HC3: Threat Actor Profile

June 26, 2024 TLP:CLEAR Report: 202406261200

Seashell Blizzard Threat Actor Profile

Executive Summary

Seashell Blizzard is a cyber threat group believed to be associated with Russian intelligence agencies, particularly with Unit 74455, the Main Centre for Special Technologies within the Main Directorate of the General Staff of the Armed Forces of the Russian Federation. The group has been operating since at least 2009 and has been implicated in numerous high-profile cyberattacks targeting governments, critical infrastructure, and organizations across the globe. During the ongoing conflict in Ukraine, much of the group's focus has been aimed toward disrupting Ukrainian operations and trying to obtain battlefield advantages; however, they have displayed a willingness and capability to shift this focus to benefit Russia's broader national interests. Their tactics include sophisticated malware deployment, spear phishing campaigns, and exploitation of software vulnerabilities. Seashell Blizzard will continue to pose as a threat to cyber operations globally, and should be considered a significant threat to the Healthcare and Public Health (HPH) sector.

Report

Seashell Blizzard (also known as APT44 and Sandworm) is a sophisticated Russian state-sponsored actor who has been operational since at least 2009. The group has a broad range of capabilities and has previously garnered attention for deploying destructive malware. They have been regarded as Russia's primary sabotage unit, but as the Russia-Ukraine conflict has progressed, a shift towards conducting espionage operations has been observed. This shift in operations is assessed to help provide advantages on the battlefield for the ongoing conflict. Seashell Blizzard has also been accredited with pursuing psychological operations by creating hacktivist personas on Telegram to claim or exaggerate the effectiveness of a campaign. According to Mandiant: "Google's Threat Analysis Group assesses that APT44 has created and controlled a persona called 'CyberArmyofRussia_Reborn,' for example. In January, the group's Telegram channel posted videos that took credit for the manipulation of human machine interfaces used in water utilities in the United States and Poland." Tactics like this fall in line with the GRU's Disruptive Playbook, which consists of five phases and is attributed to Seashell Blizzard activity:

- **Phase 1 - Living on the Edge:** Gaining access through compromised edge infrastructure (and regaining access).
- **Phase 2 - Living Off the Land:** Using tools to accomplish reconnaissance, lateral movement, and obtain information on the targeted network.
- **Phase 3 - Going for the GPO:** Establishing enduring, elevated access to facilitate the deployment of wipers through a reliable script.
- **Phase 4 - Disrupt and Deny:** Implementing wipers and innovative tools to suit a range of situations.
- **Phase 5 - Telegraphing "Success":** This involves announcing the success of an operation through Telegram, regardless of the outcome.

HC3: Threat Actor Profile

June 26, 2024 TLP:CLEAR Report: 202406261200

Phase	Assessed Technical Benefits	Assessed Strategic Benefits
Living on the Edge	• Challenging to defend and difficult to protect • Foothold for lateral movement	• Scalable across different targets • Maintain access after disruption • Generalize tactics for common enterprise technologies
Living off the Land	• Avoid detection	• Does not exposer sensitive tooling • Does not require resources to build custom tools or utilities • Generalize toolset for common enterprise operating systems
Going for the GPO	• Privileged lateral movement and execution • Can be used to impair defenses.	• Maximizes disruptive effects across a domain • Limit spillover potential
Disrupt and Deny	• Seamlessly integrate new disruptive tools when required • Sometimes erases attacker presence	• Generate immediate disruptive effect to key information resources • Create perceptions of insecurity • Feigned extortion for additional psychological effect
Telegraph "Success"	• Generate second-order psychological effects.	• Prime the information space • Generate perception of success • Reinforce perception of popular support for war via "hacktivist" personas

Figure 1: Google Playbook Phases

Seashell Blizzard stands out as a persistent and operationally sophisticated adversary, adept at employing a range of initial access methods to infiltrate target networks. These methods span from conventional tactics, such as phishing and credential harvesting, to more targeted approaches, such as exploiting known vulnerabilities and compromising supply chains. Notably, the group favors initial access vectors that would grant broader entry to potential targets, which are later refined for specific exploitation. The group often exploits edge infrastructure, including routers and VPN appliances.

Once inside a network perimeter, Seashell Blizzard engages in diverse activities, including furthering their reconnaissance efforts, data theft, downstream phishing, and deploying destructive malware such as wipers. In some cases, the group has also conducted software supply chain compromise for initial access. After initial access is obtained, the group is known for employing living off the land techniques to maintain persistence and exfiltrate data.

Targeting Operations

While much of Seashell Blizzard's focus is believed to be centered on Ukraine, aligning with Russia's geopolitical objectives, the full reach of their operations extends globally, reflecting Russia's broader national interests. Despite the ongoing conflict, the group maintains access and conducts espionage operations across various regions, including North America, Europe, the Middle East, Central Asia, and Latin America. Seashell Blizzard primarily targets government, defense, transportation, energy, media, and civil society organizations in Russia's neighboring countries.

Additional historical targeting has involved the electoral systems and institutions in Western countries, along with those from the North Atlantic Treaty Organization (NATO), with attempts to disrupt democratic

processes and the deployment of malware. Seashell Blizzard has also targeted journalists, civil society organizations, and non-governmental bodies who are engaged in either research or investigations related to the Russian government.

Notable Campaigns

Seashell Blizzard has been attributed to several notable campaigns throughout the group's existence:

1. **BlackEnergy Attacks (2015):** Seashell Blizzard gained international attention for its involvement in the BlackEnergy attacks targeting Ukraine's power grid, resulting in widespread outages.

2. **NotPetya Ransomware (2017):** Seashell Blizzard is widely believed to be behind the NotPetya ransomware attack, which caused billions of dollars in damages globally, particularly impacting Ukraine and organizations with Ukrainian connections.

3. **Olympic Destroyer Malware (2018):** Seashell Blizzard targeted the 2018 Winter Olympics in Pyeongchang, South Korea with the Olympic Destroyer malware, disrupting the event's IT infrastructure.

4. **Ukraine Electric Power Attack (2022):** Seashell Blizzard utilized a combination of GOGETTER, Neo-REGEORG, CaddyWiper, and living off the land techniques to gain access to electric utilities in Ukraine, and sent unauthorized commands from their SCADA system.

Tactics, Techniques, and Procedures (TTPs)

The following is a list of known TTPs and software used by Seashell Blizzard. A more comprehensive list of tools and TTPS can be viewed on MITRE ATT&CK and in the technical annex accessible here.

Initial Access

External Remote Service: T1133
Phishing: Spearphishing Attachment: T1566.001
Phishing: Spearphishing Link: T1566.002
Supply Chain Compromise: Compromise Software Supply Chain: T1195.002
Trusted Relationship: T1199
Valid Accounts: Domain Accounts: T1078.002

Privilege Escalation

Valid Accounts T1078
Account Manipulation T1098
Group Policy Modification: T1484.001

Persistence

Account Manipulation: T1098
Create Account: Domain Account: T1136.002
Server Software Component: SQL Stored Procedures: T1505.001
Server Software Component: Web Shell: T1505.003

HC3: Threat Actor Profile

June 26, 2024 TLP:CLEAR Report: 202406261200

Lateral Movement

Lateral Tool Transfer: T1570
Remote Services: SMB/Windows Admin Shares: T1021.002

Defense Evasion

Deobfuscate/Decode Files or Information: T1140
Impair Defenses: Disable Windows Event Logging: T1562.002
Indicator Removal: File Deletion: T1070.004
Masquerading: Match Legitimate Name or Location: T1036.005
Obfuscated Files or Information: Software Packing: T1027.002
System Binary Proxy Execution: Rundll32: T1218.011

Execution

Command and Scripting Interpreter: PowerShell: T1059.001
Command and Scripting Interpreter: Windows Command Shell: T1059.003
Command and Scripting Interpreter: Visual Basic: T1059.005
Exploitation for Client Execution: T1203
User Execution: Malicious Link: T1204.001
User Execution: Malicious File: T1204.002
Windows Management Instrumentation: T1047

Software	Description
Industroyer (Industroyer2)	Malware toolsets created to disrupt ICS/OT and components of SCADA power grids.
KillDisk	Destructive malware with disk-wiping capabilities.
BlackEnergy	Can create botnets to conduct DDoS attacks.
CaddyWiper	Wipes all files under C:\Users along with available drives from D: to Z: by overwriting with a NULL value.
NotPetya	Encrypting malware that targets Windows-based systems.
Olympic Destroyer	Destructive malware with worm-like features that renders computer systems inoperable.

Indicators of Compromise

The following resources contain Indicators of Compromise for Seashell Blizzard:

VirusTotal:https://www.virustotal.com/gui/collection/0bd93a520cae1fd917441e6e54ff263c88069ac5a7f8b9e55ef99cd961b6a1c7/iocs

Conclusion

Seashell Blizzard will continue to be a prominent threat to cyber operations globally. As the Russia-Ukraine conflict continues, Seashell Blizzard's operations will likely primarily focus on Ukraine. However, as previously observed, the group will stay ready to and capable of shifting focus and targeting neighboring and western countries as it benefits Russia's broader national interests.

HC3: Threat Actor Profile

June 26, 2024 TLP:CLEAR Report: 202406261200

References

Quorum Cyber. Seashell Blizzard Threat Actor Profile. https://www.quorumcyber.com/threat-actors/seashell-blizzard-threat-actor-profile/

Mandiant. April 17, 2024. Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm. https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm

Mandiant. July 12, 2023. The GRU's Disruptive Playbook. https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook

MITRE ATT&CK. Sandworm Team. https://attack.mitre.org/groups/G0034/

Barnett, Patrick. May 31, 2024. Understanding Sandworm, a State-Sponsored Threat Group. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2024/understanding-sandworm-a-state-sponsored-threat-group

O'Donnell-Welch, Lindsey. April 19, 2024. A Decade of Sandworm: Digging into APT44's Past and Future. Decipher. https://duo.com/decipher/a-decade-of-sandworm-digging-into-apt44-s-past-and-future

O'Donnell-Welch, Lindsey. April 17, 2024. Sandworm Group Shifts to Espionage Attacks, Hacktivist Personas, Decipher. https://duo.com/decipher/sandworm-group-shifts-to-espionage-attacks-hacktivist-personas

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback