APT28, IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Forest Blizzard, FROZENLAKE, GruesomeLarch, Group G0007

Archived: 2026-04-05 16:30:38 UTC

Enterprise T1134 .001 Access Token Manipulation: Token Impersonation/Theft

APT28 has used CVE-2015-1701 to access the SYSTEM token and copy it into the current process as part of privilege escalation.[28]

Enterprise T1098 .002 Account Manipulation: Additional Email Delegate Permissions

APT28 has used a Powershell cmdlet to grant the `ApplicationImpersonation` role to a compromised account.[2]

Enterprise T1583 .001 Acquire Infrastructure: Domains

APT28 registered domains imitating NATO, OSCE security websites, Caucasus information resources, and other organizations.[6][14][29]

.003 Acquire Infrastructure: Virtual Private Server

APT28 hosted phishing domains on free services for brief periods of time during campaigns.[26]

.006 Acquire Infrastructure: Web Services

APT28 has used newly-created Blogspot pages for credential harvesting operations.[29]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

APT28 has performed large-scale scans in an attempt to find vulnerable servers.[30]

Enterprise T1557 .004 Adversary-in-the-Middle: Evil Twin

APT28 has used a Wi-Fi Pineapple to set up Evil Twin Wi-Fi Poisoning for the purposes of capturing victim credentials or planting espionage-oriented malware.[14]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Later implants used by APT28, such as CHOPSTICK, use a blend of HTTP, HTTPS, and other legitimate channels for C2, depending on module configuration.[6][2]

.003 Application Layer Protocol: Mail Protocols

APT28 has used IMAP, POP3, and SMTP for a communication channel in various implants, including using self-registered Google Mail accounts and later compromised email servers of its victims.[6][2]

Enterprise T1560 Archive Collected Data

APT28 used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks.[3]

.001 Archive via Utility

APT28 has used a variety of utilities, including WinRAR, to archive collected data with password protection.[2]

During APT28 Nearest Neighbor Campaign, APT28 used built-in PowerShell capabilities (`Compress-Archive` cmdlet) to compress collected data.[27]

Enterprise T1119 Automated Collection

APT28 used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks.[3]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

APT28 has deployed malware that has copied itself to the startup directory for persistence.[21]

Enterprise T1037 .001 Boot or Logon Initialization Scripts: Logon Script (Windows)

An APT28 loader Trojan adds the Registry key `HKCU\Environment\UserInitMprLogonScript` to establish persistence.[31]

Enterprise T1110 Brute Force

APT28 can perform brute force attacks to obtain credentials.[30][21][32]

.001 Password Guessing

APT28 has used a brute-force/password-spray tooling that operated in two modes: in brute-force mode it typically sent over 300 authentication attempts per hour per targeted account over the course of several hours or days.[24] APT28 has also used a Kubernetes cluster to conduct distributed, large-scale password guessing attacks.[2]

.003 Password Spraying

APT28 has used a brute-force/password-spray tooling that operated in two modes: in password-spraying mode it conducted approximately four authentication attempts per hour per targeted account over the course of several days or weeks.[24][32] APT28 has also used a Kubernetes cluster to conduct distributed, large-scale password spray attacks.[2]

During APT28 Nearest Neighbor Campaign, APT28 performed password-spray attacks against public facing services to validate credentials.[27]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

APT28 downloads and executes PowerShell scripts and performs PowerShell commands.[11][21][2]

During APT28 Nearest Neighbor Campaign, APT28 used PowerShell cmdlet `Get-ChildItem` to access credentials, among other PowerShell functions deployed.[27]

.003 Command and Scripting Interpreter: Windows Command Shell

An APT28 loader Trojan uses a cmd.exe and batch script to run its payload.[31] The group has also used macros to execute payloads.[18][33][17][21]

During APT28 Nearest Neighbor Campaign, APT28 used `cmd.exe` for execution.[27]

Enterprise T1092 Communication Through Removable Media

APT28 uses a tool that captures information from air-gapped computers via an infected USB and transfers it to network-connected computer when the USB is inserted.[34]

Enterprise T1586 .002 Compromise Accounts: Email Accounts

APT28 has used compromised email accounts to send credential phishing emails.[29]

Enterprise T1584 .008 Compromise Infrastructure: Network Devices

APT28 compromised Ubiquiti network devices to act as collection devices for credentials compromised via phishing webpages.[26]

Enterprise T1213 Data from Information Repositories

APT28 has collected files from various information repositories.[2]

.002 Sharepoint

APT28 has collected information from Microsoft SharePoint services within target networks.[35]

Enterprise T1005 Data from Local System

APT28 has retrieved internal documents from machines inside victim environments, including by using Forfiles to stage documents before exfiltration.[36][3][30][2]

Enterprise T1039 Data from Network Shared Drive

APT28 has collected files from network shared drives.[2]

Enterprise T1025 Data from Removable Media

An APT28 backdoor may collect the entire contents of an inserted USB device.[34]

Enterprise T1001 .001 Data Obfuscation: Junk Data

APT28 added "junk data" to each encoded string, preventing trivial decoding without knowledge of the junk removal algorithm. Each implant was given a "junk length" value when created, tracked by the controller software to allow seamless communication but prevent analysis of the command protocol on the wire.[6]

Enterprise T1074 .001 Data Staged: Local Data Staging

APT28 has stored captured credential information in a file named pi.log.[34]

During APT28 Nearest Neighbor Campaign, APT28 staged captured credential information in the `C:\ProgramData` directory.[27]

.002 Data Staged: Remote Data Staging

APT28 has staged archives of collected data on a target's Outlook Web Access (OWA) server.[2]

Enterprise T1030 Data Transfer Size Limits

APT28 has split archived exfiltration files into chunks smaller than 1MB.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

An APT28 macro uses the command `certutil -decode` to decode contents of a .txt file storing the base64 encoded payload.[37][11]

During APT28 Nearest Neighbor Campaign, APT28 unarchived data using the GUI version of WinRAR.[27]

Enterprise T1006 Direct Volume Access

During APT28 Nearest Neighbor Campaign, APT28 accessed volume shadow copies through executing `vssadmin` in order to dump the NTDS.dit file.[27]

Enterprise T1561 .001 Disk Wipe: Disk Content Wipe

During APT28 Nearest Neighbor Campaign, APT28 used the native Microsoft utility cipher.exe to securely wipe files and folders – overwriting the deleted data using `cmd.exe /c cipher /W:C` .[27]

Enterprise T1189 Drive-by Compromise

APT28 has compromised targets via strategic web compromise utilizing custom exploit kits.[16] APT28 used reflected cross-site scripting (XSS) against government websites to redirect users to phishing webpages.[26]

Enterprise T1114 .002 Email Collection: Remote Email Collection

APT28 has collected emails from victim Microsoft Exchange servers.[3][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

APT28 installed a Delphi backdoor that used a custom algorithm for C2 communications.[13]

Enterprise T1546 .015 Event Triggered Execution: Component Object Model Hijacking

APT28 has used COM hijacking for persistence by replacing the legitimate `MMDeviceEnumerator` object with a payload.[38][13]

Enterprise T1048 .002 Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

APT28 has exfiltrated archives of collected data previously staged on a target's OWA server via HTTPS.[2]

Enterprise T1567 Exfiltration Over Web Service

APT28 can exfiltrate data over Google Drive.[21]

During APT28 Nearest Neighbor Campaign, APT28 exfiltrated data over public-facing webservers – such as Google Drive.[27]

Enterprise T1190 Exploit Public-Facing Application

APT28 has used a variety of public exploits, including CVE 2020-0688 and CVE 2020-17144, to gain execution on vulnerable Microsoft Exchange; they have also conducted SQL injection attacks against external websites.[14][2]

Enterprise T1203 Exploitation for Client Execution

APT28 has exploited Microsoft Office vulnerability CVE-2017-0262 for execution.[22]

Enterprise T1211 Exploitation for Defense Evasion

APT28 has used CVE-2015-4902 to bypass security features.[39][34]

Enterprise T1068 Exploitation for Privilege Escalation

APT28 has exploited CVE-2014-4076, CVE-2015-2387, CVE-2015-1701, CVE-2017-0263, and CVE-2022-38028 to escalate privileges.[39][34][22][27]

Enterprise T1210 Exploitation of Remote Services

APT28 exploited a Windows SMB Remote Code Execution Vulnerability to conduct lateral movement.[6][40][41]

Enterprise T1133 External Remote Services

APT28 has used Tor and a variety of commercial VPN services to route brute force authentication attempts.[2]

Enterprise T1083 File and Directory Discovery

APT28 has used Forfiles to locate PDF, Excel, and Word documents during collection. The group also searched a compromised DCCC computer for specific terms.[36][3]

Enterprise T1589 .001 Gather Victim Identity Information: Credentials

APT28 has harvested user's login credentials.[32]

Enterprise T1591 Gather Victim Org Information

APT28 has used large language models (LLMs) to gather information about satellite capabilities.[42][43]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

APT28 has saved files with hidden file attributes.[18][18]

.003 Hide Artifacts: Hidden Window

APT28 has used the WindowStyle parameter to conceal PowerShell windows.[11] [44]

Enterprise T1562 .004 Impair Defenses: Disable or Modify System Firewall

During APT28 Nearest Neighbor Campaign, APT28 added rules to a victim's Windows firewall to set up a series of port-forwards allowing traffic to target systems.[27]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

APT28 has cleared event logs, including by using the commands `wevtutil cl System` and `wevtutil cl Security`.[5][3]

.004 Indicator Removal: File Deletion

APT28 has intentionally deleted computer files to cover their tracks, including with use of the program CCleaner.[3]

.006 Indicator Removal: Timestomp

APT28 has performed timestomping on victim files.[5]

Enterprise T1105 Ingress Tool Transfer

APT28 has downloaded additional files, including by using a first-stage downloader to contact the C2 server to obtain the second-stage implant.[39][31][17][21][2]

Enterprise T1056 .001 Input Capture: Keylogging

APT28 has used tools to perform keylogging.[34][3][21]

Enterprise T1559 .002 Inter-Process Communication: Dynamic Data Exchange

APT28 has delivered JHUHUGIT and Koadic by executing PowerShell commands through DDE in Word documents.[44][45][11]

Enterprise T1036 Masquerading

APT28 has renamed the WinRAR utility to avoid detection.[2]

.005 Match Legitimate Resource Name or Location

APT28 has changed extensions on files containing exfiltrated data to make them appear benign, and renamed a web shell instance to appear as a legitimate OWA page.[2]

Enterprise T1498 Network Denial of Service

In 2016, APT28 conducted a distributed denial of service (DDoS) attack against the World Anti-Doping Agency. [14]

Enterprise T1040 Network Sniffing

APT28 deployed the open source tool Responder to conduct NetBIOS Name Service poisoning, which captured usernames and hashed passwords that allowed access to legitimate credentials.[6][40] APT28 close-access teams have used Wi-Fi pineapples to intercept Wi-Fi signals and user credentials.[14]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

APT28 encrypted a .dll payload using RTL and a custom encryption algorithm. APT28 has also obfuscated payloads with base64, XOR, and RC4.[39][37][11][18][17]

Enterprise T1588 .002 Obtain Capabilities: Tool

APT28 has obtained and used open-source tools like Koadic, Mimikatz, and Responder.[11][22][40]

Enterprise T1137 .002 Office Application Startup: Office Test

APT28 has used the Office Test persistence mechanism within Microsoft Office by adding the Registry key `HKCU\Software\Microsoft\Office test\Special\Perf` to execute code.[46]

Enterprise T1003 OS Credential Dumping

APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims. [47][3][14]

.001 LSASS Memory

APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims. [47][3] They have also dumped the LSASS process memory using the MiniDump function.[2]

.002 Security Account Manager

During APT28 Nearest Neighbor Campaign, APT28 used the following commands to dump SAM, SYSTEM, and SECURITY hives: `reg save hklm\sam, reg save hklm\system,` and `reg save hklm\security`.[27]

.003 NTDS

APT28 has used the ntdsutil.exe utility to export the Active Directory database for credential access.[2]

During APT28 Nearest Neighbor Campaign, APT28 dumped NTDS.dit through creating volume shadow copies via `vssadmin`.[27]

Enterprise T1120 Peripheral Device Discovery

APT28 uses a module to receive a notification every time a USB mass storage device is inserted into a victim.[34]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

APT28 sent spearphishing emails containing malicious Microsoft Office and RAR attachments.[37][10][11][3][22][17][21][16]

Enterprise T1598 Phishing for Information

APT28 has used spearphishing to compromise credentials.[32][16]

.003 Spearphishing Link

APT28 has conducted credential phishing campaigns with links that redirect to credential harvesting sites.[29][3][13][14][16]

Enterprise T1542 .003 Pre-OS Boot: Bootkit

APT28 has deployed a bootkit along with Downdelph to ensure its persistence on the victim. The bootkit shares code with some variants of BlackEnergy.[20]

Enterprise T1057 Process Discovery

An APT28 loader Trojan will enumerate the victim's processes searching for explorer.exe if its current process does not have necessary permissions.[31]

Enterprise T1090 .001 Proxy: Internal Proxy

During APT28 Nearest Neighbor Campaign, APT28 used the built-in `netsh portproxy` command to create internal proxies on compromised systems.[27]

.002 Proxy: External Proxy

APT28 used other victims as proxies to relay command traffic, for instance using a compromised Georgian military email server as a hop point to NATO victims. The group has also used a tool that acts as a proxy to allow

C2 even if the victim is behind a router. APT28 has also used a machine to relay and obscure communications between CHOPSTICK and their server.[6][39][3]

.003 Proxy: Multi-hop Proxy

APT28 has routed traffic over Tor and VPN servers to obfuscate their activities.[21]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

During APT28 Nearest Neighbor Campaign, APT28 used RDP for lateral movement.[27]

.002 Remote Services: SMB/Windows Admin Shares

APT28 has mapped network drives using Net and administrator credentials.[2]

During APT28 Nearest Neighbor Campaign, APT28 leveraged SMB to transfer files and move laterally.[27]

Enterprise T1091 Replication Through Removable Media

APT28 uses a tool to infect connected USB devices and transmit itself to air-gapped computers when the infected USB device is inserted.[34]

Enterprise T1014 Rootkit

APT28 has used a UEFI (Unified Extensible Firmware Interface) rootkit known as LoJax.[12][48]

Enterprise T1113 Screen Capture

APT28 has used tools to take screenshots from victims.[47][49][3][16]

Enterprise T1596 Search Open Technical Databases

APT28 has used large language models (LLMs) to assist in script development and deployment.[42][43]

Enterprise T1505 .003 Server Software Component: Web Shell

APT28 has used a modified and obfuscated version of the reGeorg web shell to maintain persistence on a target's Outlook Web Access (OWA) server.[2]

Enterprise T1528 Steal Application Access Token

APT28 has used several malicious applications to steal user OAuth access tokens including applications masquerading as "Google Defender" "Google Email Protection," and "Google Scanner" for Gmail users. They also targeted Yahoo users with applications masquerading as "Delivery Service" and "McAfee Email Protection".[50]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

APT28 executed CHOPSTICK by using rundll32 commands such as `rundll32.exe "C:\Windows\twain_64.dll"` . APT28 also executed a .dll for a first stage dropper using rundll32.exe. An APT28 loader Trojan saved a batch script that uses rundll32 to execute a DLL payload.[5][39][11][31][13][2]

Enterprise T1016 .002 System Network Configuration Discovery: Wi-Fi Discovery

During APT28 Nearest Neighbor Campaign, APT28 collected information on wireless interfaces within range of a compromised system.[27]

Enterprise T1221 Template Injection

APT28 used weaponized Microsoft Word documents abusing the remote template function to retrieve a malicious macro. [51]

Enterprise T1199 Trusted Relationship

Once APT28 gained access to the DCCC network, the group then proceeded to use that access to compromise the DNC network.[3]

Enterprise T1550 .001 Use Alternate Authentication Material: Application Access Token

APT28 has used several malicious applications that abused OAuth access tokens to gain access to target email accounts, including Gmail and Yahoo Mail.[50]

.002 Use Alternate Authentication Material: Pass the Hash

APT28 has used pass the hash for lateral movement.[34]

Enterprise T1204 .001 User Execution: Malicious Link

APT28 has tricked unwitting recipients into clicking on malicious hyperlinks within emails crafted to resemble trustworthy senders.[14][16]

.002 User Execution: Malicious File

APT28 attempted to get users to click on Microsoft Office attachments containing malicious macro scripts.[37][17][16]

Enterprise T1078 Valid Accounts

APT28 has used legitimate credentials to gain initial access, maintain access, and exfiltrate data from a victim network. The group has specifically used credentials stolen through a spearphishing email to login to the DCCC network. The group has also leveraged default manufacturer's passwords to gain initial access to corporate networks via IoT devices such as a VOIP phone, printer, and video decoder.[52][3][23][2]

.004 Cloud Accounts

APT28 has used compromised Office 365 service accounts with Global Administrator privileges to collect email from user inboxes.[2]

Enterprise T1102 .002 Web Service: Bidirectional Communication

APT28 has used Google Drive for C2.[21]

Enterprise T1669 Wi-Fi Networks

APT28 has exploited open Wi-Fi access points for initial access to target devices using the network.[27][53]

During APT28 Nearest Neighbor Campaign, APT28 established wireless connections to secure, enterprise Wi-Fi networks belonging to a target organization for initial access into the environment.[27]
