



Arab Academy for Science, Technology and Maritime Transport

**College of Computing and Information Technology
Cybersecurity Department**

Analysis of MITRE ATT&CK Groups, Software, Techniques, and Mitigations

Presented By:

Omar Hamdy 221006553

Amer Ashoush 221006722

Supervised By:

Dr. Ehab Aboseif

December - 2025

Table of Contents

1. Introduction	3
2. Methodology	3
3. Group 1: Scattered Spider (G1015)	3
3.1 Attacker Background	3
3.2 Associated Campaigns	4
3.3 Selected Software: BlackCat (S1068)	4
3.4 Technique Used: T1047 – Windows Management Instrumentation (WMI)	5
3.5 Mitigations for T1047 (WMI Abuse)	5
4. Group 2: APT29 (Cozy Bear)	6
4.1 Attacker Background	6
4.2 Key Operations & Campaigns	7
4.3 Selected Software: SUNBURST (Solorigate)	7
4.4 Technique Used: T1195.002 – Compromise Software Supply Chain	8
4.5 Mitigations for T1195.002 (Supply Chain Compromise)	8
5. Comparative Analysis	9
6. Conclusion	9
7. References	10

1. Introduction

The MITRE ATT&CK framework is widely used to understand how cyber adversaries operate, map malicious behavior, and develop stronger defensive strategies. This report examines two major threat groups, Scattered Spider and APT29, by exploring their backgrounds, key campaigns, the malware they use, and the MITRE techniques associated with their operations. The aim is to provide a clear comparison between both groups and highlight how different threat actors require different defensive approaches.

2. Methodology

The information presented in this report is based on several trusted intelligence sources. These include the official MITRE ATT&CK database, CISA cybersecurity advisories (particularly AA23-320A and its updates), threat research published by CrowdStrike, Microsoft, FireEye, Trustwave, and the Australian Cyber Security Centre, as well as publicly available threat intelligence and the provided documentation on APT29.

All findings were reviewed against corresponding MITRE technique IDs, ensuring that each technique was accurately matched with the appropriate mitigation strategies.

3. Group 1: Scattered Spider (G1015)

3.1 Attacker Background

Scattered Spider is a financially motivated, English-speaking cybercriminal group active since at least **2022**. The group is also known by many aliases, including **Roasted Oktapus**, **Octo Tempest**, **Storm-0875**, **UNC3944**, **Muddled Libra**, and **Scatter Swine**.

Initially, they targeted CRM providers, BPO companies, telecommunications firms, and technology service providers. By 2023–2025, their targeting expanded significantly, striking gaming companies, hospitality giants, retail chains, MSPs, manufacturing firms, and financial institutions.

Scattered Spider is well-known not for zero-day exploits but for **expert-level social engineering**, particularly:

- Impersonating IT/help-desk staff

- SIM swapping
- MFA fatigue/spam attacks
- Credential theft and session hijacking
- Help-desk manipulation to reset passwords or transfer MFA tokens

Once inside a network, Scattered Spider often compromises platforms such as **Okta**, **AWS**, and **Microsoft 365**. Their attacks frequently end with the deployment of ransomware, most commonly **BlackCat/ALPHV**. Analysts generally describe their operations as rapid, aggressive, and heavily dependent on human interaction.

3.2 Associated Campaigns

Early CRM/BPO Intrusions (2022–2023)

CrowdStrike reported that Scattered Spider’s earliest operations involved compromising CRM and BPO firms to access large volumes of sensitive customer data. The group sold this information or used it to extort organizations.

IT Help-Desk Impersonation & Oktapus Campaigns (2023–2024)

During this period, attackers relied on phone calls, text messages, and fake login portals to impersonate IT teams. Their goal was to trick employees into sharing MFA codes, installing remote access tools, or approving fraudulent MFA requests. These tactics allowed the group to compromise identity systems such as **Okta**.

Ransomware Extortion & Cloud Attacks (2024–2025)

CISA’s more recent advisories show that the group began deploying both **DragonForce** and **BlackCat** ransomware while using legitimate remote-access tools such as TeamViewer, **AnyDesk**, and **ConnectWise**. These campaigns targeted sectors including casinos, hospitality, telecommunications, and various large enterprises.

3.3 Selected Software: BlackCat (S1068)

BlackCat (ALPHV/Noberus) is a highly advanced ransomware family written in **Rust**, supporting both **Windows** and **Linux** environments. It operates under a **Ransomware-as-a-Service (RaaS)** model and is known for:

- Extremely fast, multi-threaded encryption
- Compatibility with VMware ESXi environments

- Modules for data theft, wiping, and persistence
- Extensive command-line configuration options

Scattered Spider uses BlackCat during its final extortion stage. After gaining privileged access, operators deploy BlackCat to encrypt systems, wipe VM snapshots, stop critical services, and remove recovery options.

3.4 Technique Used: T1047 – Windows Management Instrumentation (WMI)

BlackCat abuses Windows Management Instrumentation, a built-in administrative subsystem, to execute destructive commands. A common example is the use of:

wmic.exe Shadowcopy Delete

Using WMI allows BlackCat to:

- Delete shadow copies to prevent system recovery
- Execute system-level commands without dropping additional tools
- Blend into legitimate administrator activity
- Facilitate data destruction and prepare systems for encryption

This allows the attacker to remove shadow copies, which prevents the victim from restoring system backups. By relying on WMI, the attacker can execute system-level commands without dropping additional tools, blend in with legitimate administrative activity, and prepare the environment for full encryption. Because WMI is part of Windows and often used by administrators, detecting misuse can be difficult.

3.5 Mitigations for T1047 (WMI Abuse)

M1047 – Audit and Monitoring

Organizations should enable WMI logging and monitor for suspicious command execution, especially anything involving shadow copy deletion or remote WMI calls.

M1038 – Restrict Exploitable Services

Access to WMI should be limited to the users who genuinely need it. Remote WMI access should be disabled unless absolutely required.

M1026 – Privileged Account Management

Implementing multi-factor authentication, rotating administrator credentials, and using Just-In-Time access can prevent attackers from obtaining the elevated permissions needed to run WMI commands.

M1042 – Disable or Limit Command-Line Tools

Tools such as wmic.exe can be restricted using AppLocker or similar application control solutions.

M1040 – Behavior Prevention Tools

Modern endpoint detection and response solutions can detect unusual WMI behavior, such as mass deletion of shadow copies or commands executed at suspicious times.

Additional CISA-Recommended Mitigations

- Maintain offline, immutable backups
 - Limit admin tools to secured admin jump hosts
 - Disable shadow copies if they are not essential
-

4. Group 2: APT29 (Cozy Bear)

4.1 Attacker Background

APT29, also known as **Cozy Bear, Midnight Blizzard, The Dukes, Nobelium**, is believed to be operated by **Russia's Foreign Intelligence Service (SVR)**. Unlike financially motivated groups, APT29 focuses on **long-term espionage**, targeting:

- Government ministries
- Diplomatic organizations
- NATO members
- Think tanks
- High-tech and research organizations
- Critical infrastructure

The group is characterized by patience, stealth, and a preference for “Living off the Land” techniques to avoid detection. They often rely on legitimate system tools such as PowerShell, WMI, and other common administrative utilities to blend into normal network activity.

4.2 Key Operations & Campaigns

Democratic National Committee (DNC) Breach (2016)

APT29 infiltrated systems belonging to the Democratic National Committee, collecting politically sensitive data that later played a major role in the 2016 election investigations.

SolarWinds Supply Chain Attack (2020)

One of APT29’s most significant operations involved inserting malicious code into the SolarWinds Orion software update. Thousands of organizations around the world unknowingly installed the malware, making this one of the most damaging supply chain attacks ever recorded.

Microsoft Corporate Breach (2024)

APT29 carried out password-spraying attacks and exploited weaknesses in cloud identity management to access legacy Microsoft accounts. This attack allowed them to steal sensitive corporate emails.

4.3 Selected Software: SUNBURST (Solorigate)

SUNBURST is a sophisticated backdoor that APT29 secretly embedded into SolarWinds Orion software updates. When organizations installed what appeared to be a standard software update, they unknowingly executed the malicious code.

SUNBURST enabled:

- Covert C2 communication
- Credential harvesting
- Privilege escalation
- Lateral movement
- Stealthy surveillance inside networks

APT29 used this technique to compromise U.S. federal agencies, security firms, and multinational corporations.

4.4 Technique Used: T1195.002 – Compromise Software Supply Chain

Instead of directly targeting victims, APT29 compromised the **SolarWinds software development** environment. Malicious SUNBURST code was inserted into the build process, and the final update was digitally signed and distributed as an official product.

This technique is extremely dangerous because:

- The malicious file is **signed by the legitimate vendor**
- Victims install it willingly
- Security tools trust it
- It provides wide simultaneous access across many organizations

APT29 used this foothold to quietly harvest sensitive data across multiple sectors.

4.5 Mitigations for T1195.002 (Supply Chain Compromise)

M1051 – Software Integrity (Supply Chain Security)

Organizations should use tools that validate the integrity of software updates and monitor for unexpected changes in behavior or file structure.

M1036 – Vendor/Supplier Validation

Vendors should demonstrate strong security around their development pipelines, code repositories, and update mechanisms. Regular audits and transparency reports can help reduce risk.

M1030 – Network Segmentation

Servers running critical third-party software should be isolated. Even if an update is compromised, segmentation prevents attackers from immediately accessing sensitive assets.

M1038 – Code Signing Policy

Strict code-signing enforcement ensures that only trusted, signed software is allowed to run. While SUNBURST used a stolen signature, code signing remains a crucial defensive measure.

5. Comparative Analysis

Scattered Spider and APT29 represent **two very different threat paradigms**:

Category	Scattered Spider	APT29
Motivation	Financial gain (ransomware/extortion)	Espionage and intelligence
Style	Loud, human-operated, aggressive	Stealthy, patient, highly advanced
Primary Techniques	Social engineering, identity compromise, MFA bypass	Supply chain compromise, stealthy LoTL techniques
Tooling	Ransomware (BlackCat), remote access tools	Sophisticated backdoors (SUNBURST), custom malware
Targeting	Large enterprises (gaming, telecom, retail)	Governments, national security assets, global corporations

Despite their differences, both show the importance of:

- Protecting identity infrastructure
 - Monitoring native system tools
 - Verifying software supply chains
 - Using strong EDR and logging
-

6. Conclusion

This report demonstrates that different adversaries use different methods to achieve their goals, but both can cause significant harm if not detected early. Scattered Spider succeeds by exploiting human weaknesses and social engineering, while APT29 excels at stealthy, long-term espionage operations.

Understanding their tools and techniques through the MITRE ATT&CK framework helps defenders strengthen their visibility, detection, and overall security posture. As cyber threats grow increasingly advanced, organizations must continue improving their defensive strategies and remain informed about evolving adversarial behaviors.

7. References

- MITRE ATT&CK Group G1015 (Scattered Spider)
- MITRE ATT&CK Group G0016 (APT29)
- MITRE ATT&CK Software S1068 (BlackCat/ALPHV)
- MITRE ATT&CK Software SUNBURST
- MITRE Technique T1047 (WMI)
- MITRE Technique T1195.002 (Supply Chain Compromise)
- CISA Advisory AA23-320A & July 2025 Update
- CrowdStrike Global Threat Reports
- Microsoft Security Intelligence Reports
- Mandiant Incident Response Publications