datto

APT29 Threat Profile

Dark Halo, YTTRIUM, StellarParticle, The Dukes, NOBELIUM, Cozy Bear, UNC2452, CozyDuke

Table of Contents

APT29 is a highly sophisticated Russian state-sponsored hacker group that has been in operation since at least 2014.

APT29 was attributed to hacking the Democratic National Committee in 2015, the Solarwinds supply chain attack (aka SUNBURST) in 2020 and have been identified as the developers and operators of the WellMess malware.

Motives

As an advanced, persistent threat group, APT29 seeks to gain and maintain access to networks for intelligence purposes. APT29 is known to have high regard for operational security and will conduct low-frequency, highly obfuscated activity on victim networks.

APT29 has been known to continually attempt to regain access to networks and devices, further confirming they are looking for long-term, consistent access to specific intelligence targets.

Tactics, Techniques, and Procedures (TTPs)

APT29 utilizes sophisticated, bespoke malware implants designed to provide persistent access to target networks while remaining undetected. To remain undetected, APT29's implants have been known to masquerade as legitimate services, infrequently communicate with their command-and-control (C2) infrastructure, and closely resemble legitimate traffic when doing so.

APT29's primary goal is to maintain undetected persistence in a network in order to gather and exfiltrate data of interest for intelligence purposes. Known techniques APT29 has used to achieve persistence are via scheduled tasks, masquerading implants as legitimate applications that are already installed on the device, and wiping logs to remove evidence of their activities.

APT29's C2 communications are highly obfuscated and designed to blend into regular traffic, including sending unrelated traffic simultaneously as the real beacon to hide itself in the noise. APT29 has been known to utilize unique C2 infrastructure for each target in order to prevent one detection from revealing all their current accesses.

MITRE ATT&CK:

The following maps APT29's TTPs to MITRE ATT&CK:

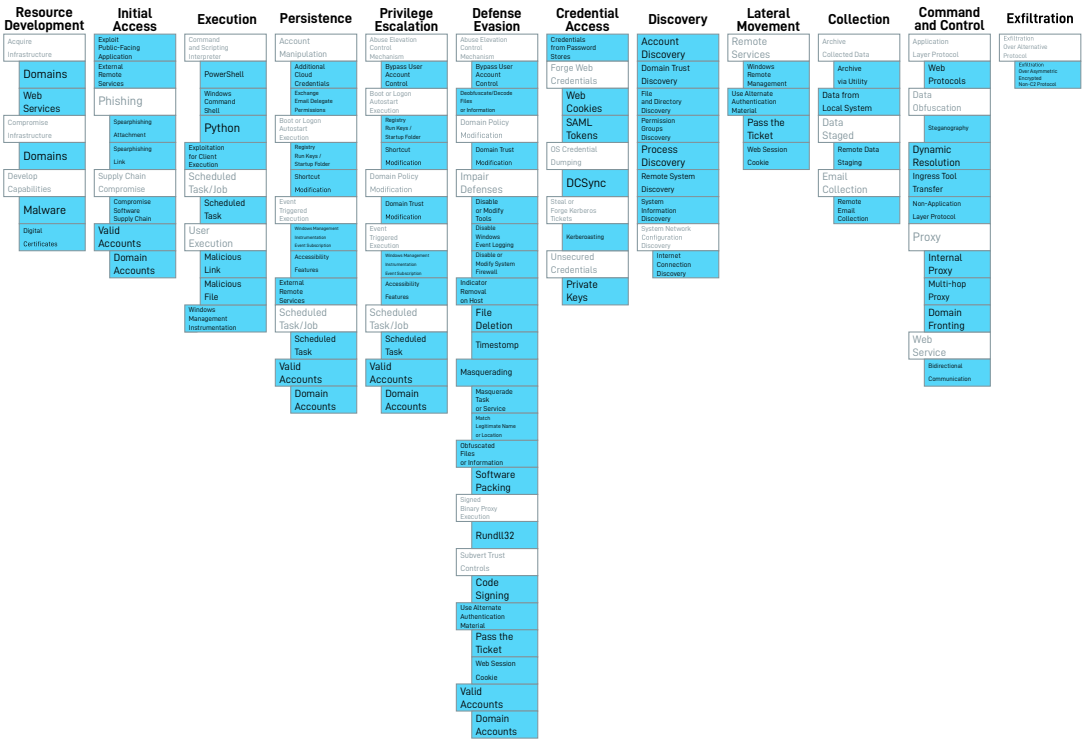

Table of Contents

Resource Development

- **Develop Capabilities: Malware (T1587.001) -** APT29 has developed multiple pieces of bespoke malware, including malware tailored to be incorporated into third-party software.
- **Develop Capabilities: Digital Certificates (T1587.003) -** APT29 has used self-signed certificates to enable TLS authentication and communication between the malware and C2..
- **Compromise Infrastructure: Domains (T1584.001) -** APT29 has compromised domains to use for C2.
- **Acquire Infrastructure: Domains (T1583.001) -** APT29 has acquired C2 domains through resellers.

Initial Access

- **Exploit public-facing application (T1190) -** APT29 has exploited multiple VPN and mail server vulnerabilities to gain, as well as regain, access to networks.
- **External Remote Services (T1133) -** APT29 has used compromised identities to access VPNs and remote access tools.
- **Supply Chain Compromise: Compromise Software Supply Chain (T1195.002) -** APT29 gained initial network access to victim networks via a trojanized update of SolarWinds Orion software.
- **Valid accounts: Domain Accounts (T1078.002) -** APT29 has used valid accounts to facilitate access and lateral movement on victim networks.

Execution

- **Command and Scripting Interpreter: PowerShell (T1059.001) -** APT29 has used PowerShell commands and scripts in its campaigns.
- **Command and Scripting Interpreter: Windows Command Shell (T1059.003) -** APT29 used cmd.exe to execute commands on remote machines.

Persistence

- **Scheduled Task/Job: Scheduled Task (T1053.005) -** APT29 has used Windows scheduled tasks to maintain persistence.

Defense Evasion

- **Obfuscated Files or Information (T1027) - A**PT29 has used encoded PowerShell commands.
- **File Deletion (T1070.004) -** APT29 has been observed removing their tools, including custom backdoors, once remote access is achieved.
- **Subvert Trust Controls: Code Signing (T1553.002) -** APT29 was able to get SUNBURST signed by SolarWinds code signing certificates by injecting the malware into the SolarWinds Orion software lifecycle.
- **Modify Registry (T1112) -** APT29 has used the registry to store scripts.
- **Signed Binary Proxy Execution: Rundll32 (T1218.011) -** Sibot has executed downloaded DLLs with rundll32.exe..

Credential Access

- **Forge Web Credentials: Web Cookies (T1606.001) -** APT29 has used stolen secret keys to generate a cookie value and bypass MFA set on OWA accounts.
- **Forge Web Credentials: SAML tokens (T1606.002) -** APT29 used compromised SAML signing certificates to create tokens.

Credential Access

- **Forge Web Credentials: Web Cookies (T1606.001) - A**PT29 has used stolen secret keys to generate a cookie value and bypass MFA set on OWA accounts.
- **Forge Web Credentials: SAML tokens (T1606.002) -** APT29 used compromised SAML signing certificates to create tokens.

Discovery

- **Process Discovery (T1057) -** APT29 has used multiple command-line utilities to enumerate running processes.
- **Security Software Discovery (T1518.001) -** APT29's SUNBURST malware uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers.

Collection

- **Archive Collected Data: Archive via Utility (T1560.001) -** APT29 has used 7-Zip to compress stolen emails into password-protected archives prior to exfiltration.

Command and Control

- **Application Layer Protocol: Web Protocols (T1071.001) -** APT29 has used HTTP for C2 and data exfiltration.
- **Application Layer Protocol: DNS (T1071.004) -** APT29 has been observed using DNS CNAME responses to update C2 domains.

- **Ingress Tool Transfer (T1105) -** APT29 has downloaded additional tools to a compromised host following initial access.
- **Dynamic Resolution (T1568) -** APT29 used dynamic DNS resolution to construct and resolve to randomly-generated subdomains for C2.

Exfiltration

- **Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002) -** APT29 has exfiltrated collected data over a simple HTTPS request to a password-protected archive staged on a victim's OWA servers.

Mitigations/Defenses

It is recommended to implement a strong foundation of security controls in order to defend your network against the APT29 threat actors.

It is recommended to implement strong security controls in order to defend your network against APT29, starting with a solid foundation.

The Center for Internet Security (CIS) Controls are a prioritized set of safeguards designed to defend against cyber attacks. The CIS Controls have three tiers, known as Implementation Groups, that build on each other.

The following table maps APT29's MITRE ATT&CK techniques to CIS v8 Safeguards:

MITRE ATT&CK	CIS Safeguards
Exploit public-facing application (T1190)	**IG1** 4.4: Implement and Manage a Firewall on Servers 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 7.1: Establish and Maintain a Vulnerability Management Process 7.2: Establish and Maintain a Remediation Process 7.3: Perform Automated Operating System Patch Management 7.4: Perform Automated Application Patch Management 12.1: Ensure Network Infrastructure is Up-to-Date
External Remote Services (T1133)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 6.3: Require MFA for Externally-Exposed Applications 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Access

— IG1 — IG2 — IG3

Supply Chain Compromise: Compromise Software Supply Chain (T1195.002)	**IG1** 7.1: Establish and Maintain a Vulnerability Management Process 7.2: Establish and Maintain a Remediation Process 7.3: Perform Automated Operating System Patch Management 7.4: Perform Automated Application Patch Management
Valid accounts: Domain Accounts (T1078.002)	**IG1** 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Access
Command and Scripting Interpreter: PowerShell (T1059.001)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Command and Scripting Interpreter: Windows Command Shell (T1059.003)	**IG2** 2.5: Allowlist Authorized Software **IG3** 2.7: Allowlist Authorized Scripts
Scheduled Task/Job: Scheduled Task (T1053.005)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 8.3: Ensure Adequate Audit Log Storage
Obfuscated Files or Information (T1027)	**IG1** 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Modify Registry (T1112)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process
Signed Binary Proxy Execution: Rundll32 (T1218.011)	**IG2** 10.5: Enable Anti-Exploitation Features
Forge Web Credentials: Web Cookies (T1606.001)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process

— IG1 — IG2 — IG3

Forge Web Credentials: SAML tokens (T1606.002)	**IG1** 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Archive Collected Data: Archive via Utility (T1560.001)	**IG1** 2.1: Establish and Maintain a Software Inventory 2.2: Ensure Authorized Software is Currently Supported 2.3: Address Unauthorized Software
Application Layer Protocol: Web Protocols (T1071.001)	**IG2** 13.3: Deploy a Network Intrusion Detection Solution **IG3** 13.8: Deploy a Network Intrusion Prevention Solution
Application Layer Protocol: DNS (T1071.004)	**IG1** 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 9.2: Use DNS Filtering Services
Ingress Tool Transfer (T1105)	**IG2** 13.3: Deploy a Network Intrusion Detection Solution **IG3** 13.8: Deploy a Network Intrusion Prevention Solution
Dynamic Resolution (T1568)	**IG1** 9.2: Use DNS Filtering Services
Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002)	**IG1** 9.2: Use DNS Filtering Services

— IG1 — IG2 — IG3

Detection Opportunities

Given APT29's highly capable abilities and evasive activities, it is recommended to implement a strong baseline of mitigation strategies mapped from known MITRE ATT&CK TTPs. Once defenses are implemented, it is recommended to iterate over them with reliable, repeatable testing and strengthening as needed:

The following detection opportunities are mapped to MITRE ATT&CK v9 techniques, CIS v8 safeguards, and provide appropriate Red Canary Atomic Red Team tests to undertake for validation:

Detection Opportunity 1: Detecting mshta.exe execution

MITRE ATT&CK: Scheduled Task/Job: Scheduled Task (T1053.005)

CIS Control(s): 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts, 8.3: Ensure Adequate Audit Log Storage

Red Canary Atomic Red Team Test(s): T1053.005 - Scheduled Task Atomic Test #1

APT29 has been observed establishing persistence through the Windows Task Scheduler. To better hide the activity, APT29 has masqueraded their 'GoldMax' implant by naming it the same as a legitimate application already installed on the device. The implant is then stored in a subfolder of the same name within ProgramData.

Alerting on the creation and modification of scheduled tasks being executed from the ProgramData folder will protect your environment from a common APT29 persistence method.

Detection Opportunity 2: Detect Rundll32.exe loading files ending with .sys

MITRE ATT&CK: Signed Binary Proxy Execution: Rundll32 (T1218.011)

CIS Control(s): 10.5: Enable Anti-Exploitation Features (IG2+)

Red Canary Atomic Red Team Test(s): T1218.011 - Rundll32 Atomic Test #8

APT29's Sibot malware downloads a DLL file from its C2, then store it as a .sys file in the '%windir%\system32\drivers' folder. From there, windll32.exe is invoked to run the .sys file.

By setting up an alert when rundll32.exe loads a file explicitly with the extension .sys, you will be defending against APT29's Sibot malware.

Detection Opportunity 3: Detect VBScript loaded in the registry

MITRE ATT&CK: Modify Registry (T1112)

CIS Control(s): 4.1: Establish and Maintain a Secure Configuration Process

Red Canary Atomic Red Team Test(s): T1112 - Modify Registry Atomic Test #2

APT29's Sibot malware has been observed loading a second-stage script into the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\sibot.

Sibot is written in VBScript, so running regular searches to look for VBScript stored in the registry will keep your systems free from malicious software used by APT29. To avoid false positives when performing the search, exclude the common AutoRun locations '\Microsoft\Windows\CurrentVersion\Run' and '\Microsoft\Windows\CurrentVersion\RunOnce'.

Resources

attack.mitre.org

fireeye.com

community.riskiq.com

microsoft.com

cyber.gov.au

whitehouse.gov

crowdstrike.com

redcanary.com

Table of Contents