blackpoint

THREAT PROFILE:

APT29

Table of Contents

Executive Summary

First Identified:
2008

Attributed Country:
Russia's Foreign Intelligence Services (SVR)

Known Associations:
- APT28
- Indrik Spider

Also Known As:
- APT-C-42
- ATK 7
- Blue Dev 5
- Blue Kitsune
- BlueBravo
- Cloaked Ursa
- CloudLook
- Cozy Bear
- Cranefly
- Dark Halo
- Fritillary
- G0016
- Grizzly Steppe
- Group 100
- Iron Hemlock
- Iron Ritual
- ITG11
- Midnight Blizzard
- Minidionis
- Nobellium
- NobleBaron
- SilverFish
- StellarParticle
- TA421
- TEMP.Monkeys
- The Dukes
- UAC-0029
- UNC3524
- UNC2452
- Yttrium

INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

Valid accounts, abuse of remote services, drive-by compromise, vulnerability exploitation, supply chain attacks, trusted relationship, social engineering (MITRE ATT&CK: T1078, T1133, T1189, T1190, T1195, T1199, T1566)

Boot or logon initialization scripts, scheduled tasks, valid accounts, manipulating accounts, creating accounts, server software component, create/modify system process, event triggered execution, boot or logon autostart execution, hijack execution flow (MITRE ATT&CK: T1037, T1053, T1078, T1136, T1505, T1543, T1546, T1547, T1574)

Abuse of remote services, software deployment tools, exploiting vulnerabilities, alternate authentication material, lateral tool transfer (MITRE ATT&CK: T1021, T1072, T1210, T1550, T1570)

Description

APT29 (AKA Cozy Bear, Midnight Blizzard, Cloaked Ursa, Grizzly Steppe, Iron Hemlock) is an advanced persistent threat (APT) group attributed to Russia's Foreign Intelligence Service (SVR) that has been active since at least 2008. Russia's SVR is the primary civilian foreign intelligence service and is reportedly responsible for the collection of foreign intelligence using human, signals, electron, and cyber methods. While Russia's Main Directorate of the General Staff (GRU) has been attributed with more destructive and well-known operations, SVR has been assessed to have the priority of remaining undetected and collecting intelligence while remaining secretive.

One of APT29's most notable attacks is the 2020 SolarWinds data breach. The SolarWinds breach was a supply chain attack where APT29 used customized malware to inject malicious code into the SolarWinds Orion software build process. The update was then delivered to clients as a normal software update; the group was also observed conducting password spraying attacks to compromise user accounts once they gained access to victim environments. More than 18,000 SolarWinds customers installed the malicious update; however, the group appeared to select only targets that would be of strategic interest for follow-on activity. The threat group was able to steal sensitive information from thousands of organizations worldwide, accessing email accounts and information that could be used for future malicious activity.

APT29 has been observed gaining initial access via social engineering attacks, password spraying attacks, using valid accounts, exploiting vulnerabilities, supply chain attacks, drive-by compromise, and abusing external remote systems.

APT29 has been attributed to Russia's Foreign Intelligence Service (SVR), primarily focusing on collection of foreign intelligence.

APT29 has been observed gaining persistence via backdoor and web shell malware variants, manipulating and adding accounts to compromised networks, conducting password spraying attacks to gain access to additional accounts, scheduled tasks, adding Registry Run keys, hijacking legitimate application-specific startup scripts to run malware on system startup, and WMI event subscriptions.

APT29 has been observed achieving lateral movement via abusing remote services, exploiting vulnerabilities, Kerberos ticket attacks, lateral tool transfer, and software deployment tools – Azure, Microsoft, and more. The group has been observed using legitimate tools, such as PsExec, to move laterally through a victim environment.

APT29 is considered a sophisticated and highly adaptable threat group based on their ability to adapt to different environments, remain undetected, and their ability to create bespoke tools and malware that can be used to conduct specific targeted attacks. It is very likely APT29 will remain a credible threat to organizations worldwide that maintain information that would be of strategic interest to Russia's government.

Previous Targets: APT29

Previous Industry Targets

- **Academics**
- **Basic Materials**
- **Consumer Cyclicals**
  - Hotels & Entertainment
  - Retail
- **Consumer Non-Cyclicals**
- **Energy**
- **Financials**
  - Insurance
- **Government**
- **Healthcare**
- **Industrials**
  - Construction & Engineering
  - Manufacturing
  - Transportation
- **Institutions & Entertainment**
- **Professional & Commercial Services**
  - Business Services
  - Legal Services
- **Real Estate**
- **Technology**
  - Telecommunications
- **Utilities**

Previous Targets: APT29

Previous Victim HQ Regions

- **Africa**
  - Uganda
- **Asia**
  - Azerbaijan, Chechnya, China, Georgia, India, Israel, Japan, Kazakhstan, Kyrgyzstan, Lebanon, Russia, Singapore, South Korea, Thailand, UAE, Uzbekistan
- **Europe**
  - Austra, Belarus, Belgium, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom
- **North America**
  - Canada, Mexico, United States
- **Oceania**
  - Australia, New Zealand
- **South America**
  - Brazil, Chile

Known Operations: APT29

2013	APT29 was attributed with targeting organizations by exploiting CVE-2013-0640 in Adobe Reader, the attacks involved the use of social engineering attacks for initial access.
2013 - 2019	Operation Ghost. APT29 was attributed with conducting a long-term campaign against government entities across Europe and North America. The group reportedly used social engineering attacks to gain access before deploying loader and backdoor malware variants to steal sensitive information.
2014	APT29 was attributed with targeting victims worldwide with the CosmicDuke malware variant. The goal of the campaign was to reportedly steal sensitive information.
2014	Operation Monkeys. APT29 was attributed with targeting a Washington D.C.-based research institute with the CozyCar malware variant. The group reported gain access via social engineering attacks luring victims to click on a flash video of office monkeys.
2015	APT29 was attributed with conducting a spearphishing attack on the U.S. Pentagon causing the shutdown of the entire Joint Staff unclassified email system and internet access during the period of the investigation.
2016	APT29 was attributed with targeting email accounts linked to Hilary Clinton's 2016 presidential campaign and the U.S. Democrat National Committee (DNC). The group reportedly used the Bit.ly URL-shortening service to hide the location of a spoofed Google login page. The group was blamed alongside APT28.
2016	APT29 was attributed with conducting sophisticated spearphishing attacks against U.S.-based think tanks and non-governmental organizations, likely in an attempt to gather information that would be of strategic interest to the Russian government.
2017	APT29 was attributed with launching a spearphishing attack against the Norwegian government, including the Ministry of Defense, Ministry of Foreign Affairs, and the Labour Party.

Known Operations: APT29

2017	APT29 was attributed with targeting Dutch ministries, including the Ministry of General Affairs. The group reportedly attempted to access sensitive government-related documents.
2018	APT29 was attributed with sending phishing emails impersonating the U.S. Department of State with links to zip files containing malicious Windows shortcuts that delivered the Cobalt Strike Beacon.
2019 - 2020	APT29 was attributed with launching an attack against SolarWinds. The group used customized malware to inject malicious code into the SolarWinds Orion software build process. The update was then delivered to clients as a normal software update; the group was also observed conducting password spraying attacks to compromise user accounts once they gained access to victim environments.
2019 - 2022	APT29 was attributed with launching a phishing campaign against multiple organizations to deploy the QUEITEXIT malware variant.
2020	APT29 was attributed with conducting phishing attacks with COVID-19 lures to target organizations across Canada, the U.S., and the U.K., likely in an attempt to collect information related to COVID-19 vaccine development and testing
2021	APT29 was attributed with targeting the Slovak government with several phishing email. The emails posed as the Slovak National Security Authority (NBU) that included malicious documents, often an ISO image file
2021	APT29 was attributed with targeted the French government, specifically compromising email accounts and then using the access to deliver malicious emails to foreign institutions.
2021	APT29 was attributed with targeting multiple organizations with the FoggyWeb malware to remotely exfiltrate the configuration database of compromised AD FD servers, decrypted token-signing certificate, and token-decryption certificate, as well as to download and execute additional components.

Known Operations: APT29

2021	APT29 was attributed with sending phishing emails purportedly from the USAID government agency that contained a malicious link that resulted in an ISO file being delivered. The file contained a malicious LNK file, a malicious DLL file, and a legitimate lure referencing foreign threats to the 2020 US Federal Elections.
2021	APT29 was attributed with conducting password spraying and brute force attacks against multiple organizations, three successful attacks resulted in information stealing malware and the group accessing basic account information.
2021	APT29 was attributed with targeting Synnex, a contractor that provides IT services for the Republican National Committee (RNC). The group reportedly used the access to attempt to breach the RNC to collect information.
2021	APT29 was attributed with targeting organizations integral to the global IT supply chain, likely in an attempt to collect sensitive information.
2021	APT29 was attributed with sending spearphishing emails generally containing and HTML attachment that delivers an ISO disk image file that contains a malicious LNK file, a malicious DLL, and a decoy document to target European diplomats.
2022	APT29 was attributed with impersonating an individual associated with the Turkish embassy and conducting spearphishing attacks. The group reportedly used COVID-19 as a lure for the attacks.
2022	APT29 was attributed with attacks targeting Microsoft 365 accounts, likely to send phishing emails from legitimate accounts and steal information contained within the accounts.
2023	APT29 was attributed with launching phishing emails utilizing a theme suggestive of an ambassador's schedule in order to deliver the GraphicalNeutrino malware variant.

Known Operations: APT29

2023	APT29 was attributed with sending phishing emails targeting diplomatic missions with Ukraine by leveraging topics that would be of interest to the targeted individual, including “BMW for Sale”, humanitarian assistance for an earthquake, and more.
2023	APT29 was attributed with sending phishing emails to diplomatic entities and systems transmitting sensitive information about the region's politics, aiding Ukrainian citizens fleeing the country, and providing help to the government of Ukraine. The group reportedly used a lure related to Poland’s Ambassador’s visit to the U.S.
2023	APT29 was attributed with conducting social engineering attacks using credential theft phishing lures sent as Microsoft Teams chats. The group sent the messages to nearly 40 organizations worldwide in the Government, Technology, Manufacturing, and Consumer Cyclicals verticals.
2023	APT29 was attributed with targeting the Microsoft Office 365 email environment of Hewlett Packard Enterprise (HPE) to steal data from the cybersecurity team and other departments.
2023	APT29 was attributed with conducing password spray, brute force, and token theft techniques to target organizations worldwide.
2023	APT29 was attributed with sending phishing emails with malicious PDF attachments to deliver malware variants. The group was observed using Zulip for C2 activities that appeared as legitimate web traffic
2023	APT29 was attributed with targeting government embassies globally by exploiting CVE-2023-38831.
2023	APT29 was attributed with targeting organizations worldwide by exploiting CVE-2023-42793, targeting servers hosting JetBrains TeamCity software.

Known Operations: APT29

2023 - 2024	APT29 was attributed with targeting Microsoft in a cyberespionage campaign. The threat group reportedly used password spraying attacks to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access Microsoft corporate email accounts.
2024	APT29 was attributed with targeting German political parties with a CDU-themed lure to deploy the WINELOADER malware variant.

Known Counter Operations: APT29

2014	Dutch Intelligence Service, AIVD, hacking team provided the FBI with crucial information about Russian interference with the U.S. elections.
2018	Special Counsel Robert Mueller indicted 12 Russian military officials and accused them of hacking into two Democratic Party computer systems to sabotage the 2016 presidential election. The group was blamed alongside APT28.
2021	The U.S. Biden administration signed an Executive Order on additional sanctions against Russia including blocking property with respect to specified harmful foreign activities of the Government of the Russian Federation.
2021	The U.S. seized two C2 and malware distribution domains used in spearphishing campaigns attributed to APT29. The goal was to disrupt the threat group follow-on exploitation of victims, as well as identifying compromised victims.

Known Exploited Vulnerabilities

CVE-2018-13379 (CVSS: 9.8)

Credential Exposure Vulnerability
Product Affected: Fortinet FortiOS SSL VPN

CVE-2019-11510 (CVSS: 10)

Arbitrary File Reading Vulnerability
Product Affected: Pulse Connect Secure VPN

CVE-2019-1653 (CVSS: 7.5)

Improper Access Control Vulnerability
Product Affected: Cisco RV320 and RV325 Routers

CVE-2019-19781 (CVSS: 9.8)

Directory Traversal Vulnerability
Product Affected: Citrix Application Delivery Controller and Citrix Gateway

CVE-2019-2725 (CVSS: 9.8)

Deserialization Vulnerability
Product Affected: Oracle WebLogic Server

CVE-2019-7609 (CVSS: 10)

Arbitrary Code Execution Vulnerability
Product Affected: Kibana

CVE-2019-9670 (CVSS: 9.8)

XML External Entity injection (XXE) Vulnerability
Product Affected: Synacor Zimbra Collaboration (ZCS)

CVE-2020-0688 (CVSS: 8.8)

Static Key Vulnerability
Product Affected: Microsoft Exchange

Known Exploited Vulnerabilities

CVE-2020-14882 (CVSS: 9.8)

RCE Vulnerability
Product Affected: Oracle WebLogic Server

CVE-2020-4006 (CVSS: 9.1)

Command Injection Vulnerability
Product Affected: VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector

CVE-2020-5902 (CVSS: 9.8)

RCE Vulnerability
Product Affected: F5 BIG-IP Traffic Management User Interface

CVE-2021-21972 (CVSS: 9.8)

RCE Vulnerability
Product Affected: VMware vCenter Server

CVE-2021-26857 (CVSS: 7.8)

Deserialization Vulnerability
Product Affected: Microsoft Unified Messaging

CVE-2021-26858 (CVSS: 7.8)

RCE Vulnerability
Product Affected: Microsoft Exchange Server

CVE-2021-27065 (CVSS: 7.8)

RCE Vulnerability
Product Affected: Microsoft Exchange Server

Known Exploited Vulnerabilities

CVE-2021-36934 (CVSS: 7.8)

Elevation of Privilege Vulnerability
Product Affected: Microsoft Windows SAM

CVE-2022-30170 (CVSS: 7.3)

Elevation of Privilege Vulnerability
Product Affected: Windows Credential Roaming Service

CVE-2023-0640 (CVSS: 9.3)

RCE Vulnerability
Product Affected: Adobe Reader and Acrobat

CVE-2023-38831 (CVSS: 7.8)

RCE Vulnerability
Product Affected: RARLAB WinRAR

CVE-2023-42793 (CVSS: 9.8)

Authentication Bypass Vulnerability
Product Affected: JetBrains TeamCity

ProxyLogon (CVE-2021-26855) (CVSS: 9.8)

RCE Vulnerability
Product Affected: Microsoft Exchange Server

ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) (CVSS: 9.8, 9.8, 7.2)

Pre-Auth Path Confusion, Privilege Escalation, Post-Auth RCE Vulnerabilities
Product Affected: Microsoft Exchange Server

Associations: APT29

Russia

APT29 has been attributed to Russia's Foreign Intelligence Service (SVR).

APT28

Both APT28 and APT29 are referred to as "GRIZZLY STEPPE" by the U.S. Government and were both connected to the 2016 DNC cyberattack, indicating that the groups likely cooperate in some capacity.

Indrik Spider

Indrik Spider is the threat group behind the WastedLocker ransomware operation; APT29 has been observed involved in attacks that resulted in WastedLocker deployments.

APT-C-42

APT29 Alias used by Qihoo 360

ATK 7

APT29 alias used by Thales

Blue Dev 5

APT29 alias used by PWC

Blue Kitsune

APT29 alias used by PWC

BlueBravo

APT29 alias used by Recorded Future

Cloaked Ursa

APT29 alias used by Palo Alto

CloudLook

APT29 alias used by Kaspersky

Associations: APT29

Cozy Bear
APT29 alias used by CrowdStrike

Cranefly
APT29 alias used by Symantec

Dark Halo
APT29 alias used by Volexity

Fritillary
APT29 Alias used by Symantec

G0016
APT29 alias used by MITRE

Grizzly Steppe
APT29 alias used by U.S. Government

Group 100
APT29 alias used by Thalos

Iron Hemlock
APT29 alias used by SecureWorks

Iron Ritual
APT29 alias used by SecureWorks

ITG11
APT29 alias used by IBM

Midnight Blizzard
APT29 alias used by Microsoft

Associations: APT29

Minidionis

APT29 alias used by Palo Alto

Nobelium

APT29 alias used by Microsoft. There has been fluctuating opinions on the validity of APT29 and Nobelium being the same group, with some researchers (including the French CERT) indicating that Nobelium is likely a separate group connected to the same government entity as APT29.

NobleBaron

APT29 alias used by Unknown

SilverFish

APT29 Alias used by Prodaft

StellarParticle

APT29 alias used by CrowdStrike

TA421

APT29 alias used by Proofpoint

TEMP.Monkeys

APT29 alias used by FireEye

The Dukes

APT29 alias used by F-Secure

UAC-0029

APT29 alias used by CERT-UA

UNC3524

APT29 alias used by Mandiant

Associations: APT29

UNC2452

APT29 alias used by Mandiant

Yttrium

APT29 alias used by Microsoft

Known Tools: APT29

7zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
AADInternals	A PowerShell module that can be used to access Azure Active Directory and Microsoft 365.
AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
AtNow	A command line utility that schedules programs and commands to run in the near future; the commands are executed within 70 seconds or less from the moment that AtNow utility is run.
BloodHound	An Active Directory reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.
Brute Ratel C4	A post-exploitation tool that enables operators to deploy agents (badgers) while inside a target environment that enable arbitrary command execution to perform lateral movement, privilege escalation, and establish additional avenues of persistence.
cmd	A program used to execute commands on a Windows computer.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
Constant Contact	A tool that is used to create and send email, schedule posts, create ads, and more. It can be used by threat actors to create phishing emails and malicious ads.
DONUT	A publicly available tool that creates position-independent shellcode that loads .NET assemblies, PE files, and other Windows payloads from memory and runs them with parameters.
Dropbox	A cloud storage service that allows users to save files online and sync them to other devices.

Known Tools: APT29

Empire	An open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure PowerShell for Windows and Python for Linux/macOS.
eTrustEx	A tool used in the EU for information exchange and secure data transfer; it has been used as a lure to target government entities in Europe.
Firebase	A set of backend cloud computing services and application development platforms that has been used by threat actors to host malicious tools and software.
fsutil	A Windows utility that performs tasks that are related to file allocation table (FAT) and NTFS file systems, such as managing reparse points, managing sparse files, or dismounting a volume.
Google Drive	A file storage and synchronization service that threat actors have used to host malware or export stolen files to.
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.
ipconfig	A command line utility that is used to display and manage the IP address assigned to the machine.
Koadic	A Windows post-exploitation framework and penetration testing tool that is publicly available on GitHub.
LegisWrite	An editing program that allows secure document creation, revision, and exchange between governments in the EU. It has been used as a lure, likely in an attempt to lure victims in the Government vertical.
meek	An open-source TOR plugin that tunnels TOR traffic through HTTPS connections.
Microsoft Teams	A instant messaging app that has been abused by malicious actors to impersonate victims' IT staff or helpdesk and deliver social engineering attacks that facilitated malware attacks.

Known Tools: APT29

Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
mshta	A Windows-native binary designed to execute Microsoft HTML Application (HTA) files.
NativeZone	An umbrella term for Nobelium's wide variety of custom Cobalt Strike Beacon loaders.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
netsh	A scripting utility used to interact with networking components on local or remote systems.
nltest	A Windows command-line utility used to list domain controllers and enumerate domain trusts.
Notion	A freemium productivity and note-taking web application. The Notion API has been used as a C2 in reported cyberattack incidents.
OneDrive	A file hosting service operated by Microsoft. It allows users to store, share, and sync files and can work as the storage backend of the web version of Microsoft 365/Office.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PowerSploit	An open source, offensive security framework comprised of PowerShell modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing anti-virus, recon, and exfiltration.
PsExec	A utility tool that allows users to control a computer from a remote location.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.

Known Tools: APT29

Reg	A Windows utility used to interact with the Windows Registry; it can be used at the command-line interface to query, add, modify, and remove information.
Rubeus	A C# toolset for raw Kerberos interaction and abuses.
rundll32	A command line utility in Microsoft Windows used to run DLLs on the Windows operating system.
Sdelete	An application that securely deletes data in a way that makes it unrecoverable.
Sharp-SMBExec	A native C# conversion of the Invoke-SMBExec PowerShell script.
SharpView	A PowerShell tool and a .NET port of PowerView used to gain situational awareness of the Active Directory.
Sliver	An open-source cross-platform adversary emulation/red team framework. It has been increasingly used by threat actors due to the number of tools available, including dynamic code generation, staged and stageless payloads, server C2, and more.
SOLARDEFLECTION	An infrastructure observed being utilized in APT29 cyberattacks.
SystemInfo	A Windows utility that can be used to gather detailed information about a computer.
Tasklist	A legitimate Windows file that is used by malware to terminate processes on the victims' computer.
TOR	An open-source software for enabling anonymous communication, making it more difficult to trace a user’s internet activity.
Trello	A web-based, kanban-style, list-making application; it has been used to host malicious tools and malware.

Known Tools: APT29

WinRM	Microsoft's version of the WS-Management protocol, which is a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows interoperation between hardware and operating systems from different vendors.
WMI	A utility that allows script languages to manage Microsoft Windows personal computers and server.
Zulip	An open-source chat and collaborative software that has been used by threat actors for C2 communication.

Known Malware: APT29

ATI-Agent	A remote access trojan (RAT) that can be used to gain persistent access to victim environments.
BEATDROP	A downloader written in C that makes use of Trello for C2. The malware first maps its own copy of ntdll.dll into memory for the purpose of executing shellcode in its own process.
BOOMBOX	A downloader that can establish persistence, execute an LDAP query, and steal information.
BURNTBATTER	An in memory loader responsible for decrypting and executing a payload from disk into a running process.
CEELOADER	A loader malware that can be used to download and execute additional malware payloads.
CloudDuke	AKA Cloud Duke, MiniDionis, CloudLook. A malware toolset that consists of a loader, a downloader, and two backdoors. The malware tools allow threat actors to access compromised devices, manipulate files, steal sensitive information, and deploy additional payloads.
CosmicDuke	AKA TinyBaron, BotgenStudios, NemesisGemina. An information stealing malware that can act as a keylogger, take screenshots, steal clipboard contents, steal user files, export information, and collect credentials.
CozyCar	AKA CozyDuke, CozyBear, Cozer, EuroAPT. A backdoor malware used by APT29 from 2010-2015. The malware can download and execute modules and steal system information.
Danfuan	A backdoor malware that is a DynamicCodeCompiler that compiles and executes received C# code.
DAVESHELL	Shellcode that functions as an in memory dropper relying on reflective injection.
EnvyScout	AKA ROOTSAW. A first-stage payload and malware dropper that has been used to deploy second stage malware, such as WINELOADER.
FatDuke	A backdoor that can execute PowerShell scripts, copy files, enumerate directories, and secure delete its DLL.

Known Malware: APT29

FOGGYWEB	A backdoor capable of remotely exfiltrating sensitive information from a compromised Active Directory Federated Services server.
GeminiDuke	A malware that collects information on local user accounts from the victim, collects information on running processes, and network settings.
Geppei	A dropper malware that uses PyInstaller, reads commands from a legitimate IIS log, and drops additional malware payloads.
GOLDFINDER	A backdoor malware written in Go that was likely used as a custom HTTP tracer tool that logged the route or hops that a packet took to reach the hardcoded C2 server.
GOLDMAX	AKA SUNSHUTTLE. A second stage C2 backdoor written in Go with Windows and Linux versions. The malware was identified during the investigation of the SolarWinds intrusion.
GraphicalNeutrino	AKA SNOWYAMBER. A backdoor used to target Windows devices that uses notion databases as a C2. The malware contacts its C2 server for shellcode payloads to download and execute. The malware uses DLL search-order hijacking in order to execute.
GraphicalProton	AKA GraphDrop, SPICYBEAT. A loader malware that is able to deliver second stage malware and uses Microsoft OneDrive for C2 communication.
HALFRIG	A stager for Cobalt Strike beacon that has been used in cyber espionage campaigns. The malware was used for the first known time in February 2023.
HAMMERTOSS	AKA HammerDuke, NetDuke, tDiscoverer. A backdoor malware that can be used to steal data from compromised systems.
ICEBEAT	A downloader malware that uses the open source Zulip messaging platform for C2.
ICEBREAKER	A modified version of VaporRage - A Shellcode downloader that has the ability to download malicious shellcode to compromised systems.

Known Malware: APT29

LiteDuke	A third stage backdoor used by APT29 from 2014-2015.
MagicWeb	A post-compromise tool used to gain persistent access to compromised environments.
MiniDuke	Malware used by APT29 from 2010-2015 and consists of multiple downloader and backdoor components. The malware can enumerate local drives, download additional malware, and gather system information.
OnionDuke	Malware that has the capability to use a DoS module, steals credentials, and uses Twitter as a backup C2.
PinchDuke	Malware that steals credentials, collects user files, searches for files created within a certain timeframe, and gathers system configuration information.
PolyglotDuke	A downloader that can retrieve payloads from the C2 and can use Twitter, Reddit, Imgur, and other websites to get a C2 URL.
POSHSPY	A backdoor used since at least 2015, it has been used as a secondary backdoor if access is lost with the first backdoor.
PowerDuke	A backdoor used by APT29 in 2016 that can overwrite and delete files, download additional payloads, and collect user and system information.
QUARTERPIG	AKA MUSKYBEAT. An in memory dropper that decodes the next-stage payload and strings using RC4 and executes in the current process. The malware shares code overlaps with the HALFRIG malware and was first used publicly in March 2023.
QuietExit	A novel backdoor malware that can be used to gain persistent access, evade detection, and communicate with the C2 server.
RAINDROP	A loader that was discovered on some victim machines during investigations related to the SolarWinds incident.
RegDuke	A first stage implant written in .NET and has been used by APT29 since at least 2017. The malware has been used to control a compromised machine.

Known Malware: APT29

ReGeorg	A web shell used to maintain persistent access to a compromised system.
SeaDuke	AKA SeaDaddy, SeaDesk, SeaDask. A malware used by APT29 from 2014-2015 that has been used a secondary backdoor for victims that were already compromised with CozyCar.
Sibot	A dual-purpose malware written in VBScript designed to achieve persistence on a compromised system as well as download and execute additional payloads.
SoreFang	A first stage downloader used by APT29 that can collect usernames, enumerate domain accounts, and deploy additional payloads.
STATICNOISE	A downloader written in C responsible for downloading and executing the final-stage payload in memory.
SUNBURST	AKA Solorigate. A trojanized DLL designed to fit within the SolarWind's Orion Software update framework.
SUNSPOT	An implant that injected the Sunburst backdoor into the SolarWinds Orion software update framework.
SUPERNOVA	An in memory web shell written in .NET C# that can be used to gain persistent access to victim environments.
TEARDROP	A memory-only dropper that was discovered on some victim machines during investigations related to the 2020 SolarWinds cyber intrusion.
TRAILBLAZER	A modular malware that can collect sensitive information.
VaporRage	AKA BOOMMIC. A Shellcode downloader that has the ability to download malicious shellcode to compromised systems.
WastedLocker	A ransomware family that has been used against a variety of targets worldwide.
WellMail	A lightweight malware written in Golang that can archive files, exfiltrate files, and identify the current username.

Known Malware: APT29

WellMess	AKA elf.wellmess. A lightweight malware written in .NET and Golang that has the ability to use DNS tunneling for C2 communications, exfiltrate data, and collect host and system information.
WINELOADER	A backdoor malware that can be used to gain persistent access to target environments and steal sensitive data.

MITRE ATT&CK® Mappings: APT29

Reconnaissance	
T1589: Gather Victim Identity Information	.001: Credentials
T1595: Active Scanning	.002: Vulnerability Scanning
T1598: Phishing for Information	
Resource Development	
T1583: Acquire Infrastructure	.001: Domains .003: Virtual Private Server .006: Web Services
T1584: Compromise Infrastructure	.001: Domains .006: Web Services
T1585: Establish Accounts	.001: Social Media Accounts
T1586: Compromise Accounts	.002: Email Accounts .003: Cloud Accounts
T1587: Develop Capabilities	.001: Malware .003: Digital Certificates
T1588: Obtain Capabilities	.002: Tool .004: Digital Certificates
T1608: Stage Capabilities	.005: Link Target
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts .003: Local Accounts .004: Cloud Accounts

MITRE ATT&CK® Mappings: APT29

Initial Access	
T1133: External Remote Services	
T1189: Drive-by Compromise	
T1190: Exploit Public-Facing Application	
T1195: Supply Chain Attack	.001: Compromise Software Dependencies and Development Tools .002: Compromise Software Supply Chain
T1199: Trusted Relationship	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link .003: Spearphishing via Service
Execution	
T1047: Windows Management Instrumentation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .005: Visual Basic .006: Python .009: Cloud API
T1072: Software Deployment Tools	
T1106: Native API	
T1129: Shared Modules	

MITRE ATT&CK® Mappings: APT29

Execution	
T1203: Exploitation for Client Execution	
T1204: User Execution	.001: Malicious Link .002: Malicious File
T1559: Inter-Process Communication	
T1569: System Services	.002: Service Execution
T1651: Cloud Administration Command	
Persistence	
T1037: Boot or Logon Initialization Scripts	.004: RC Scripts
T1053: Scheduled Task/Job	.005: Scheduled Task
T1078: Valid Accounts	.002: Domain Accounts .003: Local Accounts .004: Cloud Accounts
T1098: Account Manipulation	.001: Additional Cloud Credentials .002: Additional Email Delegate Permissions .003: Additional Cloud Roles .005: Device Registration
T1136: Create Account	.003: Cloud Account
T1505: Server Software Component	.003: Web Shell
T1543: Create or Modify System Process	.003: Windows Service

MITRE ATT&CK® Mappings: APT29

Persistence	
T1546: Event Triggered Execution	.003: Windows Management Instrumentation Event Subscription .008: Accessibility Features
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder .009: Shortcut Modification
T1574: Hijack Execution Flow	.002: DLL Side .008: Path Interception by Search Order Hijacking
Privilege Escalation	
T1055: Process Injection	.002: Portable Executable Injection
T1068: Exploitation for Privilege Escalation	
T1098: Account Manipulation	.001: Additional Cloud Credentials .002: Additional Email Delegate Permissions .003: Additional Cloud Roles .005: Device Registration
T1134: Access Token Manipulation	.001: Token Impersonation/Theft
T1484: Domain or Tenant Policy Modification	.002: Trust Modification
T1543: Create or Modify System Process	.003: Windows Service
T1547: Boot or Logon Autostart Execution	.009: Shortcut Modification
T1574: Hijack Execution Flow	.002: DLL Side .008: Path Interception by Search Order Hijacking

MITRE ATT&CK® Mappings: APT29

Defense Evasion	
T1027: Obfuscated Files or Information	.001: Binary Padding .002: Software Packing .003: Steganography .005: Indicator Removal from Tools .006: HTML Smuggling
T1036: Masquerading	.004: Masquerade Task or Service .005: Match Legitimate Name or Location
T1055: Process Injection	.002: Portable Executable Injection
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion .006: Timestomp .008: Clear Mailbox Data
T1112: Modify Registry	
T1127: Trusted Developer Utilities Proxy Execution	
T1134: Access Token Manipulation	.001: Token Impersonation/Theft
T1140: Deobfuscate/Decode Files or Information	
T1202: Indirect Command Execution	
T1211: Exploitation for Defense Evasion	
T1218: System Binary Proxy Execution	.005: Mshta .011: Rundll32
T1480: Execution Guardrails	
T1484: Domain or Tenant Policy Modification	.002: Trust Modification

MITRE ATT&CK® Mappings: APT29

Defense Evasion	
T1497: Virtualization/Sandbox Evasion	.003: Time Based Evasion
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control
T1550: Use Alternate Authentication Material	.001: Application Access Token
T1553: Subvert Trust Controls	.002: Code Signing .005: Mark-of-the-Web Bypass
T1556: Modify Authentication Process	.007: Hybrid Identity
T1562: Impair Defenses	.001: Disable or Modify Tools .002: Disable Windows Event Logging .004: Disable or Modify System Firewall .008: Disable or Modify Cloud Logs
T1564: Hide Artifacts	.001: Hidden Files and Directories
T1574: Hijack Execution Flow	.008: Path Interception by Search Order Hijacking
T1620: Reflective Code Loading	
Credential Access	
T1003: OS Credential Dumping	.002: Security Account Manager .003: NTDS .004: LSA Secrets .006: DCSync .008: /etc/passwd and /etc/shadow
T1110: Brute Force	.001: Password Guessing .003: Password Spraying
T1111: Multi-Factor Authentication Interception	

MITRE ATT&CK® Mappings: APT29

Credential Access	
T1212: Exploitation for Credential Access	
T1528: Steal Application Access Token	
T1539: Steal Web Session Cookie	
T1552: Unsecured Credentials	.001: Credentials in Files .004: Private Keys .006: Group Policy Preferences
T1555: Credentials from Password Stores	.003: Credentials from Web Browsers .005: Password Managers
T1558: Steal or Forge Kerberos Tickets	.003: Kerberoasting
T1606: Forge Web Credentials	.001: Web Cookies .002: SAML Tokens
T1621: Multi-Factor Authentication Request Generation	
T1649: Steal or Forge Authentication Certificates	
Discovery	
T1007: System Service Discovery	
T1012: Query Registry	
T1016: System Network Configuration Discovery	.001: Internet Connection Discovery
T1018: Remote System Discovery	

MITRE ATT&CK® Mappings: APT29

Discovery	
T1046: Network Service Discovery	
T1049: System Network Connections Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.002: Domain Account .004: Cloud Account
T1124: System Time Discovery	
T1135: Network Share Discovery	
T1482: Domain Trust Discovery	
T1497: Virtualization/Sandbox Evasion	.003: Time Based Evasion
T1518: Software Discovery	.001: Security Software Discovery
T1526: Cloud Service Discovery	
T1538: Cloud Service Dashboard	

MITRE ATT&CK® Mappings: APT29

Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .006: Windows Remote Management .007: Cloud Services
T1072: Software Deployment Tools	
T1210: Exploitation of Remote Services	
T1550: Use Alternate Authentication Material	.001: Application Access Token .003: Pass the Ticket .004: Web Session Cookie
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1025: Data from Removable Media	
T1039: Data from Network Shared Drive	
T1074: Data Staged	.002: Remote Data Staging
T1114: Email Collection	.002: Remote Email Collection
T1213: Data from Information Repositories	.002: SharePoint .003: Code Repositories
T1530: Data from Cloud Storage	
T1560: Archive Collected Data	.001: Archive via Utility

MITRE ATT&CK® Mappings: APT29

Command and Control	
T1001: Data Obfuscation	.002: Steganography
T1008: Fallback Channels	
T1071: Application Layer Protocol	.001: Web Protocols .004: DNS
T1090: Proxy	.001: Internal Proxy .002: External Proxy .003: Multi-hop Proxy .004: Domain Fronting
T1095: Non-Application Layer Protocol	
T1102: Web Service	.002: Bidirectional Communication
T1104: Multi-Stage Channels	
T1105: Ingress Tool Transfer	
T1132: Data Encoding	.001: Standard Encoding
T1219: Remote Access Software	
T1568: Dynamic Resolution	.002: Domain Generation Algorithms
T1571: Non-Standard Port	
T1572: Protocol Tunneling	
T1573: Encrypted Channel	.001: Symmetric Cryptography .002: Asymmetric Cryptography

MITRE ATT&CK® Mappings: APT29

Command and Control	
T1665: Hide Infrastructure	
Exfiltration	
T1030: Data Transfer Size Limits	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
T1567: Exfiltration Over Web Service	.001: Exfiltration to Code Repository .002: Exfiltration to Cloud Storage

References

- Avertium (2023, May 31) “Evolution Of Russian APT29 – New Attacks and Techniques Uncovered.” https://explore.avertium.com/resource/evolution-of-russian-apt29-new-attacks-and-techniques-uncovered
- CISA (2021, May) “Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise.” https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf
- CISA (2024, February 26) “SVR Cyber Actors Adapt Tactics for Initial Cloud Access.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a
- ESET Research (2019, October 17) “Operation Ghost: The Dukes aren’t back – they never left.” https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/
- ETDA (2024, April 22) “APT group: APT 29, Cozy Bear, The Dukes.” https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2029%2C%20Cozy%20Bear%2C%20The%20Dukes&n=1
- Homeland Security (2017, February 10) “Enhanced Analysis of GRIZZLY STEPPE Activity.” https://www.cisa.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
- Jenkins, Luke; Atkins, Josh; Black, Dan (2023, September 21) “Backchannel Diplomacy: APT29’s Rapidly Evolving Diplomatic Phishing Operations.” https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing
- Jenkins, Luke; Black, Dan (2024, March 22) “APT29 Uses WINELOADER to Target German Political Parties.” https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties
- Mandiant (2022, April 27) “Assembling the Russian Nesting Doll: UNC2452 Merged into APT29.” https://cloud.google.com/blog/topics/threat-intelligence/unc2452-merged-into-apt29/
- Microsoft Threat Intelligence (2024, January 25) “Midnight Blizzard: Guidance for responders on nation-state attack.” https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/
- MITRE (2024, April 12) “APT29.” https://attack.mitre.org/groups/G0016/
- NCCIC (2016, December 29) “GRIZZLY STEPPE – Russian Malicious Cyber Activity.” https://www.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
- NCSC, CISA, et. al. (2021, May 07) “Advisory: Further TTPs associated with SVR cyber actors.” https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf
- ProDaft (n.d.) “SilverFish Group Threat Actor Report.” https://resources.prodaft.com/silverfish-global-cyber-espionage-campaign
- SOCRadar (2023, May 17) “APT Profile: Cozy Bear / APT29.” https://socradar.io/apt-profile-cozy-bear-apt29/

References

- The BlackBerry Research & Intelligence Team (2023, March 14) “NOBELIUM Uses Poland's Ambassador’s Visit to the U.S. to Target EU Governments Assisting Ukraine.” https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine
- Van Geluwe de Berlaere, Thibault (2022, November 08) “They See Me Roaming: Following APT29 by Taking a Deeper Look at Windows Credential Roaming.” https://cloud.google.com/blog/topics/threat-intelligence/apt29-windows-credential-roaming/
- VMware TAU (2020, March 26) “The Dukes of Moscow.” https://blogs.vmware.com/security/2020/03/the-dukes-of-moscow.html

Adversary Pursuit Group

blackpoint