Assembling the Russian Nesting Doll: UNC2452 Merged into APT29

Mandiant has gathered sufficient evidence to assess that the activity tracked as UNC2452, the group name used to track the SolarWinds compromise in December 2020, is attributable to APT29.

This conclusion matches attribution statements previously made by the U.S. Government that the SolarWinds supply chain compromise was conducted by APT29, a Russia-based espionage group assessed to be sponsored by the Russian Foreign Intelligence Service (SVR). Our evaluation is based on firsthand data gathered by Mandiant and is the result of an extensive comparison and review of UNC2452 and our detailed knowledge of APT29.

The merge of UNC2452 into APT29 significantly expands our knowledge of APT29 and showcases an evolving, disciplined, and highly skilled threat actor that operates with a heightened level of operational security (OPSEC) for the purposes of intelligence collection. This blog post builds on our efforts to share information and provide awareness related to APT29's developments.

Evolving Tradecraft

APT29 is a highly sophisticated group that has continued to evolve and refine its operational and behavioral tactics, techniques, and procedures (TTPs) to better obfuscate activity and limit its digital footprint to avoid detection. The merge expands APT29's operational profile, emphasizing the group's well-resourced nature, longevity of operations, time on targets, OPSEC, adaptability, and stealth. The group has been steadily advancing its TTPs and adopting new measures as new technologies emerge.

- **High Operational Tempo and Scale**. Mandiant has tracked APT29 activity since at least 2014 and despite significant public exposure following the SolarWinds compromise in 2020, the group has continued to conduct multiple, large-scale compromises simultaneously in different time zones throughout 2020 and 2021 at a high operational tempo. In 2021 and 2022, we observed APT29 conduct large-scale phishing campaigns targeting diplomatic entities in Europe, North America, and Asia. The scale and scope of this activity suggests the group is well-resourced.
- **Wide Operational Scope**. APT29 has targeted Western and European governments and a range of additional industries including education, telecommunications, government-adjacent organizations, medical research entities, and organizations that provide third party access, such as technology companies and IT and business service providers.
- **Victimology and Data Theft**. APT29 has maintained a consistent focus on aggressively gaining and maintaining access to email mailboxes. More recently, they also targeted cloud-based resources and source code repositories to hunt for data relevant to Russian strategic interests, conduct operational planning, and to use access to third parties as a point of entry to downstream customers.

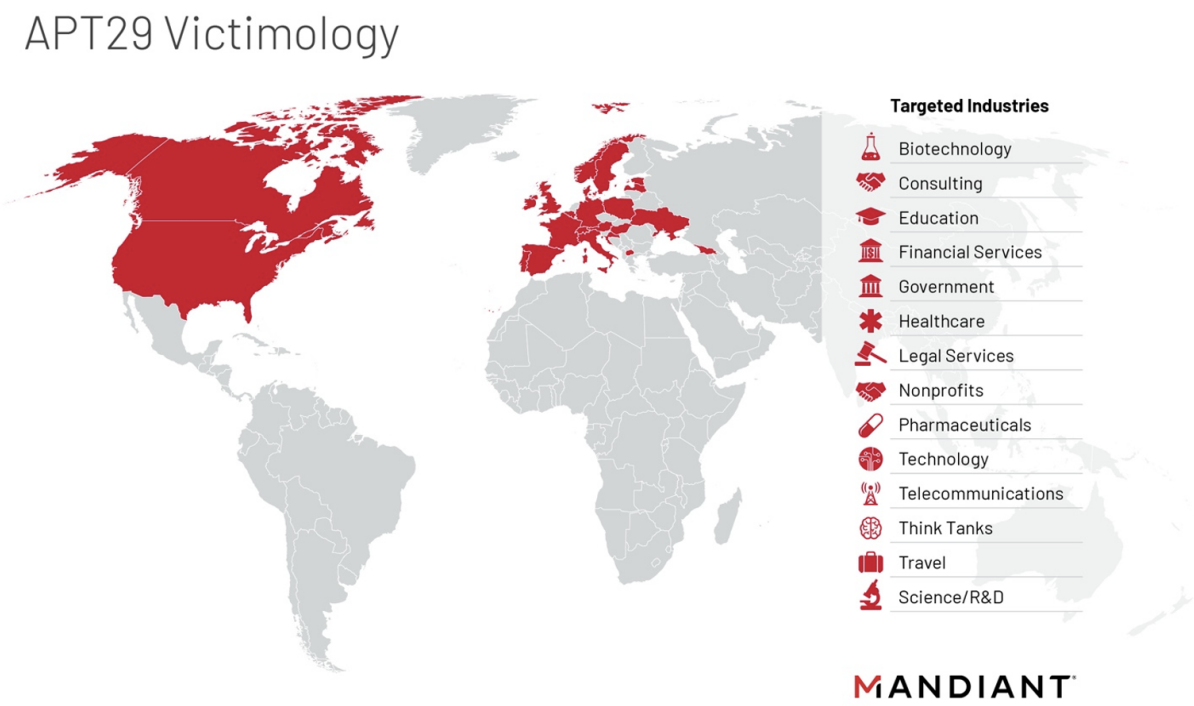

Figure 1: APT29 Victimology

Mandiant observed APT29 evolve its already advanced tradecraft to adapt to different victim environments and emerging technology in the following ways:

- **Varying Intrusion Vectors**. Since 2020, APT29 increasingly sought to exploit trust relationships between customers and third parties and abuse the supply chain, as evidenced by the prolific nature of the SolarWinds compromise. Mandiant observed APT29 leverage varying operational techniques to gain initial access to victims including stolen credentials, web server compromises, password sprays, and spear phishing. Notably, from 2021 to the present, Mandiant observed APT29 alter its TTPs slightly to deploy Cobalt Strike BEACON via spear phishing campaigns likely due to the availability and success of the publicly available malware, as well as to complicate attribution efforts given the tool's wide use.

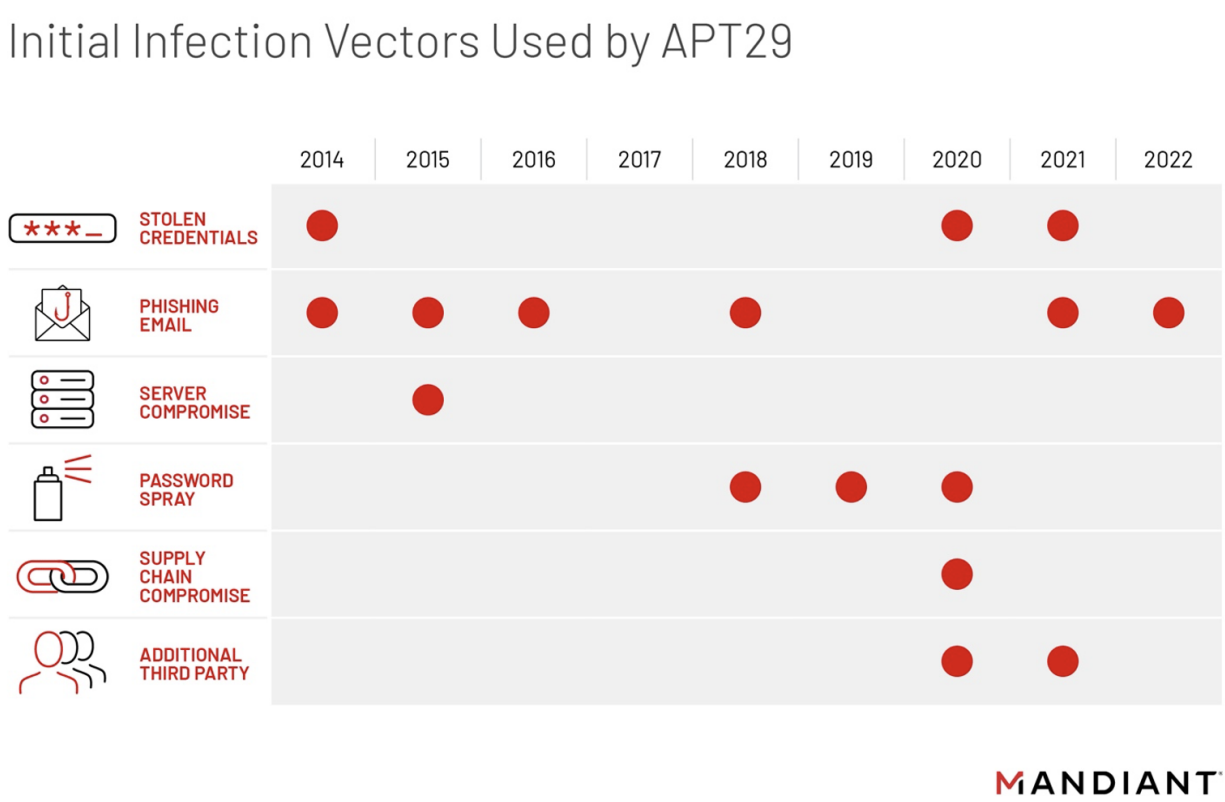

Figure 2: Initial Infection Vectors used by APT29

- **Heightened OPSEC.** APT29 is known for its extensive operational discipline and continues to maintain a strong OPSEC posture across all operations. APT29 demonstrates a heightened level of OPSEC to protect secondary backdoors, lateral movement attempts, and data theft. For instance, APT29 went to considerable lengths to hide its SUNBURST backdoor within the legitimate SolarWinds code during the initial campaign. Additionally, Mandiant previously identified the group attempts to compromise multiple accounts within an environment while keeping the use of each account separate by function, using one for reconnaissance and the others for lateral movement. This reduces the likelihood that detecting one compromised account's activity could expose the entire scope of the intrusion.

  Since 2018, APT29 has consistently enhanced the operation security of its command and control (C2) infrastructure using legitimate services and compromised infrastructure, as well as using domain fronting techniques, and reliance on anonymized internet access, such as using proxy services and the TOR network. In addition, APT29 has continued to demonstrate a clear understanding of security operations, incident response, remediation efforts, and network detection mechanisms. Table 1 provides some examples of additional OPSEC measures taken by the group.

Table 1: Examples of APT29 network- and host-based OPSEC measures

Network-based OPSEC	**Host-based OPSEC**
C2 Consideration • Used legitimate services for C2 • Adjusted C2 callout intervals Blending In • Matched hostnames to the victim environment's naming convention	Looking Legitimate • Modified a legitimate Microsoft DLL to enable the DLL Side Loading of a malicious payload • Masqueraded malicious scheduled tasks, processes, and shortcut files as legitimate tasks, binaries, and documents

- Leveraged native Microsoft tools

Infrastructure OPSEC, as detailed in this post

- Localized “last mile” infrastructure near victim organizations by using residential IP address ranges to authenticate to victim environments
- Geolocating Azure infrastructure in the same geography as the victim infrastructure
- Used a mixture of TOR, VPS, and VPNs to access victim environments
- Used IP address proxy providers that proxy traffic though mobile devices, to make traffic appear as if it was originating from domestic ISPs and devices

Separate Infrastructure

- Separated SUNBURST callback infrastructure from other follow-on malware families to preserve access and protect this toolset if follow-on activity was discovered
- Restricted C2 reuse by establishing unique C2 servers per victim and single-use C2 servers for individual hosts

- Replaced a legitimate binary with a malicious file of the same name and then reinstalled the original file after the malicious binary completed execution
- Minimized the size of exfiltrated data and used encrypted connections for data exfiltration

Disabling Security Controls

- Detected and disabled antivirus and system logging features then reenabled these features in some cases upon completion of malicious activity

- Disabled SysInternals Sysmon and Splunk Forwarders on victim machines that they accessed via Microsoft Remote Desktop

Covering Tracks

- Cleared Windows Event Logs
- Established persistence to perform reconnaissance, removed it before moving laterally to another system, and then verified that the persistence was removed
- Extensive use of Microsoft’s secure delete tool (SDELETE) following interactive operations on a host

Monitoring Remediation

- Accessed IT personnel mailboxes to monitor remediation efforts and adjust TTPs as needed

Using Varying TTPs

- Employed slight variations in TTPs and malware for spear phishing campaigns

- **Sophistication**. APT29 has a proven ability to adapt quickly during operations. The group uses innovative and novel techniques to bypass detection and strong authentication requirements in victim environments. In more recent operations, their fundamental understanding of native M365 features allowed them to move easily between on-premises and cloud resources without using a substantial amount of malware. We believe these measures, combined with a high level of OPSEC, longevity of the group’s operations, and their time on targets demonstrate a well-resourced and highly sophisticated actor.
    - **On-prem to Cloud**. APT29’s advanced knowledge of Microsoft tools and cloud environments allows the group to abuse product features to achieve and maintain access—despite strong authentication requirements– without using specific vulnerabilities or deploying custom

malware. This enables them to easily pivot from on-premises networks to cloud resources to create persistent access to targets and sensitive data. Mandiant observed APT29 target and move laterally to the M365 environment starting in 2018 by using a combination of seven primary techniques detailed in our guidance.

- **Bypassing Multi-Factor Authentication (MFA):** From 2018 to 2020, APT29 used an assortment of methods to satisfy strong authentication requirements in victim environments for lateral movement. These included enrolling devices for MFA or bypassing it via legacy authentication, adding credentials to service principals and app registrations, and utilizing precomputed cookies to bypass MFA requirements and log in successfully without raising any alarms. The group also leveraged legitimate credentials to abuse repeated MFA push notifications to an end user's legitimate device until the user accepted the authentication. We also observed the group evolve from using Golden Tickets to access sensitive data from on-premises systems to Golden SAML (Security Assertion Markup Language) for victim environments that used cloud hosted resources. Both techniques allow attackers to bypass authentication requirements and access the victim environment with any privileges and as any user, even after a domain-wide password reset of user accounts.
- **Maintaining a Light Malware Footprint**: APT29 shifted away from using a toolkit of customized tools to maintaining a relatively light malware footprint since 2018, likely due to extensive open-source reporting on the group's toolkit. This allows for fewer detection opportunities by anti-virus engines and complicates attribution efforts. The group appears to favor the use of stolen credentials, abusing native Microsoft features to maintain access to victim environments. In some cases, we have observed the group shift from deploying custom tools after gaining a foothold to deploying BEACON. This is likely due to the success, availability, modification potential, and attribution complications provided by BEACON. From 2018 to 2021, APT29 limited their use of custom tools to a little under half of all observed compromises. For compromises during that timeframe that featured custom tools, APT29 used custom malware families including SUNBURST, BEACON droppers RAINDROP and TEARDROP, a credential theft tool called MAMADOGS, and CRIMSONBOX; a .NET tool that extracts the token signing certificate from an ADFS configuration, assisting the group in forging SAML tokens.
- **Speed and Agility**. APT29 can quickly adjust their tools and TTPs to adapt to victim environments and to retain access through remediation efforts. In multiple cases, APT29 was able to gain Domain Administrator privileges less than 12 hours after the initial execution of a phishing payload. In 2020, approximately five days after the public disclosure of the SolarWinds supply chain compromise, APT29 moved the persistent BEACON backdoor to an additional system in a new subnet following an email sent from the internal information security team to IT administrators to request an image of the SolarWinds system. This suggests the group was monitoring the organizations' emails and subsequently employed countermeasures to maintain access.
- **Follow the Data.** Since 2018, Mandiant observed APT29 adjust their tactics to access victim environments to avoid losing access to critical data located on-premises and in cloud environments. Mandiant observed the group use different methods to gather emails from different victim environments. These include using publicly available tools that harvest local OST and PST files for on-premises systems and switching to abusing service principals,

adding permissions to victims' mailboxes and mailbox folders, and using application impersonation for cloud environments.

Outlook and Implications

Since Mandiant began tracking APT29 in 2014, the group has continued to advance its significant technical tradecraft and OPSEC. The consistent and steady advancement in TTPs speaks to its disciplined nature and commitment to stealthy operations and persistence. Merging UNC2452 into APT29 has given us a better understanding of how APT29's operations have evolved over the years, including how the group further honed its technical skills to bypass security controls, scale TTPs for emerging technology, blend in with victim environments, and hinder detection across all aspects of its operations. Mandiant is almost certain that APT29 will continue to evolve its operational and behavioral TTPs based on its advanced skillset and ability to creatively employ novel TTPs and tools to gain persistent access to targets.

Please refer to our white paper on remediating and hardening strategies to defend against APT29, and check out our webinar for even more information.

MITRE ATT&CK Techniques Added as a Result of the Merge

Resource Development

- T1583.003: Virtual Private Server

Initial Access

- T1195.002: Compromise Software Supply Chain
- T1199: Trusted Relationship

Execution

- T1059.007: JavaScript

Persistence

- T1098: Account Manipulation
- T1098.001: Additional Cloud Credentials
- T1547.009: Shortcut Modification
- T1574.008: Path Interception by Search Order Hijacking

Privilege Escalation

- T1055.002: Portable Executable Injection
- T1134.001: Token Impersonation/Theft
- T1484.002: Domain Trust Modification
- T1547.009: Shortcut Modification
- T1574.008: Path Interception by Search Order Hijacking

Defense Evasion

- T1027.003: Steganography
- T1027.005: Indicator Removal from Tools
- T1036.005: Match Legitimate Name or Location
- T1055.002: Portable Executable Injection
- T1070: Indicator Removal on Host
- T1070.001: Clear Windows Event Logs
- T1070.006: Timestomp
- T1134.001: Token Impersonation/Theft
- T1218.005: Mshta
- T1218.011: Rundll32
- T1480: Execution Guardrails
- T1497.003: Time Based Evasion
- T1550.001: Application Access Token
- T1562.001: Disable or Modify Tools
- T1574.008: Path Interception by Search Order Hijacking

Credential Access

- T1003.003: NTDS
- T1003.006: DCSync
- T1003.008: /etc/passwd and /etc/shadow
- T1110.003: Password Spraying
- T1111: Two-Factor Authentication Interception
- T1552.001: Credentials In Files
- T1552.004: Private Keys
- T1552.006: Group Policy Preferences
- T1555.005: Password Managers
- T1558: Steal or Forge Kerberos Tickets
- T1558.003: Kerberoasting
- T1606.001: Web Cookies
- T1606.002: SAML Tokens

Discovery

- T1016.001: Internet Connection Discovery
- T1046: Network Service Scanning
- T1497.003: Time Based Evasion
- T1526: Cloud Service Discovery

Lateral Movement

- T1550.001: Application Access Token

Collection

- T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1074: Data Staged

- T1114.002: Remote Email Collection
- T1213.002: Sharepoint
- T1213.003: Code Repositories
- T1560.001: Archive via Utility

Command and Control

- T1071: Application Layer Protocol
- T1071.004: DNS
- T1090.003: Multi-hop Proxy
- T1568.002: Domain Generation Algorithms
- T1571: Non-Standard Port
- T1573.001: Symmetric Cryptography

Exfiltration

- T1030: Data Transfer Size Limits
- T1567: Exfiltration Over Web Service
- T1567.001: Exfiltration to Code Repository