ADVISORY FOR ICM SECTOR

Secret Blizzard Targets Internet Service Providers to Deliver ApolloShadow

Original report published on: July 31, 2025[1]

Executive Summary

Microsoft Threat Intelligence has uncovered a campaign by Russian-nexus APT, Secret Blizzard (also known as VENOMOUS BEAR, Uroburos, Snake, Blue Python, Turla, Wraith, ATG26, and Waterbug), that uses Internet Service Provider (ISP) level Adversary-in-the-Middle (AiTM) attacks against foreign diplomats in Moscow. The campaign is suspected to leverage Russia's System for Operative Investigative Activities (SORM) lawful internet traffic interception to redirect victims to a captive portal (commonly required for public to request Wi-Fi access). Victims are tricked into installing a malicious tool, ApolloShadow which enables TLS interception, credential theft, and persistent espionage when installed.

Although the campaign has been active since at least 2024, this report newly confirms that Secret Blizzard is operating directly at the ISP level, highlighting how state-level internet surveillance infrastructure can be exploited by attackers, creating systemic vulnerabilities for high-value targets.

Background

In this campaign, Secret Blizzard uses its Adversary-in-the-Middle (AiTM) position at the ISP level in Russia to redirect target devices to the pre-access network portal. At the portal, when the Windows device performs its built-in connectivity check to the legitimate service *hxxp://www.msftconnecttest[.]com/redirect*, the actor intercepts the request and redirects the system to a malicious domain, prompting the download and execution of ApolloShadow. The malware checks the process privilege level, and if the device is not running on default administrative settings, it presents a User Access Control (UAC) prompt to install root certificates, disguised as a Kaspersky installer (*CertificateDB.exe*), enabling TLS interception and elevated privileges.

The malware uses two execution paths. On low-privilege paths, it collects and encodes host IP information, and exfiltrates it via a Digicert URL that appears legitimate but is redirected by the AiTM actor to the attacker-controlled command-and-control server, while obfuscating critical strings and scripts to evade detection. With elevated privileges, ApolloShadow modifies network profiles to allow the device to be discoverable, adjusts firewall rules to allow file sharing and network discovery, installs root certificates for Windows, and creates a persistent administrative account with the username *UpdatusUser*. These steps establish persistent access, enable network-level monitoring, and prepare the host for ongoing espionage, leveraging SORM-supported infrastructure for direct ISP-layer control.

Detection and Mitigation

While Secret Blizzard is not currently targeting Singapore, it is a threat that target ISP users. IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the ApolloShadow malware identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
    - Create, test and validate detection rules against the threat behaviours.

    - Validate and deny/disable processes, ports and protocols that have no business need.
- Detect unexpected website redirections or downloads using ISP infrastructure such as:
    - Monitoring DNS queries for anomalous domain resolutions
    - Applying anomaly detection to identify deviations from normal user behavior

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

SHA256 Hash	Description
13fafb1ae2d5de024e68f2e2fc820bc79ef0690c40dbfd70246bcc394c52ea20	ApolloShadow malware
e94c00fde5bf749ae6db980eff492859d22cacb4bc941ad4ad047dca26fd5616	

Domain	Description
kav-certificates[.]info	Secret Blizzard-controlled domain that downloads the malware

IP Address	Description
45.61.149[.]109	Secret Blizzard-controlled IP address

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1189	Drive-by Compromise
Execution	T1204.002	User Execution: Malicious File
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Persistence	T1136.001	Create Account: Local Account
Persistence	T1553.004	Subvert Trust Controls: Install Root Certificate
Privilege Escalation	T1548.002	Abuse Elevation Control Mechanism: Bypass User Access Control
Defense Evasion	T1112	Modify Registry
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1553.004	Subvert Trust Controls: Install Root Certificate
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location
Defense Evasion	T1562.004	Impair Defenses: Disable or Modify System Firewall
Credential Access	T1557	Adversary-in-the-Middle
Discovery	T1016	System Network Configuration Discovery
Collection	T1005	Data from Local System
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Command and Control	T1132.001	Data Encoding: Standard Encoding

References

1. Frozen in transit: Secret Blizzard's AiTM campaign against diplomats