Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Analyst Note

November 13, 2024 TLP:CLEAR Report: 202411131500

New Spear Phishing Campaign by Midnight Blizzard

Executive Summary

On October 29, 2024, the cybersecurity platform Microsoft Threat Intelligence observed the Russian advanced persistent threat (APT) Midnight Blizzard conducting a spear phishing campaign against multiple sectors around the world. Attributed to Russia's Foreign Intelligence Service, the platform's investigation reported that the objective of the campaign is likely based on reconnaissance or cyberespionage. This follows other recent campaigns by the threat actor, including one in January 2024, in which it targeted two American multinational technology companies. Tracing their longstanding and dedicated epionage of foreign interests as far back as early 2008, this group is largely known to target multiple industries, primarily across the United States and Europe. What follows is an examination of Midnight Blizzard; its newest campaign; a timeline of recent threat actor activity; its impact to the HPH sector; common tactics, techniques, and procedures (TTPs); exploited vulnerabilities; indicators of compromise; MITRE ATT&CK techniques; and recommended defense and mitigations against the group.

Overview of Midnight Blizzard

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	
Target Countries	Belgium, Brazil, China, Georgia, India, Japan, Kazakhstan, Mexico, New Zealand, the Netherlands, Norway, Portugal, Romania, South Korea, Turkey, Ukraine, the United Kingdom, and the United States	

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 cyberespionage 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 which has disruptive capabilities to conduct advanced cyber espionage operations.

Recent Spear Phishing Campaign

During their October 2024 phishing campaign, the threat actor was observed impersonating Microsoft employees and sending e-mails with social engineering lures related to Microsoft, Amazon Web Services (AWS), and the concept of Zero Trust. Through the phishing e-mails, remote desktop protocol (RDP) configuration files signed with a LetsEncrypt certificate were delivered. The RDP configuration files contain automatic settings and resource mappings that are established after successfully connecting to an RDP server controlled by the threat actor. While the campaign had all the signatures of a Midnight Blizzard phishing campaign, its use of an RDP configuration file was noted as a novel access vector for the group.

These e-mails were sent to thousands of individuals across government, academia, defense, non-governmental organizations, and other sectors in the United States, the United Kingdom and other European countries, Australia, and Japan. The threat actor's primary objective was intelligence gathering.

Successfully executed attacks provided the threat actor with sensitive information from the compromised device as the threat actor-controlled server mapped the victims' local device resources to the server. Resources sent to the server may include but are not limited to: all logical hard disks, clipboard contents, printers, connected peripheral devices, audio, and authentication features and facilities of the Windows operating system, including smart cards. Additionally, the unauthorized access could allow the threat actor to deploy malware on local drives and mapped network shares to maintain persistence once the RDP session is terminated.

This follows a security brief from Amazon last week, which took down domains mimicking its service after Midnight Blizzard sent Ukrainian language phishing e-mails with RDP configuration files. This phishing campaign aimed to steal Windows credentials from Russian adversaries by targeting government, private company, and military entities. Like their most recent campaign targeting multiple sectors, it is worth noting that these phishing e-mails were sent to significantly more targets than their typical, narrowly targeted approach.

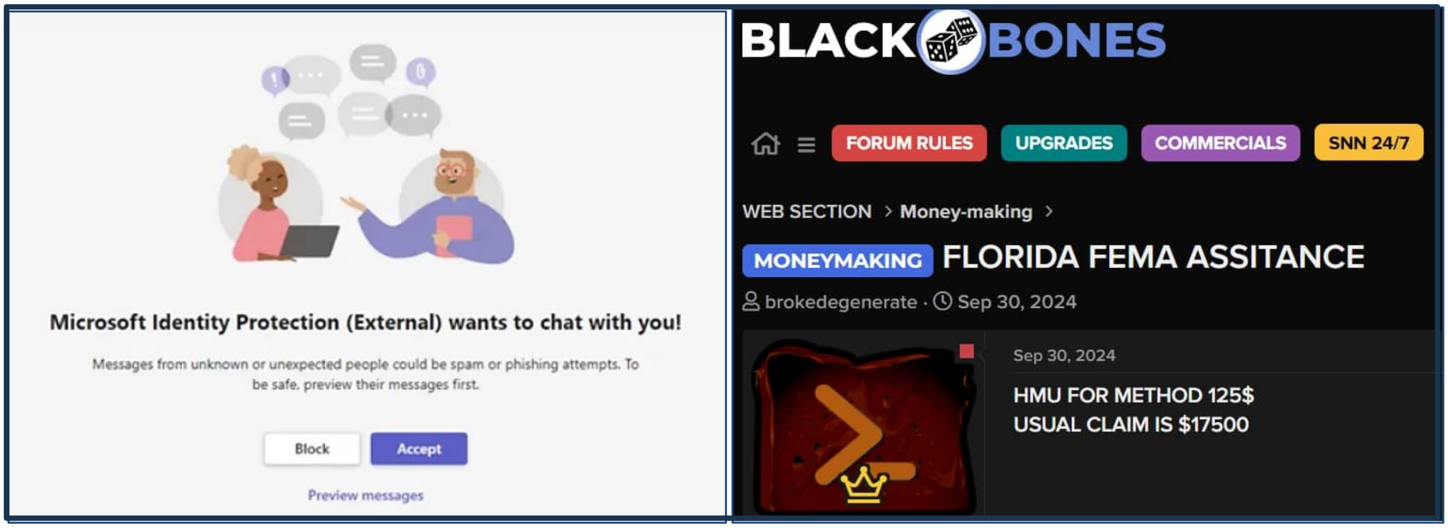
Timeline of Threat Actor Activity

Year	Incident
2014	Midnight Blizzard carries out the 'Office Monkeys' campaign targeting a Washington D.C.-based private research institute.
2015	Midnight Blizzard gains 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	Targets 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 then. 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	Compromises three European Union (EU) National Affairs ministries and a Washington D.C.-based embassy of an EU nation state.
2020	Conducts vulnerability scanning of public-facing IP addresses to compromise COVID-19 vaccine

Year	Incident
	developers in Canada, the U.S., and the UK. Distributes 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, reveals 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.
2024	Government, private company, and military sectors targeted with Ukrainian language phishing e-mails with RDP configuration files by Midnight Blizzard.
2024	Government, academia, defense, non-governmental organizations targeted with phishing campaign impersonating Microsoft employees and using RDP files by Midnight Blizzard.

Impact to HPH Sector

Several Russian APTs and cybercriminal groups (i.e. LockBit, Royal, Black Basta, ALPHV) regularly attack the Healthare 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 previously 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, diagnoses, prescriptions, etc., are all information that could be used by sophisticated threat actors for targeting a specific person or organization.



Microsoft Identity Protection (External) wants to chat with you!

Messages from unknown or unexpected people could be spam or phishing attempts. To be safe, preview their messages first.

FLORIDA FEMA ASSITANCE

brokedegenerate · Sep 30, 2024

Sep 30, 2024

HMU FOR METHOD 125$
USUAL CLAIM IS $17500

Figure 1: Microsoft Teams message request from Midnight Blizzard social engineering attack. *(Source: SOCRadar)* Cybercrime forum, BlackBones, posts instructions on how to submit fraudulent FEMA claims. *(Source: HackRead)*

Through much of 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 with Midnight Blizzard.

In a 2023 malware campaign, cyberattackers 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 this kind of social engineering attacks ie still successful.

In 2024, during the period between Hurricane Helene and Hurricane Milton, cybercriminals exploited the urgency and confusion of the catastrophe to take advantage of disaster victims and relief organizations. These scams, which targeted both individuals and organizations, involved fraudulent Federal Emergency Management Agency (FEMA) claims, phishing campaigns, and malware disguised as legitimate FEMA documents.

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.
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 the military.
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

Custom Malware	Decription
	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 that 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.

Cybersecurity Advisories on SVR and/or Midnight Blizzard (2023-2024)

On October 10, 2024, the National Security Agency (NSA) along with the Federal Bureau of Investigation (FBI), the United States Cyber Command's Cyber National Mission Force (CNMF), and the United Kingdom National Cyber Security Centre (NCSC) released a joint cybersecurity advisory updating their guidance on Russian SVR cyber operations. It provides a detailed list of publicly disclosed common vulnerabilities and exposures (CVEs) and a list of mitigations to improve cybersecurity posture based on the SVR cyber actors' operations.

On February 26, 2024, the Cybersecurity & Infrastructure Security Agency (CISA), the NCSC, and other international partners released a cybersecurity advisory on the recent TTPs of Midnight Blizzard from February 2023 to February 2024. It provides an overview of TTPs deployed by the actor to gain initial access into the cloud environment and includes advice to detect and mitigate this activity.

Exploited Vulnerabilities

In April 2021, the U.S., UK, and Canadian governments published a joint CSA highlighting the SVR's exploitation of CVEs for initial access. Since then, SVR cyber actors have exploited vulnerabilities at a mass scale to target victims worldwide across a variety of sectors, including:

Exploited Vulnerabilities (Source: October 10, 2024 Joint Cybersecurity Advisory)		
CVE-ID	Severity	Description
CVE-2022-27924	7.5 High	CVE-2022-2794 is a command injection vulnerability [CWE-74] that allows an unauthenticated

Exploited Vulnerabilities (Source: October 10, 2024 Joint Cybersecurity Advisory)		
		attacker to inject arbitrary memcache commands into a targeted Zimbra instance, causing an overwrite of arbitrary cached entries. SVR cyber actors exploited Zimbra mail servers targeting hundreds of domains worldwide, including through exploitation of the CVE. This allowed the actors to access user credentials and mailboxes without victim interaction. Following the exploitation of those systems, the SVR deployed infrastructure to enable collection from the victims.
CVE-2023-42793	9.8 Critical	Starting in September 2023, SVR cyber actors have exploited JetBrains TeamCity CVE-2023-42793, which enabled arbitrary code execution via insecure handling of specific paths allowing for authentication bypass.

Based on the SVR cyber actors' TTPs and previous targeting, the authoring agencies assess they have the capability and interest to exploit additional CVEs for initial access, remote code execution, and privilege escalation, including the ones listed below. The below CVEs have all been publicly disclosed; organizations should implement vendor-issued security patches if they have not already.

CVE-ID	Vendor/Product	Description
CVE-2023-20198	Cisco IOS XE Software web UI feature	Privilege escalation vulnerability [CWE-269] that allows an attacker to create a local user and password combination.
CVE-2023-4911	RHSA GNU C Library's dynamic loader ld.so	Buffer overflow vulnerability [CWE-122] that could allow a local attacker to execute code with elevated privileges.
CVE-2023-38545	Haxx Libcurl	SOCKS5 heap buffer overflow vulnerability [CWE-122]
CVE-2023-38546	Haxx Libcurl	Missing authorization vulnerability [CWE-862] that allows an attacker to insert cookies in a running program if certain conditions are met.
CVE-2023-40289	Supermicro X11SSM-F, X11SAE-F, and X11SSE-F 1.66	Command injection vulnerability [CWE-74] that allows an attacker to elevate privileges.
CVE-2023-24023	Bluetooth BR/EDR devices with Secure Simple Pairing and Secure Connections pairing in Bluetooth Core Specification 4.2 through 5.4	Allows certain man-in-the-middle attacks [CWE-300] that force a short key length [CWE-326] and might lead to discovery of the encryption key and live injection, aka BLUFFS.
CVE-2023-40088	Android	Use after free [CWE-416] vulnerability that could lead to remote (proximal, adjacent) code execution.
CVE-2023-40076	Google Android 14.0	Permissions bypass vulnerability [CWE-200] that allows an attacker to access credentials and escalate local privileges.
CVE-2023-40077	Google Android 11-14	Use after free [CWE-416] vulnerability that can lead to escalation of privileges.
CVE-2023-45866	Bluetooth HID Hosts in BlueZ	Improper authentication vulnerability [CWE-287] that could allow a nearby attacker to inject keystrokes and carry out arbitrary commands.
CVE-2022-40507	Qualcomm	Double free vulnerability [CWE-415]
CVE-2023-36745	Microsoft Exchange Server	Remote code execution [CWE-502]
CVE-2023-4966	Citrix NetScaler ADC, NetScaler Gateway	Buffer overflow vulnerability [CWE 119]
CVE-2023-6345	Google Chrome	Integer overflow vulnerability [CWE 190] that allows a remote attacker to potentially perform a sandbox escape via a malicious file.
CVE-2023-37580	Zimbra	Cross-site scripting (XSS) vulnerability [CWE-79]
CVE-2021-27850	Apache Tapestry	Critical unauthenticated remote code execution vulnerability [CWE-502]
CVE-2021-41773	Apache HTTP server 2.4.99	Directory traversal vulnerability [CWE-35]
CVE-2021-42013	Apache HTTP server 2.4.50	Remote code execution vulnerability [CWE-22]
CVE-2018-13379	Fortinet FortiGate SSL VPN	Path traversal vulnerability [CWE-35]
CVE-2023-42793	JetBrains TeamCity	Authentication bypass vulnerability [CWE-288]
CVE-2023-29357	SharePoint Server	Elevation of privilege vulnerability [CWE-303]
CVE-2023-24955	SharePoint Server	Remote code execution vulnerability [CWE-94]

CVE-ID	Vendor/Product	Description
CVE-2023-35078	Ivanti Endpoint Manager Mobile versions through 11.10	Authentication bypass vulnerability [CWE-288]
CVE-2023-5044	Kubernetes Ingress-nginx	Code injection vulnerability [CWE-94]

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 that are affiliated with Midnight Blizzard.

Microsoft Threat Intelligence IoCs		
E-mail sender domains		
sellar[.]co.uk	totalconstruction[.]com.au	cewalton[.]com
townoflakelure[.]com	swpartners[.]com.au	
RDP file names		
AWS IAM Compliance Check.rdp AWS IAM Configuration.rdp AWS IAM Quick Start.rdp AWS SDE Compliance Check.rdp AWS SDE Environment Check.rdp AWS SDE Environment Check.rdp AWS Secure Data Exchange – Compliance Check.rdp AWS Secure Data Exchange Compliance.rdp	Device Configuration Verification.rdp Device Security Requirements Check.rdp IAM Identity Center Access.rdp IAM Identity Center Application Access.rdp Zero Trust Architecture Configuration.rdp Zero Trust Security Environment Compliance Check.rdp ZTS Device Compatibility Test.rdp	
RDP remote computer domains		
For full list, see link here.		

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
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			

Quorum Cyber IoCs
731d724e8859ef063c03a8b1ab7f81ec
846e27a652a5e1bfbd0ddd38a16dc865
9466c865f7498a35e4e1a8f48ef1dffd

SOCRadar IoCs
msftprotection.onmicrosoft[.]com
identityVerification.onmicrosoft[.]com
accountsVerification.onmicrosoft[.]com
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: October 10, 2024 Joint Cybersecurity Advisory)		
Tactic	ID	Use
Exploit Public Facing Application	T1190	The actors exploit multiple CVEs for initial access and/or privilege escalation.
Escalation of privileges	T1068	The actors escalate privileges on a compromised host.
Phishing	T1566	The actors commonly conduct spear phishing campaigns.
Valid accounts	T1078	The actors conduct password spraying to access victim environments.
Compromise software supply chain	T1195.002	The actors use trojanized software updates to compromise downstream customers.
Trusted Relationship	T1199	The actors abuse trusted relationships to target other connections.
Compromise Infrastructure	T1584	The actors compromise infrastructure to incorporate in future operations.
Hide Infrastructure	T1665	The actors use residential proxies and TOR to obfuscate infrastructure.
Acquire Infrastructure	T1583	The actors use cryptocurrencies, fake identities, and low reputation email accounts to lease infrastructure.
Compromise Infrastructure Botnet	T1584.005	The actors compromise numerous third-party systems to form a botnet.

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

MITRE ATT&CK Methodologies (Source: CISA)

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)
	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)

MITRE ATT&CK Methodologies (Source: Mandiant)

	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 Component: Web Shell	SVR threat actors typically deploy a web shell on Microsoft 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 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 official endorsement by HC3, these recommendations are annotated (with links) here because of their knowledge of this particular threat actor and of APTs in general.

October 29, 2024 Joint Cybersecurity Advisory Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of the threat actor's activity:

- Prioritize rapid deployment of patches and software updates as soon as they become available. Enable automatic updates where possible.
- Reduce attack surface by disabling Internet-accessible services that you do not need, or restrict access to trusted networks, and remove unused applications and utilities from workstations and development environments.
- Perform continuous threat hunting activities.
- Ensure proper configuration of systems; check for open ports and obsolete or unused protocols, especially on Internet-facing systems.
- Isolate Internet-facing services in a network Demilitarized Zone (DMZ) to reduce exposure of internal networks.
- Require and enforce multi-factor authentication whenever possible.
- Require additional identity challenges for enrollment of new devices when users are permitted to self-enroll multi-factor authentication mechanisms or register devices on the corporate network.
- Notify users across multiple platforms when devices have been successfully registered to help identify unexpected registrations. Train and encourage users to notice and report unexpected registrations.
- Enable robust logging for authentication services and Internet-facing functions.
- Regularly audit cloud-based accounts and applications with administrative access to email for unusual activity.
- Limit token access lifetimes and monitor for evidence of token reuse.
- Enforce least-privileged access and disable external management capabilities.
- Baseline authorized devices and apply additional scrutiny to systems accessing network resources that do not adhere to the baseline.
- Disable remote downloading of information to non-enrolled devices when possible.

Due to CISA's known tracking of Midnight Blizzard and their recent joint advisor 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.

The Way Forward

In addition to a HC3 Analyst Note on Healthcare Sector DDoS Guide on how to safeguard against ransomware/extortion attacks, some cybersecurity professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via email and network access.
- Assess enterprise risk against all potential vulnerabilities and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

At no cost, the Cybersecurity & Infrastructure Security Agency (CISA) also offers Cyber Hygiene Vulnerability Scanning services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations. This service helps organizations monitor and evaluate their external network posture.

The probability of cyber threat actors targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent an cyberattack remain the best ways forward for healthcare organizations.

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 Cyber 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: Analyst Note – Healthcare Sector DDoS Guide (May 30, 2024)
- 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

Collins, Benedict. "Microsoft says Russian hackers have launched major spear phishing attacks against US government officials." TechRadar. October 30, 2024. https://www.techradar.com/pro/microsoft-says-russian-hackers-have-launched-major-spear-phishing-attacks-against-us-government-officials

"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/

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

"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

Greig, Jonathan. "Russia's 'Midnight Blizzard' hackers target government workers in novel info-stealing campaign." The Record. October 29, 2024. https://therecord.media/russia-midnight-blizzard-hackers-target-government-sector

"Global Midnight Blizzard spear-phishing operation underway." SC Media. October 30, 2024. https://www.scworld.com/brief/global-midnight-blizzard-spear-phishing-operation-underway

"H-ISAC Threat Bulletin: Russian Threat Actor Midnight Blizzard Conducts Large Scale Spearphishing Campaign Containing RDP Files." American Hospital Association. Accessed October 31, 2024. https://www.aha.org/h-isac-white-reports/2024-10-30-h-isac-threat-bulletin-russian-threat-actor-midnight-blizzard-conducts-large-scale

HackRead User: Waqas. "Scammers Hit Florida Hurricane Victims with Fake FEMA Claims, Malware Files." HackRead. October 9, 2024. https://hackread.com/scammers-florida-hurricane-victim-fake-fema-malware/

"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

"Joint Cybersecurity Advisory: Update on SVR Cyber Operations and Vulnerability Exploitation." Federal Bureau of Investigation, National Security Agency, Cyber National Mission Force, and National Cyber Security Centre. October 10, 2024. https://media.defense.gov/2024/Oct/09/2003562611/-1/-1/0/CSA-UPDATE-ON-SVR-CYBER-OPS.PDF

Khaitan, Ashish. "A Deep-Dive into Russian Midnight Blizzard's Campaign that Targeted Ukrainian Military, Government." The Cyber Express. October 30, 2024. https://thecyberexpress.com/midnight-blizzard-cyberattacks/

Kovacs, Eduard. "Microsoft Warns of Russian Spear-Phishing Attacks Targeting Over 100 Organizations." Security Week. October 30, 2024. https://www.securityweek.com/microsoft-warns-of-russian-spear-phishing-attacks-targeting-over-100-organizations/

"Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files." Microsoft. October 29, 2024. https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/

"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