**Cyber Security Advisories**

**Date: 18 February 2025**

1. **CMTX-P-022025575: The BadPilot Campaign (A subgroup of Seashell Blizzard) Threat Actor Activity , (TLP: CLEAR) (Recipients can spread this to the world, there is no limit on disclosure i.e. information may be shared without restriction)**

Alert Brief:

The Seashell Blizzard subgroup, part of the Russian state-sponsored actor operations, is primarily involved in extensive global cyber access operations, referred to as the "BadPilot campaign." This subgroup has been active since at least 2021 and is noted for its opportunistic tactics that allow it to maintain persistent access to high-value targets across various sectors. Their activities have evolved from a focus on Ukraine to a broader global reach, targeting sensitive industries and leveraging various exploitation methods to achieve their objectives.

This group utilizes opportunistic access methods and covert persistence techniques to gather credentials, execute commands, and facilitate lateral movement. These actions have at times resulted in significant regional network compromises. Subsequent operations after initial access suggest that this campaign allowed Seashell Blizzard to breach global targets across critical sectors such as energy, oil and gas, telecommunications, shipping, arms manufacturing, and various international governments.

ALIASES- APT44, BE2 APT, Quedagh, Sandworm Team, UAC-0082

Distribution Method:

Seashell Blizzard employs several distribution methods to execute its cyber operations, including:

1. Trojanized Software: Malware implants are spread through compromised legitimate software.

2. Supply-Chain Attacks: Focused on regional managed IT service providers, particularly within Ukraine, to gain access to diverse targets .

3. Web Shells: Deployment of web shells (like LocalOlive) after exploiting vulnerabilities, particularly in Microsoft Exchange and Zimbra .

4. Seashell Blizzard has often employed customized methods to target victims, such as scanning and exploiting specific infrastructure vulnerabilities (like CVE-2024-1709 and CVE-2023-48788), phishing, and altering the legitimate functionality of existing systems to either broaden network access or acquire sensitive information.

5. Chisel (Tunnelling Utility)-When Seashell Blizzard identifies targets of strategic importance, it typically deepens its network compromise by deploying tunneling tools like Chisel, plink, and rsockstun to create dedicated channels into the affected network segments.

Impacts:

The impacts of the Seashell Blizzard subgroup's operations include:

1. Access to Sensitive Information: Gaining control over networks in critical sectors such as energy and telecommunications.

2. Credential Theft: Compromising user credentials, which can lead to further network breaches

3. Operational Disruption: Targeting organizations critical to national interests, particularly in relation to geopolitical dynamics

4. Financial Losses: Organizations face significant costs associated with breaches and recovery efforts.

5. Long-term Espionage: Ongoing access allows for prolonged surveillance and data collection .

6. Infrastructure Damage: Potential for physical damage to critical infrastructure due to cyber operations .

7. Strategic Disadvantages: Affected sectors may face challenges in maintaining operations due to compromised security .

8. Increased Security Measures: Organizations must enhance their security postures, diverting resources from other priorities .

Mitigations:

To defend against the Seashell Blizzard subgroup's activities, organizations should implement the following measures:

1. Strengthen Operating Environment Configuration: Regularly update and patch systems to close vulnerabilities.

2. Utilize Vulnerability Management Systems: Employ tools like Microsoft Defender Vulnerability Management to oversee and remediate vulnerabilities

3. Require Multifactor Authentication (MFA): Implement MFA to enhance identity verification, despite some attacks attempting to bypass it.

4. Adopt Phishing-resistant Authentication: Use FIDO tokens or Microsoft Authenticator with passkeys to mitigate phishing risks.

5. Implement Conditional Access Policies: Enforce strong authentication measures for accessing critical applications .

6. Educate Employees: Conduct training on recognizing and responding to phishing attempts and other social engineering tactics .

7. Monitor Network Traffic: Regularly analyze network activity for unusual patterns that may indicate a breach .

8. Incident Response Planning: Develop and regularly update incident response plans to quickly address breaches when they occur .

9. Leverage Microsoft Defender External Attack Surface Management (EASM): Utilize this tool to continuously discover and map your digital attack surface, providing an external perspective on your online infrastructure. It uses vulnerability and infrastructure data to generate Attack Surface Insights, which report critical risks.

10. Enable Network Level Authentication (NLA) for Remote Desktop Services: Ensure that NLA is enabled for Remote Desktop connections to strengthen security.

11. Use AppLocker: Restrict or allow specific software tools within the organization, such as blocking reconnaissance, fingerprinting, and RMM tools, or limiting access to designated users only.

Recommendations:

1. Regularly Review Security Policies: Ensure that security protocols are up-to-date and aligned with the latest threat intelligence.

2. Engage in Threat Intelligence Sharing: Collaborate with industry peers and threat intelligence groups to stay informed about emerging threats.

3. Conduct Penetration Testing: Regularly test security defenses to identify vulnerabilities before they can be exploited by adversaries.

4. Invest in Security Technologies: Utilize advanced security solutions such as endpoint detection and response (EDR) and intrusion detection systems (IDS).

5. Establish a Cybersecurity Culture: Promote a culture of security awareness across all levels of the organization.

6. Utilize Threat Hunting: Implement proactive threat hunting practices to identify and mitigate threats before they result in a breach.

7. Backup Critical Data: Regularly back up important data and systems to facilitate recovery in case of a ransomware attack or data loss .

8. Conduct Regular Audits: Perform security audits to ensure compliance with security standards and best practices.

INDICATORS OF COMPROMISE:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Chisel:

b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b   (with the exe names as " MsChSoft.exe  MsNan.exe Msoft.exe Chisel.exe Win.exe MsChs.exe)

LocalOlive:

636e04f0618dd578d107f440b1cf6c910502d160130adae5e415b2dd2b36abcb

c7379b2472b71ea0a2ba63cb7178769d27b27e1d00785bfadac0ae311cc88d8b

b38f1906680c80e1606181b3ccb8539dab5af2a7222165c53cdd68d09ec8abb0

9f3d8252e8f3169751a705151bdf675ac194bfd8457cbe08e1f3c17d7e9e9be2

68c7aab670ee9d7461a4a8f06333994f251dc79813934166421091e2f1fa145c

LocalOlive web shell:

def.aspx

Seashell Blizzard infrastructure:

103.201.129.130

104.160.6.2

195.26.87.209

148.251.53.222

89.149.200.91

hwupdates.com

cloud-sync.org

Actor-controlled email address:

akfcjweiopgjebvh@proton.me

ohipfdpoih@proton.me

miccraftsor@outlook.com

amymackenzie147@protonmail.ch

ehklsjkhvhbjl@proton.me

MirrowSimps@outlook.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-I-324022025: Malicious Domains used for Phishing**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, email-based fraud and malware distribution.

> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

> Implement Multi-Factor Authentication to add a layer of security.

- -------------------------< Malicious Domain>-----------------

gov.in.inedex.in

dc.crsorgi.gov.in.imgpdf.top

dc.crsrogi.gov.in.web-index.cloud

gov.in.inedex.in

sebi-gov.mohdatif.in

sebi.gov.in.mohdatif.in

sebi.gov.mohdatif.in

www.dc.crsorgi.gov.in.imgpdf.top

www.dc.crsrogi.gov.in.web-index.cloud

www.upi.imgpdf.top

\*.imgpdf.top

- -------------------------</Malicious Domain>-----------------