HC3: Threat Actor Profile

June 6, 2024 TLP:CLEAR Report: 202406061500

Threat Actor Profile: Midnight Blizzard

Executive Summary

In January 2024, security teams for two American multinational technology companies detected a nation-state attack on their corporate e-mail systems. The threat actor attributed to the cyberattacks was identified as Midnight Blizzard, also known as APT29, a Russian threat group publicly linked to the Foreign Intelligence Service of the Russian Federation. Tracing their longstanding and dedicated espionage of foreign interests as far back as early 2008, this group is known to target multiple industries primarily across the United States and Europe. An overview of the threat group can be found in a recent HC3 Threat Briefing on Russian Threat Actors, amongst other HC3 products detailed later. What follows is an examination of Midnight Blizzard; a timeline of recent threat actor activity; its impact to the HPH sector; common tactics, techniques, and procedures; exploited vulnerabilities, indicators of compromise, MITRE ATT&CK methodologies, and recommended defense and mitigations against the group.

Overview

Midnight Blizzard At A Glance	
Names Utilized	APT29, ATK7, Blue Bravo, Blue Kitsune, Cloaked Ursa, Cozer, CozyBear, CozyCar, CozyDuke, Dark Halo, The Dukes, EuroAPT, Grizzly Steppe, G0016, Group 100, Hammer Toss, IRON HEMLOCK, IRON RITUAL, ITG11, Minidionis, NOBELIUM, NobleBarron, Office Monkey , SeaDuke, StellarParticle, TA421, UNC2452, UNC3524, YTTRIUM
Threat Type	Advanced Persistent Threat (APT) actor
Tactics Utilized	Phishing, spear-phishing, custom malware, access via service and dormant accounts and password spray, cloud-based token authentication, enrolling new devices to the cloud, residential proxies.
Malware Toolsets	CloudDuke, Cobalt Strike Beacon, CosmicDuke, CozyDuke, GeminiDuke, Hammertoss, LiteDuke, MiniDuke, OnionDuke, PinchDuke, PolyglotDuke, RegDukeand SeaDuke
Motivations	Espionage and intelligence gathering
Target Sectors	Governments and government subcontractors, political and non-governmental organizations, research firms, and critical industries such as aviation, energy, healthcare, education, finance, law enforcement, military, and technology principally in the United States and Europe.
Target Countries	Belgium, Brazil, China, Georgia, India, Japan, Kazakhstan, Mexico, New Zealand, the Netherlands, Norway, Portugal, Romania, South Korea, Turkey, Ukraine, and the United States

Image Source: CrowdStrike

Midnight Blizzard is a Russia state-nexus adversary, assessed as likely to be acting on behalf of the Foreign Intelligence Service of the Russian Federation (also known as SVR or Служба внешней разведки Российской Федерации, abbreviated to СВР РФ). The initial emergence of the threat group's operations occurred in 2008, when the first MiniDuke malware samples were compiled according to cybersecurity research company Kaspersky. Today, they are a well-resourced, highly dedicated and organized cyber-espionage group that seeks to collect intelligence in support of foreign and security policy goals.

The threat group's motivations can be evaluated by observing the strategies that they apply within the context of their campaigns. The group is known for its interest in secret geopolitical data that would be advantageous to the Russian state. Midnight Blizzard operates within the context of the SVR, an

intelligence agency that has disruptive capabilities to conduct advanced cyber-espionage operations. In light of the recent corporate e-mail breach on two American multinational technology companies, one cybersecurity reseacher highlighted the group's counterintelligence goals – specifically, that Midnight Blizzard is interested in learning what company executives know about their group and methods.

Timeline of Threat Actor Activity

Year	Incident
2014	Midnight Blizzard carried out the 'Office Monkeys' campaign targeting a Washington D.C.-based private research institute.
2015	Midnight Blizzard gained initial access to the Pentagon's network via phishing and introduced the 'Hammertoss' technique to use dummy Twitter accounts for command-and-control (C2) communication.
2016	In a campaign known as 'GRIZZLY STEPPE,' Midnight Blizzard breached the Democratic National Committee's servers close to the U.S. election via a phishing campaign, directing victims to change their passwords using a spoofed website.
2017	Targeted the Norwegian government and several Dutch ministries.
2018	The WellMess malware was observed in attacks against Japanese firms in 2018; however, it was not linked to a specific threat actor at the time. WellMess was linked to Russia's APT29 in 2020, when the U.S., U.K., and Canada stated Russian hackers used it in attacks against academic and pharmaceutical research institutes involved in developing the COVID-19 vaccine.
2019	Compromised three European Union (EU) National Affairs ministries and a Washington D.C.-based embassy of an EU nation state.
2020	Conducted vulnerability scanning of public-facing IP addresses to compromise COVID-19 vaccine developers in Canada, the U.S., and the U.K. Distributed SUNBURST malware, attacking SolarWinds Orion software to drop a remote access trojan (RAT) that impacted many global organizations.
2022	Crowdstrike shared a blog about a campaign called StellarParticle linked to Cozy Bear. The campaign, conducted with GoldMax and TrailBlazer malware, revealed that since mid-2019, APT29 has used an MFA bypass to access Office 365 accounts with stolen cookies. A lure document that allegedly belonged to APT29 was found, which contained a malicious script and appeared to have been created by the Embassy of Israel.
2023	Midnight Blizzard conducts targeted social engineering operations via Microsoft Teams.
2024	Two American multinational technology companies detected a nation-state attack on their corporate e-mail systems, and both attributed it to Midnight Blizzard.

Impact to HPH Sector

Several Russian APTs and cybercriminal groups (i.e. LockBit, Royal, Black Basta, ALPHV) regularly attack the Healthcare and Public Health (HPH) sector. While Midnight Blizzard is not impartial in its targeting of multiple sectors and industries, its focus on the HPH sector has seen significant consequences in the past. Like APT28, another threat group linked to Russian security services, Midnight Blizzard has targeted foreign pharmaceutical companies and clinical researchers in pursuit of COVID-19 intellectual property, including vaccine and treatment research. In the HPH sector, medical records about innovative medical procedures, diagnosis, prescriptions, etc., are all information that could be used by sophisticated threat actors for targeting a specific person or organization.

Throughout 2020, Midnight Blizzard targeted various organizations involved in COVID-19 vaccine development in Australia, Canada, the United States, and the United Kingdom. The threat group, which

uses a variety of tools and techniques such as spear-phishing, used custom malware known as 'WellMess' and 'WellMail' to target a number of organizations globally, including those organizations involved with COVID-19 vaccine development. WellMess and WellMail had not previously been publicly associated to Midnight Blizzard, says the NCSC.

In a 2023 malware campaign, cyber attackers exploited Microsoft Teams by posing as human resources representatives. Microsoft Teams is a staple in the HPH sector, making it a prime target for cybercriminals. One cybersecurity research company noted that Midnight Blizzard utilized this phishing approach, demonstrating that these kind of social engineering attacks are still successful.

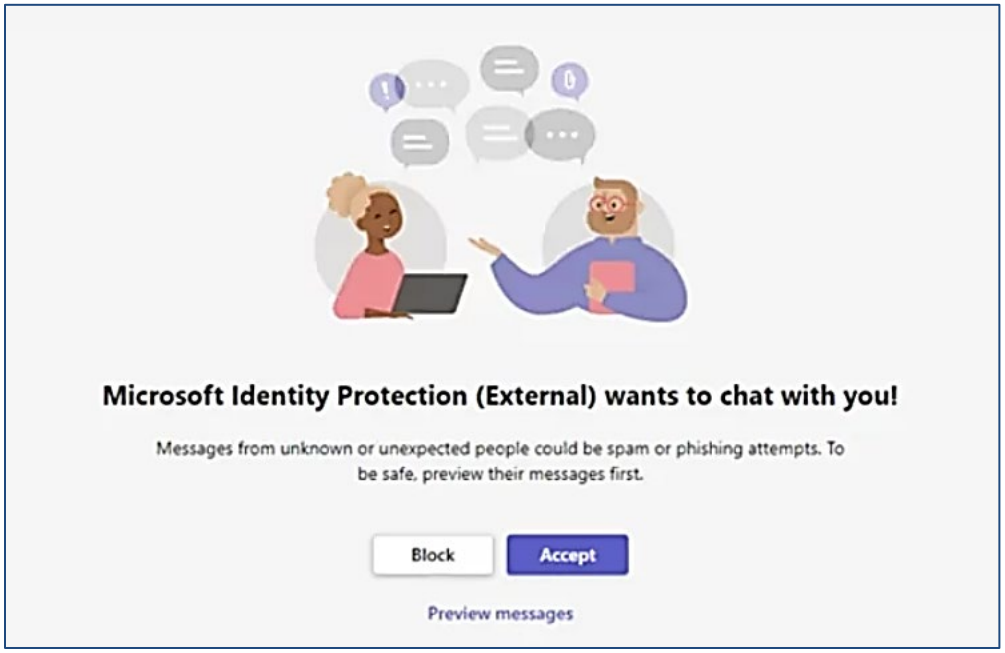

Figure 1: Microsoft Teams message request from a Midnight Blizzard social engineering attack. *(Source: SOCRadar)*

Common Tactics, Techniques, and Procedures (TTPs)

Signs of a Midnight Blizzard attack may be hard to spot due to the group's diverse offensive tactics. The group has traditionally used phishing and highly-targeted spear-phishing attacks in combination with sophisticated custom malware to exploit newly disclosed vulnerabilities, and even zero-day vulnerabilities, in popular software applications. As an asset of the Russian Intelligence Services, Midnight Blizzard is well-funded with deep political connections that may provide valuable information for orchestrating highly-targeted attacks.

Associated Malware

Custom Malware	Decription
CloudDuke	CloudDuke is a malware toolset known to consist of, at least, a downloader, a loader, and two backdoor variants, including MiniDionis/Cloudlook. The CloudDuke downloader will download and execute additional malware from a preconfigured location. CloudDuke was in use primarily during the summer of 2015.
Cobalt Strike Beacon	In the November 2018 phishing campaign linked to Midnight Blizzard, the threat actor group utilized Cobalt Strike Beacon instead of any bespoke malware or toolkits. The Beacon payload was configured with a modified variation of the publicly available "Pandora" Malleable C2 Profile and used the C2 domain – pandorasong[.]com.

HC3: Threat Actor Profile

June 6, 2024 TLP:CLEAR Report: 202406061500

Custom Malware	Description
CosmicDuke	The CosmicDuke toolkit is an information stealer malware. It is augmented by a variety of components that the toolkit operators may include with the main component to provide additional functionalities, such as multiple methods of establishing persistence, as well as modules that attempt to exploit privilege escalation vulnerabilities. CosmicDuke was utilized from January 2010 to the summer of 2015, and was observed targeting a wide range of organizations, including those in the energy and telecommunications sectors, and governments and militaries.
CozyDuke	CozyDuke is a modular malware platform formed around a core backdoor component. It can be instructed by the C2 server to download and execute arbitrary modules, providing a vast array of functionalities. In addition to modules, CozyDuke can also be instructed to download and execute other, independent executables. In some observed cases, these executables were self-extracting archive files containing common hacking tools, such as PSExec and Mimikatz, combined with script files that execute these tools. CozyDuke was utilized by Midnight Blizzard from January 2010 to the spring of 2015.
GeminiDuke	The GeminiDuke toolset consists of a core information stealer, a loader and multiple persistence-related components. Unlike CosmicDuke and PinchDuke, it primarily collects information on the target system's configuration. GeminiDuke was actively utilized from January 2009 to December 2012.
HammerDuke/ Hammertoss/ tDiscoverer	Midnight Blizzard likely used Hammertoss as a backup for their two primary backdoors to execute commands and maintain access in the case of the group's principal toolset being discovered. Hammertoss was in use from at least January 2015 to July 2015.
LiteDuke	A third-stage information stealer that uses multiple layers of encryption for obfuscation and multiple techniques for persistence, including Windows Registry keys, PowerShell, and Windows Management Instrumentation.
MiniDuke	A second-stage downloader developed in x86 assembly rather than a compiled programming language, which uses a domain-generating algorithm to dynamically locate C2 servers
OnionDuke	The OnionDuke toolkit includes at least a dropper, a loader, an information stealer trojan and multiple modular variants. OnionDuke was the only tool used by Midnight Blizzard that is not spread using phishing, and instead was spread via a malicious Tor exit node. OnionDuke was observed from February 2013 to the spring of 2015.
PinchDuke	This was the first toolkit widely attributed to Midnight Blizzard. The toolkit consists of multiple loaders and a core information stealer trojan. The malware gathers system configuration information, steals user credentials, and collects user files from the compromised host, transferring these via HTTP(S) to a C2 server. PinchDuke was reported as being used from November 2008 to the summer of 2010, and was observed in attacks against Chechnya, Turkey, Georgia, and several former Soviet states before evolving to the CosmicDuke toolkit in 2010.
PolyglotDuke	A second-stage downloader malware capable of using steganography and Twitter, Reddit, and Imgur websites to fetch C2 server locations.
RegDuke	A first-stage malware written in .NET that can download secondary malware using DropBox as its C2 server and maintain persistence by injecting itself into the winword.exe binary.
SeaDuke	SeaDuke is a backdoor malware that focuses on executing commands retrieved from its C2 server, such as uploading and downloading files, executing system commands, and evaluating additional Python code. SeaDuke was active from October 2014 to May 2016, and was observed during the DNC attack by Midnight Blizzard in 2015.

SVR TTPs Observed in CY 2023

On February 26, 2024, the Cybersecurity & Infrastructure Security Agency (CISA), the British National Cyber Security Centre (NCSC), and other international partners released a cybersecurity advisory on the recent TTPs of Midnight Blizzard within the last 12 months. The following describes in detail how SVR actors are adapting to continue their cyber operations for intelligence gain.

Access via Service and Dormant Accounts

Previous SVR campaigns reveal the actors have successfully used brute forcing [T1110] and password

spraying to access service accounts. This type of account is typically used to run and manage applications and services. There is no human user behind them, so they cannot be easily protected with multi-factor authentication (MFA), making these accounts more susceptible to a successful compromise. Service accounts are often also highly privileged depending on which applications and services they are responsible for managing. Gaining access to these accounts provides threat actors with privileged initial access to a network to launch further operations.

SVR campaigns have also targeted dormant accounts belonging to users who no longer work at a victim organization, but whose accounts remain on the system [T1078.004].

Following an enforced password reset for all users during an incident, SVR actors have also been observed logging into inactive accounts and following instructions to reset the password. This has allowed the actor to regain access following incident response eviction activities.

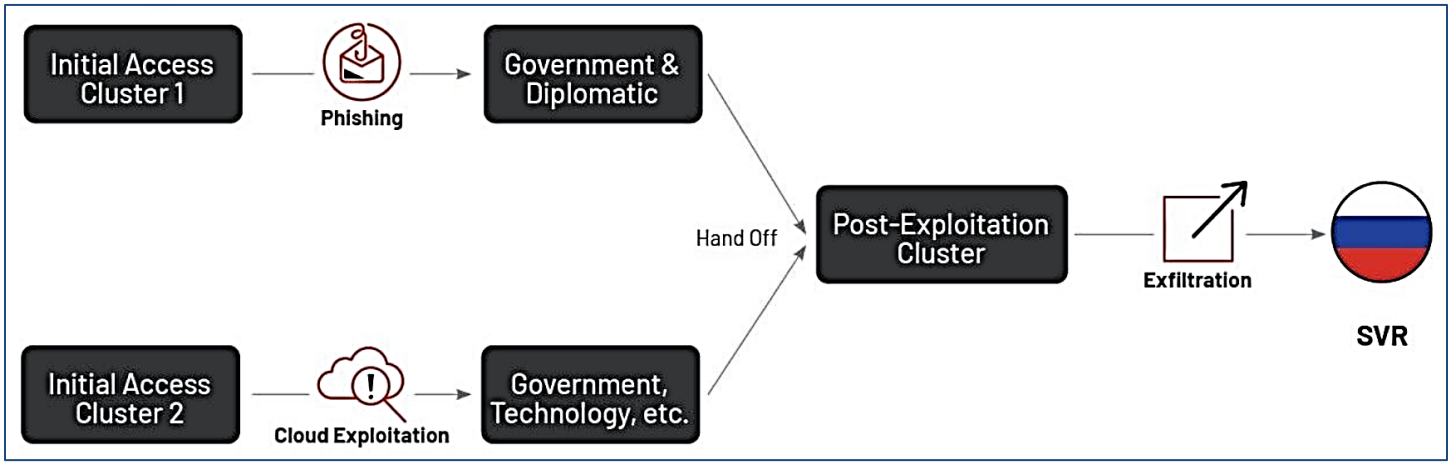

Figure 2: Midnight Blizzard's Distinct Initial Access Clusters. *(Source: Mandiant)*

Cloud-Based Token Authentication

Account access is typically authenticated by either username and password credentials, or system-issued access tokens. The NCSC and partners have observed SVR actors using tokens to access their victims' accounts without needing a password [T1528].

The default validity time of system-issued tokens varies dependent on the system; however, cloud platforms should allow administrators to adjust the validity time as appropriate for their users. More information can be found on this in the mitigations section of this advisory.

Enrolling New Devices to the Cloud

On multiple occasions, the SVR have successfully bypassed password authentication on personal accounts using password spraying and credential reuse. SVR actors have also then bypassed MFA through a technique known as "MFA bombing" or "MFA fatigue," in which the actors repeatedly push MFA requests to a victim's device until the victim accepts the notification [T1621].

Once an actor has bypassed these systems to gain access to the cloud environment, SVR actors have been observed registering their own device as a new device on the cloud tenant [T1098.005]. If device validation rules are not set up, SVR actors can successfully register their own device and gain access to

the network. By configuring the network with device enrollment policies, there have been instances where these measures have defended against SVR actors and denied them access to the cloud tenant.

Residential Proxies

As network-level defenses improve detection of suspicious activity, SVR actors have looked at other ways to stay covert on the internet. A TTP associated with this actor is the use of residential proxies [T1090.002]. Residential proxies typically make traffic appear to originate from IP addresses within internet service provider (ISP) ranges used for residential broadband customers, and hide the true source. This can make it harder to distinguish malicious connections from typical users. This reduces the effectiveness of network defenses that use IP addresses as indicators of compromise, and so it is important to consider a variety of information sources, such as application and host-based logging, for detecting suspicious activity.

Exploited Vulnerabilities

Exploited Vulnerabilities (Source: Quorum Cyber)					
CVE-ID	Severity	CWE	Description	Exploit Type	Patch
CVE-2018-13379 (Fortinet FortiOS)	9.8 Critical	CWE-22: Improper Limitation of a Pathname to a Restricted Directory	An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") under SSL VPN web portal allows an unauthenticated threat actor to download system files via special crafted HTTP resource requests.	WebApp	Patch
CVE-2019-9670 (Zimbra Collaboraton Suite)	9.8 Critical	CWE-611: Improper Restriction of XML External Entity Reference	An XML External Entity injection (XXE) vulnerability in the mailboxed component in Synacor Zimbra Collaboration Suite.	Remote Code Execution	Patch
CVE-2019-11510	10.00 Critical	CWE-22: Improper Limitation of a Pathname to a Restricted Directory	Successful exploitation of this vulnerability allows an unauthenticated remote threat actor to send a specially crafted URI to perform an arbitrary file reading vulnerability.	WebApp	Patch
CVE-2019-19781 (Citrix ADC Network Gateway)	9.8 Critical	CWE-22: Improper Limitation of a Pathname to a Restricted Directory	An issue was discovered in Citrix Application Delivery Controlled (ADC) that allows Directory Traversal.	Remote Code Execution	Patch
CVE-2020-4006	9.1 Critical	CWE-78: Improper Neutralization of Special Elements used in an OS Command	A command injection vulnerability.	Unknown	Patch

Indicators of Compromise (IoCs)

The following are IoCs compiled from various cybersecurity research organizations.

Quorum Cyber IoCs			
Midnight Blizzard Associated IP Addresses			
193[.]36[.]119[.]162	91[.]132[.]139[.]195	141[.]255[.]164[.]11	193[.]36[.]116[.]119
185[.]99[.]133[.]226	5[.]252[.]177[.]21	111[.]90[.]150[.]140	23[.]106[.]123[.]15
111[.]90[.]147[.]248	141[.]255[.]164[.]40	91[.]234[.]254[.]144	31[.]42[.]177[.]78
141[.]255[.]164[.]36	193[.]239[.]84[.]199	193[.]36[.]119[.]184	185[.]66[.]91[.]180
107[.]152[.]35[.]77	111[.]90[.]151[.]120	13[.]57[.]184[.]217	13[.]59[.]205[.]66

HC3: Threat Actor Profile

June 6, 2024 TLP:CLEAR Report: 202406061500

Midnight Blizzard Associated Domains
avsvmcloud[.]com
literaturaelsalvador[.]com
signitivelogics[.]com
totalmassasje[.]no
2bdo5s70oc51vu3de3bvrq60eiw[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
2e7hv525mpn9uiljt3ev[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
7sbvaemscs0mc925tb99[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8cngei63kcpgho7kern0le2ve2sn0te2[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
8tvp0990935eitt5hjvcbmv[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
act4fk13agv8olsou30e2st[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
appsync-api[.]us-east-1[.]avsvmcloud[.]com
athe4f602s6ce101uj21[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
gq1h856599gqh538acqn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
hvpgv9psvq02ffo77et[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ihvpgv9psvq02ffo77et[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jbq3rh7rjdghmmcxco0ge2sd[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
k5kcubuassl3alrf7gm3[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
ld3iu5dr2341o83hhr5p[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
mhdosoksaccf9sni9icp[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
Midnight Blizzard Associated File Hashes (SHA256)
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
1cffaf3be725d1514c87c328ca578d5df1a86ea3b488e9586f9db89d992da5c4
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
381a3c6c7e119f58dfde6f03a9890353a20badfa1bfa7c38ede62c6b0692103c
Midnight Blizzard Associated File Hashes (SHA1)
1acf3108bf1e376c8848fbb25dc87424f2c2a39c
1fb12e923bdb71a1f34e98576b780ab2840ba22e
2f1a5a7411d015d01aaee4535835400191645023
395da6d4f3c890295f7584132ea73d759bd9d094
72e5fc82b932c5395d06fd2a655a280cf10ac9aa
75af292f34789a1c782ea36c7127bf6106f595e8
76640508b1e7759e548771a5359eaed353bf1eec
9858d5cb2a6614be3c48e33911bf9f7978b441bf
Midnight Blizzard Associated File Hashes (MD5)
1c3b8ae594cb4ce24c2680b47cebf808
2c4a910a1299cdae2a4e55988a2f102e
56ceb6d0011d87b6e4d7023d7ef85676
731d724e8859ef063c03a8b1ab7f81ec
846e27a652a5e1bfbd0ddd38a16dc865
9466c865f7498a35e4e1a8f48ef1dffd

SOCRadar IoCs
msftprotection.onmicrosoft[.]com
identityVerification.onmicrosoft[.]com
accountsVerification.onmicrosoft[.]com

HC3: Threat Actor Profile

June 6, 2024 TLP:CLEAR Report: 202406061500

SOCRadar IoCs
azuresecuritycenter.onmicrosoft[.]com
teamsprotection.onmicrosoft[.]com

MITRE ATT&CK Framework Methodologies

MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques designed for threat hunters, defenders, and red teams to help classify attacks, identify attack attribution and objectives, and assess an organization's risk. While not exclusive, below are some sample MITRE ATT&CK techniques from various cybersecurity reseach companies that have been annotated as having been used by this threat actor. A full list of the MITRE ATT&CK techniques utilized by Midnight Blizzard can be found here.

MITRE ATT&CK Methodologies (Source: Avertium)			
Initial Access	Execution	Defense Evasion	Discovery
T1566: Phishing	T1102: Web Service	T1070: Indicator Removal of Host	T1057: Process Discovery
	T1055: Process Injection	T1176: Browser Extensions	
		T1574: Hijack Execution Flow	
		T1134: Access Token Manipulation	

MITRE ATT&CK Methodologies (Source: CISA)			
Tactic	ID	Technique	Procedure
Credential Access	T1110	Brute Force	The SVR use password spraying and brute forcing as an initial infection vector.
Initial Access	T1078.004	Valid Accounts: Cloud Accounts	The SVR use compromised credentials to gain access to accounts for cloud services, including system and dormant accounts.
Credential Access	T1528	Steal Application Access Token	The SVR use stolen access tokens to login to accounts without the need for passwords.
Credential Access	T1621	Multi-Factor Authentication Request Generation	The SVR repeatedly push MFA requests to a victim's device until the victim accepts the notification, providing SVR access to the account.
Command and Control	T1090.002	Proxy: External Proxy	The SVR use open proxies in residential IP ranges to blend in with expected IP address pools in access logs.
Persistence	T1098.005	Account Manipulation: Device Registration	The SVR attempt to register their own device on the cloud tenant after acquiring access to accounts.

MITRE ATT&CK Methodologies (Source: Mandiant)		
ATT&CK Tactic Category	Technique	Sub-Technique
Resource Development	Acquire Infrastructure (T1583)	Virtual Private Server (T1583.003)
	Compromise Infrastructure (T1584)	
	Stage Capabilities (T1608)	Link Target (T1608.005)
	Obtain Capabilities (T1588)	Digital Certificates (T1588.004)
Initial Access	Phishing (T1566)	Spearphishing Attachment (T1566.001)
		Spearphishing Link (T1566.002)
	External Remote Services (T1133)	
Execution	User Execution (T1204)	Malicious Link (T1204.001)
		Malicious File (T1204.002)
	Command and Scripting Interpreter (T1059)	PowerShell (T1059.001)
		Windows Command Shell (T1059.003)
		JavaScript (T1059.007)

HC3: Threat Actor Profile

June 6, 2024 TLP:CLEAR Report: 202406061500

	Scheduled Task/Job (T1053)	Scheduled Task (T1053.005)
Persistence	Scheduled Task/Job (T1053)	Scheduled Task (T1053.005)
Privilege Escalation	Process Injection (T1055)	
	Scheduled Task (T1053)	Scheduled Task (T1053.005)
Defense Evasion	Process Injection (T1055)	
	Obfuscated Files or Information (T1027)	Indicator Removal from Tools (T1027.005)
		HTML Smuggling (T1027.006)
		Embedded Payloads (T1027.009)
	Virtualization/Sandbox Evasion (T1497)	System Checks (T1497.004)
	Modify Registry (T1112)	
	Deobfuscate/Decode Files or Information (T1140)	
	Reflective Code Loading (T1620)	
	Indicator Removal (T1070)	File Deletion (T1070.004)
		Timestomp (T1070.006)
	Masquerading (T1036)	
Discovery	Process Discovery (T1057)	
	Software Discovery (T1518)	
	Query Registry (T1012)	
	Account Discovery (T1087)	Local Account (T1087.001)
		Domain Account (T1087.002)
	System Information Discovery (T1082)	
	File and Directory Discovery (T1083)	
Command and Control	Web Service (T1102)	
	Application Layer Protocol (T1071)	Web Protocols (T1071.001)
		DNS (T1071.004)
	Encrypted Channel (T1573)	Asymmetric Cryptography (T1573.002)
	Non-Application Layer Protocol (T1095)	
	Non-Standard Port (T1571)	
	Ingress Tool Transfer (T1105)	
Exfiltration	Data Transfer Size Limits (T1030)	

MITRE ATT&CK Methodologies (Source: Quorum Cyber)		
Tactic	Technique	Procedure
Reconnaissance	T1595.002: Active Scanning	SVR threat actors scan for publicly available exploits.
Initial Access	T1190: Exploit Public Facing Application	SVR threat actors use publicly available exploits to conduct widespread exploitation of vulnerable systems, including against Citrix, Pulse Secure, FortiGate, Zimbra and VMware.
Initial Access	T1195.002: Supply Chain Compromise: Compromise Software Supply Chain	SVR threat actors target organizations that supply software to intelligence targets.
Initial Access	T1199: Trusted Relationship	SVR threat actors leveraged access gained from the SolarWinds campaign to compromise a certificate issued by Mimecast, which it then used to authenticate a subset of Mimecast's products with customer systems.
Execution	T1059.005: Command and Scripting Interpreter: Visual Basic	SVR deployed Sibot, custom downloader written in VBS, after compromising victims via SolarWinds.
Persistence	T1505.003: Server Software	SVR threat actors typically deploy a web shell on Microsoft

	Component: Web Shell	Exchange servers following successful compromise.
Persistence	T1078: Valid Accounts	SVR actors have maintained persistence on high-value targets using stolen credentials.

Defense and Mitigations

Midnight Blizzard's consistent record of compromising U.S. government entities and infiltrating large corporate IT companies such as SolarWinds demonstrates its dedication and competency. Defending an organization targeted by this threat group requires nothing less than a full-fledged enterprise cybersecurity program utilizing the most advanced security solutions, including email and web-content filtering, advanced antivirus to detect malware and prevent it from ingressing an organization's network, and Endpoint Detection and Response (EDR) or Managed Detection and Response (MDR) to effectively and efficiently identify malware infections, and take swift action to reduce its dwell time and prevent it from impacting critical assets.

An effective cybersecurity program capable of defending against Midnight Blizzard should also be designed with the principle of least privilege, defense in depth, Zero Trust architecture, and multi-factor authentication in mind to segment and secure critical assets and reduce the potential damage attackers can cause if they do gain an initial foothold.

Additionally, due to their key insights on Midnight Blizzard that were highlighted throughout this report, several cybersecurity research companies (Avertium, SOCRadar, and Quorum Cyber) have their own defense and mitigation recommendations for this threat actor. While not an exhaustive list nor an offical endorsement by HC3, these recommendations are annotated (with links) here because of their knowledge of this particular threat actor, and of APTs in general. However, because of CISA's known tracking of Midnight Blizzard and their recent joint advisory with British NCSC, their defense and mitigations are listed below.

CISA Defense and Mitigations

- Use multi-factor authentication (2-factor authentication/two-step verification) to reduce the impact of password compromises. See NCSC guidance: Multifactor Authentication for Online Services and Setting up 2-Step Verification (2SV).
- Accounts that cannot use 2SV should have strong, unique passwords. User and system accounts should be disabled when no longer required with a "joiners, movers, and leavers" process in place and regular reviews to identify and disable inactive/dormant accounts. See NCSC guidance: 10 Steps to Cyber Security.
- System and service accounts should implement the principle of least privilege, providing tightly scoped access to resources required for the service to function.
- Canary service accounts should be created that appear to be valid service accounts, but are never used by legitimate services. Monitoring and alerting on the use of these account provides a high confidence signal that they are being used illegitimately and should be investigated urgently.
- Session lifetimes should be kept as short as practical to reduce the window of opportunity for an adversary to use stolen session tokens. This should be paired with a suitable authentication method that strikes a balance between regular user authentication and user experience.
- Ensure device enrollment policies are configured to only permit authorized devices to enroll. Use zero-touch enrollment where possible, or if self-enrollment is required, then use a strong form of 2SV that is

resistant to phishing and prompt bombing. Old devices should be prevented from (re)enrolling when no longer required. See NCSC guidance: Device Security Guidance.

- Consider a variety of information sources, such as application events and host-based logs to help prevent, detect and investigate potential malicious behavior. Focus on the information sources and indicators of compromise that have a better rate of false positives. For example, looking for changes to user agent strings that could indicate session hijacking may be more effective than trying to identify connections from suspicious IP addresses.

Relevant HHS Reports

HC3: Alert – Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (April 26, 2022)

HC3: Alert - Russian State-Sponsored and Criminal Cryber Threats to Critical Infrastructure (May 9, 2022)

HC3: Alert – Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability (March 16, 2022)

HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (January 11, 2022)

HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (March 1, 2022)

HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (March 1, 2022)

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

HC3: Analyst Note – The Russia-Ukraine Cyber Conflict and Potential Threats to the U.S. Health Sector (March 1, 2022)

HC3: Analyst Note – SolarWinds Critical Remote Code Execution Flaws (October 25, 2023)

HC3: Sector Alert – New Phishing Campaign Launched by SOLARWINDS Attackers (May 28, 2021)

HC3: Threat Briefing – An Analysis of the Russia/Ukraine Conflict (May 17, 2022)

HC3: Threat Briefing – APT and Cybercriminal Targeting of HCS (June 9, 2020)

HC3: Threat Briefing – COVID-19 Related Nation-State and Cyber Criminal Targeting of the Healthcare Sector (May 14, 2020)

HC3: Threat Briefing – Major Cyber Organizations of the Russian Intelligence Services (May 19, 2022)

HC3: Threat Briefing – Russian Threat Actors Targeting the HPH Sector (February 15, 2024)

References

"Advisory: APT29 targets COVID-19 vaccine development." National Cyber Security Centre. July 16, 2020. https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

"APT29 targets COVID-19 vaccine development." Security Magazine. July 20, 2020. https://www.securitymagazine.com/articles/92870-apt29-targets-covid-19-vaccine-development

"Cyber threats in Australian healthcare sector face increase in complexity and volume, following global patterns." Industrial Cyber. March 8, 2023. https://industrialcyber.co/medical/cyber-threats-in-australian-healthcare-sector-face-increase-in-complexity-and-volume-following-global-patterns/

"Dark Web Profile: APT29/Cozy Bear." SOCRadar. March 17, 2023. https://socradar.io/apt-profile-cozy-bear-apt29/

"Evolution of Russian APT29 – New Attacks and Techniques Uncovered." Avertium. July 25, 2023. https://explore.avertium.com/resource/evolution-of-russian-apt29-new-attacks-and-techniques-uncovered

Farrell, James. "Who is Midnight Blizzard? Russian-Linked Group Has Repeatedly Targeted Microsoft, Company Says." Forbes. March 8, 2024. https://www.forbes.com/sites/jamesfarrell/2024/03/08/who-is-midnight-blizzard-russian-linked-group-has-repeatedly-targeted-microsoft-company-says/?sh=5e1d72889018

"Healthcare Security Alert: Microsoft Teams Malware." ClearData. September 12, 2023. https://www.cleardata.com/healthcare-security-alert-microsoft-teams-malware/

Jenkins, Luke and Josh Atkins, Dan Black. "Backchannel Diplomacy: APT29's Rapidly Evolving Diplomatic Phishing Operations." Mandiant. September 21, 2023. https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing

"Midnight Blizzard: Guidance for responders on nation-state attack." Microsoft. January 25, 2024. https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

"Midnight Blizzard Threat Actor Profile." Quorum Cyber. Accessed March 22, 2024. https://www.quorumcyber.com/threat-actors/midnight-blizzard-threat-actor-profile/

"MITRE ATT&CK Groups: APT29." MITRE ATT&CK. Accessed March 22, 2024. https://attack.mitre.org/groups/G0016/

Newman, Lily Hay. "Big-Name Targets Push Midnight Blizzard Hacking Spree Back Into the Limelight." Wired. January 25, 2024. https://www.wired.com/story/microsoft-hpe-midnight-blizzard-email-breaches/

"SVR Cyber Actors Adapt Tactics for Initial Cloud Access." Cybersecurity & Infrastructure Security Agency. February 26, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

"Threat Intelligence Midnight Blizzard Threat Actor Profile." Quorum Cyber. July 4, 2023. https://www.quorumcyber.com/wp-content/uploads/2023/09/Quorum-Cyber-Midnight-Blizzard-APT29-

Threat-Actor-Profile.pdf

"Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard." Microsoft. March 8, 2024. https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

"Who is APT29?" BlackBerry. Accessed March 22, 2024. https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/apt29#:~:text=APT29%20(AKA%20CozyBear%2C%20The%20Dukes,product%20of%20the%20Russian%20government%27s

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback