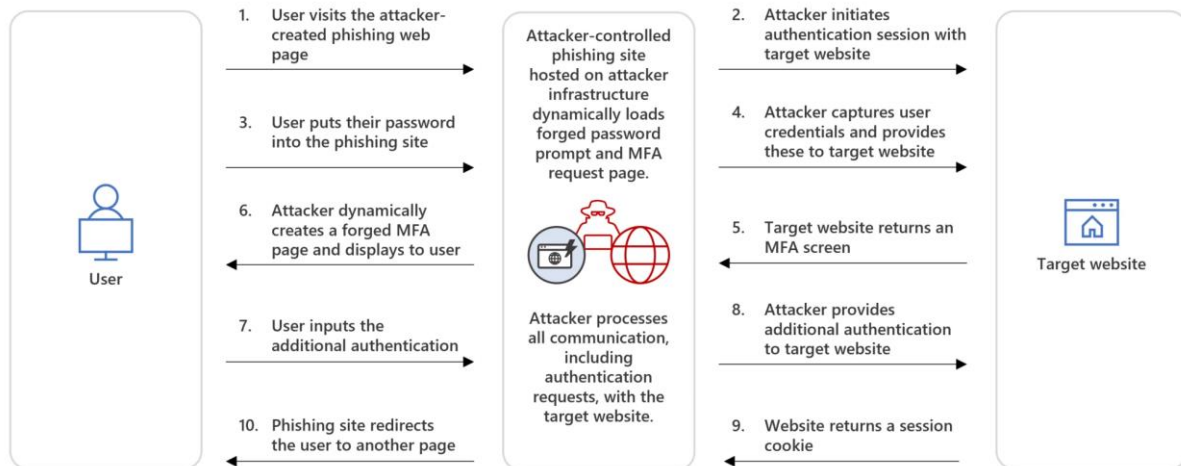
Improper Authorization Vulnerability In Confluence Data Center and Server

- 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 eksploicje
- 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)
 - Atlassian 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.”

MFA Bypass/phishing kits AITM BITM

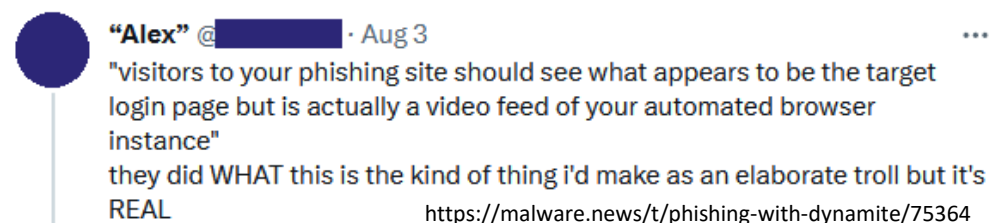
Ze wzrostem adopcji MFA, pojawił się wzrost i zapotrzebowanie na metody obejścia MFA (*nie działa na thin-client z cert-pinning, lub np. FIDO*)

- **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

 Octo Tempest: Evolving targeting, actions, outcomes, and monetization of attacks

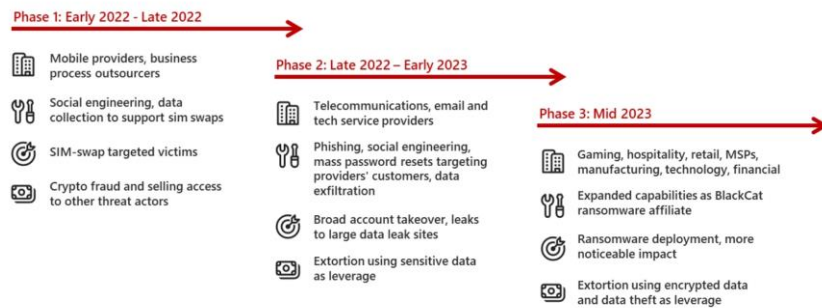


Figure 1. The evolution of Octo Tempest's targeting, actions, outcomes, and monetization

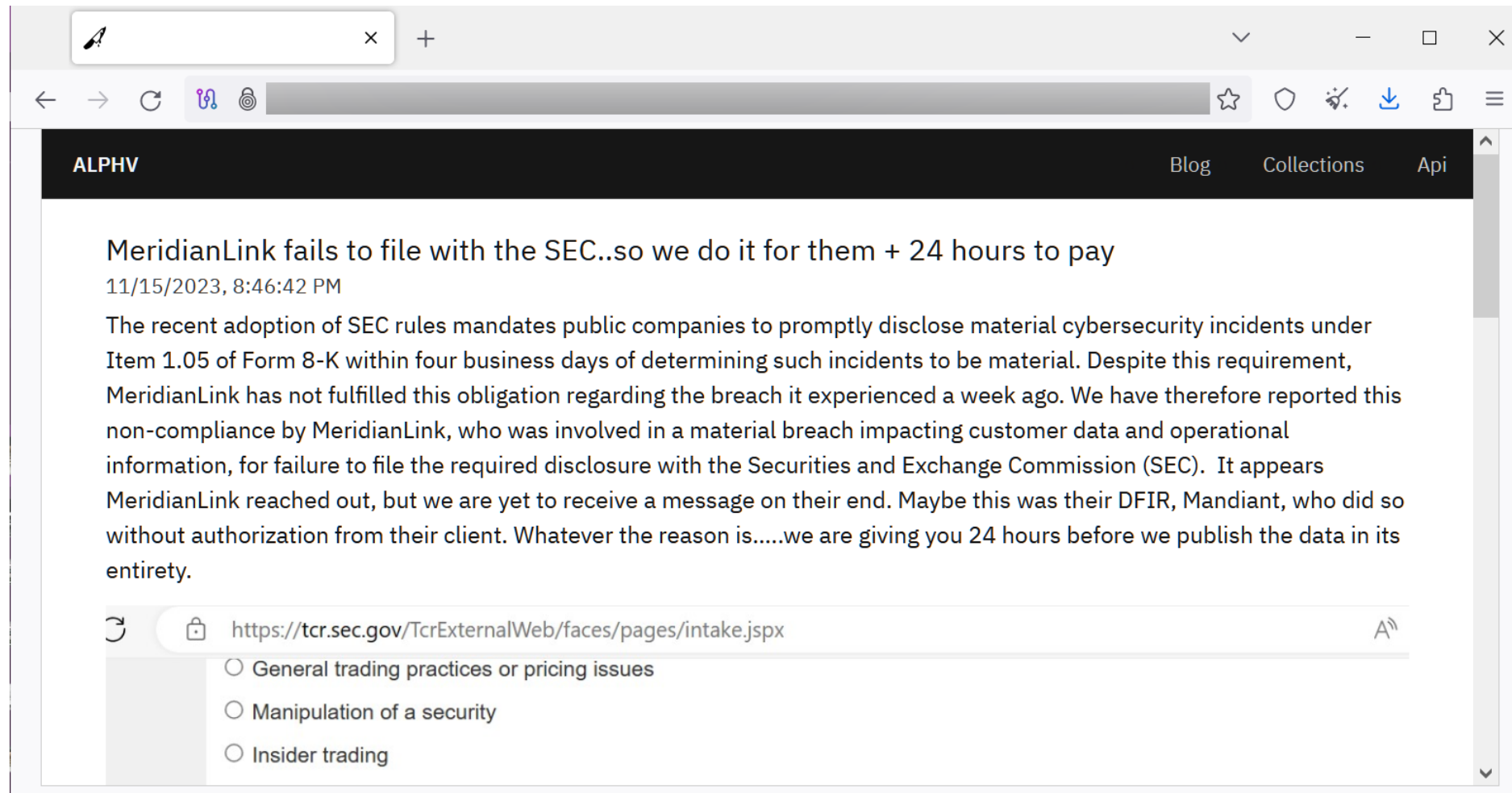
• LockBit

- 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 wyrzucić presję.

ALPHV/BlackCat oraz nowy pomysł na presje



The screenshot shows a web browser window with a single tab. The address bar contains the URL <https://tcr.sec.gov/TcrExternalWeb/faces/pages/intake.jspx>. The page content is from a blog titled "ALPHV" and features a post with the following text:

MeridianLink fails to file with the SEC..so we do it for them + 24 hours to pay
11/15/2023, 8:46:42 PM

The recent adoption of SEC rules mandates public companies to promptly disclose material cybersecurity incidents under Item 1.05 of Form 8-K within four business days of determining such incidents to be material. Despite this requirement, MeridianLink has not fulfilled this obligation regarding the breach it experienced a week ago. We have therefore reported this non-compliance by MeridianLink, who was involved in a material breach impacting customer data and operational information, for failure to file the required disclosure with the Securities and Exchange Commission (SEC). It appears MeridianLink reached out, but we are yet to receive a message on their end. Maybe this was their DFIR, Mandiant, who did so without authorization from their client. Whatever the reason is.....we are giving you 24 hours before we publish the data in its entirety.

Below the text, there is a dropdown menu with the following options:

- General trading practices or pricing issues
- Manipulation of a security
- Insider trading

Działo się dużo

