Storm-0978 attacks reveal financial and espionage motives

microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

July 11, 2023

By

Microsoft has identified a phishing campaign conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America. The campaign involved the abuse of CVE-2023-36884, which included a remote code execution vulnerability exploited before disclosure to Microsoft via Word documents, using lures related to the Ukrainian World Congress.

Storm-0978 (DEV-0978; also referred to as RomCom, the name of their backdoor, by other vendors) is a cybercriminal group based out of Russia, known to conduct opportunistic ransomware and extortion-only operations, as well as targeted credential-gathering campaigns likely in support of intelligence operations. Storm-0978 operates, develops, and distributes the RomCom backdoor. The actor also deploys the Underground ransomware,

which is closely related to the Industrial Spy ransomware first observed in the wild in May 2022. The actor's latest campaign detected in June 2023 involved abuse of CVE-2023-36884 to deliver a backdoor with similarities to RomCom.

Storm-0978 is known to target organizations with trojanized versions of popular legitimate software, leading to the installation of RomCom. Storm-0978's targeted operations have impacted government and military organizations primarily in Ukraine, as well as organizations in Europe and North America potentially involved in Ukrainian affairs. Identified ransomware attacks have impacted the telecommunications and finance industries, among others.

Microsoft 365 Defender detects multiple stages of Storm-0978 activity. Customers who use Microsoft Defender for Office 365 are protected from attachments that attempt to exploit CVE-2023-36884. In addition, customers who use Microsoft 365 Apps (Versions 2302 and later) are protected from exploitation of the vulnerability via Office. Organizations who cannot take advantage of these protections can set the *FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION* registry key to avoid exploitation. More mitigation recommendations are outlined in this blog.

Targeting

Storm-0978 has conducted phishing operations with lures related to Ukrainian political affairs and targeting military and government bodies primarily in Europe. Based on the post-compromise activity identified by Microsoft, Storm-0978 distributes backdoors to target organizations and may steal credentials to be used in later targeted operations.

The actor's ransomware activity, in contrast, has been largely opportunistic in nature and entirely separate from espionage-focused targets. Identified attacks have impacted the telecommunications and finance industries.

Tools and TTPs

Tools

Storm-0978 uses trojanized versions of popular, legitimate software, leading to the installation of RomCom, which Microsoft assesses is developed by Storm-0978. Observed examples of trojanized software include Adobe products, Advanced IP Scanner, Solarwinds Network Performance Monitor, Solarwinds Orion, KeePass, and Signal. To host the trojanized installers for delivery, Storm-0978 typically registers malicious domains mimicking the legitimate software (for example, the malicious domain *advanced-ip-scaner[.]com*).

In financially motivated attacks involving ransomware, Storm-0978 uses the Industrial Spy ransomware, a ransomware strain first observed in the wild in May 2022, and the Underground ransomware. The actor has also used the Trigona ransomware in at least one identified attack.

Additionally, based on attributed phishing activity, Storm-0978 has acquired exploits targeting zero-day vulnerabilities. Identified exploit activity includes abuse of CVE-2023-36884, including a remote code execution vulnerability exploited via Microsoft Word documents in June 2023, as well as abuse of vulnerabilities contributing to a security feature bypass.

Ransomware activity

In known ransomware intrusions, Storm-0978 has accessed credentials by dumping password hashes from the Security Account Manager (SAM) using the Windows registry. To access SAM, attackers must acquire SYSTEM-level privileges. Microsoft Defender for Endpoint detects this type of activity with alerts such as *Export of SAM registry hive*.

Storm-0978 has then used the Impacket framework's SMBExec and WMIExec functionalities for lateral movement.

Microsoft has linked Storm-0978 to previous management of the Industrial Spy ransomware market and crypter. However, since as early as July 2023, Storm-0978 began to use a ransomware variant called Underground, which contains significant code overlaps with the Industrial Spy ransomware.

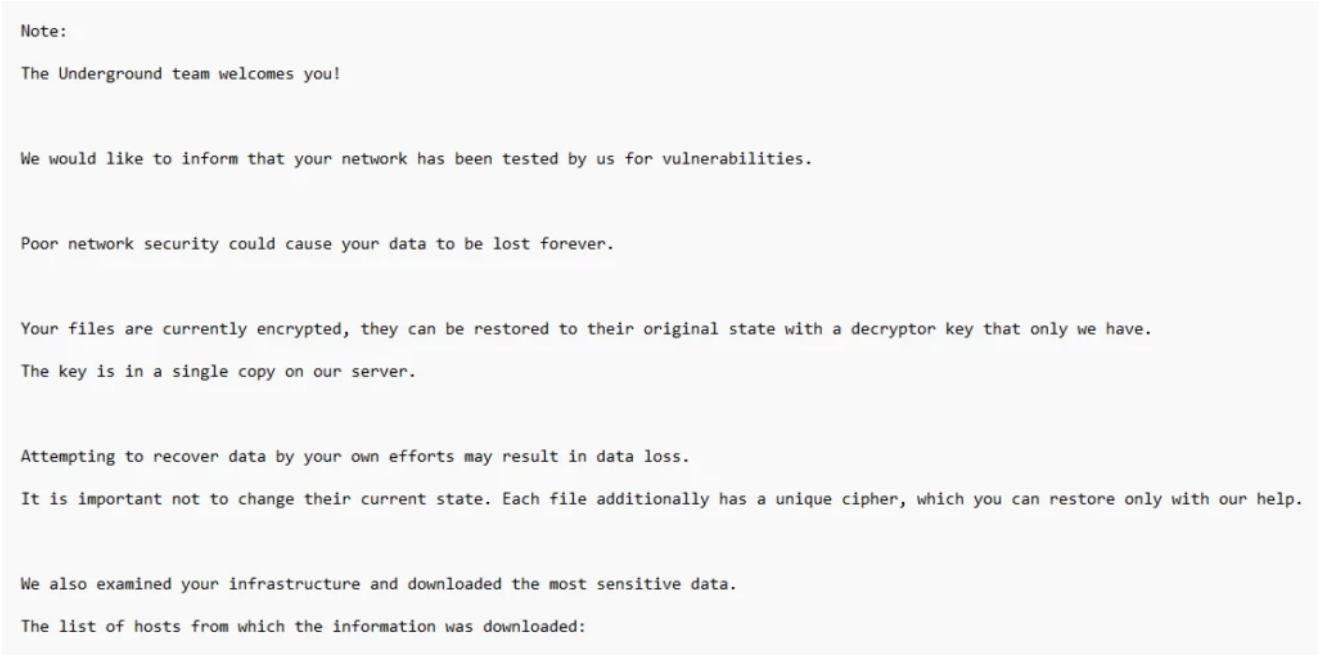


Figure 1. Storm-0978 ransom note references the "Underground team" and contains target-specific details of exfiltrated information

The code similarity between the two ransomware variants, as well as Storm-0978's previous involvement in Industrial Spy operations, may indicate that Underground is a rebranding of the Industrial Spy ransomware.

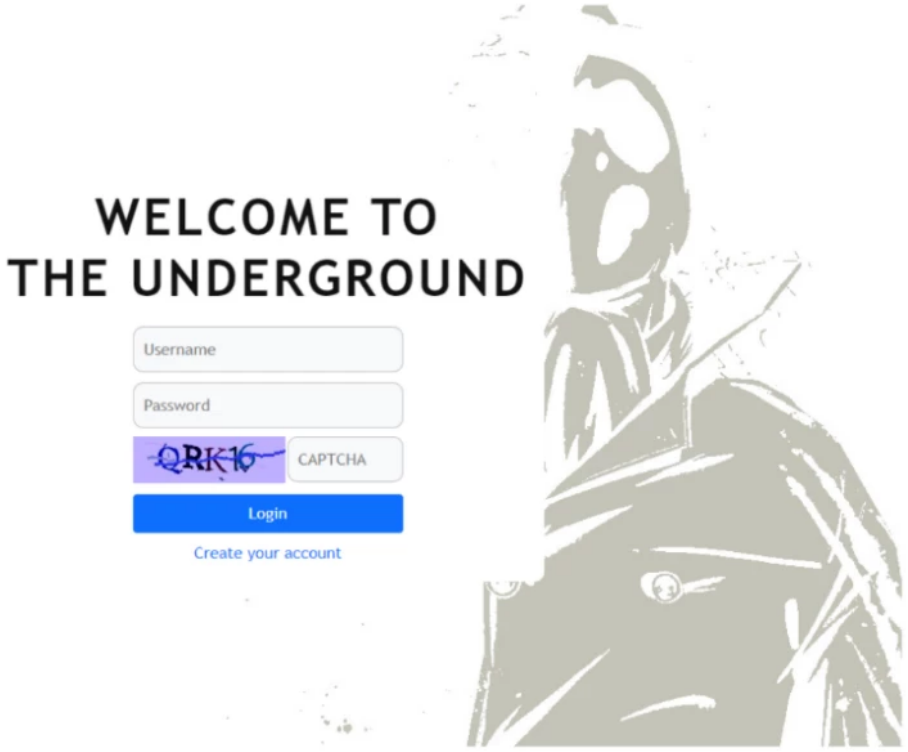


Figure 2. Underground ransomware .onion site

Espionage activity

Since late 2022, Microsoft has identified the following campaigns attributable to Storm-0978. Based on the post-compromise activity and the nature of the targets, these operations were likely driven by espionage-related motivations:

June 2023 – Storm-0978 conducted a phishing campaign containing a fake OneDrive loader to deliver a backdoor with similarities to RomCom. The phishing emails were directed to defense and government entities in Europe and North America, with lures related to the Ukrainian World Congress. These emails led to exploitation via the CVE-2023-36884 vulnerability.

Microsoft Defender for Office 365 detected Storm-0978's initial use of the exploit targeting CVE-2023-36884 in this phishing activity. Additional recommendations specific to this vulnerability are detailed below.

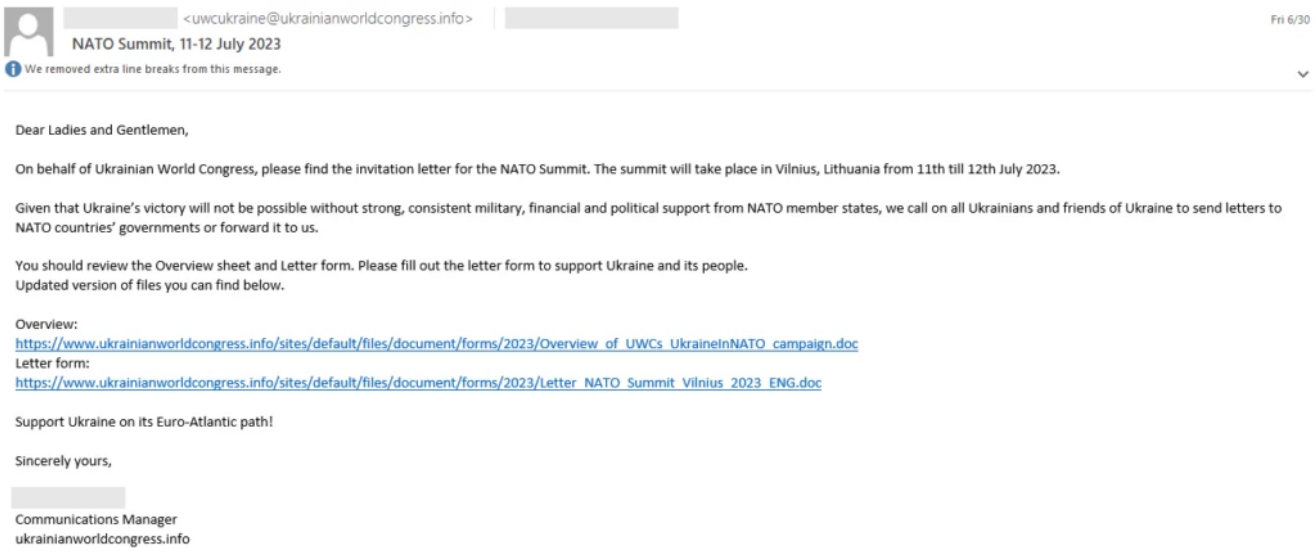
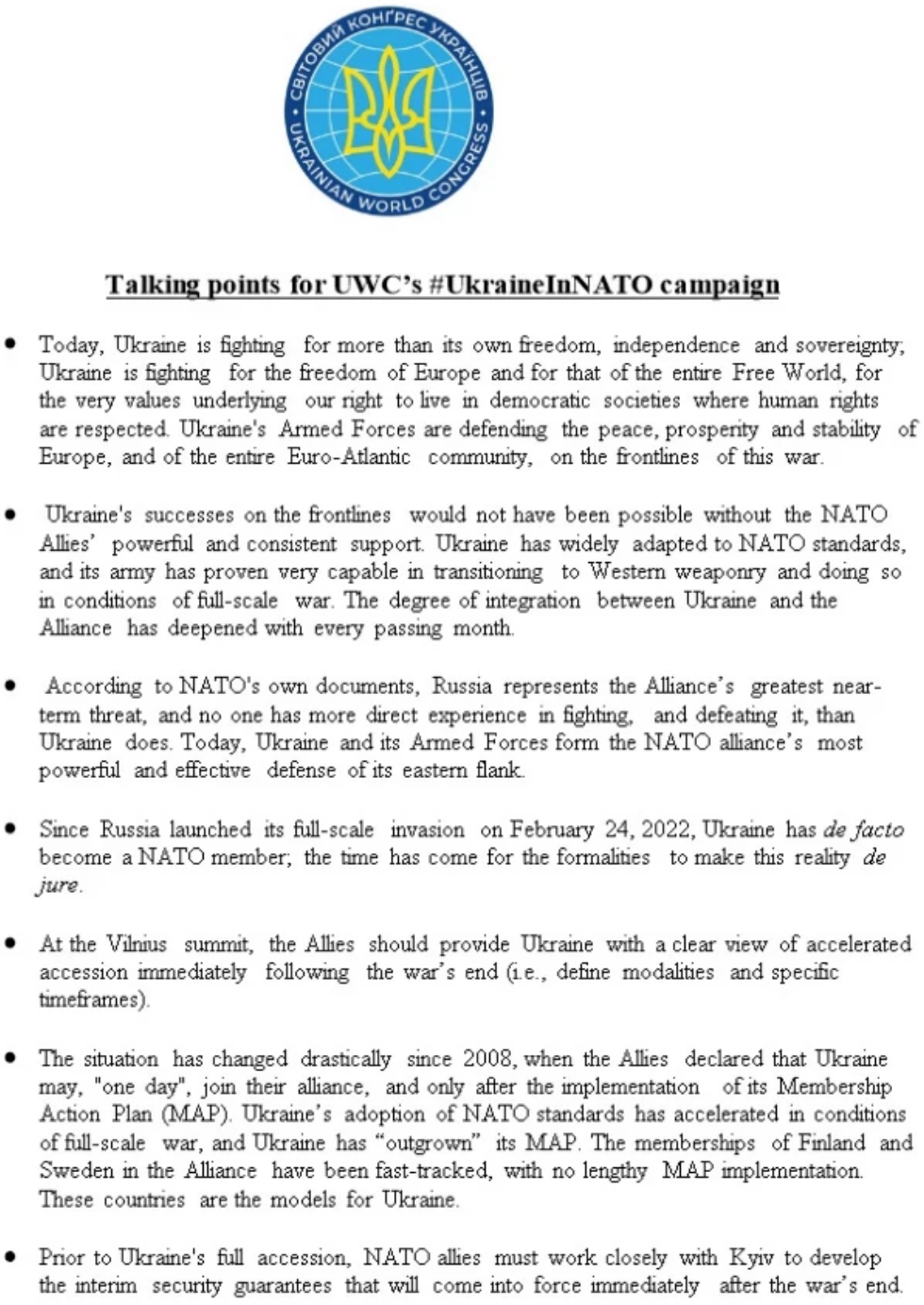


Figure 3. Storm-0978 email uses Ukrainian World Congress and NATO themes



Talking points for UWC's #UkraineInNATO campaign

- Today, Ukraine is fighting for more than its own freedom, independence and sovereignty; Ukraine is fighting for the freedom of Europe and for that of the entire Free World, for the very values underlying our right to live in democratic societies where human rights are respected. Ukraine's Armed Forces are defending the peace, prosperity and stability of Europe, and of the entire Euro-Atlantic community, on the frontlines of this war.
- Ukraine's successes on the frontlines would not have been possible without the NATO Allies' powerful and consistent support. Ukraine has widely adapted to NATO standards, and its army has proven very capable in transitioning to Western weaponry and doing so in conditions of full-scale war. The degree of integration between Ukraine and the Alliance has deepened with every passing month.
- According to NATO's own documents, Russia represents the Alliance's greatest near-term threat, and no one has more direct experience in fighting, and defeating it, than Ukraine does. Today, Ukraine and its Armed Forces form the NATO alliance's most powerful and effective defense of its eastern flank.
- Since Russia launched its full-scale invasion on February 24, 2022, Ukraine has *de facto* become a NATO member; the time has come for the formalities to make this reality *de jure*.
- At the Vilnius summit, the Allies should provide Ukraine with a clear view of accelerated accession immediately following the war's end (i.e., define modalities and specific timeframes).
- The situation has changed drastically since 2008, when the Allies declared that Ukraine may, "one day", join their alliance, and only after the implementation of its Membership Action Plan (MAP). Ukraine's adoption of NATO standards has accelerated in conditions of full-scale war, and Ukraine has "outgrown" its MAP. The memberships of Finland and Sweden in the Alliance have been fast-tracked, with no lengthy MAP implementation. These countries are the models for Ukraine.
- Prior to Ukraine's full accession, NATO allies must work closely with Kyiv to develop the interim security guarantees that will come into force immediately after the war's end.

Figure 4. Storm-0978 lure document with Ukrainian World Congress and NATO content

Notably, during this campaign, Microsoft identified concurrent, separate Storm-0978 ransomware activity against an unrelated target using the same initial payloads. The subsequent ransomware activity against a different victim profile further emphasizes the distinct motivations observed in Storm-0978 attacks.

December 2022 – According to CERT-UA, Storm-0978 compromised a Ukrainian Ministry of Defense email account to send phishing emails. Identified lure PDFs attached to emails contained links to a threat actor-controlled website hosting information-stealing malware.

October 2022 – Storm-0978 created fake installer websites mimicking legitimate software and used them in phishing campaigns. The actor targeted users at Ukrainian government and military organizations to deliver RomCom and likely to obtain credentials of high-value targets.

Recommendations

Microsoft recommends the following mitigations to reduce the impact of activity associated with Storm-0978's operations.

- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a majority of new and unknown variants.
- Run EDR in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Enable investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Use Microsoft Defender for Office 365 for enhanced phishing protection and coverage against new threats and polymorphic variants. Defender for Office 365 customers should ensure that Safe Attachments and Safe Links protection is enabled for users with Zero-hour Auto Purge (ZAP) to remove emails when a URL gets weaponized post-delivery.
- Microsoft 365 Defender customers can turn on attack surface reduction rules to prevent common attack techniques used in ransomware attacks:
    - Block process creations originating from PsExec and WMI commands – Some organizations might experience compatibility issues with this rule on certain server systems but should deploy it to other systems to prevent lateral movement originating from PsExec and WMI, including Impacket's WMIexec.
    - Block executable files from running unless they meet a prevalence, age, or trusted list criterion
    - Use advanced protection against ransomware
    - Block all Office applications from creating child processes

CVE-2023-36884 specific recommendations

- Customers who use Microsoft Defender for Office 365 are protected from attachments that attempt to exploit CVE-2023-36884.
- In addition, customers who use Microsoft 365 Apps (Versions 2302 and later) are protected from exploitation of the vulnerability via Office.

- In current attack chains, the use of the Block all Office applications from creating child processes attack surface reduction rule prevents the vulnerability from being exploited
- Organizations who cannot take advantage of these protections can set the *FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION* registry key to avoid exploitation.
    - No OS restart is required, but restarting the applications that have had the registry key added for them is recommended in case the value was already queried and is cached.
    - Please note that while these registry settings would mitigate exploitation of this issue, it could affect regular functionality for certain use cases related to these applications. For this reason, we suggest testing. To disable the mitigation, delete the registry key or set it to “0”.

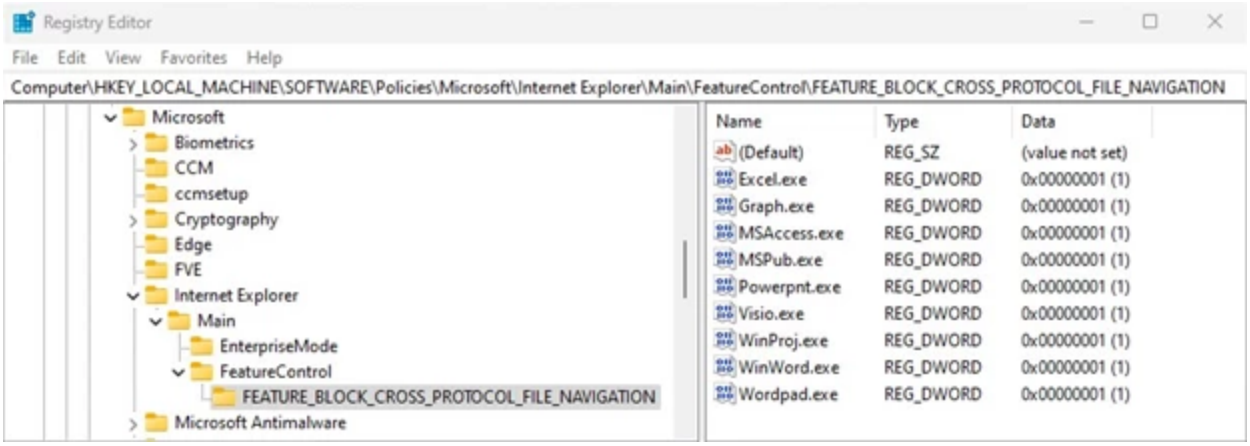


Figure 5. Screenshot of settings for the FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION key to prevent exploitation of CVE-2023-36884

Detection details

Microsoft Defender for Office 365

Microsoft Defender for Office 365 customers are protected from attachments that attempt to exploit CVE-2023-36884.

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects post-compromise components of this threat as the following malware:

Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate threat activity on your network:

Emerging threat activity group Storm-0978 detected

Microsoft Sentinel

Microsoft Sentinel also has detection and threat hunting content that customers can use to detect the post exploitation activity detailed in this blog in addition to Microsoft 365 Defender detections list above.

The following content can be used to identify activity described in this blog post:

References

Further reading

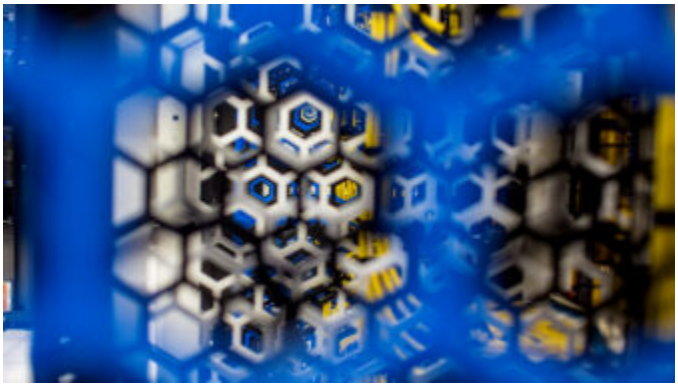
For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on Twitter at https://twitter.com/MsftSecIntel.

Related Posts

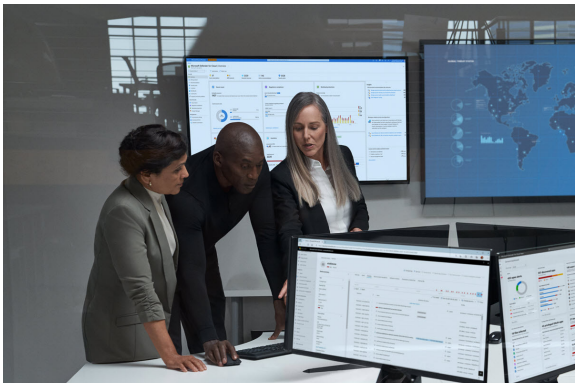
Microsoft shifts to a new threat actor naming taxonomy

Microsoft is excited to announce that we are shifting to a new threat actor naming taxonomy aligned to the theme of weather. The complexity, scale, and volume of threats is increasing, driving the need to reimagine not only how Microsoft talks about threats but also how we enable customers to understand those threats quickly and with clarity.



Cadet Blizzard emerges as a novel and distinct Russian threat actor

Microsoft attributes several campaigns to a distinct Russian state-sponsored threat actor tracked as Cadet Blizzard (DEV-0586), including the WhisperGate destructive attack, Ukrainian website defacements, and the hack-and-leak front “Free Civilian”.



Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets

Today, Microsoft is reporting on a distinct subset of Mint Sandstorm (formerly known as PHOSPHORUS), an Iranian threat actor that specializes in hacking into and stealing sensitive information from high-value targets. This subset is technically and operationally mature, capable of developing bespoke tooling and quickly weaponizing recently disclosed vulnerabilities.