Snowblind: The Invisible Hand of Secret Blizzard

: 12/4/2024

Black Lotus Labs Posted On December 4, 2024

Executive Summary

Lumen's Black Lotus Labs has uncovered a longstanding campaign orchestrated by the Russian-based threat actor known as "Secret Blizzard" (also referred to as Turla). This group has successfully infiltrated 33 separate command-and-control (C2) nodes used by Pakistani-based actor, "Storm-0156." Known for their focus on espionage, Storm-0156 is associated in public reporting with two activity clusters, "SideCopy" and "Transparent Tribe." This latest campaign, spanning the last two years, is the fourth recorded case of Secret Blizzard embedding themselves in another group's operations since 2019 when they were first seen repurposing the C2s of an Iranian threat group.

In December 2022, Secret Blizzard initially gained access to a Storm-0156 C2 server and by mid-2023 had expanded their control to a number of C2s associated with the Storm-0156 actor. From their vantage point within these servers, Secret Blizzard leveraged the pre-existing access obtained by Storm-0156 to deploy their own malware, "TwoDash" and "Statuezy," into a handful of networks linked to various entities within the Afghan government. Notably, in April 2023, Secret Blizzard advanced their operations by moving into the workstations of Pakistani-based operators. Through this channel, they potentially acquired a wealth of data. This bounty included insights into Storm-0156's tooling, credentials for both C2s and targeted networks, as well as exfiltrated data collected from prior operations.

By mid-2024, Secret Blizzard had expanded their focus to include the use of two other malware families, Waiscot and CrimsonRAT, which they appropriated from the Pakistani workstations. CrimsonRAT was previously found in use against government and military targets in India. Secret Blizzard later took advantage of their access to gather data from prior deployments of the malware.

Lumen Technologies extends its gratitude to our partners at the Microsoft Threat Intelligence Team (MSTIC) for their invaluable contributions in tracking and mitigating this threat. This report is released in conjunction with the MSTIC blog, which provides further insight into these events.

Introduction

Black Lotus Labs has monitored a diverse array of nation-state actors, including a previous report on a Secret Blizzard campaign that utilized strategic compromises against Ukrainian websites, which is one characteristic that distinguishes this group more than any other: their audacity in exploiting other threat actors' C2 servers for their own purposes. This strategy allows Secret Blizzard to remotely acquire sensitive files that were previously exfiltrated from compromised networks, without employing (and possibly exposing) their own tools; crucially, operations such as these avoid or delay attribution. In scenarios where the other threat actors have not acquired all the data of interest on their targets, they can search the data collected on C2 nodes for stolen authentication materials to gain access or use existing access to expand collection and deploy their agents into a network. By doing so, Secret Blizzard essentially takes advantage of the foothold created by the original threat actor.

While this method of data collection offers unique benefits, a malicious actor who stops there would be limited to gathering data or gaining access only within networks controlled by a single C2 node. Secret Blizzard continued to exploit trust relations by moving from an actor's C2 nodes into the operator's workstations. We believe that nation-state and cybercriminal endpoints and malware are especially vulnerable to exploitation since they are unable to use modern security stacks for monitoring access and protecting against exploitation. When threat actors have installed security products, it has resulted in the disclosure of their previously unknown exploits and tools. We suspect that the routine deletion of log data, a standard best practice for threat actors, compounds the exposure.

This report illustrates the meticulous and systematic approach Secret Blizzard took to expand their operations in the middle east over the past two years. We will start by briefly describing the Storm-0156 (SideCopy/Transparent Tribe) modus operandi, then show how Storm-0156's access was leveraged, allowing Secret Blizzard to target Afghanistan government networks beginning in 2022. We suspect they manipulated the trust relationship from those Storm-0156 C2s to move into the Pakistani computer network operators' workstations, pilfering data from those nodes along the way, to include the Waiscot and CrimsonRAT malware used to interact with Indian-based networks.

Technical Details

Overview of Storm-0156 Modus Operandi and Previously Undocumented Tradecraft

Black Lotus Labs had previously tracked an activity cluster associated with Storm-0156, a nation-state actor operating out of Pakistan. This threat actor uses a diverse array of both open-source tools such as AllaKore, and custom remote access trojans over the past several years. While Storm-0156 has demonstrated proficiency in adapting their tools to different operating systems, including the recent integration of python-based tools for Linux systems, their fundamental tactics, techniques, and procedures (TTPs) have remained relatively unchanged. Broadly speaking, Storm-0156's engagements primarily target regional governmental organizations, with a persistent focus on Afghanistan and India, including entities in government, technology, and industrial control systems such as power generation and distribution.

In January 2023, Lumen observed a Storm-0156 campaign, using a single VPS,185.217.125[.]195 that had a "hak5 Cloud C2" banner and was administered from known Storm-0156 C2s. This banner indicated that the server was acting as a cloud-based C2 configured to control a suite of Hak5 tools. Hak5 equipment is unique as it offers hardware-based solutions for "red teams, pentesters, cyber security students and IT professionals." Unlike the commodity RATs previously used by Storm-0156, Hak5 equipment requires having physical access to a workstation, a network cable, or proximity to a WiFi Pineapple. While the use of close access equipment has been observed before, it is seldom reported upon. Once installed, these devices can either surreptitiously retrieve data or run predefined scripts. The advantage of hardware-based attacks lies in their design, which allows users to effectively bypass standard EDR/XDR protections.

This campaign came to light after the new server was administered from two known Storm-0156 operational nodes; the first node, 209.126.6[.]227, connected from January through February 2023. The second node, 209.126.81[.]42 reported by Qi'anxin, connected to this new server from February through July 2023. Analysis of the telemetry associated with this Hak5 Cloud C2 revealed a significant volume of data flow associated with a limited number of entities. These were an Indian Ministry of Foreign Affairs office in Europe, an Indian national defense organization and several other government bodies, all taking place from December 2022 through March 2023.

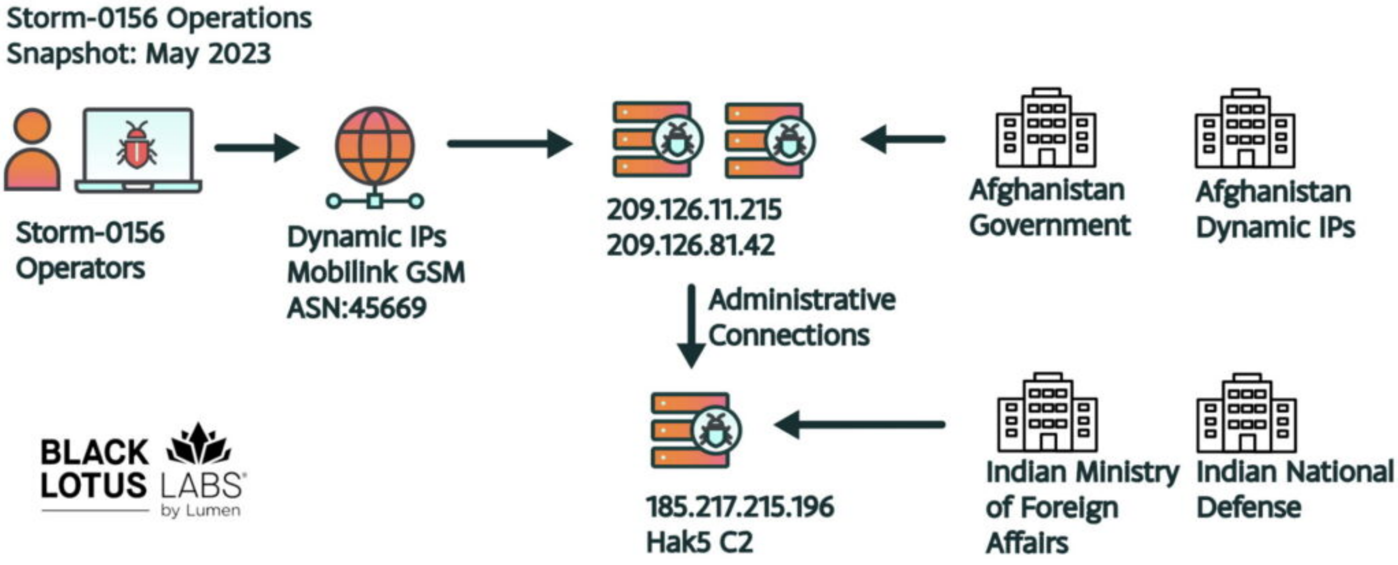

Figure 1: Logical Connections between Storm-0156's Hak5 Cloud C2 and known C2s.

Secret Blizzard Gains Access to Storm-0156 C2s

While monitoring the Storm-0156 campaigns, we uncovered 11 C2 nodes that were active from December 2022 through mid-2023. Black Lotus Labs observed malware samples or public reporting corresponding for 8 of the 11 nodes. Closer analysis revealed that these 11 all communicated with three newly identified VPS IP addresses. The VPSs caught our eye, as they were leased through a provider that we had not seen used in previous Storm-0156 campaigns. Our counterparts at MSTIC were able to confirm that the three nodes were associated with Secret Blizzard, who used the following three IP addresses from at least December 2022 through August 2023: 146.70.158[.]90, 162.213.195[.]129, 146.70.81[.]81.

Although we cannot be certain how Secret Blizzard identified the remaining three nodes that did not correspond to public malware samples or reporting, we suspect they could have used a method of Remote Desktop Protocol (RDP) pivoting outlined here by Team Cymru. The full list of Storm-0156 IP addresses and the timeframe of interaction with the 2023 Secret Blizzard C2s are as follows:

- 154.53.42[.]194; Dec 11, 2022 – Oct 7, 2024
- 66.219.22[.]252; Dec 12, 2022 – July 9, 2023
- 66.219.22[.]102; Dec 27, 2022 – Aug 9, 2023
- 144.126.152[.]205; Dec 28, 2022 – Mar 2, 2023
- 185.229.119[.]60; Jan 31 – Mar 14, 2023
- 164.68.108[.]153; Feb 22 – Aug 21, 2023
- 209.126.6[.]227; Feb 27 – Mar 22, 2023
- 209.126.81[.]42; April 30 – July 4, 2023
- 209.126.7[.]8; May 5 – Aug 22, 2023
- 154.38.160[.]218; April 12 – Aug 23, 2023
- 144.126.154[.]84; June 23 – Aug 21, 2023

We observed a continuation of this same behavior in 2024; however, Secret Blizzard rotated their C2 nodes in 2024 to the following IP addresses; 146.70.158[.]90, 162.213.195[.]192. The list of nine Storm-0156 IP addresses and the timeframe of interaction with the 2024 Secret Blizzard C2s are shown below:

- 173.212.252[.]2; May 29 – Oct 10, 2024
- 185.213.27[.]94; May 26 – Aug 24, 2024
- 167.86.113[.]241; May 28 – Aug 9, 2024
- 109.123.244[.]46; May 28 – Oct 18, 2024
- 23.88.26[.]187; May 29 – Oct 20, 2024
- 173.249.7[.]111; Aug 28 – Oct 24, 2024
- 62.171.153[.]221; May 27 – Oct 21, 2024
- 173.212.252[.]2; May 29 – Nov 20, 2024
- 149.102.140[.]36; May 28 – Sept 2, 2024

Secret Blizzard Drops their own Tooling into Afghan Government Networks

During our monitoring of Secret Blizzard's interactions with the Storm-0156 C2 nodes, we identified beaconing activity from various Afghan government networks that Storm-0156 threat actors had previously compromised. This leads us to believe, with high confidence, that Secret Blizzard used their access to the Storm-0156 C2s to gather essential network information and deploy their own malware, “Two-Dash,” into the Afghan government networks.

We observed communications from several IP addresses based in Afghanistan. The duration and volume of data transferred indicated that three of these IP addresses showed beaconing activity for just a week, suggesting that Secret Blizzard chose not to maintain long-term access. However, three other networks appeared to be of greater interest, as they showed beaconing activity over months with significant data transfers:

- Secret Blizzard C2 node, 146.70.158[.]90, found interacting with six IP addresses and was active from at least January 23, 2023, through September 4, 2023.
- Secret Blizzard C2 node, 162.213.195[.]129, communicated with five IP addresses and was active from December 29, 2022, through September 4, 2023.
- Secret Blizzard C2 node, 167.88.183[.]238, transmitted to only one IP address on April 17, 2023.

From at least May through October 2024, we observed persistent connections from the same handful of Afghan government networks, the only notable difference is that the C2 rotated aligning with the prior Storm-0156 infections to 143.198.73[.]108.

Into the Void: Surreptitious Entry to The Pakistani Operator Network

The most critical observation of this campaign was the detection of Two-Dash beaconing activity, not only from Storm-0156 C2 nodes in Afghanistan, but also from a dynamic IP address originating in Pakistan.

On May 4th, 2023, the Pakistani IP address 182.188.171[.]52 connected to a known AllaKore C2 node via Remote Desktop Protocol (RDP) from 6:19:00 through 10:48:00 UTC. During this time window, the same Pakistani IP address 182.188.171[.]52 established a connection to the known Secret Blizzard IP address 146.70.158[.]90, from 05:57:00 through 08:13:00. Given the connection duration of almost two hours, and the fact that the Secret Blizzard IP address 146.70.158[.]90 was used as a C2 server to both Storm-0156 C2 nodes and Afghan government victims, it is highly indicative that they compromised Storm-0156 operators themselves. We then observed intermittent connections from various dynamic IP addresses that geolocate to Pakistan connecting to known Secret Blizzard C2s.

We suspect they leveraged access to the Storm-0156 C2 panel, then abused a trust relationship to move laterally into the Storm-0156 operator’s workstation. This achievement could have enabled them to access additional networks previously compromised by Storm-0156, which includes other middle eastern governmental entities.

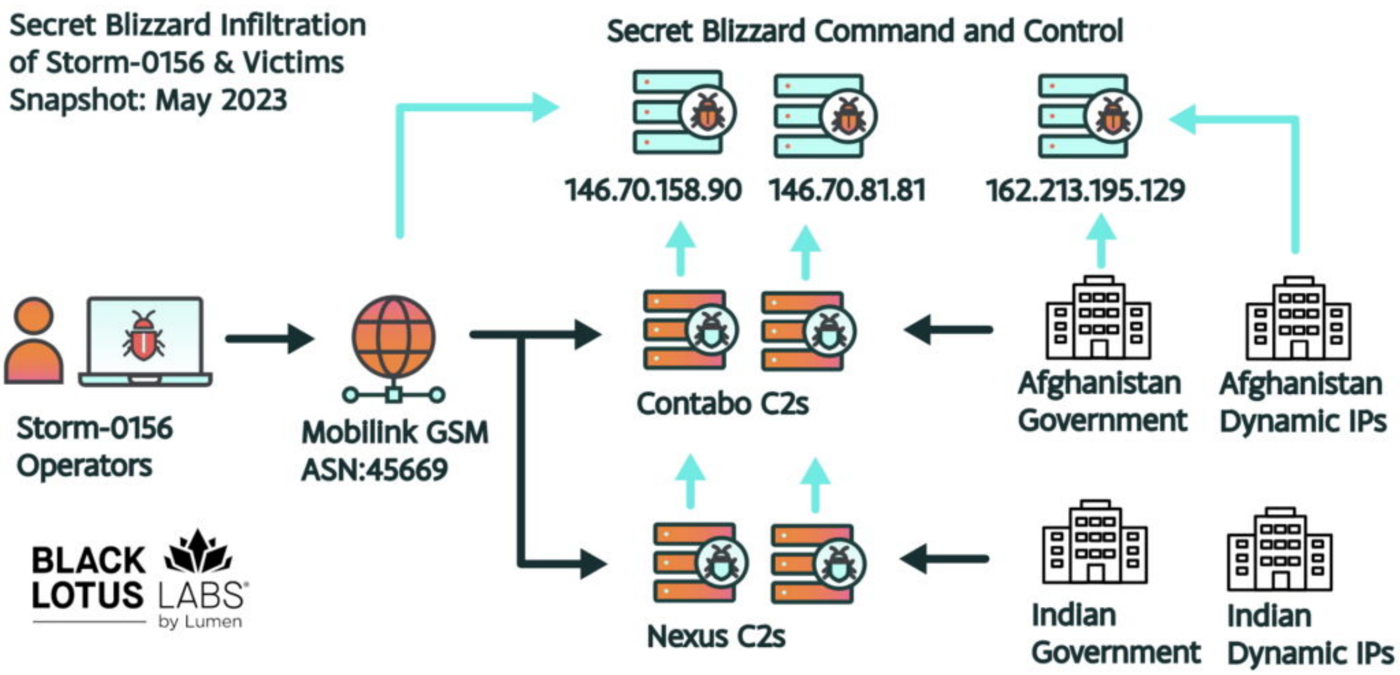

Figure 2: Secret Blizzard infiltrating both Storm-0156 and Afghan government networks

Double Secret Probation: Secret Blizzard Targets C2s Associated with Indian Network

Starting in 2024, Lumen's continuous monitoring of the Secret Blizzard infrastructure revealed interactions with a subset of CrimsonRAT C2 nodes, which had previously been used to target the Indian government and military. Notably, Secret Blizzard only engaged with seven CrimsonRAT C2s, though our data indicated that several more were available. This selective engagement implies that, while they had the capability to access all nodes, their tool deployment was strategically limited to those associated with the highest priority targets in India. The seven that were most attractive were:

- 38.242.219[.]13; May 29 – Oct 20, 2024
- 5.189.183[.]63; June 2 – Aug 11, 2024
- 62.171.153[.]221; May 27 – Oct 13, 2024
- 38.242.211[.]87; May 29 – Oct 5, 2024
- 45.14.194[.]253; May 26 – Sept 18, 2024
- 173.212.206[.]227; May 29 – Aug 2, 2024
- 209.145.52[.]172; May 27 – Nov 21, 2024

Lumen also observed Storm-0156's Indian-based targeting with a previously undocumented malware family dubbed Waiscot, which was a Go-compiled remote access trojan. The Waiscot malware along with other Storm-0156 malware families were used to interact with the following Indian-based IP addresses:

- 130.185.119[.]198; Dec 9, 2022 – Aug 14, 2024
- 173.249.18[.]251; Feb 15 – Aug 24, 2023
- 176.57.184[.]97; May 31 – Oct 20, 2024
- 209.126.11[.]251; May 25 – June 13, 2024

We also observed other malware families used to target Indian-based organizations such as ActionRat, those IP addresses and timeframes were as follows:

- 144.91.72[.]17; Dec 16, 2022 – April 26, 2023
- 84.247.181[.]64; May 27 – Nov 17, 2024

An interesting observation was that although Lumen detected Secret Blizzard interacting with various C2s, we did not see Secret Blizzard deploying their own agents, like Two-Dash or Statuezy, into Indian networks. It remains unclear whether they moved downstream into those victims, as they might have either taken relevant data from the C2s or were using the existing agents that Storm-0156 had already established to submit their data requests.

Conclusion

The Secret Blizzard activity cluster, along with its parent organization, the Russian FSB, has consistently employed sophisticated tradecraft to achieve their goals while maintaining the secrecy of their operations. Unlike other Russian groups, which often use a variety of techniques to create plausible deniability—such as operating through residential proxy networks managed by cybercriminals or using commercially available frameworks like Cobalt Strike—Turla has opted for a unique strategy. Compromising the command-and-control servers of other threat actors not only helps them gather the information they seek but also shifts the blame to other groups if incident response efforts reveal exploitation on these networks. We have documented this case study because we believe this approach will likely persist, especially as Western nations, including the United States and European allies, continue to uncover and condemn Russian activities in cyberspace.

Black Lotus Labs continues to monitor and track nation-state Russian activity clusters to help protect and better secure the internet. To that end, we have blocked traffic across the Lumen global backbone to all the architecture related to both Secret Blizzard and the various sub-clusters of Storm-0156. We have added the indicators of compromise (IoCs) from this campaign into the threat intelligence feed that fuels the Lumen Connected Security portfolio. We will continue to monitor new infrastructure, targeting activity, and expanding TTPs, and we will continue to collaborate with the security research community to share findings related to this activity.

We strongly recommend treating all compromises as equally concerning, regardless of whether the activity flags for a nation-state malware family or appears related to cybercrime, as both have been co-opted by Secret Blizzard in the past. We encourage the community to monitor for and alert on these and any similar IoCs. We also advise the following:

- A well-tuned EDR solution that routinely receives signature updates for all network assets, as well as centralized monitoring looking for signs of lateral movement within a network.
- Look for large data transfers out of the network, even if the destination IP address is physically located in the same geographical area.
- All organizations: Consider comprehensive secure access service edge (SASE) or similar solutions to bolster their security posture and enable robust detection on network-based communications.

Analysis of Secret Blizzard's activity was performed by Danny Adamitis. Technical editing by Ryan English.

For additional IoCs associated with this campaign, please visit our GitHub page.

If you would like to collaborate on similar research, please contact us on social media @BlackLotusLabs.

This information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk.

Post Views: 31,203
