Midnight Blizzard Uncovered: A Comprehensive Analysis of Cyber Threat Tactics and Implications

Varadharaj Varadhan Krishnan

Independent Researcher, Seattle, USA

Abstract: ***This paper provides a comprehensive analysis of Midnight Blizzard, a Russian state - sponsored cyber espionage group also known as Nobelium, APT29, Cozy Bear, and The Dukes. Known for their sophisticated cyberattacks primarily targeting western governments and critical infrastructure, this group's activities are emblematic of the advanced persistent threats. Through detailed examination of various high - profile attacks, including the SolarWinds breach and attempts against Microsoft M365, this paper dissects the operational tactics, techniques, and procedures (TTPs) of Midnight Blizzard. Utilizing a combination of open - source intelligence, incident reports, and security analyses, the study highlights the strategic motivations behind the group's operations and their implications for cybersecurity defenses. The analysis aims to equip organizations with a deeper understanding of the threat posed by Midnight Blizzard and provides actionable insights into developing strong defenses against well - resourced and technically adept adversary like Midnight Blizzard.***

Keywords: Midnight Blizzard, Advanced Persistent Threat (APT), State - Sponsored Cyber Attacks, Cybersecurity Defense, SolarWinds Attack, Microsoft M365 Security

1. Introduction

In recent years, the cybersecurity landscape has seen a significant evolution in the sophistication and frequency of cyberattacks. State - sponsored threat actors have emerged as formidable adversaries, using advanced techniques to breach high - value targets for espionage, data theft, and infrastructure disruption. Understanding the tactics and strategies of threat actors like Midnight Blizzard is vital for organizations to build a stronger defense. This threat actor, identified as a Russian state - sponsored entity also known by other names like Nobelium, APT29, Cozy Bear, and The Dukes, has demonstrated a pattern of sophisticated cyberattacks aimed at strategic espionage and intelligence gathering [1] [2] [4]. The group is renowned for its persistent attacks tailored to align with Russian foreign policy interests, and it employs a variety of methods to compromise sensitive information for that cause [1]. This paper aims to dissect the operations of Midnight Blizzard to uncover the methodologies it employed in past attacks. By analyzing their attack patterns and targets, the paper seeks to provide insights into their operational tactics, techniques, and procedures. Midnight Blizzard has been implicated in numerous high - profile cyber incidents, with tactics that include spear - phishing, password spraying, and exploiting software vulnerabilities. One of their notable methods involves compromising third - party services to breach primary targets indirectly. The group has strategically targeted entities across the United States and Europe, focusing on governmental, diplomatic, and technological sectors to fulfill its agenda of intelligence gathering and espionage [3] [4]. Based on the study of all the past attacks, this paper aims to provide guidance to organizations on the best practices to follow to defend against such advanced persistent threat actors.

2. Literature Review

Understanding cyber threat actors like Midnight Blizzard requires a comprehensive analysis of publicly available information and reports produced by cybersecurity industry leaders. Researchers have often employed models like the Cyber Kill Chain and the Diamond Model of Intrusion Analysis to dissect the actions of the threat actors and understand their tactics, techniques, and procedures (TTPs). These frameworks help map out adversarial behavior and identify mitigation strategies for each stage of an attack. Extensive research has been conducted on threat actors like Midnight Blizzard; these studies often focus on the geopolitical motives driving these actors and their typical cyber espionage tactics specific to those attacks and timelines. For example, works by FireEye and Crowdstrike have detailed the profiles of these groups, their historical activities, and their evolving strategies [1 - 10] [22]. Despite the wealth of research available on individual attacks by Midnight Blizzard, there are gaps in understanding all of their attacks together and providing more actionable insights to improve defense posture for organizations. There is a lack of comprehensive data on the effectiveness of various defensive strategies against such sophisticated attacks. This limits the ability to prioritize the defense strategies to counter such threats.

3. Methodology

This paper utilizes a combination of cybersecurity reports, case studies, and incident reports to dissect the activities of Midnight Blizzard. Primary sources include public disclosures from affected companies like Microsoft's detailed incident reports and reports by cybersecurity firms like FireEye and CrowdStrike. Secondary sources comprise scholarly articles and white papers that discuss related cyber threat actors and their methodologies. These diverse sources ensure a rich dataset that captures both the technical aspects of the cyberattacks and the strategic intentions behind them. The analysis employs a couple of different techniques to dissect and understand the operations of Midnight Blizzard. *Threat Analysis*: This involves examining the tactics, techniques, and procedures (TTPs) used by Midnight Blizzard. *Cross - case Analysis*: Comparing the activities of Midnight Blizzard with similar known threat actors to identify

Paper ID: SR24508112247 DOI: https://dx.doi.org/10.21275/SR24508112247

unique attributes and shared tactics to identify new trends and their repeated use. *Applying Data Inclusion and Exclusion Criteria*: The inclusion criteria are defined to ensure that the data is directly relevant to Midnight Blizzard. This includes verified attacks attributed to this actor as well as data from reputable sources. Exclusion criteria remove data that is speculative and cannot be cross verified with another source. This selective approach helps focus the analysis on high - quality, relevant data that contributes directly to understanding the strategic operations of Midnight Blizzard.

4. Analysis of Midnight Blizzard

Midnight Blizzard, also known by aliases such as APT29, Cozy Bear, and The Dukes, is a Russian state - sponsored cyber espionage group. The group has been active since at least 2008, primarily focusing on intelligence gathering that aligns with Russian national interests. Midnight Blizzard is widely recognized for their involvement in high - profile cyber - attacks, including interference in US political processes and targeting governments and their diplomats across various countries. This actor is part of a broader strategy employed by the Russian government to exert influence globally, gather sensitive information, and potentially pre - position within critical infrastructures for future operations. Details about the identities of members of Midnight Blizzard remain largely undisclosed. The group is however a classic example of advanced persistent threat (APT) groups, with specialized units responsible for developing tools, reconnaissance, data exfiltration, and analyzing stolen data.

Table 1: Timeline of Attacks by Midnight Blizzard [1 - 9] [11] [12] [13] [15] [20 - 39]

Year	Attack	Summary
2013	MiniDuke - Attack against NATO countries using a PDF backdoor.	MiniDuke involved a sophisticated malware distributed via PDF documents that targeted NATO countries and ex - Soviet states, compromising government systems with espionage capabilities.
2014	CosmicDuke (CozyDuke) - Targets government and military.	CosmicDuke, also known as CozyDuke, delivered malware through phishing attacks aimed at government and military targets, extracting sensitive information.
2014	‘Office Monkeys’ campaign by Midnight Blizzard.	This campaign involved targeted attacks against a Washington D. C. - based private research institute, utilizing crafted spear - phishing emails to gain access.
2015	Pentagon Email System Breach.	Hackers gained initial access to the Pentagon’s email systems affecting thousands of personnel, deploying tools that could intercept and exfiltrate email communications.
2015	‘Hammertoss’ technique for C2 via Twitter by Midnight Blizzard.	Hammertoss was a novel command - and - control technique using Twitter to communicate with malware implanted within compromised networks, directing the download of additional payloads.
2016	DNC Hack (GRIZZLY STEPPE) via phishing.	The breach of the DNC's servers was executed close to the U. S. election, involving spear - phishing emails that deceived recipients into compromising their credentials.
2016	Spear - phishing of U. S. Think Tanks and NGOs.	APT29 targeted U. S. think tanks and NGOs with spear - phishing campaigns, aiming to access emails and documents related to the presidential election.
2017	Attacks on the Norwegian Government and Dutch ministries.	Spear - phishing campaigns were launched against Norwegian and Dutch government bodies, attempting to infiltrate networks and steal governmental secrets.
2018	Attacks on Foreign Ministries with spear - phishing.	The group used spear - phishing emails to target foreign ministries in North America and Europe, seeking to access confidential diplomatic communications.
2019	Breaches EU National Affairs ministries and an embassy.	The campaign compromised three EU National Affairs ministries and a Washington D. C. - based embassy, gaining access to internal communications and sensitive data.
2020	COVID - 19 Vaccine Research attacks and SUNBURST malware.	APT29 conducted vulnerability scanning and deployed the SUNBURST malware to target COVID - 19 vaccine developers, aiming to steal research data and disrupt vaccine development.
2020	SolarWinds Orion Hack with SUNBURST malware.	This massive supply chain attack involved the deployment of SUNBURST malware through compromised SolarWinds Orion software updates, affecting numerous global organizations.
2021	SolarWinds Orion Hack continued impacts.	The repercussions of the SolarWinds hack continued to unfold, with new findings and further exploitations of the compromised systems coming to light.
2021	Attempted RNC Hack.	An unsuccessful attempt to access systems associated with the Republican National Committee
2022	Targeted attacks against Microsoft services.	Sophisticated cyber - attacks targeted Microsoft, aiming to penetrate its services and extract customer data as well as corporate secrets.
2023	Social engineering via Microsoft Teams.	APT29 executed targeted social engineering attacks through Microsoft Teams, using fake profiles and deceptive messages to manipulate targets into disclosing sensitive information.
2024	Hewlett - Packard Enterprise (HPE) Attack	Midnight Blizzard / Cozy Bear is suspected of compromising a small percentage of mailboxes of HPE employees
2024	Continued attacks on Microsoft focusing on cloud services.	Persistent and advanced cyber - attacks targeted Microsoft M365 cloud services.

4.1. Malware Attributed to Midnight Blizzard

Midnight Blizzard has a notorious reputation for their sophisticated malware and tooling. Over the years, this group has developed and deployed a variety of malware toolkits designed to infiltrate, persist, and exfiltrate sensitive information from targeted systems. These toolkits are crafted with specific functionalities to enhance the stealth and effectiveness of their operations, from initial access to data exfiltration. Below is a comprehensive list of some of the most significant malware used by Midnight Blizzard [1 - 39].

AADInternals GoldFinder PinchDuke Sliver
AdFind GoldMax PolyglotDuke SoreFang
BloodHound HAMMERTOSS POSHSPY SUNBURST
BoomBox Impacket PowerDuke SUNSPOT
CloudDuke ipconfig PsExec Systeminfo
Cobalt Strike LiteDuke QUIETEXIT Tasklist
CosmicDuke meek Raindrop TEARDROP
CozyCar Mimikatz RegDuke Tor
EnvyScout MiniDuke ROADTools TrailBlazer
FatDuke NativeZone SDelete VaporRage
FoggyWeb Net SeaDuke WellMail
GeminiDuke OnionDuke Sibot WellMess

4.2. Common Vulnerabilities Exploited

Midnight Blizzard consistently leveraged a range of vulnerabilities to execute their attacks.
Their arsenal not only includes custom - built malware but also exploits known software vulnerabilities, which they often use to escalate privileges on compromised systems and move laterally across the victim organization. The list below details some of the key vulnerabilities that Midnight Blizzard has repeatedly exploited in its attacks.

- CVE - 2020 - 1472 (Zerologon): A severe vulnerability in the Netlogon protocol allowed unauthenticated attackers with network access to domain controllers to compromise all Active Directory identity services.
- CVE - 2019 - 19781: A critical vulnerability in Citrix Application Delivery Controller (ADC) and Citrix Gateway, which allows an unauthenticated attacker to perform arbitrary code execution.
- CVE - 2020 - 0688: A Microsoft Exchange vulnerability that allows authenticated users to perform arbitrary code execution. Midnight Blizzard used this vulnerability in targeted phishing campaigns to gain initial access within an environment.
- CVE - 2017 - 0005: A vulnerability that allows remote code execution through specially crafted packets sent to Microsoft SMB servers.

4.3. Tactics, Techniques, and Procedures (TTPs)

Midnight Blizzard utilizes a diverse array of TTPs. Some of the notable ones are

- *Spear - Phishing*: Midnight Blizzard frequently utilized spear - phishing emails tailored to specific individuals or organizations. These emails may contain malicious links or attachments designed to install malware or steal credentials.
- *Supply Chain Compromise*: One of their most sophisticated methods involves tampering with the supply chain of software or hardware. This was spectacularly demonstrated in the SolarWinds Orion breach, where they inserted malicious code into legitimate software updates.
- *Exploitation of Known Vulnerabilities*: They actively exploited known security vulnerabilities in popular software and systems. This includes vulnerabilities in VPNs, remote access services, and enterprise applications.
- *Custom Malware Deployment*: Midnight Blizzard is known for creating and using custom malware, such as WellMess and WellMail, to infiltrate and control victim networks. These tools are often very well obfuscated to evade detection and provide deep access.
- *Social Engineering*: Beyond phishing, they engaged in other forms of social engineering to deceive individuals into granting access to their systems. This can include vishing (voice phishing) and exploiting trusted relationships within enterprise and M365 applications.
- *Credential Theft and Use*: After gaining initial access, they often steal credentials to move laterally within an organization by impersonating or using service accounts to access sensitive data stores.
- *Living Off the Land*: Midnight Blizzard used built - in tools and features of compromised systems to conduct their activities, reducing their malware footprint and blending in with normal network activity to avoid detection.
- *Cloud Services Exploitation*: They were adept at using public cloud services and corresponding vulnerabilities in cloud services, especially misconfigurations or compromised credentials.
- *Zero - Day Exploits*: Though they are not publicized, like many sophisticated threat actors, Midnight Blizzard is suspected of using zero - day exploits (previously unknown vulnerabilities) for highly targeted attacks.
- *Backdoor Installation*: They often install backdoors in compromised networks, allowing them persistent, covert access that can be utilized long after the initial breach has been contained or closed.

Table 2: Initial Access Methods Usage by Year [30 - 39]

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Stolen Credentials	●						●	●			
Phishing Email	●	●	●		●			●	●	●	●
Server Compromise		●									
Password Spray					●	●	●				●
Supply Chain							●				
Third Party							●	●			

4.4. SolarWinds Attack, December 2020

Midnight Blizzard's SolarWinds attack is recognized as one of the most sophisticated and severe cybersecurity breaches in history. It was executed via a supply chain attack that primarily targeted the SolarWinds Orion platform, a widely used network management software. The breach was disclosed publicly in December 2020, but the groundwork for the attack was laid much earlier. SolarWinds attack was a wakeup call for the entire cybersecurity industry about software supply chain security. Here is the time of the incident.

Table 3: SolarWinds Incident Timeline [14] [28] [32]

Date	Event	Details
13 - Dec - 20	FireEye Discovers SUNBURST	FireEye reports a breach of their red team tool set and identifies the initial attack vector, codenamed SUNBURST.
14 - Dec - 20	Large - Scale Cyber Campaign	CISA issues an alert about a large - scale compromise of multiple US agencies, with early indications of additional attack vectors leveraging SAML.
17 - Dec - 20	Hybrid Attacks on Cloud Resources	MSRC reports that adversaries also attacked cloud systems, introducing a new attack method called "Golden SAML", targeting Office 365 by leveraging SAML tokens generated by the attackers.
17 - Dec - 20	Palo Alto Networks Discovers SUPERNOVA	A second attack vector is discovered, leveraging a zero - day authentication bypass exploit in the SolarWinds product, codenamed SUPERNOVA.
25 - Dec - 20	Cloud - Only Attack Vectors Indicated	CrowdStrike reports an attempted attack against their Office 365 tenant using a supply chain attack method that leveraged credentials of a cloud reseller.
2 - Jan - 21	Scope of the Attack Grows	Reports reveal that at least 250 federal agencies and organizations were breached. Discussions about SolarWinds' cost savings from security budget cuts and moving development to Eastern Europe arise.
5 - Jan - 21	US Names Russia as Perpetrator	A joint official statement by CISA, NSA, and FBI names Russia as the likely perpetrator of the attack.

Initial Breach: The attackers first infiltrated SolarWinds' software development or build environment in early September 2019. They inserted malicious code into the Orion software updates, creating a backdoor Trojan known as SUNBURST. The malicious code was stealthily embedded into legitimate software updates released between March and June 2020. The compromised updates were unknowingly distributed to as many as 30, 000 of SolarWinds’ customers, which included numerous U. S. government agencies, critical infrastructure operators, and private organizations. Once installed, the SUNBURST malware lay dormant for two weeks, avoiding immediate detection by mimicking normal network traffic and storing reconnaissance data within legitimate plugin configuration files.

Lateral Movement: After the dormancy period, the malware would retrieve and execute commands that allowed it to transfer files, execute scripts, profile the system, reboot the machine, and disable system services. They used this capability to move laterally within the network, escalate privileges, and gain further access to other organization resources. They used the initial backdoor to install additional payloads and exploited the trust relationships between IT systems to access otherwise secured data. Notably, the attackers utilized sophisticated techniques such as modifying or creating SAML tokens (in attacks dubbed "Golden SAML") to forge authentications and access cloud resources, including email services.

Detection and Response: The breach was first identified by FireEye, a cybersecurity firm that noticed a suspicious authentication activity within their own environment. This led to the discovery of the SUNBURST backdoor. Following that, other affected organizations and cybersecurity entities began their own investigations and responses.

Impact: The scope of the attack was vast, affecting major federal agencies, including parts of the Pentagon, the Department of Homeland Security, the State Department, the National Nuclear Security Administration, and more. The attack exposed significant vulnerabilities in the supply chain and third - party software security practices. The SolarWinds attack underscores the complexity and stealth of modern cyber espionage and the lengths to which adversaries will go to gain strategic intelligence. The attack has led to increased scrutiny of supply chain security and the implementation of more rigorous software development controls.

4.5. Microsoft Attack, Jan 2024

On January 12, 2024, the Microsoft security team detected and responded to a cyberattack attributed to Midnight Blizzard. The ongoing investigation revealed that Midnight Blizzard has also targeted other organizations that promoted Microsoft to notify those entities. Armed with prior knowledge of Midnight Blizzard, Microsoft was able to identify the attack by reviewing Exchange Web Services (EWS) activity logs and their M365 audit logging features [1] [2] [31]. The following section dissects the workings of the attack. The attacker employed password spray attacks to compromise a non - production test tenant account at Microsoft, where multifactor authentication (MFA) was not enabled. This initial foothold was achieved through low - volume, targeted password spray attempts designed to evade detection. Post gaining initial access, Midnight Blizzard exploited OAuth applications by creating and modifying them to gain elevated access within Microsoft's corporate environment. These applications allowed persistent access and data extraction capabilities through the misuse of permissions like the full_access_as_app role in Office 365 Exchange Online.

The attacker utilized these OAuth applications to authenticate to Microsoft Exchange Online and target corporate email accounts for data collection. To mask their activities, Midnight Blizzard employed residential proxy networks, routing their malicious traffic through legitimate IP addresses to complicate detection efforts. Microsoft identified the attack activities by analyzing Exchange Web Services (EWS) activity and leveraging their extensive knowledge of the threat actor's tactics. M365 audit logging features played a critical role in uncovering malicious operations. In response to the attack, Microsoft quickly published advisory notifications and customer education activities about

- Auditing and reducing excessive privileges, particularly for OAuth applications.

- Implementing conditional access and continuous review of sign - in activities.
- Enhancing detection capabilities against sophisticated obfuscation techniques used by Midnight Blizzard.

Investigations are ongoing about further attacks on Microsoft customers using the sensitive data acquired through this attack.

5. Recommendations to Defend

Midnight Blizzard demonstrated their prowess through advanced, targeted attacks against various high - profile targets, including government institutions and major corporations. They are the poster child for powerful and state - sponsored advanced persistent threats. They employ a diverse array of tactics and technologies to infiltrate and persist within their targets' systems. The group's operations vividly illustrate that there is no "silver bullet to defend against such a well - resourced adversary [14] [15].

Defending against Midnight Blizzard demands a comprehensive approach that combines basic security hygiene with advanced security capabilities. Organizations must adopt a layered security strategy that encompasses not only basic cybersecurity practices but also employs advanced capabilities and processes to counter sophisticated threat actors like Midnight Blizzard. This section will explore best practices to enhance organizational resilience against Midnight Blizzard's efforts.

5.1 Strengthen Identity and Access Management (IAM) Posture

- Implement Multi - Factor Authentication (MFA): Ensure that MFA is enabled across all systems, particularly for accounts with elevated privileges or access to sensitive data.
- Use Least Privilege Principle: Limit user and application access rights to the minimum necessary to perform their tasks. Regularly review and adjust permissions.
- Audit User and Service Accounts: Regularly review user and service accounts for any anomalies or unnecessary privileges. Disable or remove obsolete accounts.

5.2 Enhance Endpoint and Network Security Posture

- Deploy Endpoint Detection and Response (EDR): Use advanced EDR tools to monitor for suspicious activities and potential breaches.
- Segment Networks: Use network segmentation to limit lateral movement by an attacker within the network.
- Monitor and Control Network Traffic: Implement tools to inspect and control inbound and outbound network traffic, looking for signs of malicious activity.

5.3 Email and Cloud Applications Security Posture

- Protect Email Gateways: Use advanced email security solutions that can filter phishing attempts, malicious attachments, and links.
- Audit OAuth Applications: Regularly review and audit OAuth applications for unusual or excessive permissions. Restrict the registration of new OAuth applications as necessary.
- Implement Cloud Security Posture Management (CSPM): Use CSPM tools to identify misconfigurations and compliance risks in cloud environments.

5.4 Incident Response and Threat Hunting

- Comprehensive Incident Response Plan: Ensure that the incident response plan is updated regularly and includes procedures for dealing with ransomware and state - sponsored attacks.
- Conduct Regular Tabletops: Test the incident response plan with tabletop exercises and red teaming activities to assess the readiness of the response team.
- Proactive Threat Hunting: Establish a threat hunting team tasked with actively searching for advanced threats that may evade traditional detection.

5.5 Advanced Security Capabilities

- Apply Behavioral Analytics: Use security solutions that incorporate user and entity behavior analytics (UEBA) to detect unusual behavior patterns that might indicate a breach.
- Embrace Zero Trust Network Access (ZTNA) Approach: Move away from the "Trust but verify model" to the "Don't trust and verify" model. ZTNA significantly reduces the attack surface and limits lateral movements as well.

5.6 Basic Security Hygiene

- Keep Software Updated: Regularly update all software to patch known vulnerabilities that could be exploited by attackers.
- Vulnerability Management Program: Regularly scan for vulnerabilities in the IT infrastructure and prioritize remediation based on the risk profile.

6. Conclusion

The detailed examination of Midnight Blizzard within this paper provides a comprehensive understanding of their tactics, techniques, and procedures. By dissecting past incidents and highlighting recurring patterns of behavior, this analysis provides organizations with the knowledge needed to anticipate and counter future threats posed by such advanced persistent threats. Their sophisticated use of malware, exploitation of software vulnerabilities, and the orchestration of complex spear - phishing and supply chain attacks demonstrate their high level of technical competence; understanding these are important for developing effective defensive strategies. Organizations must implement a robust security framework that combines rigorous security hygiene with advanced security capabilities. The insights provided in this paper are actionable and serve as a guide, too. These actionable insights are intended to empower organizations to defend against the specific TTPs used by this group and to bolster their defenses against the broader spectrum of cyber threats they may face from APTs.

References

[1] Microsoft Threat Intelligence. (2024). Midnight Blizzard: Guidance for responders on nation - state attack. Retrieved from https: //www.microsoft. com/en - us/security/blog/2024/01/25/midnight - blizzard - guidance - for - responders - on - nation - state - attack/

[2] Microsoft Threat Intelligence. (2023). Midnight Blizzard conducts targeted social engineering over Microsoft Teams. Retrieved from https: //www.microsoft. com/en - us/security/blog/2023/08/02/midnight - blizzard - conducts - targeted - social - engineering - over - microsoft - teams/

[3] Microsoft Security Team. (2021, December 15). A report on NOBELIUM's unprecedented nation - state attack. Microsoft Security Blog. https: //www.microsoft. com/en - us/security/blog/2021/12/15/a - report - on - nobeliums - unprecedented - nation - state - attack/

[4] Microsoft Security Team. (2022, August 24). MagicWeb: NOBELIUM's post - compromise trick to authenticate as anyone. Microsoft Security Blog. https: //www.microsoft. com/en - us/security/blog/2022/08/24/magicweb - nobeliums - post - compromise - trick - to - authenticate - as - anyone/

[5] Mandiant Team. (2024). Abusing replication: Stealing ADFS secrets over the network. Mandiant. Retrieved from https: //www.mandiant. com/resources/blog/abusing - replication - stealing - adfs - secrets - over - the - network

[6] Mandiant. (2022, August). Remediation & hardening strategies for M365 to defend against APT29. Mandiant. https: //www.mandiant. com/sites/default/files/2022 - 08/remediation - hardening - strategies - for - m365 - defend - against - apt29 - white - paper. pdf

[7] CrowdStrike. (2023). Cozy Bear on the prowl. CrowdStrike. Retrieved from https: //www.crowdstrike. com/resources/crowdcasts/cozy - bear - on - the - prowl/

[8] SOC Radar. (n. d.). APT Profile: Cozy Bear (APT29). SOC Radar. Retrieved from https: //socradar. io/apt - profile - cozy - bear - apt29/

[9] CrowdStrike. (2021, June 10). How CrowdStrike protects against recent Cozy Bear phishing campaign. CrowdStrike Blog. Retrieved from https: //www.crowdstrike. com/blog/how - crowdstrike - protects - against - recent - cozy - bear - phishing - campaign/

[10] Cybersecurity and Infrastructure Security Agency (CISA). (2024). CISA directs federal agencies to immediately mitigate significant risk from Russian state - sponsored cyber activity. CISA. Retrieved from https: //www.cisa. gov/news - events/news/cisa - directs - federal - agencies - immediately - mitigate - significant - risk - russian - state - sponsored - cyber

[11] Obsidian Security. (2024). Lessons learned from the Microsoft breach by Midnight Blizzard. Obsidian Security. Retrieved from https: //www.obsidiansecurity. com/lessons - learned - from - the - microsoft - breach - by - midnight - blizzard/

[12] AttackIQ. (no data.). CISO guide to APT29. AttackIQ. Retrieved from https: //go. attackiq. com/rs/041 - FSQ - 281/images/CISO_Guide_APT29. pdf

[13] National Security Agency (NSA). (2023). Russian cyber actors target cloud - hosted infrastructure. NSA. Retrieved from https: //www.nsa. gov/Press - Room/Press - Releases - Statements/Press - Release - View/Article/3686651/russian - cyber - actors - target - cloud - hosted - infrastructure/

[14] Orca Security. (n. d.). How to defend against APT29 (Cozy Bear) attacks. Orca Security Blog. Retrieved from https: //orca. security/resources/blog/how - to - defend - against - apt29 - cozy - bear - attacks/

[15] The White House. (2021, April 15). Fact sheet: Imposing costs for harmful foreign activities by the Russian government. Retrieved from https: //www.whitehouse. gov/briefing - room/statements - releases/2021/04/15/fact - sheet - imposing - costs - for - harmful - foreign - activities - by - the - russian - government/

[16] Government of the United Kingdom. (2021, April 15). Russia: UK and US expose global campaigns of malign activity by Russian intelligence services. Retrieved from https: //www.gov. uk/government/news/russia - uk - and - us - expose - global - campaigns - of - malign - activity - by - russian - intelligence - services

[17] F - Secure Labs. (2015, September 17). The Dukes: 7 years of Russian cyberespionage. Retrieved from https: //www.f - secure. com/documents/996508/1030745/dukes_whitepaper. pdf

[18] Department of Homeland Security and Federal Bureau of Investigation. (2016, December 29). GRIZZLY STEPPE – Russian malicious cyber activity. Retrieved from https: //www.us - cert. gov/sites/default/files/publications/JAR_16 - 20296A_GRIZZLY%20STEPPE - 2016 - 1229. pdf

[19] Alperovitch, D. (2016, June 15). Bears in the midst: Intrusion into the Democratic National Committee. CrowdStrike. Retrieved from https: //www.crowdstrike. com/blog/bears - midst - intrusion - democratic - national - committee/

[20] Government of the United Kingdom. (2021, April 15). UK exposes Russian involvement in SolarWinds cyber compromise. Retrieved from https: //www.gov. uk/government/news/russia - uk - exposes - russian - involvement - in - solarwinds - cyber - compromise

[21] National Security Agency, Federal Bureau of Investigation, Department of Homeland Security. (2021, April 15). Russian SVR targets U. S. and allied networks. Retrieved from https: //media. defense. gov/2021/Apr/15/2002621240/ - 1/ - 1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021. PDF

[22] UK National Cyber Security Centre. (2021, April 15). UK and US call out Russia for SolarWinds compromise. Retrieved from https: //www.ncsc. gov. uk/news/uk - and - us - call - out - russia - for - solarwinds - compromise

[23] FireEye. (2020, December 13). Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims with SUNBURST backdoor. Retrieved from https: //www.fireeye. com/blog/threat -

research/2020/12/evasive - attacker - leverages - solarwinds - supply - chain - compromises - with - sunburst - backdoor. html

[24] Microsoft Security Blog. (2021, March 4). GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's layered persistence. Retrieved from https: //www.microsoft. com/security/blog/2021/03/04/goldmax - goldfinder - sibot - analyzing - nobelium - malware/

[25] CrowdStrike. (2021, January 11). SUNSPOT: An implant in the build process. Retrieved from https: //www.crowdstrike. com/blog/sunspot - malware - technical - analysis/

[26] Volexity. (2020, December 14). Dark Halo leverages SolarWinds compromise to breach organizations. Retrieved from https: //www.volexity. com/blog/2020/12/14/dark - halo - leverages - solarwinds - compromise - to - breach - organizations/

[27] UK National Cyber Security Centre. (2021, May 7). Further TTPs associated with SVR cyber actors. Retrieved from https: //www.ncsc. gov. uk/files/Advisory - further - TTPs - associated - with - SVR - cyber - actors. pdf

[28] Palo Alto Networks Unit 42. (2020, December 23). SolarStorm supply chain attack timeline. Retrieved from https: //unit42. paloaltonetworks. com/solarstorm - supply - chain - attack - timeline/

[29] SentinelOne Labs. (2021, June 1). NobleBaron | New poisoned installers could be used in supply chain attacks. Retrieved from https: //labs. sentinelone. com/noblebaron - new - poisoned - installers - could - be - used - in - supply - chain - attacks/

[30] CrowdStrike. (2022, January 27). Early bird catches the wormhole: Observations from the StellarParticle campaign. Retrieved from https: //www.crowdstrike. com/blog/observations - from - the - stellarparticle - campaign/

[31] Microsoft Threat Intelligence Center (MSTIC). (2021, May 27). New sophisticated email - based attack from NOBELIUM. Retrieved from https: //www.microsoft. com/security/blog/2021/05/27/new - sophisticated - email - based - attack - from - nobelium/

[32] Microsoft Security Blog. (2021, May 28). Breaking down NOBELIUM's latest early - stage toolset. Retrieved from https: //www.microsoft. com/security/blog/2021/05/28/breaking - down - nobeliums - latest - early - stage - toolset/

[33] Microsoft Security Response Center (MSRC). (2021, June 25). New NOBELIUM activity. Retrieved from https: //msrc - blog. microsoft. com/2021/06/25/new - nobelium - activity/

[34] Microsoft Defender Research Team. (2018, December 3). Analysis of cyberattack on U. S. think tanks, non - profits, public sector by unidentified attackers. Retrieved from https: //www.microsoft. com/security/blog/2018/12/03/analysis - of - cyberattack - on - u - s - think - tanks - non - profits - public - sector - by - unidentified - attackers/

[35] ESET Research. (2019, October). OPERATION GHOST: The Dukes aren't just a band from the 70s. Retrieved from https: //www.welivesecurity. com/wp - content/uploads/2019/10/ESET_Operation_Ghost_Dukes. pdf

[36] UK National Cyber Security Centre. (2020, July 16). Advisory: APT29 targets COVID - 19 vaccine development. Retrieved from https: //www.ncsc. gov. uk/files/Advisory - APT29 - targets - COVID - 19 - vaccine - development - V1 - 1. pdf

[37] PwC UK. (2020, July 16). How WellMess malware has been used to target COVID - 19 vaccines. Retrieved from https: //www.pwc. co. uk/issues/cyber - security - services/insights/cleaning - up - after - wellmess. html

[38] PwC UK. (2020, August 17). WellMess malware: Analysis of its Command and Control (C2) server. Retrieved from https: //www.pwc. co. uk/issues/cyber - security - services/insights/wellmess - analysis - command - control. html

[39] Mandiant. (2020, April 27). Assembling the Russian Nesting Doll: UNC2452 Merged into APT29. Retrieved from https: //www.mandiant. com/resources/blog/unc2452 - merged - into - apt29