February 20, 2025

HUNTER471

EMERGING THREATS

BadPilot Campaign

Researchers at Microsoft published an analysis of a subgroup within infamous Russian state-sponsored actor Seashell Blizzard conducting a campaign code named BadPilot since 2021. During this campaign, the subgroup compromised internet-facing infrastructure in order to gain and establish persistence to globally diverse high-value targets, including energy, telecommunications, shipping, arms manufacturing and international government entities. The threat actor initially concentrated their efforts on Ukraine and eventually expanded globally, targeting entities in the United States, United Kingdom, Canada and Australia. Seashell Blizzard expanding beyond their usual Eastern European activity is important that the community takes note of, as the threat group is considered highly sophisticated with a diverse spectrum of capabilities that consist of cyber espionage to the destruction of targeted systems. The subgroup conducting BadPilot has been observed to be exploiting known vulnerabilities, such as CVE-2024-1709 (ConnectWise ScreenConnect) and CVE-2023-48788 (Fortinet FortiClient EMS), as well as abusing remote access tools such as Atera Agent and Splashtop Remote Services to maintain access. Due to the observed reach of the BadPilot campaign reaching a global scale, it is important that organizations prepare themselves and stay on top of the activity related to this subgroup going forward.

THREAT SUMMARY

Researchers at Microsoft published an analysis of a subgroup within infamous Russian state-sponsored actor Seashell Blizzard conducting a campaign code named BadPilot since 2021. During this campaign, the subgroup compromised internet-facing infrastructure in order to gain and establish persistence to globally diverse high-value targets, including energy, telecommunications, shipping, arms manufacturing and international government entities. The threat actor initially concentrated their efforts on Ukraine and eventually expanded globally, targeting entities in the United States, United Kingdom, Canada and Australia. Seashell Blizzard expanding beyond their usual Eastern European activity is important that the community takes note of, as the threat group is considered highly sophisticated with a diverse spectrum of capabilities that consist of cyber espionage to the destruction of targeted systems.

The subgroup conducting BadPilot has been observed to be exploiting known vulnerabilities, such as CVE-2024-1709 (ConnectWise ScreenConnect) and CVE-2023-48788 (Fortinet FortiClient EMS), as well as abusing remote access tools such as Atera Agent and Splashtop Remote Services to maintain access. Due to the observed reach of the BadPilot campaign reaching a global scale, it is important that organizations prepare themselves and stay on top of the activity related to this subgroup going forward.

TITAN References: TITAN Profile Report: Seashell Blizzard

Related Hunt Package Collections: Seashell Blizzard Threat Group

SYNOPSIS

Microsoft researchers published a detailed analysis of the BadPilot campaign, a multi-year initial access operation being orchestrated by a subgroup within Russian state actor Seashell Blizzard. Targeting entities across the world, the researchers observed the subgroup being utilized by Seashell Blizzard to horizontally scale operations, acting as the initial access medium for Seashell Blizzard operations. These activities were observed to take place with the exploitation of vulnerabilities found on internet-facing infrastructure discovered via scanning and/or knowledge repositories. Additionally, the subgroup has operated with TTPs (Tactics, Techniques, and Procedures) related to credential theft and supply chain attacks.

Researchers are aware of the following vulnerabilities being exploited (or attempted): CVE-2021-34473 (Microsoft Exchange), CVE-2022-41352 (Zimbra Collaboration Suite), CVE-2023-32315 (OpenFire), CVE-2023-42793 (JetBrains TeamCity), CVE-2023-23397 (Microsoft Outlook), CVE-2024-1709 (ConnectWise ScreenConnect), and CVE-2023-48788 (Fortinet FortiClient EMS).

Furthermore, they have abused legitimate IT remote management software such as Atera Agent and Splashtop in order to stealthily conduct operations and maintain persistence post-initial access. Usage of data exfiltration with Rclone, Chisel and Plink has also been observed by researchers, as well as a newly discovered technique that switches their traffic to use the Tor network to obfuscate connections. Given Seashell Blizzard's history of high-impact operations, including destructive attacks like NotPetya in 2017, the BadPilot campaign represents a significant escalation in their cyber capabilities and intent.

Organizations potentially targeted and falling within targeted sectors should bolster their security postures, ensure timely patching of known vulnerabilities, and implement robust monitoring to detect and mitigate such advanced persistent threats.

RELATED HUNT PACKAGES

Suspicious BITS Activity - ScriptBlock

https://hunter.cyborgsecurity.io/details/use-case/a829ece6-c94c-4dae-b34c-e2b80309d2a1

Suspicious BITS Activity

https://hunter.cyborgsecurity.io/details/use-case/a96fd1ad-53c7-4125-9dfd-1dffa2f68f2d

Single Character Batch Script File Executed on Endpoint

https://hunter.cyborgsecurity.io/details/use-case/73fd8d9a-edb6-4db6-aab8-0dbc916f0fb4

Potential Exfiltration - Common Rclone Arguments

https://hunter.cyborgsecurity.io/details/use-case/f075c217-783e-459a-aeb4-42ea91e07af7

CertUtil file download

https://hunter.cyborgsecurity.io/details/use-case/f7b279bf-f1f9-4506-b636-e66f1834a278

Suspicious Change in File or Folder Ownership - Potential Sensitive File Access or Ransomware

https://hunter.cyborgsecurity.io/details/use-case/274a8f6a-8d3f-4987-8596-2a77cfd05d8e

Methods for Downloading Files with PowerShell

https://hunter.cyborgsecurity.io/details/use-case/c7b320fb-ac67-45b0-92c4-b0f1e10b4e46

Remote Atera Agent Download - Command Line

https://hunter.cyborgsecurity.io/details/use-case/bb771c73-e7ab-4705-92a2-ce322b33621d

Remote Atera Agent Download - Web

https://hunter.cyborgsecurity.io/details/use-case/7ccc1404-1499-45ba-9c7d-59f42ba321e3

Attempted Credential Dump From Registry Via Reg.exe

https://hunter.cyborgsecurity.io/details/use-case/8dfe6e0a-597c-4f0e-82f6-c19d733a8c1c

Dump LSASS via Renamed procdump

https://hunter.cyborgsecurity.io/details/use-case/3e8f06d3-4946-4c4a-85b0-cd2804d3401b

MITRE CONTEXT

- Actors:
  - Sandworm
  - Seashell Blizzard
  - APT44
- Threat Names:
  - MITRE Technique IDs:
    - T1219
    - T1036
    - T1105
    - T1222.001
    - T1059
    - T1059.001
    - T1048
    - T1197
    - T1003
  - MITRE Technique Names:
    - Ingress Tool Transfer
    - Remote Access Software
    - PowerShell
    - Command and Scripting Interpreter
    - OS Credential Dumping
    - Masquerading
    - BITS Jobs
    - Exfiltration Over Alternative Protocol
    - Windows File and Directory Permissions Modification
  - MITRE Tactic Names:
    - Execution
    - Credential Access
    - Defense Evasion
    - Command and Control
    - Exfiltration
  - Exploits Vulns:
    - CVE-2024-1708
    - CVE-2024-1709

REFERENCE

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