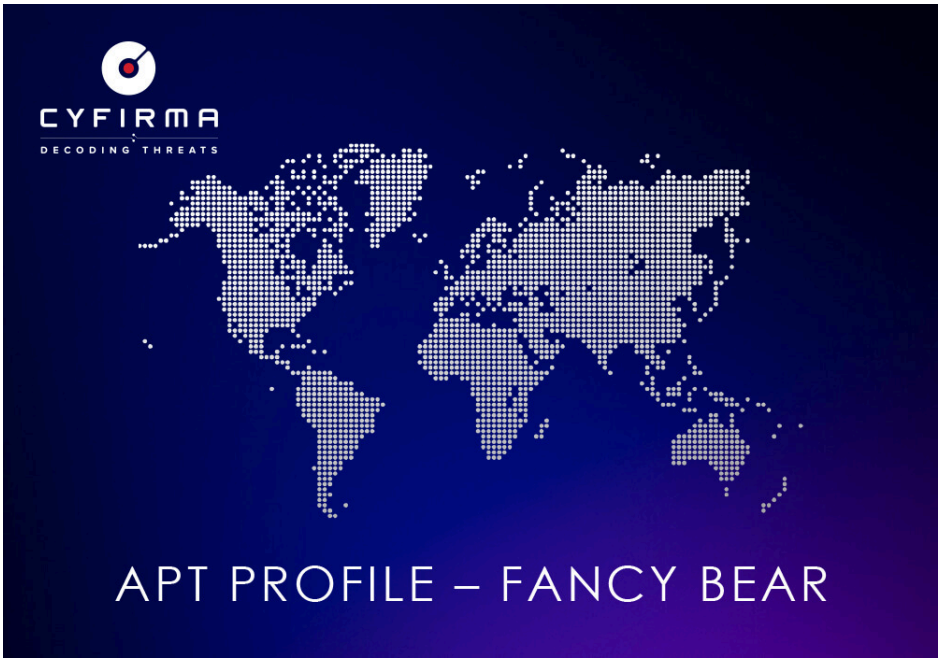
APT PROFILE – FANCY BEAR - CYFIRMA

Archived: 2026-04-05 17:58:38 UTC

Published On : 2025-07-16



Fancy Bear, also known as APT28, is a notorious Russian cyberespionage group with a long history of targeting governments, military entities, and other high-value organizations worldwide. Active since 2007, they are infamous for their stealthy and well-coordinated cyberattacks. Fancy Bear has been implicated in attempts to influence election processes in countries like the U.S., France, and Germany.

Alias:
APT 28, APT-28, APT28, Blue Athena, Blue Delta, FROZENLAKE, Fancy Bear, Fighting Ursa, Forest Blizzard, Group 74, GruesomeLarch, IRON TWILIGHT, ITG05, Pawn Storm, SIG40, STRONTIUM, Sednit, Sofacy, Sofacy Group, Strontium, Swallowtail, TA422, TAG-110, TG-4127, Threat Group-4127, Tsar Team, UAC-0001, UAC-0028, UAC-0063, Unit 26165, Unit 74455.

Motivation:
Financial, Reputational Damage, Espionage, Political Agenda

Target Technologies:
Office Suites Software, Operating Systems, Web Applications

Tools Used:
Forfiles, Computrace, Living off the Land, DealersChoice, Sedkit, Mimikatz.

Malware used by Fancy Bear:
STEELHOOK, HeadLace, Sedreco, Winexe, OCEANMAP, OLDBAIT, ProcDump, WinIDS, certutil, CHOPSTICK, HIDEDRV, SkinnyBoy, XAgentOSX

Targeted Country
Afghanistan, Brazil, Cambodia, France, Georgia, Germany, India, Indonesia, Kazakhstan, Malaysia, Moldova, Pakistan, Romania, Russia, South Africa, Syria, Thailand, Turkey, Ukraine, the United States, Vietnam, and Australia.

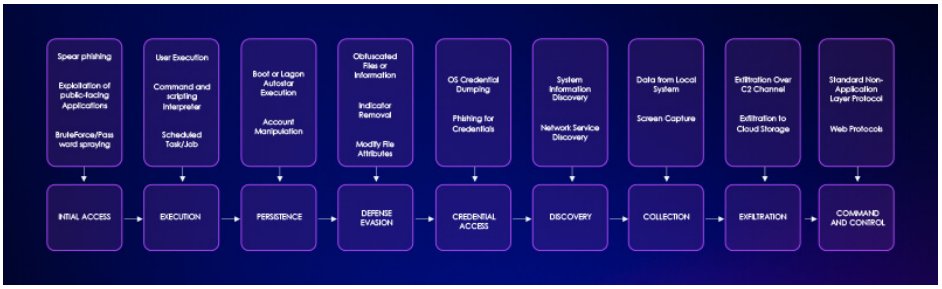
Targeted Industries

MITRE ATT&CK Techniques used by Fancy Bear

Reconnaissance	Privilege Escalation	Lateral Movement
T1598	T1068	T1210
T1595.002	T1037.001	T1550.002
T1589.001	T1078	T1021.002
T1598.003	T1078.004	T1550.001
Resource Development	T1546.015	T1091
T1583.006	T1547.001	Collection
T1588.002	T1134.001	T1213
T1583.001	Defense Evasion	T1005
T1586.002	T1027	T1025
Initial Access	T1211	T1113

T1189	T1036	T1560
T1133	T1070.001	T1560.001
T1199	T1014	T1119
T1078	T1221	T1039
T1566.001	T1078	T1056.001
T1566.002	T1078.004	T1074.001
T1078.004	T1564.001	T1114.002
T1091	T1564.003	T1074.002
T1190	T1134.001	T1213.002
Execution	T1218.011	Command and Control
T1203	T1542.003	T1573.001
T1059.003	T1036.005	T1071.001
T1204.001	T1550.002	T1102.002
T1059.001	T1550.001	T1090.003
T1204.002	T1140	T1071.003
T1559.002	T1070.004	T1090.002
Persistence	T1070.006	T1092
T1505.003	Credential Access	T1105
T1542.003	T1110.003	T1001.001
T1037.001	T1110.001	Exfiltration
T1133	T1003	T1048.002
T1078	T1110	T1030
T1078.004	T1040	T1567
T1137.002	T1528	Impact
T1546.015	T1003.003	T1498
T1098.002	T1003.001	
T1547.001	T1056.001	
	Discovery	
	T1057	
	T1120	
	T1040	
	T1083	

Attack Flow Diagram: APT Fancy Bear



Recently Exploited Vulnerabilities by Fancy Bear

CVE-2023-23397
CVE-2023-38831
CVE-2023-20085

Fancy Bear's Recent Campaign Highlights and Trends

Recent Campaign Highlights

Fancy Bear has continued to demonstrate high activity, particularly in targeting entities related to the war in Ukraine and broader Western interests.

Targeting Ukrainian Officials and Military Suppliers:

- Objective: To gain insight into the Ukrainian military's supply chain and broader intelligence on the conflict.
- Method: Spearphishing campaigns targeting email accounts of high-ranking Ukrainian officials and executives at defense contractors in other countries who supply weapons and equipment to Kyiv.
- Exploits: They leveraged cross-site scripting (XSS) vulnerabilities in various webmail software products, including Roundcube, Horde, MDaemon, and Zimbra. They also exploited a more recent vulnerability in Roundcube, CVE-2023-43770.
- Malware: Custom JavaScript malware payloads capable of exfiltrating data (email messages, address books, contacts, login history). In some cases, they could steal passwords and bypass 2FA by exploiting vulnerabilities that forced password re-entry on spoofed pages.

Targeting Western Logistics and Technology Companies:

- Objective: Cyber espionage against companies facilitating foreign aid to Ukraine.
- Method: This campaign has been broadly identified by a joint advisory from multiple intelligence agencies across North America, Europe, and Australia. Specific TTPs likely overlap with their general espionage methods.

Leveraging Real Government Documents as Lures:

- Objective: To infect and spy on government officials in Central Asia (e.g., Kazakhstan, Kyrgyzstan, Mongolia) and other regions (Israel, India, parts of Europe). This aligns with Russia's aim to maintain political alignment and counter competing influences in Central Asia.
- Method: Spearphishing using seemingly legitimate documents from the Kazakhstan government (e.g., diplomatic statements, correspondence, internal notes) as lures.
- Malware: Files laced with malware, including HATVIBE and CHERRYSPY. HATVIBE acts as a loader, fetching and executing CHERRYSPY, which provides persistent, clandestine backdoor access. The infection chain involved malicious macro files in Word that downgraded security settings and launched the malware. This activity shows overlap with ZEBROCY backdoor usage, also attributed to Fancy Bear.

Trends

- Continued Focus on Geopolitical Objectives: Their primary motivation remains intelligence gathering to support Russian geopolitical interests, particularly in the context of the war in Ukraine.
- Exploitation of Webmail Vulnerabilities: A persistent trend of exploiting vulnerabilities in widely used webmail clients to gain initial access and steal credentials.
- Sophisticated Phishing and Social Engineering: Their phishing lures are highly tailored and often mimic legitimate sources (e.g., Ukrainian news outlets, government documents) to increase effectiveness. They understand their targets' interests and leverage current events.
- Adaptation and Evasion: Fancy Bear continuously updates its malware and TTPs to evade detection. This includes switching implants, changing command and control (C2) channels, modifying persistence methods, and using anti-analysis techniques like code obfuscation, adding junk data, and clearing event logs.
- Credential Harvesting: A core component of their attacks, aiming to steal login information for persistent access.
- Broad Victimology: While their primary focus remains specific geopolitical targets, their campaigns often ensnare a broader range of victims in various countries across Europe, Asia, and even Latin America.
- Use of Legitimate Infrastructure: They have been known to relay C2 traffic through proxy networks of previously compromised victims and may abuse legitimate cloud services.
- Disinformation and Persona Creation: While not always tied to a specific recent campaign, a historical trend for Fancy Bear (e.g., Guccifer 2.0, Fancy Bears' Hack Team) is to create online personas to disseminate stolen information, sow disinformation, and deflect blame.

Tactics, Techniques, and Procedures (TTPs)

Fancy Bear's TTPs align with the MITRE ATT&CK framework and demonstrate their advanced capabilities:

Initial Access:

- Spear phishing Attachment/Link (T1566.001/002): The most common initial access vector.
- Highly tailored emails with malicious attachments (e.g., weaponized documents with macros).
- Emails containing links to spoofed login pages for webmail services or malware drop sites.
- Exploitation of Public-Facing Applications (T1190): Leveraging vulnerabilities (e.g., XSS in webmail platforms like Roundcube, Horde, MDaemon, Zimbra) to execute malicious code.
- Brute Force/Password Spraying (T1110.003): Historically used against web services, as seen in the Norwegian parliament hack.

Execution:

- User Execution (T1204): Requires victims to open malicious documents or click on malicious links.
- Command and Scripting Interpreter (T1059): Using JavaScript within browser contexts (XSS) or PowerShell for various tasks (e.g., downloading stages).
- Scheduled Task/Job (T1053): Setting up tasks to run malware periodically (e.g., HATVIBE running every four minutes).
- Malicious Macro (T1204.002): Embedded in documents to trigger infection chains.

Persistence:

- Boot or Logon Autostart Execution (T1547): Using Startup folders for persistent execution of malware.
- Account Manipulation (T1098): Stealing credentials to maintain access to accounts.
- Scheduled Task/Job (T1053): Re-establishing execution of malware.

Defense Evasion:

- Obfuscated Files or Information (T1027): Obfuscating code, adding junk data to encoded strings.
- Indicator Removal (T1070): Clearing event logs (e.g., Security and System event registries) to hide activity.
- Modify File Attributes (T1564.004): Resetting timestamps on files to hinder forensic analysis.
- Proxy/C2 Channels (T1090): Routing C2 traffic through compromised victim networks.
- Implant Switching: Frequently rotating implants to avoid detection.
- Valid Accounts (T1078): Using stolen legitimate credentials.

Credential Access:

- OS Credential Dumping (T1003): Stealing credentials/hashes from systems, potentially through exploits that capture inputs or by leveraging specific tools.
- Phishing for Credentials (T1566.002): Direct harvesting of credentials via spoofed login pages.

Discovery:

- System Information Discovery (T1082): Understanding the compromised environment.
- Network Service Discovery (T1046): Mapping network drives.

Collection:

- Data from Local System (T1005): Stealing email messages, address books, contacts, login histories.
- Screen Capture (T1113): Taking screenshots of the victim's machine.

Exfiltration:

- Exfiltration Over C2 Channel (T1041): Sending collected data back to C2 servers.
- Exfiltration to Cloud Storage (T1567.002): Known to use services like Google Drive for data exfiltration.

Command and Control (C2):

- Standard Non-Application Layer Protocol (T1091): Using various protocols for C2 communication.
- Web Protocols (T1071.001): Utilizing HTTP/HTTPS for C2.
- Legitimate Services (T1102): Abusing legitimate cloud services for C2 communication.
