Advanced Persistent Threat Groups

Lazarus Group and Fancy Bear

(Crowdstrike, 2024)

APT28 Fancy Bear

Fancy Bear is a Russian Military Group of intelligence hackers, they have been known to attack US elections specifically the 2016 election where they publicly leaked Hillary Clinton's campaign secrets. (Greenberg, 2020)

APT 38 Lazarus Group

The APT with countless lives, this APT's country of Origin is North Korea, and active from 2009 to the present day. The Lazarus Group is a large subset of state-sponsored cyber activities of the Democratic People's Republic of Korea (DPRK). (Zettl-Schabath, Jazxhi and Borrett, 2024) Lazarus Group is the umbrella term for all North Korean state-sponsored activity.

This North Korean state-sponsored threat group (APT 38) specializes in financial cyber ops. APT38 has targeted banks, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries. (MITRE, 2014)

(Vectra, 2024)

(BBCNewsbeat, 2016)

APT28's famous exploits

As mentioned ATP28 compromised the Hillary Clinton campaign, The Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 to interfere with the US presidential election. (MITRE, 2017)

In 2018, The USA indicted 5 GRU Unit 26165 officers who were part of APT28's cyber ops attack against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, among other organizations. Some of these attacks were conducted with assistance from the Sandworm Team (GRU Unit 74455). (MITRE, 2017)

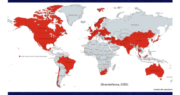
APT38's famous exploits

Famous operations from APT38 are the 2016 Bank of Bangladesh heist; where $81 million was stolen, attacks Against Bancomext; a Mexican Bank, 2018 Banco De Chile; a Chilean bank. (MITRE, 2014)

US Department of Justice Indicted a North Korean hacker named Park Jin Hyok, they charged him with cyber espionage operations such as the Sony Pictures hack, WannaCry virus, and Lockheed Martin hack. Also indicted for financially-motivated operations such as the Bangladesh bank heist. (Cimpanu, 2018)

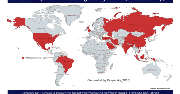
(Datta, 2023)

World Map of countries targeted by APT28 (Fancy Bear)



APT28 is known to target these sectors of Western industries and critical infrastructure: Finance, Health, State, Defense, IT, Media, Education, Embassies, Fuel, Chemical, Aviation and others such as construction and automotive. (Brandefense, 2022)

World Map of countries targeted by APT38 (Lazarus Group)



Lazarus APT Group is known to target the following sectors: Banks, Defense Industries, Software Businesses, Pharmaceutical companies, Cryptocurrency exchanges, Manufacturing, and electrical industries. (Brandefense, 2022b)

APT 28s Mission

The main mission is to gather security and policy intelligence, as Russia considers this data a way to make an opportunity to influence public opinion and make predictions for future policies. Russia considers Western Security alliances like NATO and OSCE in Europe as a threat to their nation. The attacks Russia would actively carry out would be information theft and espionage against the Western organisations and individules connected to them. (Brandefense, 2022a)

APT28/Fancy Bear known Aliases

Kaspersky	Mandiant	CrowdStrike	ESET	Talos	Trend Micro	Microsoft	Symantec	NSA	SecureWorks	IBM	US Government
Sofacy	APT28	Fancy Bear	Sednit	Group 74	Pawn Storm	Strontium	Swallowtail	SIG40	Iron Twilight	ITG05	Grizzly Steppe

(Brandefense, 2022a)

APT 38s Mission

The main mission of this North Korean state-sponsored hacking organisation is Extortion of Money, Information Theft, Sabotage, and Espionage. (Brandefense, 2022b)

Lazarus Group is a very sophisticated North Korean APT. They are known by many aliases, the US intelligence organisations refer to the North Korean government cyber activities as Hidden Cobra. (Brandefense, 2022b)

Lazarus Groups known Aliases

Andariel	APT38	COVELLITE	Group 77	HIDDEN COBRA	Lazarus	Operation AppleJesus	Operation Troy	Subgroup: Andariel	ZINC
APT-C-26	Bluenoroff	Dark Seoul	Guardian of Peace	Labyrinth	NICKEL ACADEMY	NewRomantic Cyber Army Team	Silent Chollima	Unit 121	WHOis Team
Appleworm	Bureau 121	GOP	Hastati Group	Chollima	Operation DarkSeoul	Operation GhostSecret	Subgroup: Bluenoroff	Whois Hacking Team	(Brandefense, 2022b)

Tactics, Techniques and Procedures (TTPs)

Campaigns (MITRE, 2009)

ID	Name	First Seen	Last Seen	Techniques
C0022	Operation Dream Job	September 2019	August 2020	"Account Discovery: Domain Account, Acquire Infrastructure: Server, Acquire Infrastructure: Domains, Acquire Infrastructure: Web Services, Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Utility, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Brute Force, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Compromise Infrastructure: Domains, Compromise Infrastructure: Server, Data from Local System, Debugger Evasion, Develop Capabilities: Code Signing Certificates, Develop Capabilities: Malware, Encrypted Channel: Symmetric Cryptography, Establish Accounts: Social Media Accounts, Establish Accounts: Email Accounts, Exfiltration Over C2 Channel, Exfiltration Over Web Service: Exfiltration to Cloud Storage, File and Directory Discovery, Gather Victim Identity Information, Gather Victim Org Information, Gather Victim Org Information: Identify Roles, Impersonation, Indicator Removal: File Deletion, Ingress Tool Transfer, Internal Spearphishing, Masquerading: Masquerade File Type, Native API, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information: Encrypted/Encoded File, Obtain Capabilities: Code Signing Certificates, Obtain Capabilities: Tool, Phishing: Spearphishing via Service, Phishing: Spearphishing Attachment, Phishing: Spearphishing Link, Scheduled Task/Job: Scheduled Task, Search Open Websites/Domains: Social Media, Server Software Component: IIS Components, Stage Capabilities: Upload Malware, Stage Capabilities: Upload Tool, Subvert Trust Controls: Code Signing, System Binary Proxy Execution: Rundll32, System Binary Proxy Execution: Regsvr32, System Location Discovery: System Language Discovery, Template Injection, User Execution: Malicious Link, User Execution: Malicious File, Virtualization/Sandbox Evasion: System Checks, Virtualization/Sandbox Evasion: Time Based Evasion, Windows Management Instrumentation, XSL Script Processing" (MITRE, 2009)

Techniques Used, These are the general APT MITRE ATT&CK Navigator Tactics.
Both Lazarus and Fancy Bear use the techniques below

Tactical ID	Tactics	Technical ID	Technical
TA0043	Reconnaissance	T1595, T1592, T1590, T1598, T1597, T1596, T1593, T1594, T1589, T1591	Active scanning, Gather victim host information, Gather victim network information, Phishing for information, Search closed sources, Search open websites/domains, Search victim-owned websites, Gather victim identity information, Gather victim org information. (MITRE, 2022)
TA0042	Resource Development	T1650, T1583, T1586, T1584, T1587, T1585, T1588, T1608	Acquire access, Acquire infrastructure, Compromise accounts, Compromise infrastructure, Develop capabilities, Establish accounts, Obtain capabilities, Stage capabilities. (MITRE, 2022)
TA0001	Initial Access	T1659, T1190, T1133, T1200, T1566, T1091, T1195, T1199, T1189, T1078	Content injection, Exploit public-facing application, External remote services, Hardware additions, Phishing, Replication through removeable media, Supply chain compromise, Trusted relationship, Drive-by compromise, Valid Accounts. (MITRE, 2022)
TA0002	Execution	T1651, T1059, T1609, T1610, T1559, T1053, T1648, T1129, T1072, T1569, T1204, T1203, T1106, T1047	Cloud administration command, Command and scripting interpreter, Container administration command, Deploy container, Inter-process communication, Scheduled task, Serverless execution, Shared modules, Software development tools, System services, User execution, Exploitation for client execution, Native API, Windows management instrumentation. (MITRE, 2022)
TA0003	Persistence	T1197, T1547, T1037, T1176, T1554, T1136, T1543, T1546, T1133, T1574, T1525, T1556, T1137, T1653, T1542, T1053, T1505, T1205, T1098, T1078	BITS Jobs, Boot or log-on Autostart execution, Boot or logon initialization scripts, Browser Extensions, Compromise host software binary, Create account, Create or modify system process, Event triggered execution, External remote services, Hijack execution flow, Implant internal image, Modify authentication process, Office application startup, Power settings, Pre-OS boot, Scheduled task, Server software component, Traffic signaling, Account manipulation, Valid accounts. (MITRE, 2022)
TA0004	Privilege Escaltion	T1548, T1134, T1547, T1037, T1543, T1484, T1611, T1546, T1068, T1574, T1055, T1053, T1098, T1078	Abuse elevation control mechanism, Access token manipulation, Boot or log-on Autostart execution, Boot or logon initialization scripts, Create or modify system process, Domain or tenant policy modification, Escape to host, Event triggered execution, Exploition for privilege escalation, Hijack execution flow, Process Injection, Scheduled Task, Account manipulation, Valid Accounts. (MITRE, 2022)
TA0005	Defense Evasion	T1548, T1134, T1197, T1612, T1610, T1006, T1484, T1480, T1211, T1222, T1564, T1574, T1562, T1036, T1556, T1578, T1666, T1112, T1601, T1599, T1027, T1647, T1542, T1055, T1207, T1014, T1553, T1216, T1205, T1127, T1535, T1550, T1497, T1600, T1622, T1140, T1656, T1070, T1202, T1620, T1218, T1221, T1078, T1220	Abuse elevation control mechanism, Access token manipulation, BITS jobs, Build image on host, Deploy container, Direct volume access, Domain or tenant policy modification, Execution guardrails, Exploitation for defence evasion, File and directory permissions modification, Hide artifacts, Hijack execution flow, Impair defences, Masquerading, Modify authentication process, Modify cloud compute infrastructure, Modify cloud resource hierarchy, Modify registry, Modify system image, Network boundary bridging, Obfuscated files or data, Plist file modification, Pre-OS boot, Process injection, Rogue domain controller, Rootkit, Subvert trust controls, System script proxy execution, Traffic signaling, Trusted developer utilities proxy execution, Unused/outdated cloud regions, Use alternate authentication material, Virtualization/sandbox evasion, Weaken encryption, Debugger evasion, Deobfuscate files or data, Impersonation, Indicator removal, Indirect command execution, Reflective code loading, System binary proxy execution, Template injection, Valid accounts, XSL script processing. (MITRE, 2022)
TA0006	Credential Access	T1557, T1555, T1212, T1187, T1606, T1056, T1556, T1111, T1621, T1040, T1003, T1528, T1649, T1558, T1539, T1552, T1110	Adversary-in-the-middle, Credentials from password stores, Exploitation for credential access, Forced authentication, Forge web credentials, Input capture, Modify authentication process, Multi-factor authentication interception, Multi-factor authentication request generation, Network sniffing, OS credential dumping, Steal application access token, Steal or forge authentication certificates, Steal or forge kerberos tickets, Steal web session cookie, Unsecured credentials, Bruteforce (MITRE, 2022)
TA0007	Discovery	T1087, T1217, T1580, T1538, T1526, T1619, T1613, T1652, T1482, T1615, T1654, T1135, T1040, T1201, T1120, T1069, T1018, T1518, T1614, T1007, T1497, T1010, T1622, T1083, T1046, T1057, T1012, T1082, T1016, T1049, T1033, T1124	Account discovery, Browser information discovery, Cloud infrastructure discovery, Cloud service dashboard, Cloud service discovery, Cloud storage object discovery, Container and resource discovery, Device driver discovery, Domain trust discovery, Group policy discovery, Log enumeration, Network share discovery, Network sniffing, Password policy discovery, Peripheral device discovery, Permissions groups discovery, Remote system discovery, Software discovery, System location discovery, System service discovery, Virtualization/sandbox evasion, Application window discovery, Debugger evasion, File and directory discovery, Network service discovery, Process discovery, Query registry, System information discovery, System network configuration discovery, System owner/user discovery, System time discovery. (MITRE, 2022)
TA0008	Lateral Movement	T1210, T1570, T1563, T1021, T1091, T1072, T1080, T1550, T1534	Exploitation of remote services, Lateral tool transfer, Remote service session hijacking, Remote services, Replication through removable media, Software development tools, Taint shared content, Use alternate authentication material, Internal spear-phishing. (MITRE, 2022)
TA0009	Collection	T1557, T1123, T1119, T1185, T1115, T1530, T1602, T1213, T1039, T1025, T1074, T1114, T1056, T1113, T1125, T1560, T1005	Adversary-in-the-middle, Audio capture, Automated collection, Browser session hijacking, Clipboard data, Data from cloud storage, Data from configuration repository, Data from information repositories, Data from shared network drive, Data from removable media, Data staging, Email collection, Input capture, Screen capture, Video capture, Archive collected data, Data from local system. (MITRE, 2022)
TA0011	Command and Control	T1071, T1092, T1659, T1132, T1001, T1568, T1573, T1665, T1095, T1572, T1090, T1219, T1205, T1102, T1008, T1105, T1104, T1571	Application layer protocol, Communication through removable media, Content injection, Data encoding, Data obfuscation, Dynamic resolution, Encrypted channel, Hide infrastructure, Non-application layer protocol, Protocol tunneling, Proxies, Remote access software, Traffic Signaling, Web services, Fallback channels, Ingress tool transfer, Multi-stage channels, Non-standard port. (MITRE, 2022)
TA0010	Exfiltration	T1020, T1030, T1048, T1011, T1052, T1567, T1029, T1537, T1041	Automated exfiltration, Data transfer size limits, Exfiltration over alternative protocol, Exfiltration over other network medium, Exfiltration over physical medium, Exfiltration over web service, Scheduled transfer, Transfer data to cloud account, Exfiltration over C2 channel. (MITRE, 2022)
TA0040	Impact	T1531, T1486, T1565, T1491, T1561, T1499, T1657, T1495, T1490, T1498, T1496, T1485, T1489, T1529	Account access removal, Data encrypted for impact, Data manipulation, Defacement, Disk wipe, Endpoint denial of service, Financial theft, Firmware corruption, Inhibit system recovery, Network denial of service, Resource hijacking, Data destruction, Service stop, System shutdown/reboot. (MITRE, 2022)

APT38's Attack Lifecycle against Financial Institutions

Figure 1: APT38 Attack Lifecycle

(Google Cloud, 2024)

Legal and Regulatory Responses for Lazarus Group

Lazarus Group being a controlled entity for the government of North Korea has to be in accordance with Executive Order 13722. Which is a sanction the US government have for North Korea, this "prohibits the exportation and reexportation of goods, services (including financial services), and technology to North Korea; and prohibits new investment in North Korea." (US Treasury, 2016) due to having strong connections to Reconnaissance General Bureau (RGB), which is North Koreas primary intelligence bureau. (U.S. Department of the Treasury, 2019)

Lazarus Group was the APT most likely responsible for the WannaCry ransomware virus, it affected around 300,000 computers and over 150 countries demanding $300 in cryptocurrency. Many companies got affected such as Renault, FedEx, and Deutsche Bahn. The worst affected was the National Health Service (NHS England). (Schmitt and Fahey, 2017)

The WannaCry attacks pose an interesting question of laws that can't be fully resolved in a cyber context, the WannaCry effects fall in a legal grey zone where the violations remain unsettled, even though they affected the delivery of medical care and interfered with law enforcement agency's. (Schmitt and Fahey, 2017)

North Korea have so many sanctions already and they have ways to get around them that they don't care if they get more sanctions.

Legal and Regulatory Responses for Fancy Bear

The UK sanctioned two Russian GRU officers and the whole GRU military intelligence unit 26165 with asset freezes and travel bans, for a cyber attack on Germany's parliament in 2015 where they targeted information systems stole significant amounts of data and affected email accounts owned by German MPs. (GOV.UK, 2020)

The UK has laid the required instruments for its cyber sanctions regime to allow the UK to impose travel bans and asset freezes on organisations or individuals. (GOV.UK, 2020)

"Russia's pattern of behavior blatantly disregards the Framework for Responsible State Behavior in Cyberspace, as affirmed by all United Nations Member States. The United States is committed to the security of our allies and partners and upholding the rules-based international order, including in cyberspace. We call on Russia to stop this malicious activity and abide by its international commitments and obligations. With the EU and our NATO Allies, we will continue to take action to disrupt Russia's cyber activities, protect our citizens and foreign partners, and hold malicious actors accountable." (U.S. Department of State, 2024)

The US Department of State has stated on their website that they have indicted and sanctioned actors associated with APT28 and says this:

Conclusion

To conclude APT28 (Fancy Bear) and APT38 (Lazarus Group) are two of the most significant state-sponsored advanced persistent threat groups that are still active to this day, both groups deploy unique tactics to achieve their respective goals.

APT28 is associated with Russia's military intelligence (GRU) which is known to target defence, governments, and political sectors in the areas and countries on the world map for Fancy Bear. They use techniques like phishing, malware, ransomware, and tailored implants such as Sofacy, X-Agent, X-Tunnelt, WinIDS, Foozer and DownRage droppers. (CrowdStike editorialteam, 2024)

APT38 is a financial branch of North Korea's Lazarus group, this particular group focuses on cyber heists to fund state activities like North Korea's nuclear program. This group uses techniques like custom malware and spear-phishing to get access and steal from financial institutions. APT38 have stolen hundreds of millions of funds from various institutions, they aggressively exploit vulnerabilities to bypass banking systems worldwide. They are known for the 2016 SWIFT banking attacks and they have attempted to steal over $1.1billion. (Google Cloud, 2024)

The magnitude and scope of nation-state-sponsored cybercrime are demonstrated by APT28 and APT38. Their actions highlight the pressing need for strong global cybersecurity defences and collaborative laws to lessen potential dangers. To combat the increasingly complex and well-funded activities of these organisations, sharing intelligence, tailored legislation, and proactive mitigations are crucial.