مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

BadPilot Campaign Expands Global Cyber Attacks

Tracking #:432316866

Date:13-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft disclosed a report revealing a significant multi-year operation known as the BadPilot campaign that has compromised internet-facing infrastructure across over 15 countries.

TECHNICAL DETAILS:

A new report from Microsoft reveals a significant multi-year operation, dubbed *BadPilot*, conducted by a subgroup of hacking group Sandworm, tracked as *Seashell Blizzard*. This subgroup has executed a series of cyberattacks across over 15 countries, including high-value geopolitical targets and critical sectors such as energy, oil and gas, telecommunications, and international governments.

The campaign, which has been operational since late 2021, primarily exploits security flaws in internet-facing infrastructure to gain initial access to systems. The attackers employ both opportunistic and highly targeted techniques to establish persistence, move laterally across networks, and exfiltrate sensitive data.

Detailed Analysis

Threat Actor: A subgroup within a sophisticated state-sponsored hacking group, known within the cybersecurity community under names such as APT44, Blue Echidna, FROZENBARENTS, Grey Tornado, Iron Viking, Razing Ursa, Telebots, UAC-0002, and Voodoo Bear, and tracked by Microsoft as Seashell Blizzard. Attributed to Sandworm.

Target Sectors: Energy, oil and gas, telecommunications, shipping, arms manufacturing, international governments, and organizations providing support or of geopolitical significance. Since April 2022, organizations that are either geopolitically significant or provide military and/or political support. Heavy reliance on cracked software in government institutions, can create a major attack surface.

Global Reach: The attack spans regions including North America, Europe, Asia, the Middle East, and Africa. Notable countries affected include the United States, Canada, Argentina, China, India, Kazakhstan, Myanmar, Nigeria, and more.

Tactics, Techniques, and Procedures (TTPs):

- **Initial Access:** Exploitation of known vulnerabilities in Internet-facing systems, including:
  - Microsoft Exchange Server (CVE-2021-34473 aka ProxyShell)
  - Zimbra Collaboration (CVE-2022-41352)
  - Openfire (CVE-2023-32315)
  - JetBrains TeamCity (CVE-2023-42793)
  - Microsoft Outlook (CVE-2023-23397)
  - Fortinet FortiClient EMS (CVE-2023-48788)
  - Connectwise ScreenConnect (CVE-2024-1709)
  - JBOSS (Unknown CVE)

- **Persistence:**
  - Deployment of legitimate remote access software (Atera Agent, Splashtop Remote Services).
  - Use of web shells (LocalOlive) for command-and-control.
  - Malicious modifications to Outlook Web Access (OWA) sign-in pages to harvest credentials.
  - Deployment of a previously undocumented RDP backdoor codenamed Kalambur that's disguised as a Windows update
  - Deployment of a bespoke utility dubbed ShadowLink that allows the compromised system to be accessible via the TOR anonymity network.

- **Lateral Movement:**
  - Credential theft and exploitation.
  - Use of tunneling utilities (Chisel, plink, rsockstun).

- **Objectives:**
  - Espionage.
  - Data exfiltration.
  - Maintaining persistent access to high-value targets.
  - Destructive and disruptive attacks (data wipers, pseudo-ransomware), at least three attacks since 2023.

- **Malware and Tools:**
  - DarkCrystal RAT (DCRat)
  - Warzone
  - RADTHIEF ('Rhadamanthys Stealer')
  - KillDisk (HermeticWiper)
  - Prestige (PRESSTEA)
  - Kapeka
  - LocalOlive web shell
  - ShadowLink
  - Kalambur RDP backdoor
  - BACKORDER
  - OpenSSH

Attack chain:

- The threat actor exploits vulnerable internet-facing systems using exploits like ProxyShell, ConnectWise ScreenConnect (CVE-2024-1709) and Fortinet FortiClient EMS (CVE-2023-48788).
- Following exploitation, they obtain credentials and establish persistence via backdoors like Kalambur, ShadowLink, or webshells such as LocalOlive
- Using the established persistence mechanisms, the actor moves laterally through the network, leveraging tools like Chisel and Plink.
- The threat actor then exfiltrates data and maintains access to high-value targets for espionage, sabotage, and disruption.

Indicators of Compromise:
Attached File

RECOMMENDATIONS:

- Immediate Patch and Vulnerability Management: Ensure all systems, particularly those using software such as Microsoft Exchange, FortiClient, Zimbra, and ConnectWise ScreenConnect, are updated and patched with the latest security fixes.
- Deploy advanced intrusion detection systems (IDS) and enable continuous network monitoring to detect unusual activity such as abnormal remote access, DNS record changes, or the presence of backdoors.
- Enforce MFA across all critical systems, especially those involved in authentication and remote access protocols like RDP.
- Monitor the listed IOCs: Implement IOCs in Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR), and firewalls.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/