Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

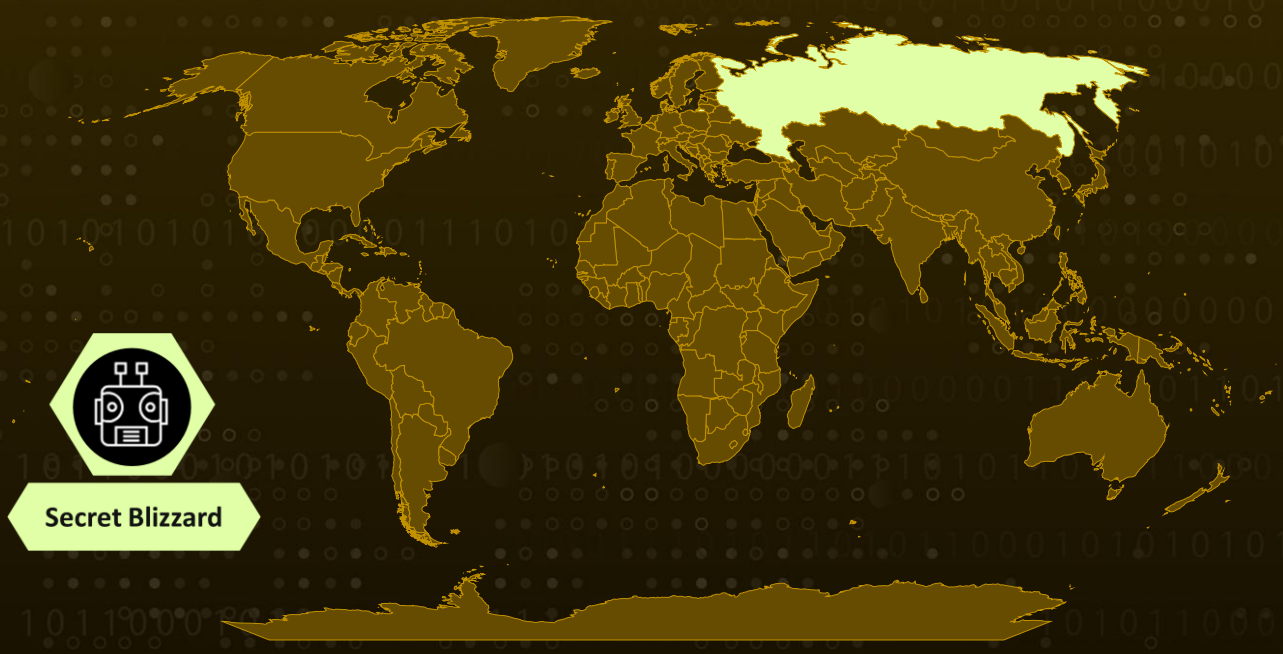
Secret Blizzard Strikes Moscow with ApolloShadow

Date of Publication	Admiralty Code	TA Number
August 1, 2025	A1	TA2025237

Summary

Attack Discovered: February 2025
Targeted City: Moscow
Targeted Industry: Diplomats
Malware: ApolloShadow
Actor: Secret Blizzard (aka Turla, Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Pensive Ursa, Blue Python, G0010, Hippo Team, Pfinet, Snake, UAC-0003, UAC-0024, UAC-0144, Uroburos)
Attack: The Russian state-sponsored group Secret Blizzard is running a targeted cyber-espionage operation against diplomats in Moscow. By leveraging an adversary-in-the-middle (AiTM) position, likely made possible through cooperation with local internet service providers, they intercept network traffic and redirect victims to a deceptive captive portal. There, targets are tricked into downloading a fake Kaspersky Anti-Virus installer that silently drops ApolloShadow malware. This malware installs a rogue trusted root certificate, allowing the attackers to maintain long-term access and intercept encrypted communications. Secret Blizzard also uses stealthy techniques to map networks, evade defenses, and extract sensitive intelligence without being detected.

Attack Regions



Attack Details

#1 A sophisticated cyberespionage campaign, orchestrated by the Russian state-sponsored group Secret Blizzard, has been quietly targeting foreign embassies in Moscow. Active since at least 2024, the operation poses a serious threat to diplomatic missions by leveraging an adversary-in-the-middle (AiTM) position, likely enabled by Russia's internal surveillance systems such as SORM. This privileged access allows the attackers to intercept and manipulate internet traffic, particularly for victim's dependent on local internet service providers. The initial stage of the attack involves redirecting victims to a captive portal, tricking them into downloading and executing a custom malware strain known as ApolloShadow, which is cleverly disguised as a legitimate Kaspersky Anti-Virus installer.

#2 Once the malware is executed, it begins a series of actions to establish a persistent and privileged foothold. ApolloShadow first checks the ProcessToken for elevated privileges and, if needed, displays a User Account Control (UAC) prompt to get the user to install malicious root certificates. This key tactic is a cornerstone of the attack, as the rogue certificates allow the attackers to strip TLS/SSL encryption from web traffic, exposing even secure communications. The malware also employs command and scripting interpreters to run obfuscated scripts that hinder detection and reverse engineering.

#3 To maintain long-term access, the attackers implement several robust persistence mechanisms. A key tactic is the creation of a stealthy admin-level user account named "UpdatusUser" using the NetUserAdd Windows API, which is protected with a hardcoded, non-expiring password. Furthermore, ApolloShadow deliberately manipulates network configurations, changing all network types to "Private." This subtle change weakens firewall restrictions, making the host more vulnerable to lateral movement across the internal environment and facilitating the attackers' ability to extend their control. The malware also decodes and runs a second-stage VBScript payload delivered via its command-and-control (C2) infrastructure.

#4 The malware masquerades its C2 traffic by making requests to a non-existent /registered resource on a digicert.com subdomain. The attackers use DNS hijacking to redirect this seemingly legitimate communication to their own C2 servers, allowing them to issue commands and exfiltrate data without triggering immediate network alerts. ApolloShadow exhibits adaptive behavior, collecting detailed system and network information from the compromised host, which is then encoded and exfiltrated. This strategic gathering of intelligence is a primary objective of the espionage campaign, providing the attackers with critical insights into the diplomatic network.

Recommendations

Use a Trusted, Secure Connection for All Internet Activity: Whenever you go online, especially when accessing sensitive information, make sure your internet traffic is routed through a secure, encrypted tunnel. This can be done by using a reliable Virtual Private Network (VPN). Ideally, choose a VPN provider that operates independently and isn't influenced by governments or organizations that could misuse your data.

Limit Access: Give users only the access they truly need to do their jobs, nothing more. Turn on multifactor authentication (MFA) to add an extra layer of security. Regularly review how admin accounts are being used and avoid using one super-powerful account across your whole network. Also, try to limit who has admin access on individual machines. These steps make it much harder for attackers to move around if they get in and help you catch suspicious activity early.

Keep a Close Watch on User Groups: Regularly check who's in high-privilege groups like Administrators, Remote Desktop Users, and Enterprise Admins. Attackers often sneak their accounts into these groups to stay hidden and keep access for longer. Spotting unexpected changes early can help you kick them out before they do more damage.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0010 Exfiltration	TA0011 Command and Control
T1557 Adversary-in-the-Middle	T1036 Masquerading	T1036.005 Match Legitimate Resource Name or Location	T1068 Exploitation for Privilege Escalation

T1132 Data Encoding	T1132.001 Standard Encoding	T1041 Exfiltration Over C2 Channel	T1059 Command and Scripting Interpreter
T1059.005 Visual Basic	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1548 Abuse Elevation Control Mechanism
T1548.002 Bypass User Account Control	T1112 Modify Registry	T1070 Indicator Removal	T1070.004 File Deletion
T1136 Create Account	T1559 Inter-Process Communication	T1559.001 Component Object Model	T1553 Subvert Trust Controls
T1553.004 Install Root Certificate	T1087 Account Discovery	T1071 Application Layer Protocol	T1082 System Information Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	kav-certificates[.]info
IPv4	45[.]61[.]149[.]109
SHA256	13fafb1ae2d5de024e68f2e2fc820bc79ef0690c40dbfd70246bcc394c52ea20
Filename	CertificateDB.exe

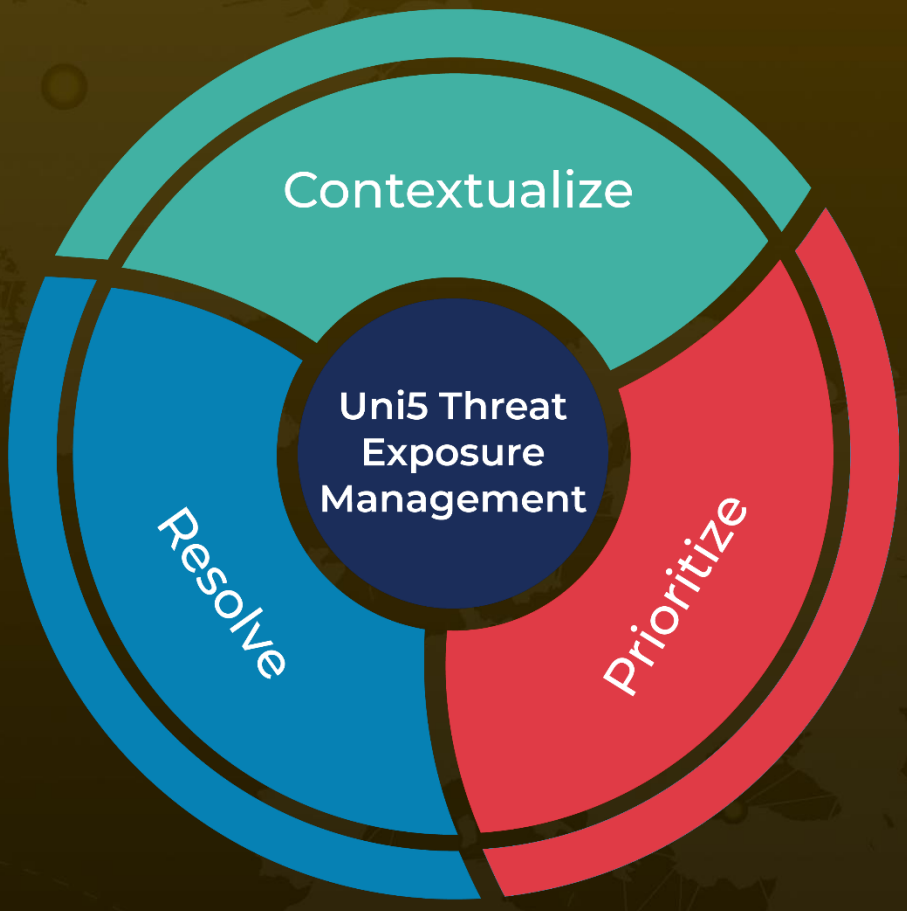
References

https://www.microsoft.com/en-us/security/blog/2025/07/31/frozen-in-transit-secret-blizzards-aitm-campaign-against-diplomats/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 1, 2025 • 6:20 AM

More at www.hivepro.com