Quorum Cyber

Threat Intelligence Midnight Blizzard Threat Actor Profile

TLP Status: CLEAR

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Document Control 3
Revision History 3
Related Documents 3
Threat Actor Profile 4
Overview 4
Targeted Sectors 4
Threat Actor Motivations 4
Threat Actor Activity Timeline 4
Associated Malware 5
Exploited Vulnerabilities 6
Indicators of Compromise 7
Mitre Methodologies 9
Cyber Kill Chain 12
Containment, Mitigations and Remediations 12
Additional information 13

Document Control

Revision History

Version	Date	Summary of Changes
0.1	07/04/2023	Initial Report
0.2	03/08/2023	Report Update
1.0	07/09/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

Threat Actor Profile

Overview

Midnight Blizzard, also known as APT29, is a threat actor group suspected to be attributed to the Russian Foreign Intelligence Service (SVR). The initial emergence of Midnight Blizzard operations occurred in 2008 when the first MiniDuke malware samples were compiled according to Kaspersky. APT29 employs a wide variety of advanced techniques in their cyber operations in support of the SVR's intelligence requirements.

Midnight Blizzard has been suspected of being involved in several high-profile attempted intrusions and compromises, including the Office Monkeys campaign in 2014 targeting a Washington D.C.-based private research institute, the Pentagon in 2015, the Democratic National Committee (DNC) and US think tanks in 2016, the Norwegian Government and several Dutch ministries in 2017. The group has also targeted organisations within the education sector that are affiliated with medical research. It is highly likely that the group targets such institutions for espionage purposes, in order to exfiltrate data relating to western medical advances.

Midnight Blizzard applies a wide range of bespoke tools developed in a variety of programming languages, which demonstrates the resources at their disposal. The group also utilises publicly available commodity tools such as Mimikatz and Cobalt Strike.

Targeted Sectors

Midnight Blizzard heavily targets organisations responsible for influencing the foreign policy of NATO countries. It has also been documented as focusing on organisations from a range of sectors, including education, energy, telecommunications, government and military.

Threat Actor Motivations

The motives of Midnight Blizzard can be evaluated by observing the strategies 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. As such, Midnight Blizzard acts with the motivations of espionage purposes.

Threat Actor Activity Timeline

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 DNC servers close to the US election via a phishing campaign directing victims to change their passwords using a spoofed website

2017: Targets the Norwegian Government and several Dutch ministries

2019: Compromises three 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 developers in Canada, the US, and the UK

2020: Distributes SUNBURST malware, attacking SolarWinds Orion software to drop a remote access trojan (RAT) that impacted many global organisations

2023: Midnight Blizzard conducts targeted social engineering operations via Microsoft Teams

Associated Malware

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.

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 utilised from January 2010 to the summer of 2015 and was observed targeting a wide range of organisations including those in the energy and telecommunications sectors, and governments and the military.

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 utilised from January 2009 to December 2012.

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 utilised by Midnight Blizzard from January 2010 to the spring of 2015.

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

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.

Hammertoss: 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 principle toolset being discovered. Hammertoss was in use from at least January 2015 to July 2015.

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 utilised 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.

PowerDuke: PowerDuke has been delivered to targets via emails with Microsoft Word or Excel file with malicious macros. If successfully exploited, a PNG image is downloaded from the compromised web server and the PowerDuke trojan is hidden in the PNG images using steganography. PowerDuke was first seen in August 2016 and used in the most recent operation widely attributed to Midnight Blizzard, in the November 2016 post-election spear phishing campaign.

POSHSPY: POSHSPY is a backdoor that leverages PowerShell and Windows Management Instrumentation (WMI). Its use of a PowerShell payload means that only legitimate system processes are utilised and that the malicious code execution can only be identified through enhanced logging or in memory. POSHSPY has been active since at least early 2015.

Exploited Vulnerabilities

CVE-ID	Severity	CWE	Description	Exploit Type	Patch
CVE-2018-13379 (Fortinet FortiOS)	**CVSSv3 Score: 9.8 – Critical**	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	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 Collaboration Suite)	**CVSSv3 Score: 9.8 – Critical**	CWE-611: Improper Restriction of XML External Entity Reference	An XML External Entity injection (XXE) vulnerability in the mailboxd component in Synacor Zimbra Collaboration Suite.	Remote Code Execution	Patch
CVE-2019-11510	**CVSSv3 Score: 10.0 – Critical**)	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	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)	**CVSSv3 Score: 9.8 – Critical**)	CWE-22: Improper Limitation of a Pathname to a Restricted	An issue was discovered in Citrix Application Delivery Controller (ADC)	Remote Code Execution	Patch

		Directory ('Path Traversal')	that allows Directory Traversal.		
CVE-2020-4006 (VMware Workspace ONE Access)	**CVSSv3 Score: 9.1 – Critical)**	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	A command injection vulnerability.		Patch

Indicators of Compromise

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
- 731d724e8859ef063c03a8b1ab7f81ec
- 846e27a652a5e1bfbd0ddd38a16dc865
- 9466c865f7498a35e4e1a8f48ef1dffd

Mitre Methodologies

The table below outlines the tactics, techniques and procedures (TTPs) utilised by the SVR associated threat actor groups, such as Midnight Blizzard [1]:

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 organisations 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.

[1] https://www.aha.org/system/files/media/file/2021/05/Advisory-further-TTPs-associated-with-SVR-cyber-actors.pdf

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.

Initial Access:

Midnight Blizzard has consistently used spear phishing as an initial attack vector for compromise. Initially this primarily involved using an attachment to deliver files with exploits to initial victims. Since 2015, this has evolved to spear phishing seeking to trick victims into clicking on a link to download a legitimate decoy document alongside a malicious Windows shortcut file (LNK), while sometimes using compromised legitimate domains. This was most recently observed in the suspected 2018 Midnight Blizzard phishing campaign and the 2016 PowerDuke campaign.

Execution:

Midnight Blizzard primarily uses Scripting, PowerShell, Service Execution, WMI, and Exploitation for Client Execution tactics to achieve execution in targeted environments. Since 2014, attacks and tools developed by Midnight Blizzard have typically utilised PowerShell scripts to download/install and execute commands, as well as to evade detection.

Persistence:

Midnight Blizzard has commonly used Scheduled Task, Registry Run Keys and WMI Event Subscription tactics to maintain persistence on target networks. In particular, their techniques have progressed to use WMI Event Subscription to maintain persistence through their backdoor POSHSPY since approximately 2015.

Privilege Escalation:

Midnight Blizzard has been reported to have exploited vulnerabilities, bypassing Windows User Account Control (UAC), and using accessibility features to escalate privileges. Most notably, this entailed the use of the 'Sticky Keys' accessibility feature from approximately 2014 onwards. By using a PowerShell script to install a Tor service, they were able to replace the Sticky Keys binary with the Windows Command Processor "cmd.exe".

Defence Evasion:

The majority of defence evasion techniques used by Midnight Blizzard have been implemented from 2014 onwards and have been summarised below:

- Obfuscated Files or Information - The PowerDuke malware uses an alternate data stream (ADS) PNG file to hide and encrypt itself using Tiny Encryption Algorithm (TEA), while POSHSPY backdoor appends a file signature header (randomly selected from six file types) to encrypted data prior to upload or download
- File Deletion - In more recent toolsets from approximately October 2014 onwards, Midnight Blizzard has utilised file deletion techniques
- Indicator Removal on Host - Midnight Blizzard has used multiple versions of malware, and also minimised re-use of commonly identified indicators like MD5s and C2s. It has also used Secure Delete (SDelete) to remove artifacts from target systems by overwriting the entire contents of the registry hive

- Scripting - Since 2014, attacks and tools developed by Midnight Blizzard commonly utilise PowerShell scripts to download/install and execute commands, as well as to evade detection.

Credential Access:

Early APT29 malware families utilised credential dumping and input capture/keylogging. More recently, the group has also been linked to commercially available tools with credential access capability, such as Mimikatz and Cobalt Strike.

Discovery:

PowerDuke, attributed to APT29 in 2016, contains several commands to obtain system information. For instance, PowerDuke has commands to get text of the current foreground window, to get its current directory name as well as the size of a file, to get the current user's name and SID and to get information about the victim.

Lateral Movement:

Midnight Blizzard has traditionally used remote file copy, pass the hash, pass the ticket and Windows Admin Shares techniques to move laterally in target environments. In particular, with some SeaDuke malware variants from October 2014 onwards, Midnight Blizzard used a Kerberos golden ticket attack through Mimikatz.

Collection:

Several collection techniques have been used by Midnight Blizzard, including capturing data from the local system, removable media, network shared drives, the clipboard and Microsoft Outlook.

Exfiltration:

Midnight Blizzard has used valid accounts, exfiltration over alternative protocols, automated exfiltration and data compression to exfiltrate data. For instance, Hammertoss has been seen to upload information from victim networks to accounts on cloud storage services using login credentials received using steganography.

Command and Control:

Midnight Blizzard utilises a range of C2 techniques, which include the following:

- Standard Application Layer Protocol
- Custom Cryptographic Protocol
- Standard Cryptographic Protocol
- Data Encoding
- Web Service
- Domain Fronting.

Cyber Kill Chain

Outlined below is the typical cyber kill chain employed by Midnight Blizzard, the specific details of which were derived from the attack against the DNC during the 2016 election:

Reconnaissance:

During the first stage, Midnight Blizzard collected information on the target. In the DNC breach, two main reconnaissance techniques were used: network scanning and credential harvesting. The network scanning looked for websites that were vulnerable to cross-site scripting (XSS) and structured query language (SQL) injections, whereas the credential harvesting involved crafting pages to harvest legitimate user credentials.

Weaponisation:

At this stage, Midnight Blizzard embedded malicious macros into files such as PDFs and Microsoft Word sent through spear phishing emails. Microsoft Office documents were weaponised to create a macro that would deploy a backdoor PowerShell code called POSHSPY/PowerDuke in the case of the DNC breach.

Delivery:

Midnight Blizzard sent spear phishing emails to infect their targets with malicious attachments or URLs with malicious payloads.

Exploitation:

The group used social engineering techniques, in the form of spear phishing, to gain entry into the network.

Installation:

This stage covers the installation of the malicious code in the target's system which allowed Midnight Blizzard to maintain persistence until detected. In the DNC breach, users were sent a spear-phishing email that had a zip file attachment. The zip file contained a document with a dropper to install the backdoor to the Midnight Blizzard C2 server.

Command and Control:

In the DNC attack, the infected system was the DNC servers that provided a communication channel for the group.

Containment, Mitigations and Remediations

It is strongly recommended that the security best practices outlined below are followed to bolster the security posture against potential attack from Midnight Blizzard [2]:

- SVR threat actors regularly exploit publicly known vulnerabilities and complex supply chain attacks to gain initial access onto target networks. Managing and applying security updates as quickly as possible will help reduce the

[2] https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf

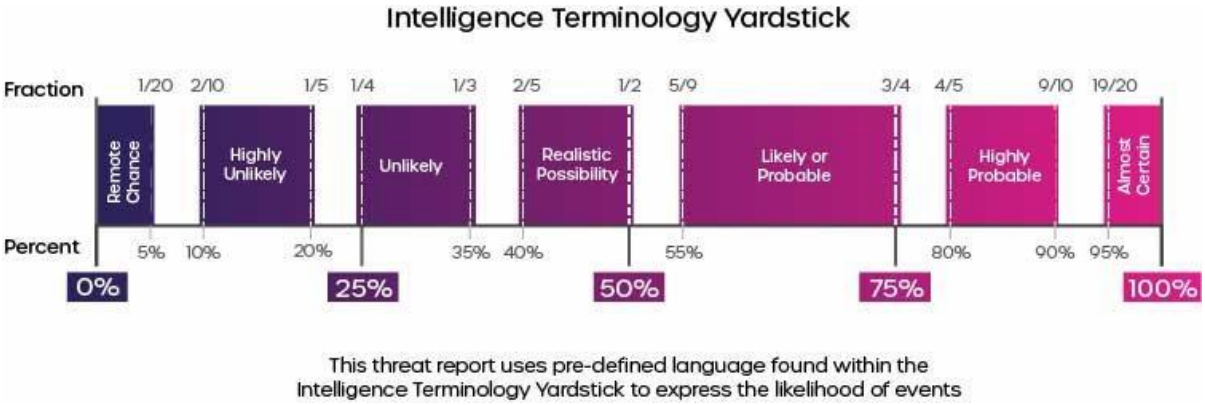
attack surface available for SVR actors and force them to use higher equity tooling to gain a foothold in the networks.

- Despite the complexity of supply chain attacks, following basic cyber security principles will make it harder for sophisticated threat actors to compromise target networks. By implementing network security controls and effectively managing user privileges, organisations will help prevent lateral movement between hosts, which will limit the effectiveness of complex attacks.
- Detecting supply chain attacks will always be difficult. However, an organisation may be able to detect this type of activity through heuristic detection methodologies, such as the volume of emails being accessed or by identifying anomalous network traffic.
- Organisations should ensure sufficient logging (both cloud and on-premises) is enabled and stored for a suitable amount of time, to identify compromised accounts, exfiltrated material and threat actor infrastructure. Mail retention and content policies should also be implemented to reduce the amount of sensitive information available upon successful compromise.
- As part of Microsoft's 'Advanced Auditing' functionality, they have introduced a new mailbox auditing action called 'MailItemsAccessed' which helps with investigating the compromise of email accounts. This is part of Exchange mailbox auditing and is enabled by default for users that are assigned an Office 365 or Microsoft 365 E5 licence or for organisations with a Microsoft 365 E5 compliance add-on subscription.
- Protect devices and networks by keeping them up to date. Use the latest supported versions, apply security patches promptly, use anti-virus platforms and scan regularly to guard against known malware threats.
- Enforce multi-factor authentication to reduce the impact of password compromises.
- Ensure that users are trained to report suspected phishing emails.

Additional information

- Mitre ATT&CK Profile
- SOCRadar Profile
- Kaspersky Profile
- Exabeam Report
- BlackBerry Threat Profile

Intelligence Cut-off Date (ICoD): 07/09/2023 at 10:00 UTC



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events