2025

Threat Intelligence & Profiling

CYBERSECURITY INCIDENT CASE STUDY

IBRAHIM AKINTEYE

Threat Actor Overview – APT29

The Russian Foreign Intelligence Service (SVR) is thought to support APT29, a sophisticated and elusive threat group that goes by several names, including Cozy Bear, The Dukes, Midnight Blizzard, and Nobelium. APT29 is an intelligence-gathering nation-state-sponsored actor. By obtaining sensitive information from foreign governments, organizations, and individuals, their operations seek to further Russian geopolitical interests.

Although they have been active since at least 2008, they rose to prominence in 2014 after allegedly carrying out a string of targeted attacks on prominent locations, such as the Democratic National Committee, the US White House, and the Department of State.

To support Russia's strategic goals on the international scene, APT29 engage in espionage to gather intelligence on defense, economic, and foreign policy issues. They concentrate on gaining long-term, covert access to target networks for ongoing intelligence collection.
They are frequently confused with Fancy Bear (APT28), another well-known Russian hacking group. Threat intelligence reports, on the other hand, have continuously pointed out significant variations in their tactics, techniques, and procedures (TTPs), pointing to different operational goals and approaches.

Target Profile

APT29's operations have been observed globally to exhibits preference for organizations involved in foreign policy and international and entities engaged in research and development that can provide strategic insights into geopolitical developments.

They frequently target research institutes, think tanks, and government networks in North America, Asia, Europe, and NATO member nations. The actor searches for sensitive data kept in these organizations' networks and for different people engaged in defense and geopolitical research.

Over the years, the team has shown incredible perseverance, flexibility, and technical skill while being at the vanguard of significant cyber incidents. Their campaigns, which frequently aim to steal sensitive data, have targeted a wide range of organizations, including critical infrastructure, private companies, and government agencies.

MITRE ATT&CK Mapping

APT29 employs a range of tactics and techniques as defined in the MITRE ATT&CK framework. Below are three tactics with associated techniques and real-world applications:

Initial Access

Initial Access involves techniques that adversaries use to infiltrate a network, often through spearphishing or exploiting public-facing web servers. These methods help establish a foothold, which may provide ongoing or limited access depending on factors like password changes. APT29 is known for its patience and its ability to exploit both human trust and supply-chain vulnerabilities. A common tactic is spearphishing with malicious attachments, where attackers send emails containing malware to specifically targeted individuals, companies, or industries. Unlike general phishing, spearphishing is tailored and more precise in its approach.

Technique: Supply Chain Compromise (SolarWinds) / Spearphishing Attachment (Nightingale)

Technique ID: T1195.002 / T1566.001

Application: SolarWinds: APT29 gained access to the SolarWinds build environment, injecting malicious code into the Orion software updates. This allowed them to pivot into thousands of downstream targets via a "trusted" source.

Operation Nightingale: The group utilized highly targeted spear phishing emails directed at healthcare and vaccine research organizations, containing malicious attachments (like .iso or .lnk files) to bypass email filters.

Rationale: Supply chain attacks provide "one-to-many" access with high stealth, while spear phishing exploits the "human firewall," which is often the weakest link in high-security healthcare environments.

Execution

Execution involves the running of adversary-controlled code on a local or remote system. APT29 focuses on techniques that blend with legitimate administrative activity to avoid detection by Endpoint Detection and Response (EDR) tools.

Technique : User Execution : Malicious File

Technique ID : T1204.002

Application: SolarWinds: Once the compromised Orion update was installed by a user, the SUNBURST backdoor was executed as a part of a legitimate Windows service (SolarWinds.BusinessLayerHost.exe).

Operation Nightingale: Attackers relied on users to open "lures"—disguised as COVID-19 research or internal memos, which executed the EnvyScout or WellMess malware payloads.

Rationale: By nesting malicious execution within trusted, signed processes (SolarWinds) or requiring human interaction (Nightingale), APT29 evades automated sandbox detection that typically flags standalone malicious binaries.

Command and Control (C2)

C2 is how an attacker communicates with compromised systems. APT29 is a master of "hiding in plain sight" by mimicking standard enterprise traffic.

Technique : Application Layer Protocol: Web Protocol

Technique ID : T1071.001

Application: SolarWinds: The SUNBURST malware used HTTP/HTTPS to communicate with its C2 server, masquerading its traffic as SolarWinds' "Orion Improvement Product" (OIP) traffic to stay unnoticed by network monitors.

Operation Nightingale: The group utilized Google Drive and Microsoft OneDrive as C2 hubs. They uploaded and downloaded files from these legitimate cloud services to transmit instructions and exfiltrate data.

Rationale: Using standard HTTPS and reputable cloud domains makes the C2 traffic indistinguishable from normal business operations. Most security teams do not block or heavily scrutinize traffic to Google or Microsoft, providing APT29 with a permanent, covert "backdoor."

Case Study: SolarWinds Supply Chain Attack

Year and Context:

In 2020, APT29 executed a supply chain attack by inserting SUNBURST malware into SolarWinds Orion updates, using techniques like password spraying, token theft, and spear phishing to compromise user accounts and access.

Victims:

By compromising a widely used tool, Cozy Bear gained access to numerous U.S. federal agencies, major corporations, and critical infrastructure worldwide, resulting in a massive breach that exposed sensitive government data, corporate secrets, and national security assets.

Key Actions Taken by the Attacker:

The SolarWinds breach showcased Cozy Bear's advanced capabilities through a multi-year campaign that embedded the SUNBURST malware into trusted software updates, granting covert access to high-value targets' networks. After gaining access via SUNBURST, Cozy Bear used tools like Cobalt Strike and TEARDROP, along with exploiting privileged accounts and SAML tokens, to maintain persistence, move laterally, and evade detection even by advanced security teams.

- Inserted malicious code (SUNBURST) into SolarWinds Orion software updates.
- Distributed the compromised updates to approximately 18,000 customers.
- Selected high-value targets for further exploitation, establishing persistent access and exfiltrating sensitive data.

MITRE ATT&CK Techniques Mapped to APT29's Actions:

- By applying the MITRE ATT&CK framework, their operational methods and tools can be clearly mapped and understood.
- Initial Access: Supply Chain Compromise (T1195)
- Execution: Command and Scripting Interpreter: PowerShell (T1059.001), Cloud API (T1059.009), Malicious file (T1204.002)
- Persistence: Create Account (T1136)
- Defense Evasion: Obfuscated Files or Information (T1027), File Deletion (T1070.004)
- Credential Access: Credentials from Password Stores: Sub-technique: Credentials from Web Browsers (T1555.003)
- Lateral Movement: Remote Services: Remote Desktop Protocol (T1021.001), Windows Management Instrumentation (T1047)
- Command and Control: Application Layer Protocol: Web Protocols (T1071.001)

This attack demonstrated APT29's advanced capabilities in executing long-term, stealthy operations that can compromise numerous organizations through a single supply chain vector.

References

Picus Security Blog: APT29 Explained: Cozy Bear's Evolution, Techniques, and Notorious Cyber Attacks (https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques)

Check Point Research: Unmasking APT29: The Sophisticated Phishing Campaign Targeting European Diplomacy (https://blog.checkpoint.com/research/unmasking-apt29-the-sophisticated-phishing-campaign-targeting-european-diplomacy/)

Recorded Future Blog: SolarWinds: The CSO Perspective (https://www.recordedfuture.com/blog/solarwinds-cso-perspective)

FireEye/Mandiant Blog: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor (https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor)

MITRE ATT&CK Group: ATT&CK Matrix for Enterprise (https://attack.mitre.org/)

MITRE ATT&CK Group: APT29 (https://attack.mitre.org/groups/G0016/)

MITRE ATT&CK Group: SolarWinds Compromise: (https://attack.mitre.org/campaigns/C0024/)

Kaspersky: What’s behind APT 20? (https://www.kaspersky.com/enterprise-security/mitre/apt29)

MalPedia: APT29 (https://malpedia.caad.fkie.fraunhofer.de/actor/apt29)

Used ChatGPT streamline research discoveries and to summarize literature material.