**Final CTI Report: Cozy Bear (APT29)**

Ismael A. Rodriguez

The University of Arizona

CYBV435 Cyber Threat Intelligence

John Barker

10/15/2024

**Overview of APT29**

APT29, also known as Cozy Bear, is a sophisticated Russian state-sponsored advanced persistent threat (APT) group believed to be linked to Russia's Foreign Intelligence Service (SRV). It has been active since at least the mid-2000s and is known for conducting cyber espionage operations targeting government entities, political organizations, and private-sector institutions across various industries worldwide. It is one of the most notorious cyber espionage groups, often operating alongside other Russian-affiliated APT groups like APT28 (Fancy Bear).

APT29 gained significant attention for its involvement in high-profile cyber espionage campaigns, most notably during the 2016 U.S. presidential election. However, its operations trace back further, with activity observed as early as 2008, when it initially targeted Western governments and defense contractors. Over time, the group has evolved its tactics, techniques, and procedures (TTPs) to remain effective against modern security measures and maintain stealth through sophisticated malware and evasion tactics. Cozy Bear is known for its highly targeted spear-phishing campaigns and customized malware to gain access to and persist within the network and living off the land using legitimate software and tools available on the target's system to blend in with regular activity, making detection more difficult.  The group employs a variety of techniques to achieve its objectives.

One of the critical aspects of APT29s success has been its ability to remain under the radar for extended periods, often maintaining persistent access to networks for years without detection. The group has been highly adaptive, evolving from simple phishing campaigns to advanced techniques such as supply chain attacks and exploiting vulnerabilities in cloud services. In 2015, Cozy Bear, also known as APT29, was implicated in breaking the networks for the White House and the U.S. State Department. This operation demonstrated the group's ability to infiltrate high-value targets and remain undetected

for significant periods. During the 2016 U.S. elections, Cozy Bear and APT28 were involved in cyberattacks on the Democratic National Committee (DNC). While APT28 focused more on releasing stolen information, Cozy Bear's operations were stealthier, likely aiming to gather intelligence rather than disrupt.

## Allegiances and Nation-State Sponsor

APT29, also known as Cozy Bear, is widely believed to be closely tied to the Russian government, specifically the Foreign Intelligence Service (SRV), Russia's premier civilian intelligence agency. This connection to the SRV places APT29 at the heart of Russia's broader geopolitical and intelligence-gathering apparatus. As a successor to the KGB's foreign intelligence branch, the SRV is responsible for espionage outside Russia, including intelligence gathering on foreign governments, industries, and individuals. Cozy Bear operates as an extension of this mission, focusing on cyber espionage to support Russia's strategic interests globally.

The connection between APT29 and the Russian SVR has been substantiated by multiple cybersecurity firms and intelligence agencies, including the U.S. National Security Agency (NSA), the U.K.'s National Cyber Security Centre (NCSC), and the Canadian Communications Security Establishment (CSE). These agencies have released joint statements attributing APT29's operations to Russian state-sponsored cyber espionage efforts. The SVR's sponsorship of APT29 means that the group's operations are tightly aligned with the Kremlin's foreign policy objectives. APT29 conducts campaigns designed to bolster Russia's strategic positioning.

APT29's primary targets include Western governments, international organizations, and defense contractors, focusing on gathering intelligence that could provide Russia with a competitive advantage in diplomatic negotiations and global decision-making. The group's operations often seek to acquire intellectual property and research, particularly in high-tech industries such as energy, defense, and, more recently, healthcare, as evidenced by their attempts to steal COVID-19 vaccine data.

By penetrating the networks of Western nations, APT29 enables Russia to access sensitive data that could shift the balance of power in international negotiations. This intelligence is valuable in fields such as military strategy, foreign policy, and economic planning, allowing Russia to anticipate and counter the moves of rival nations. Cozy Bear's involvement in attacks like the 2016 DNC breach, although primarily focused on espionage, helped fuel a narrative of foreign interference in democratic processes. This plays into broader Russian objectives to undermine trust in Western institutions, creating internal discord that benefits Moscow's strategic interests. In addition, by stealing intellectual property and technological research, particularly from industries like healthcare and energy, APT29 enables Russia to close technological gaps without requiring direct innovation. This has been particularly evident in their targeting of COVID-19 vaccine research, which aimed to give Russia a geopolitical and economic advantage during the global pandemic.

**Industries/Organizations Targeted by APT29**

APT29, also known as Cozy Bear, is a group primarily focused on espionage. They carefully select targets based on the strategic interests of the Russian state. The group has been observed targeting various sectors and organizations, emphasizing industries that offer high-value intelligence, critical infrastructure, and sensitive geopolitical information.

**1. Government and Diplomatic Entities**

APT29 primarily focuses on gathering intelligence from government institutions and diplomatic organizations. These targets provide the group with critical political, military, and policy-related data.

- **U.S. Government Agencies (2014-2015)**: One of APT29's most notorious attacks involved the breaches of the White House and the U.S. State Department in 2014 and 2015. In these attacks, APT29 managed to infiltrate unclassified email systems, gaining access to sensitive U.S. foreign policy and diplomatic communications information.
- **Norwegian Parliament Attack (2020)**: In 2020, APT29 was linked to a cyberattack on Storting, the Norwegian parliament. This breach targeted the email accounts of parliament members and employees, potentially seeking intelligence on Norway's political decision-making and international relations.

**2. Political Organizations**

APT29 has shown a keen interest in political entities, particularly during heightened political activity, such as elections.

- **Democratic National Committee (DNC) Hack (2016)**: In one of its most famous operations, APT29, alongside APT28 (Fancy Bear), was involved in the hacking of the **DNC** during the 2016 U.S. presidential election. While APT28's goal appeared to be influencing the election outcome through information leaks, APT29's operations were likely focused on gathering political intelligence and understanding the strategies of U.S. political leaders.
- **German Bundestag Attack (2015)**: In 2015, Cozy Bear reportedly compromised the **German Bundestag**, targeting email accounts of members of parliament. This attack was part of a broader campaign targeting European political entities aimed at collecting intelligence on EU policies and internal discussions.

**3. Healthcare and Research Institutions**

Recently, APT29 has expanded its operations to include healthcare and research institutions, especially considering global crises such as the COVID-19 pandemic.

- **COVID-19 Vaccine Research Targeting (2020)**: During the COVID-19 pandemic, the UK's National Cyber Security Centre (NCSC), the U.S. NSA, and Canada's CSE accused APT29 of attempting to steal vaccine research from organizations in all three countries. Targets included pharmaceutical companies and research institutions involved in developing vaccines and treatments for COVID-19. This effort demonstrated Russia's interest in acquiring vaccine data to gain a geopolitical advantage in managing the pandemic.
- **Healthcare and Biomedical Targets (Ongoing)**: Besides COVID-19-related activities, APT29 has a broader interest in the healthcare sector. It targets institutions conducting cutting-edge biomedical research and healthcare systems in various countries, particularly those in NATO states. The goal is often to steal proprietary information on treatments, research, and medical technologies.

**4. Defense and Military Contractors**

APT29 has consistently targeted defense contractors and military organizations to collect intelligence on adversary nations' weapon systems, defense strategies, and military capabilities.

- **U.S. Defense Contractors**: In various campaigns, APT29 has targeted U.S. defense contractors to gather intelligence on technologies related to **aerospace, military communications, and weapons systems**. These efforts allow the Russian government to close gaps in its military development by leveraging stolen research and technological advancements from Western companies.

- **European Defense Targets**: APT29 has also been involved in attacks on European defense contractors. These companies often have access to sensitive military technologies and intelligence shared between NATO allies, making them prime targets for espionage.

**5. Energy Sector**

The energy sector has long been an exciting area for APT29, as Russia seeks to maintain its dominance in global energy markets and understand rival nations' energy policies.

- **Oil and Gas Companies**: APT29 has targeted oil and gas companies worldwide, especially in Europe and North America. These attacks aim to gather intelligence on energy production, exploration data, and future projects. For example, Cozy Bear has been linked to efforts to infiltrate **Norwegian oil and gas companies**, likely to obtain data on exploration in the Arctic, an area of strategic importance to Russia.
- **Energy Infrastructure**: The group has also been observed targeting organizations involved in critical energy infrastructure, including nuclear power facilities. These operations help Russia gain insights into the vulnerabilities of energy grids and potentially disrupt energy supplies if needed during geopolitical conflict.

**6. Technology and Telecommunications**

APT29 frequently targets high-tech companies and telecommunications organizations to obtain intellectual property, trade secrets, and sensitive communications data.

- **SolarWinds Breach (2020)**: One of the largest and most significant cyber espionage campaigns linked to APT29 involved the **SolarWinds supply chain attack** in 2020. The group compromised SolarWinds' Orion software, which thousands of companies and government organizations use globally. This allowed APT29 to gain backdoor access to the networks of numerous high-

profile targets, including government agencies, critical infrastructure, and private sector companies.

- **Telecommunications Industry**: APT29 is vested in targeting telecommunications companies, especially those providing secure communications for government officials and military personnel. These attacks help Russia intercept communications and gain valuable insights into adversaries' strategies and operations.

## Motives and Goals of APT29

APT29, also known as Cozy Bear, operates with clear, strategic motivations rooted in the geopolitical interests of the Russian Federation. As an advanced persistent threat (APT) group linked to the Russian Foreign Intelligence Service (SVR), APT29's actions serve the intelligence-gathering and security needs of the Russian state. The group's activities are not random but are part of a larger framework designed to advance Russia's influence, national security, and competitive position on the global stage. Below is a detailed explanation of APT29's core motives and goals linked to Russia's broader geopolitical objectives.

### 1. Intelligence Gathering for Strategic Advantage

APT29’s primary motivation is acquiring valuable intelligence from many high-profile targets. This intelligence directly supports the Russian government's foreign policy, military strategy, and economic competitiveness.

- **Government and Political Intelligence**: APT29 focuses on penetrating government institutions and political organizations, gathering data on foreign policy strategies, military operations, diplomatic discussions, and internal government communications. This intelligence enables Russia to stay ahead of geopolitical developments, anticipate adversaries' actions, and

strengthen its diplomatic standing. For example, in the **2016 DNC hack**, Cozy Bear sought political insights and strategies that could benefit Russian intelligence in navigating U.S. political dynamics.

- **Defense and Military Intelligence**: Another key motive of APT29 is to steal military and defense-related information. This includes research on advanced weapons systems, military communication technologies, and defense strategies. By compromising defense contractors and military entities, APT29 provides Russia with critical knowledge that can be used to close technological gaps and anticipate military moves from NATO allies and other geopolitical rivals.

**2. Economic and Technological Superiority**

APT29's espionage campaigns frequently target industries where Russia seeks to gain an economic or technological advantage. These include the healthcare, energy, and telecommunications sectors, among others.

- **Stealing Intellectual Property**: One of the group's central objectives is to obtain intellectual property from cutting-edge companies and research institutions, enabling Russia to advance its economic and technological capabilities without needing independent innovation. For instance, the **2020 campaign targeting COVID-19 vaccine research** was a clear example of APT29's efforts to gather proprietary scientific data, potentially giving Russia an edge in global vaccine development and distribution during a crisis.
- **Energy and Resource Dominance**: Energy security is a cornerstone of Russian foreign policy. Cozy Bear's attacks on oil and gas companies and energy infrastructure align with Russia's goal of controlling global energy markets. By obtaining insights into rival nations' energy strategies and infrastructure vulnerabilities, Russia can secure its position as a dominant energy supplier, particularly in Europe and Asia.

### 3. Strengthening Russia's Cyber Capabilities

APT29's operations contribute directly to Russia's broader goal of establishing cyber dominance. Cyber espionage is a crucial component of modern geopolitical warfare, and APT29 plays a key role in Russia's efforts to enhance its offensive and defensive cyber capabilities.

- **Long-Term Persistence in Networks**: APT29 maintains undetected, long-term access to critical networks. This persistence enables the group to siphon off valuable data over months or even years continuously. The **SolarWinds attack in 2020**, which compromised numerous U.S. government agencies and private companies, highlighted the group's capacity to gain sustained access to sensitive networks, giving Russia a long-term intelligence advantage.
- **Building Cyber Warfare Expertise**: APT29 helps Russia hone its cyber espionage and warfare expertise by continuously executing complex cyber operations. Each successful campaign meets immediate intelligence needs and advances Russia's broader objective of building a highly skilled and formidable cyber force capable of disrupting adversary networks and defending its systems against foreign attacks.

### 4. Undermining Western Alliances and Democratic Institutions

APT29's operations often align with Russia's broader geopolitical objective of weakening Western alliances and undermining trust in democratic institutions.

- **Sowing Discord in Democracies**: While APT29 primarily focuses on espionage, its operations indirectly support efforts to destabilize democracies. For example, during the **2016 U.S. presidential election**, Cozy Bear's infiltration of the DNC contributed to a more extensive Russian campaign to interfere in U.S. political processes. Although APT29 was more focused on

intelligence gathering than influencing public opinion directly (unlike APT28), its actions nonetheless played a role in undermining trust in electoral systems and sowing political discord.

- **Targeting NATO and EU Allies**: APT29 has a history of targeting NATO members and EU countries, particularly those with strong ties to the United States. By gathering intelligence on NATO operations, diplomatic strategies, and defense planning, Russia seeks to exploit divisions within these alliances and weaken their collective ability to respond to Russian aggression or influence. For example, the **2015 attack on the German Bundestag** was part of a more significant effort to gain insights into European political decision-making, potentially helping Russia to anticipate or counteract NATO strategies.

**5. Protecting Russia's Global Position**

At the heart of APT29's operations is the overarching goal of preserving and enhancing Russia's global standing, particularly in the face of perceived threats from Western powers. Cyber espionage provides Russia a low-cost, high-impact method of achieving this without resorting to open conflict.

- **Countering Western Influence**: Russia views Western democracies, particularly the U.S. and its NATO allies, as adversaries seeking to diminish Russia's global influence. Cozy Bear's operations support the Russian government's efforts to counteract Western policies, particularly those that challenge Russian dominance in Eastern Europe and the former Soviet states. By collecting intelligence on Western governments and organizations, APT29 allows Russia to anticipate and mitigate potential threats to its geopolitical interests.
- **Securing Russia's Sphere of Influence**: Finally, APT29's cyber espionage activities contribute to Russia's broader goal of securing its influence, particularly in regions like Eastern Europe, Central Asia, and the Middle East. APT29 helps Russia control areas critical to its security and economic interests by obtaining intelligence that informs Russian diplomatic and military strategies.

## Tactics, Techniques, and Tools (TTPs)

APT29, also known as Cozy Bear, is recognized for its sophisticated tactics, techniques, and tools (TTPs) used in cyber espionage operations. The group continuously evolves its methods to remain stealthy, persistent, and practical, enabling it to target high-value organizations without detection for extended periods. Below is a comprehensive explanation of APT29's key TTPs, including examples of specific malware and attack methods that have made the group one of the most dangerous and adaptable cyber espionage actors.

### 1. Initial Access: Spear-Phishing

APT29's operations often begin with highly targeted spear-phishing campaigns. The group sends deceptive emails that lure recipients into downloading malware or clicking on malicious links that initiate the attack chain. Spear-phishing remains one of the most effective techniques for gaining an initial foothold within a target organization.

- **Spear-Phishing with Malicious Attachments**: APT29 often sends emails with seemingly legitimate attachments (e.g., Word or Excel documents) embedded with malware. Upon opening the attachment, the malware executes, giving the attackers an entry point into the victim's network. In one campaign, APT29 used a spear-phishing email disguised as an update on COVID-19, which contained malicious documents that exploited vulnerabilities in Microsoft Office.
- **Spear-Phishing Links**: Instead of attachments, Cozy Bear sometimes embeds malicious links within the email. When clicked, the link redirects the victim to a compromised website that installs malware on their system. APT29 has been known to use this technique in attacks against

government and research institutions, particularly during election periods and times of global crisis.

**2. Custom Malware and Exploits**

APT29 is notorious for developing and using custom malware families tailored for espionage and stealthy network infiltration. These malware tools are designed to evade detection and maintain persistence in the target network.

- **CozyDuke (MiniDuke)**: CozyDuke is one of the most well-known malware families associated with APT29. This tool is a sophisticated backdoor to maintain long-term access to the victim's network. CozyDuke is delivered via spear-phishing emails, allowing attackers to execute arbitrary commands on infected systems and enabling data exfiltration and system manipulation. It was famously used during APT29's attacks on U.S. government entities in 2015.
- **CloudDuke (OfficeMon)**: CloudDuke is another tool frequently used by APT29. It primarily targets cloud services and cloud-hosted infrastructure. This malware takes advantage of vulnerabilities in cloud environments, allowing attackers to compromise sensitive systems while evading traditional network security measures. CloudDuke was observed during campaigns targeting Western government agencies and defense contractors.
- **WellMess and WellMail**: These malware variants were used in APT29's 2020 campaign targeting COVID-19 vaccine research. WellMess is a lightweight, customizable malware designed to exfiltrate data from infected systems, while WellMail is used for command-and-control communications between compromised devices and attacker infrastructure.

**3. Command and Control (C2) Infrastructure**

APT29 leverages complex command-and-control (C2) mechanisms to maintain communication with compromised systems without detection. It frequently uses multi-stage C2 infrastructure to ensure its malware operates covertly and can persist within a network for extended periods.

- **Domain Fronting**: APT29 uses domain fronting, which disguises malicious traffic as legitimate by routing it through well-known cloud services like **Google Cloud** or **Amazon Web Services (AWS)**. This makes it difficult for security tools to distinguish between legitimate traffic and malicious activity. Domain fronting was observed in the **SolarWinds supply chain attack**, where APT29 used this technique to communicate with the backdoors they had implanted in compromised networks.
- **Encryption for C2 Communications**: Cozy Bear uses advanced encryption techniques for their C2 communications, ensuring that even if their traffic is detected, it is challenging for defenders to decipher the contents. The group often rotates C2 domains and uses multiple layers of obfuscation to complicate detection efforts further.

**4. Lateral Movement**

Once inside a network, APT29 employs various tactics to move laterally across systems, expanding its reach within the target organization. The group uses legitimate tools and credentials to blend in with regular network activity, making it harder for security teams to detect suspicious behavior.

- **Credential Dumping**: Cozy Bear frequently uses tools such as **Mimikatz** to extract credentials from compromised systems. APT29 can quickly move across a network and access sensitive data without triggering alarms by obtaining user credentials, especially those with administrative privileges.
- **Pass-the-Hash and Pass-the-Ticket Attacks**: After stealing credentials, APT29 employs techniques like **Pass-the-Hash** and **Pass-the-Ticket** to authenticate themselves on other

machines without needing the actual password. These methods allow the group to elevate privileges and further infiltrate the network.

- **Living off the Land**: APT29 is known for "living off the land," using legitimate administrative tools and system commands (e.g., PowerShell, WMI) already in the environment. By relying on native system tools, the group minimizes the need for additional malware, making their operations more difficult to detect. This technique was used extensively in the **2015 attack on the U.S. State Department**, where APT29 used PowerShell scripts to control compromised systems.

**5. Persistence Mechanisms**

APT29 excels at maintaining long-term access to target networks. The group uses multiple techniques to ensure it can continue operations even if some aspects of its campaign are detected and removed.

- **Persistence via Scheduled Tasks**: One of APT29's standard persistence techniques involves creating scheduled tasks or registry entries that automatically execute malware upon system startup. This allows them to re-establish their foothold even if the initial infection is detected and removed.
- **Domain Persistence**: In some instances, APT29 compromises the victim's domain controllers, giving them profound control over the network. This method was observed in the **2014-2015 White House and State Department breaches**, where the group maintained persistence even after the network was partially remediated.

**6. Data Exfiltration**

APT29 prioritizes stealth during data exfiltration, using various methods to discreetly steal valuable information without triggering security alerts.

- **Encrypted Exfiltration**: APT29 typically encrypts stolen data before exfiltrating it from the network. This ensures that even if the traffic is intercepted, the contents are indecipherable to defenders. Cozy Bear often exfiltrates data in small chunks over extended periods to avoid raising suspicion.
- **Exfiltration via Cloud Services**: APT29 often exfiltrates data through cloud services like **Dropbox** or **Google Drive**. Using standard and trusted services, the group can hide in plain sight, making it difficult for network defenders to spot malicious traffic.

**7. Exploiting Supply Chains**

APT29 is known for its ability to conduct sophisticated supply chain attacks, where they compromise a trusted software provider to gain access to multiple downstream targets. The most prominent example of this is the **SolarWinds attack**.

- **SolarWinds Supply Chain Attack (2020)**: APT29 successfully compromised the **SolarWinds Orion** software update mechanism, injecting a backdoor into the updates that were pushed to thousands of SolarWinds customers, including U.S. government agencies, critical infrastructure, and private corporations. This supply chain attack gave APT29 access to numerous high-value targets with a single breach, demonstrating their ability to conduct large-scale operations with significant geopolitical impact.

## Kill-Chain Analysis

The Cyber Kill Chain is a framework developed by Lockheed Martin that outlines the stages of a cyber-attack, from reconnaissance to exfiltration. APT29, also known as Cozy Bear, follows a

sophisticated attack methodology that covers all stages of the kill chain, allowing them to conduct long-term espionage operations while remaining undetected. Below is a detailed mapping of APT29's operations across all stages of the kill chain, along with clear examples from past attacks.

**1. Reconnaissance**

APT29 gathers information about potential targets in the reconnaissance phase to determine the best attack approach. This phase is crucial for identifying weaknesses in target networks and selecting a suitable attack vector.

- **Example**: Before launching spear-phishing attacks, APT29 conducts extensive open-source intelligence (OSINT) gatherings on the employees of targeted organizations. This includes mining social media, LinkedIn profiles, and public websites for personal information that can be used to craft convincing phishing emails. For instance, in the **2016 DNC hack**, APT29 gathered detailed information about key staff members and their communication patterns, which they then used to create targeted spear-phishing campaigns.

**2. Weaponization**

After gathering sufficient information, APT29 proceeds to the weaponization phase, where it develops or selects a malicious payload, such as malware or exploit kits, to use in the attack. APT29 is known for creating custom malware tailored to its specific targets.

- **Example**: In the **SolarWinds attack (2020)**, APT29 injected a backdoor called **SUNBURST** into a legitimate software update for SolarWinds' Orion platform. This backdoor was designed to be highly stealthy, allowing the group to infiltrate multiple high-profile organizations with a single supply chain compromise.

**3. Delivery**

Delivery involves transmitting the weaponized payload to the target, often through phishing emails, compromised websites, or infected software updates. APT29 has used various delivery mechanisms depending on the target's vulnerabilities.

- **Example**: APT29 is known for its **spear-phishing** campaigns, where malicious attachments or links are delivered via email. For instance, during their **attack on U.S. State Department and White House networks in 2014-2015**, Cozy Bear sent spear-phishing emails with malicious links, which, when clicked, executed malware on the recipients' machines.
- **Supply Chain Attacks**: The SolarWinds supply chain attack used a more sophisticated delivery method. By compromising SolarWinds' software update system, APT29 delivered its malware to thousands of customers who trusted SolarWinds as a legitimate vendor.

**4. Exploitation**

Once the malicious payload is delivered, the exploitation phase begins. This is where APT29 takes advantage of vulnerabilities or misconfigurations within the target system to execute their malware or gain further access.

- **Example**: APT29 exploits software or human behavior vulnerabilities in many attacks. In the **SolarWinds attack**, once the backdoor (SUNBURST) was delivered, it exploited the fact that SolarWinds software had high-level access across numerous systems, allowing the malware to execute and establish a foothold without triggering alarms.
- **Zero-Day Exploits**: In other campaigns, APT29 has used **zero-day exploits** in Microsoft Office and other software to execute malicious code, particularly during spear-phishing campaigns that involve weaponized document attachments.

**5. Installation**

During the installation phase, APT29 establishes a persistent presence within the target network by installing malware that allows them to maintain access over an extended period, even after initial detection attempts.

- **Example**: APT29 often installs custom malware such as **CozyDuke** or **CloudDuke** to establish persistence in target networks. In the **2015 White House and State Department breaches**, APT29 installed malware to maintain access for months without detection, facilitating continuous data collection and system monitoring.
- **WellMess and WellMail**: In the **COVID-19 vaccine research attacks (2020)**, APT29 installed lightweight malware tools like **WellMess** and **WellMail**, which were designed for data exfiltration and communication with command-and-control (C2) servers, allowing for prolonged espionage activities.

**6. Command and Control (C2)**

In the C2 phase, APT29 establishes communication between the infected systems and their remote servers, allowing them to issue commands, control the malware, and extract data from compromised networks.

- **Example**: APT29 uses sophisticated **command-and-control (C2) infrastructure** that is multi-layered and often obfuscated through techniques like **domain fronting**. In the **SolarWinds attack**, APT29 used trusted cloud services like AWS and Azure for their C2 infrastructure, making it difficult for defenders to detect malicious traffic since it appeared to come from legitimate sources.
- **Dynamic C2 Infrastructure**: APT29 frequently rotates C2 domains and IP addresses to evade detection and ensure continuous control over compromised systems. This was seen in the

SolarWinds attack, where their use of widely trusted cloud infrastructure masked the true nature of their communications.

**7. Actions on Objectives**

In this final stage, APT29 usually achieves its goal of exfiltrating sensitive data. The group prioritizes stealth and persistence, often extracting data over long periods to avoid triggering alarms.

- **Example**: In the **DNC hack (2016)**, APT29 exfiltrated sensitive emails and documents related to the U.S. presidential election. While APT28 (Fancy Bear) focused on releasing stolen information publicly, APT29's objective appeared to be gathering intelligence for Russia's geopolitical benefit, likely to understand U.S. political strategies and influence foreign policy.
- **Exfiltration of COVID-19 Research (2020)**: APT29's attacks on healthcare and research organizations aimed to steal valuable intellectual property related to COVID-19 vaccine development. The group used **WellMess** to exfiltrate data from compromised systems, ensuring the stolen information could be transmitted back to Russian intelligence services without detection.

## Indicators of Compromise (IoCs)

An Indicator of Compromise (IoC) is a forensic artifact or evidence suggesting a cyber threat may have compromised a system. For APT29 (Cozy Bear), several IoCs have been identified for cyber espionage activities. Below is an example of a key IoC related to Cozy Bear, along with a clear explanation of its relevance and how it can be used for detection.

**1. SUNBURST Backdoor in SolarWinds Attack (2020)**

One of the most significant IoCs associated with APT29 is the **SUNBURST backdoor** used in the SolarWinds supply chain attack in 2020. This IoC became widely known after discovering the SolarWinds

compromise, in which APT29 inserted malicious code into the SolarWinds Orion software update, enabling the group to install the SUNBURST backdoor on thousands of victim networks.

**Description of the IoC**

- **File Name**: SolarWinds.Orion.Core.BusinessLayer.dll
- **File Hashes**:
    - SHA256: b91ce2fa41029f6955bff20079468448f1a920a52ad6abf5f67e6cd6d1ab66d4
    - MD5: 32519c18ff10df13ac78c8b1b9e3497b
- **Malicious Behavior**: This DLL file was a tampered version of a legitimate SolarWinds Orion software component. The SUNBURST backdoor established communication with APT29's command-and-control (C2) servers, allowing attackers to control infected systems remotely.
- **C2 Domains**:
    - avsvmcloud[.]com was the main command-and-control (C2) domain used by SUNBURST to communicate with APT29's infrastructure.
    - Additional domains were dynamically generated by the backdoor using a Domain Generation Algorithm (DGA) and were observed changing frequently to evade detection.

**Reasoning for Detection Use**

The **SUNBURST backdoor** and its associated indicators are extremely valuable for detection for several reasons:

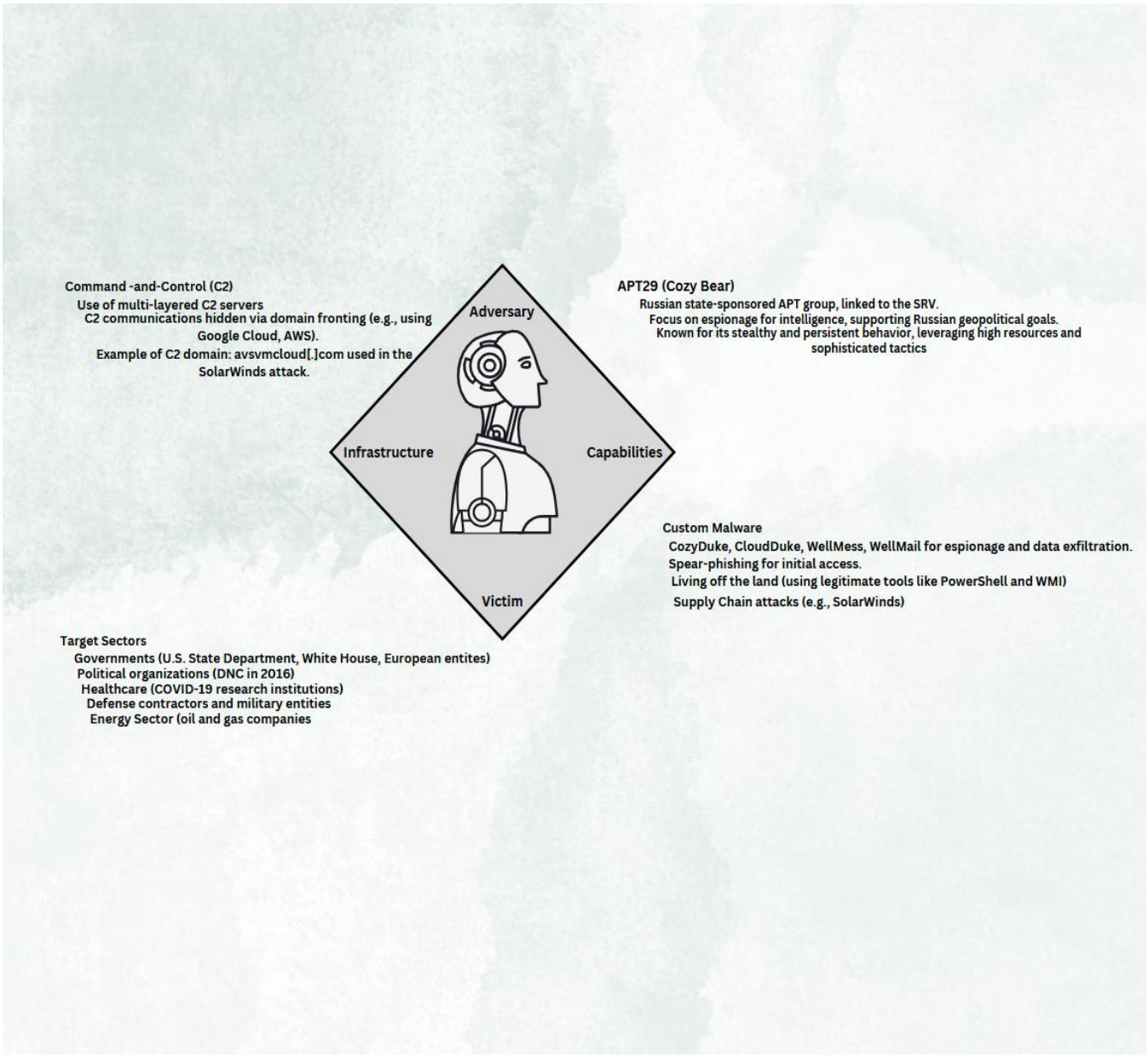
- **Supply Chain Compromise**: The backdoor was distributed through legitimate software updates, making it difficult for traditional antivirus or endpoint detection solutions to flag the compromised file. This makes file hashes and C2 domain information critical in identifying affected systems.

- **Command-and-Control Communications**: Detection tools can be configured to monitor outbound network traffic to suspicious domains like avsvmcloud[.]com or the other dynamically generated C2 domains. Since APT29 often hides C2 traffic using trusted cloud services (e.g., AWS), identifying this traffic can signal an infection.
- **File Hashes**: Security teams can use the provided **SHA256,** and **MD5** hashes to scan their networks for the presence of the tampered SolarWinds file (SolarWinds.Orion.Core.BusinessLayer.dll). If these hashes are found on any machine, it is a strong indicator that the SUNBURST malware has compromised the system.

**Practical Detection Implementation**

1. **Network Monitoring**: Configure network monitoring tools like an IDS (Intrusion Detection System) or firewall to alert you of any communication with known malicious C2 domains, such as avsvmcloud[.]com.
2. **Hash-Based Detection**: File integrity monitoring tools scan network endpoints for malicious SolarWinds files by comparing file hashes (e.g., SHA256 or MD5). Systems that match these hashes are likely compromised.
3. **Threat Intelligence Feeds**: Leverage threat intelligence platforms that provide up-to-date IoCs associated with APT29, including newly discovered hashes, domains, or IP addresses. Security teams can continuously update their detection mechanisms with this information to stay ahead of evolving threats.

# Diamond Model



**References**

*APT29*. (n.d.). Pete Slade. https://peteslade.com/education/glossary/apt-29

Targett, E. (2023, May 24). *Microsoft customer support hacked in new campaign by APT29*. The Stack. https://www.thestack.technology/microsoft-customer-support-hacked-nobelium-apt29-solarwinds/

Mandiant. (2022, April 27). UNC2452 Merged into APT29 | Russia-Based Espionage Group. *Google Cloud Blog*. https://cloud.google.com/blog/topics/threat-intelligence/unc2452-merged-into-apt29

editorialteam. (n.d.). *CrowdStrike's work with the Democratic National Committee: Setting the record straight*. https://www.crowdstrike.com/en-us/blog/bears-midst-intrusion-democratic-national-committee/

Mandiant. (2023, September 21). Backchannel diplomacy: APT29's rapidly evolving diplomatic phishing operations | Mandiant. *Google Cloud Blog*. https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing

*Ransomware activity targeting the healthcare and public health sector | CISA*. (2020, November 2). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a

Advisory: APT29 targets COVID-19 vaccine development. (2020, January 16). https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF

Mandiant. (2020, December 13). SolarWinds supply chain attack uses SUNBURST backdoor. *Google Cloud Blog*. https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

Barrett, B. (2018, April 20). DNC lawsuit against Russia reveals new details about 2016 hack. *WIRED*. https://www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/

Sánchez, J. (n.d.). *Tracking threat actors using images and artifacts*. https://blog.virustotal.com/2024/05/tracking-threat-actors-using-images-and.html

*APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524, Midnight Blizzard, Group G0016 | MITRE ATT&CK®*. (n.d.). https://attack.mitre.org/groups/G0016/