Advanced Persistent Threat Groups

Lazarus Group and Fancy Bear

APT 38 Lazarus Group

Lazarus Group, also known as Hidden Cobra, is a North Korean state-sponsored cyber threat group that has been operating since at least 2009. The group is responsible for a number of high-profile cyberattacks, including the Sony Pictures Entertainment hack in 2014, the WannaCry ransomware attack in 2017, and the cyberattack on Bangladesh Bank in 2016. The group is also believed to be responsible for a number of attacks against financial institutions, cryptocurrency exchanges, and critical infrastructure.

Lazarus Group is known for its use of a variety of malware, including custom-developed tools and commercially available malware. The group has also been known to use social engineering techniques to gain access to victim networks.

The motivations behind Lazarus Group's attacks are not entirely clear, but it is believed that the group is primarily motivated by financial gain. However, the group has also been known to conduct espionage operations and to target political dissidents.

Lazarus Group is a significant threat to the cybersecurity of financial institutions and critical infrastructure around the world. The group's attacks have caused billions of dollars in damage and have disrupted the operations of many organizations.

APT28 Fancy Bear

Fancy Bear is a Russian military threat actor group that has been active since at least 2004. It is also known as APT28, Sofacy Group, Pawn Storm, and Sednit. The group is believed to be responsible for a number of high-profile cyberattacks, including the hacking of the Democratic National Committee (DNC) in 2016.

Fancy Bear is known for its use of spear phishing emails to gain access to victim networks. The group has also been known to use zero-day exploits and custom malware. Fancy Bear is believed to be responsible for a number of attacks against government agencies, military organizations, and political campaigns.

The motivations behind Fancy Bear's attacks are not entirely clear, but it is believed that the group is primarily motivated by espionage. However, the group has also been known to conduct disruptive attacks, such as the hacking of the DNC.

Fancy Bear is a significant threat to the cybersecurity of governments and organizations around the world. The group's attacks have caused billions of dollars in damage and have disrupted the operations of many organizations.

APT38's famous exploits

One of APT38's most famous exploits was the Bangladesh Bank heist in 2016. The group used a combination of spear phishing emails and malware to gain access to the bank's network. They then stole $81 million by transferring funds to fake accounts.

APT38 has also been responsible for a number of other high-profile attacks, including the WannaCry ransomware attack in 2017 and the cyberattack on Sony Pictures Entertainment in 2014. The group is known for its use of custom malware and its ability to evade detection.

APT28's famous exploits

One of APT28's most famous exploits was the hacking of the Democratic National Committee (DNC) in 2016. The group used a combination of spear phishing emails and malware to gain access to the DNC's network. They then stole and released thousands of emails and documents.

APT28 has also been responsible for a number of other high-profile attacks, including the hacking of the German Bundestag in 2015 and the hacking of the French presidential election in 2017. The group is known for its use of custom malware and its ability to evade detection.

World Map of countries targeted by APT38 (Fancy Bear)

World Map of countries targeted by APT28 (Lazarus Group)

APT 28s Mission

The mission of APT28 is to collect intelligence that can be used to advance the interests of the Russian state. This includes intelligence on political, military, economic, and social issues. APT28 is also known to conduct disruptive attacks, such as the hacking of the DNC in 2016.

APT28's mission is driven by the Russian government's desire to maintain its power and influence around the world. The group is believed to be responsible for a number of attacks against countries that are perceived to be hostile to Russia, such as Ukraine and Georgia.

APT28(Fancy Bear) Known Missions

APT 38s Mission

The mission of APT38 is to steal money and intellectual property from financial institutions around the world. The group is believed to be responsible for a number of high-profile cyberattacks, including the Bangladesh Bank heist in 2016 and the WannaCry ransomware attack in 2017.

APT38's mission is driven by the North Korean government's desire to generate revenue and to gain access to sensitive information. The group is believed to be responsible for a number of attacks against countries that are perceived to be hostile to North Korea, such as South Korea and the United States.

Lazarus Groups Known Missions

Tactics, Techniques and Procedures (TTPs)

Comparison: APT28, APT38

APT	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
APT28	Spear Phishing Attachment Spear Phishing Link Drive-by Compromise Exploit Public-Facing Application External Remote Services Valid Accounts	Command and Scripting Interpreter Exploitation for Client Execution Inter-Process Communication Native API Scheduled Task/Job User Execution Windows Management Instrumentation	Account Manipulation Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Create or Modify System Process Event Triggered Execution External Remote Services Hijack Execution Flow Implant Internal Image Modify Authentication Process Office Application Startup Pre-OS Boot Scheduled Task/Job Server Software Component Valid Accounts	Abuse Elevation Control Mechanism Access Token Manipulation Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Create or Modify System Process Domain Policy Modification Escape to Host Event Triggered Execution Exploitation for Privilege Escalation Hijack Execution Flow Process Injection Scheduled Task/Job Valid Accounts	Abuse Elevation Control Mechanism Access Token Manipulation Deobfuscate/Decode Files or Information Direct Volume Access Domain Policy Modification Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Modification Hide Artifacts Hijack Execution Flow Impair Defenses Indicator Removal on Host Indirect Command Execution Masquerading Modify Authentication Process Modify Cloud Compute Infrastructure Modify Registry Modify System Image Network Boundary Bridging Obfuscated Files or Information Pre-OS Boot Process Injection Rogue Domain Controller Rootkit Subvert Trust Controls System Binary Proxy Execution Template Injection Traffic Signaling Trusted Developer Utilities Proxy Execution Use Alternate Authentication Material Valid Accounts Virtualization/Sandbox Evasion Weaken Encryption XSL Script Processing	Adversary-in-the-Middle Brute Force Credentials from Password Stores Exploitation for Credential Access Forced Authentication Forge Web Credentials Input Capture Modify Authentication Process Network Sniffing OS Credential Dumping Steal Application Access Token Steal or Forge Kerberos Tickets Steal Web Session Cookie Unsecured Credentials	Account Discovery Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery File and Directory Discovery Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Information Discovery System Location Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization/Sandbox Evasion	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking Remote Services Taint Shared Content Use Alternate Authentication Material	Adversary-in-the-Middle Archive Collected Data Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository Data from Information Repositories Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged Email Collection Input Capture Screen Capture Video Capture	Application Layer Protocol Communication Through Removable Media Data Encoding Data Obfuscation Dynamic Resolution Encrypted Channel Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy Remote Access Software Traffic Signaling Web Service	Automated Exfiltration Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over C2 Channel Exfiltration Over Other Network Medium Exfiltration Over Physical Medium Exfiltration Over Web Service Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Defacement Disk Wipe Endpoint Denial of Service Firmware Corruption Inhibit System Recovery Network Denial of Service Resource Hijacking Service Stop System Shutdown/Reboot
APT38	Spear Phishing Attachment Spear Phishing Link Drive-by Compromise Exploit Public-Facing Application External Remote Services Valid Accounts	Command and Scripting Interpreter Exploitation for Client Execution Inter-Process Communication Native API Scheduled Task/Job User Execution Windows Management Instrumentation	Account Manipulation Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Create or Modify System Process Event Triggered Execution External Remote Services Hijack Execution Flow Implant Internal Image Modify Authentication Process Office Application Startup Pre-OS Boot Scheduled Task/Job Server Software Component Valid Accounts	Abuse Elevation Control Mechanism Access Token Manipulation Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Create or Modify System Process Domain Policy Modification Escape to Host Event Triggered Execution Exploitation for Privilege Escalation Hijack Execution Flow Process Injection Scheduled Task/Job Valid Accounts	Abuse Elevation Control Mechanism Access Token Manipulation Deobfuscate/Decode Files or Information Direct Volume Access Domain Policy Modification Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Modification Hide Artifacts Hijack Execution Flow Impair Defenses Indicator Removal on Host Indirect Command Execution Masquerading Modify Authentication Process Modify Cloud Compute Infrastructure Modify Registry Modify System Image Network Boundary Bridging Obfuscated Files or Information Pre-OS Boot Process Injection Rogue Domain Controller Rootkit Subvert Trust Controls System Binary Proxy Execution Template Injection Traffic Signaling Trusted Developer Utilities Proxy Execution Use Alternate Authentication Material Valid Accounts Virtualization/Sandbox Evasion Weaken Encryption XSL Script Processing	Adversary-in-the-Middle Brute Force Credentials from Password Stores Exploitation for Credential Access Forced Authentication Forge Web Credentials Input Capture Modify Authentication Process Network Sniffing OS Credential Dumping Steal Application Access Token Steal or Forge Kerberos Tickets Steal Web Session Cookie Unsecured Credentials	Account Discovery Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery File and Directory Discovery Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Information Discovery System Location Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization/Sandbox Evasion	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking Remote Services Taint Shared Content Use Alternate Authentication Material	Adversary-in-the-Middle Archive Collected Data Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository Data from Information Repositories Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged Email Collection Input Capture Screen Capture Video Capture	Application Layer Protocol Communication Through Removable Media Data Encoding Data Obfuscation Dynamic Resolution Encrypted Channel Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy Remote Access Software Traffic Signaling Web Service	Automated Exfiltration Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over C2 Channel Exfiltration Over Other Network Medium Exfiltration Over Physical Medium Exfiltration Over Web Service Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Defacement Disk Wipe Endpoint Denial of Service Firmware Corruption Inhibit System Recovery Network Denial of Service Resource Hijacking Service Stop System Shutdown/Reboot

Techniques Used: Threat actor groups APT 38(TA) APT28 Analysis

Both Lazarus and Fancy Bear can Orchestrate Sabre

APT38's Attack Lifecycle for Financial Institutions

APT38 Attack Lifecycle	Initial Intrusion	Network Propagation	Preparation	Exploitation	Post-Exploitation
Reconnaissance Resource Development	Spear Phishing Watering Hole Strategic Web Compromise Supply Chain Compromise	Credential Theft Lateral Movement Persistence Privilege Escalation Defense Evasion	Internal Reconnaissance Collection Command and Control	Fraudulent Transfer Destructive Malware	Data Exfiltration Cover Tracks

Legal and Regulatory Responses for Lazarus Group

In response to the cyberattacks carried out by Lazarus Group, a number of countries and international organizations have taken legal and regulatory action. These actions have included sanctions, indictments, and the freezing of assets.

In March 2018, the US Department of the Treasury designated Lazarus Group as a threat to the cybersecurity of the US financial system. This designation allowed the US government to impose sanctions on individuals and entities associated with Lazarus Group.

In May 2018, a US grand jury indicted three North Korean nationals for their role in the Sony Pictures Entertainment hack. The indictment charged the defendants with conspiracy to commit computer fraud, wire fraud, and money laundering.

In addition to these actions, a number of countries have also taken steps to improve their cybersecurity defenses in response to the threat posed by Lazarus Group. These steps have included increasing the sharing of information about cyberattacks and investing in new cybersecurity technologies.

Legal and Regulatory Responses for Fancy Bear

The legal and regulatory responses to the cyberattacks carried out by Fancy Bear have been varied. In some cases, governments have taken action against individuals and entities that have been identified as being associated with the group. In other cases, governments have imposed sanctions on countries that have been accused of supporting Fancy Bear.

The US Department of the Treasury has also issued a number of reports on Fancy Bear's activities. These reports have provided valuable information about the group's tactics, techniques, and procedures.

Conclusion

In conclusion, APT28 (Fancy Bear) and APT38 (Lazarus Group) are two of the most significant state-sponsored threat actors that have been active in recent years. Both groups have been responsible for a wide range of cyberattacks, including espionage, financial theft, and disruption of critical infrastructure.

APT28 is a Russian-backed group that is believed to be responsible for a number of high-profile attacks, including the hacking of the Democratic National Committee (DNC) in 2016, the hacking of the German Bundestag in 2015, and the hacking of the French presidential election in 2017. The group is known for its use of spear phishing emails and custom malware. APT28 is also known to conduct disruptive attacks, such as the hacking of the DNC.

APT38 is a North Korean-backed group that is believed to be responsible for a number of high-profile attacks, including the Bangladesh Bank heist in 2016 and the WannaCry ransomware attack in 2017. The group is known for its use of custom malware and its ability to evade detection. APT38 is also known to conduct financially motivated attacks.

The motivations behind APT28 and APT38's attacks are not entirely clear, but it is believed that both groups are primarily motivated by financial gain. However, both groups have also been known to conduct espionage operations and to target political dissidents.

The cyberattacks carried out by APT28 and APT38 have had a significant impact on the cybersecurity landscape. These attacks have caused billions of dollars in damage and have disrupted the operations of many organizations.