KV-Botnet: Don’t call it a Comeback

blog.lumen.com/kv-botnet-dont-call-it-a-comeback/

Black Lotus Labs Posted On February 7, 2024

0
18.9K Views

0

Shares

BLACK
LOTUS LABS®
by Lumen

Executive Summary

On December 13, 2023, Lumen’s Black Lotus Labs reported our findings on the KV-botnet, a covert data transfer network used by state-sponsored actors based in China to conduct espionage and intelligence activities targeting U.S. critical infrastructure. Around the time of the first publication, we identified a spike in activity that we assess aligns with a significant effort by the operators managing this network to combat takedown efforts underway by the U.S. Government.

According to a Department of Justice (DOJ) press release, the Federal Bureau of Investigation (FBI) conducted a court-authorized takedown of KV-botnet in early December 2023. Based on the date the earliest warrant was signed, December 6, 2023, Black Lotus Labs believes the takedown operation was likely underway between December 6 and December 8, 2023. We observed a brief but concentrated period of exploitation activity in early December 2023, as the threat actors attempted to re-establish their command and control (C2) structure and return the botnet to working order. Over a three-day period from December 8 to December 11, 2023, KV-botnet operators targeted approximately 33% of the NetGear ProSAFE devices on the Internet for re-exploitation, a total of 2,100 individual devices. This shift in priorities by the operators appeared to cause rippling effects on the other clusters within KV-botnet, resulting in, for example, a 50% decrease in bots in the scanning and reconnaissance cluster we referred to as “JDY.” Despite the botnet operator’s best efforts, Lumen Technologies’ quick null-routing along with the effects of the FBI’s court-authorized action, appear to have had a significant impact on the uptime, breadth, and sustainability of KV-botnet.

Our follow up report is intended to document the post-publication activity and provide a timeline from the vantage point of Lumen’s global visibility. Lumen Technologies would like to commend the FBI for their efforts in countering Chinese cyber activity against U.S. critical infrastructure. Lumen Technologies shared threat intelligence to warn agencies across the U.S. Government of the emerging risks that could impact our nation’s strategic assets.

Technical Details

Introduction

In December 2023, Lumen’s Black Lotus Labs reported on a complex network called “KV-botnet” that infected small-office, home-office (SOHO) routers and firewall devices across the globe. These compromised devices associated with the KV-cluster were chained together to form a covert data transfer network supporting various Chinese state-sponsored actors including Volt Typhoon.

In the weeks following our original publication, Lumen observed significant behavioral changes in the C2 nodes associated with one of the botnet’s secondary activity clusters. The “JDY” cluster, principally used for scanning potential targets, fell silent for roughly fifteen days following our report. We assess that during this period, the threat actor had been focused on re-establishing other critical elements of the botnet, such as the primary infection arm referred to as the “KV” cluster. As the threat actor attempted to restore integrity and transition the KV cluster to auxiliary C2 nodes, Black Lotus Labs monitored the activity through Lumen’s global telemetry, and null routed the new infrastructure in early January 2024.

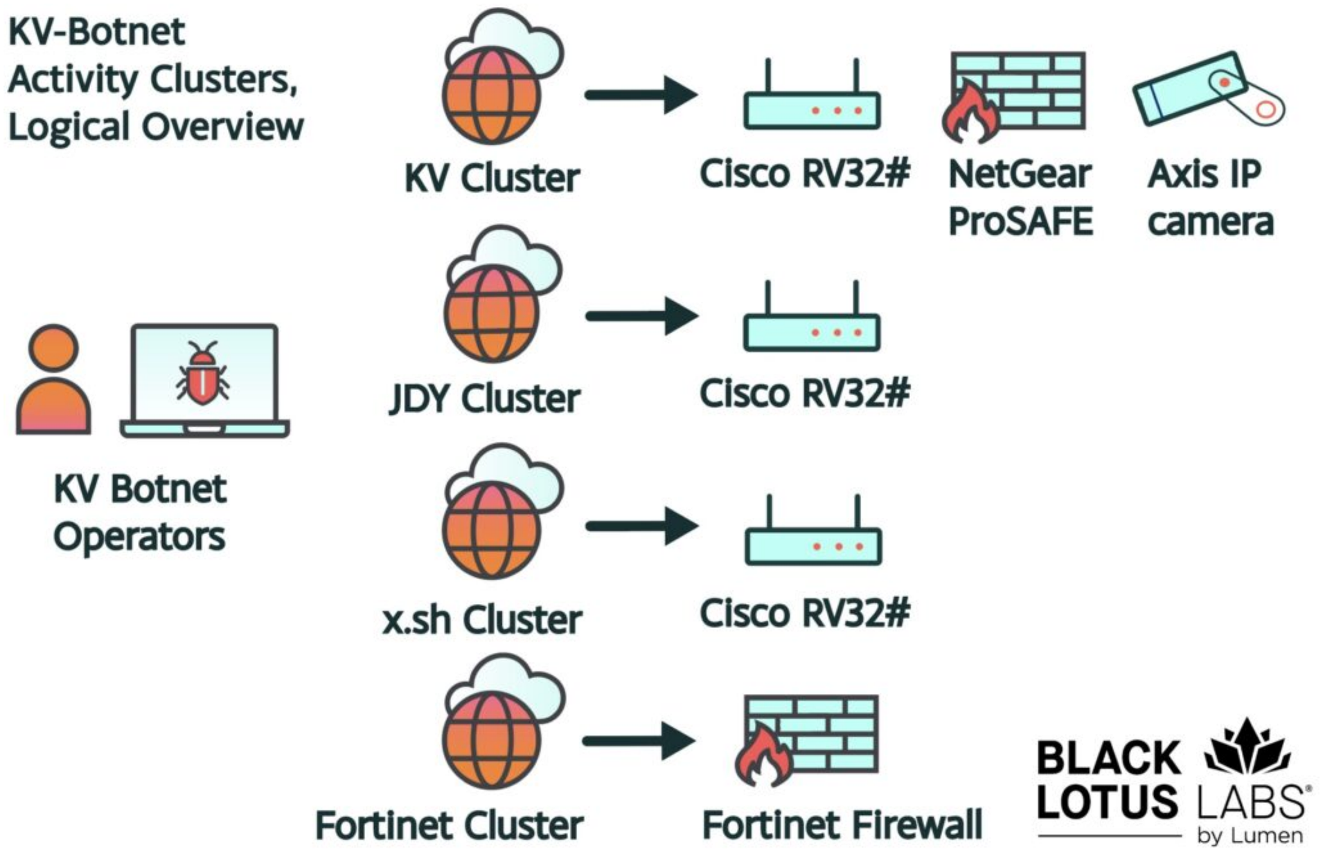

Figure 1: Showing the logical overview of the various activity clusters that comprise the KV-botnet

KV Cluster Activity: Court-Authorized Disruption Effort

Coinciding with our first publication, Black Lotus Labs observed a dramatic shift in the operations of the KV cluster. Our telemetry revealed a spike in the targeting of NetGear ProSAFE firewalls, which we can now attribute to the actions taken by the FBI.

The DOJ press release on January 31, 2024, indicates that takedown actions began with a signed warrant issued on December 6, 2023. We can assume the FBI began issuing commands to the bots to remove the malware and enhance protective measures of the previously infected devices sometime on or after December 6. We observed the KV-botnet operators begin to restructure, committing eight straight hours of activity on December 8, 2023, nearly ten hours of operations the following day on December 9, 2023, followed by one hour on December 11, 2023. During this four-day period, we observed the threat actor interact with over 3,000 unique IP addresses. Most of these IP addresses were identified as

NetGear ProSAFEs, Cisco RV320/325, Axis IP cameras, and DrayTek Vigor routers. The device breakdown of the 3,045 devices that received connections from the exploit server was as follows:

- NetGear ProSAFE: 2,158
- Cisco RV 320/325: 310
- Axis IP cameras: 29
- DrayTek Vigor: 17
- Undetermined: 531

During this surge, the actor displayed a clear preference in device type, as over 2,100 of the approximately 3,000 IP addresses were NetGear ProSAFEs. Their focus led us to search for the total number of these devices connected to the internet; we found the KV threat actor interacted with approximately 32.63% of the 6,613 NetGear ProSAFE devices that existed worldwide during that time, based upon available Censys data.

As documented in the malware analysis section of our initial report, the KV malware resides completely in-memory and therefore did not have a persistence mechanism. This means that by simply power cycling these devices, the malware is removed from the system and requires the actor to re-exploit the device in order to regain access.

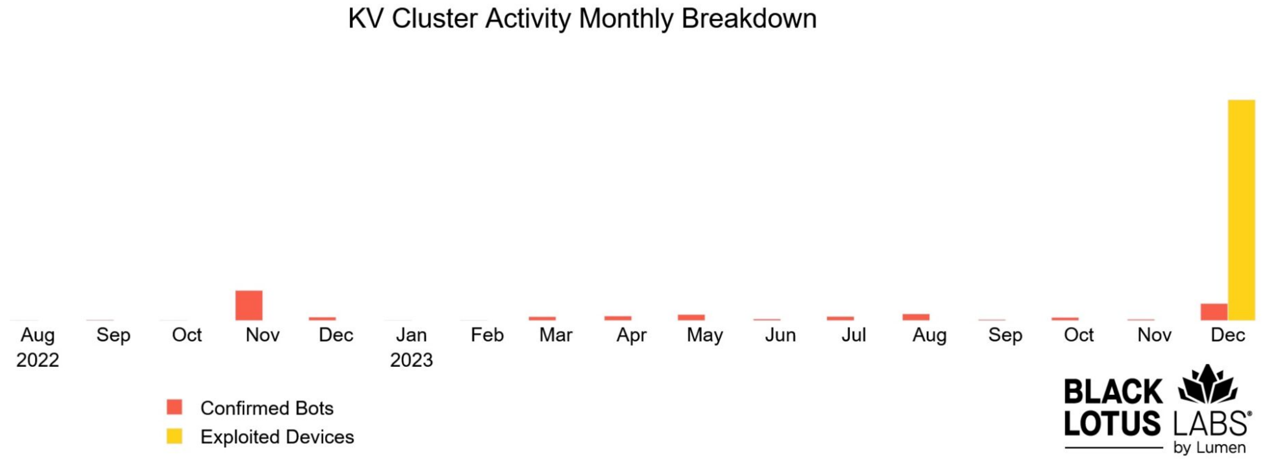

Figure 2: Showing the number of unique IP addresses receiving connections from the payload server during December 2023, compared to the number of known bots per month.

Throughout the KV lifecycle, the average number of exploited bots per month averaged just over 100. The massive surge in exploitation attempts from the payload server in early December 2023, suggests the threat actor was likely monitoring their victimized devices and noticed the sudden adverse action. As they detected their infrastructure going offline, the KV-botnet operators actively tried to re-exploit those devices to maintain operations. Analyzing historical Lumen telemetry, we found that 630 of the 3,045 total reinfected devices had interactions with the payload server over multiple days in December, indicating a net reinfection rate of 20.69% over this period.

Searching our historical telemetry led us to a secondary, or backup, set of servers that became operational on approximately December 5, 2023. We assess that these servers were active until at least January 3, 2024. At that time, Lumen took additional actions to null-route these IP addresses and impede their efforts to reinfect the SOHO devices. As noted in the initial KV-botnet report, we focused more of our attention on the “KV cluster” as it was more closely aligned with manual, targeted, high-value operations and tracking.

We carefully monitored this space over the month of January 2024 and have not detected any net new C2 servers being activated. The lack of an active C2 server combined with the FBI court-authorized action against KV-botnet and Lumen Technologies persistent null-routing of current and new KV cluster infrastructure provides a good indication that the KV activity cluster is no longer effectively active.

The Router Proxy “JDY Cluster”

The cluster designated “JDY” was primarily used to perform mass internet scanning, presumably for reconnaissance. Based on our telemetry, we suspect the FBI’s takedown effort was focused on the activities of the KV-cluster, as JDY bots had signs of life through the middle of January 2024. We assess that as a byproduct of the FBI activity, the threat actor’s resources were diverted away from rebuilding the JDY cluster, resulting in a 15-day lapse in operational router proxy server activity.

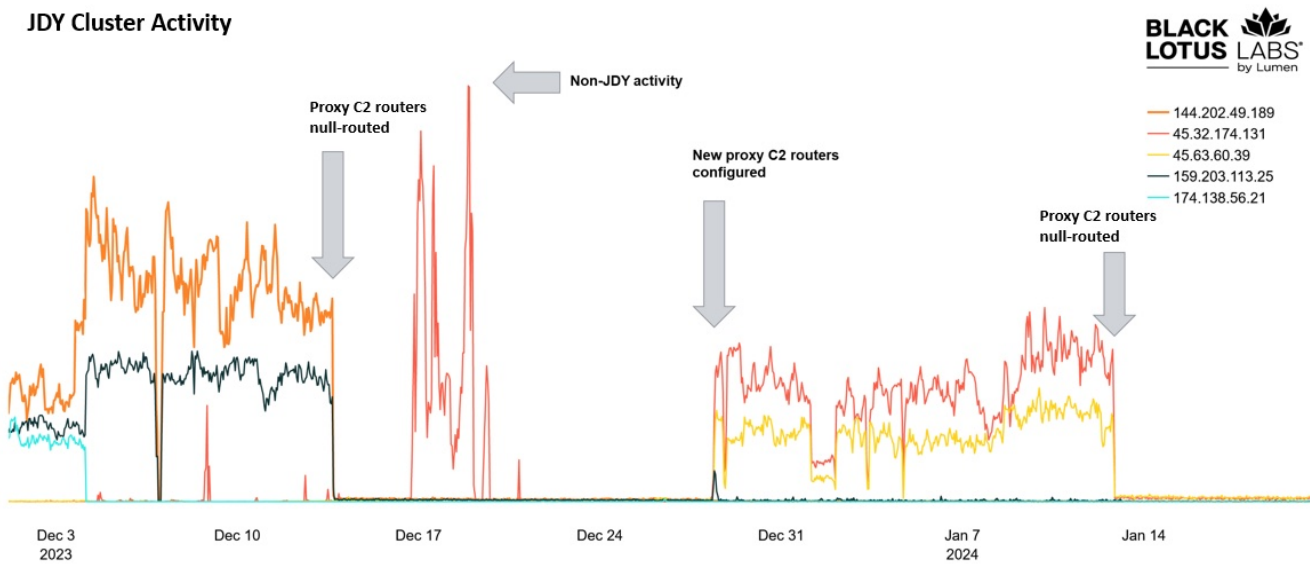

Figure 3: Showing a break in operations associated with the JDY activity cluster and a decline in bots once C2 communications were re-established.

The decline in the number of bots communicating with the router proxy server from December 2023 was significant. Originally hovering around 1,500 bots, the numbers fell to approximately 650 in mid-January 2024, a reduction of over 50%. In our original activity, Lumen Technologies null-routed the December router proxy servers on the 13th of that month; more recently we null-routed the newly established servers upon their discovery on January 12, 2024, to further hamper communications between the bots and their C2.

Public Emergence of the "x.sh" Cluster

In early January 2024, additional public reporting discussed a third activity cluster dubbed "x.sh." Black Lotus Labs telemetry indicates this activity cluster goes back to at least January 2023. Lumen acknowledges that the same exploit was used to compromise the JDY and x.sh Cisco routers, based upon artifacts that were discoverable via scan data. Furthermore, the x.sh cluster has a similar operational security measure as the KV and JDY clusters: the operators only host the payloads for a short window of time, typically an hour, presumably when they are exploiting new devices.

Black Lotus Labs has not been able to recover the malware samples associated with the x.sh cluster payload servers. And while the JDY, KV, and Fortinet clusters all shared some backend infrastructure, x.sh used a different set of infrastructure. Considering all factors, we assess with moderate confidence that x.sh is a separate activity cluster and distinct from the other three.

Conclusion

As with the original report, we assess that this trend of utilizing compromised firewalls and routers will continue to emerge as a core component of threat actor operations, both to enable access to high-profile victims and to establish covert infrastructure. There is a large supply of vastly out-of-date and generally considered end-of-life edge devices on the internet, no longer eligible to receive patches yet still performing well enough to stay in service for end users. Attackers will continue to target medium to high-bandwidth devices as a springboard in the geographic areas of their targets, given that users will be unlikely to notice an impact, or to have the necessary monitoring forensic tools to detect an infection.

We assess that KV-botnet has encountered significant resistance over the past several weeks. We believe that the main arm of the botnet, the KV cluster, has been rendered inert due to the action of U.S. law enforcement. We assess that the Fortinet activity had dissipated sometime in August of 2023. The JDY cluster has lost over half of its bots in the past month, but still remains operational. Finally, the signal associated with the x.sh cluster has been lost, likely due to public exposure.

In order to better visualize the data points that were highlighted throughout this report, we have created a timeline that encompasses some of the more prominent events between mid-November 2023 and January 2024.

Timeline

Date	Time	Activity
November 14, 2023	04:09:29 UTC	Threat actor swapped out the previously observed “BBC” x.509 certificate and replaced it with the “JDY” x.509 certificate
November 29, 2023	06:00 – 07:00 UTC, 12:00 – 13:00 UTC	Threat actor performed first wave of exploitation against Axis IP cameras; hitting approximately 36 IPs
November 30, 2023	11:00 – 12:00 UTC	Threat actor performed second wave of exploitation against Axis IP cameras; hitting approximately 232 IPs
December 5, 2023	08:09 UTC	New auxiliary call back server, 152.32.138[.]247, was observed performing its first interaction with a KV bot
December 5, 2023	14:00 – 15:00 UTC	Threat actor performed another wave of exploitation against NetGear ProSAFE devices; hitting approximately 171 IPs
December 6, 2023		First FBI warrant (#5432) signed authorizing takedown actions of KV-botnet
December 8, 2023	07:00 – 15:00 UTC	Threat actor performs 8 straight hours of operations; hitting approximately 2098 IPs
December 9, 2023	03:00 – 13:00 UTC	Threat actor performs 10 straight hours of operations; hitting approximately 3246 IPs
December 11, 2023	02:00 – 03:00 UTC	Threat actor performs 1 hour of operations; hitting approximately 270 IPs
December 11, 2023	14:45 UTC	New payload server 95.162.229[.]105 interacted with bot
December 12, 2023	17:51 UTC	Lumen null-routed KV cluster servers: 45.11.92[.]176, 193.36.119[.]48, 216.128.180[.]232.
December 13, 2023	06:50 UTC	Lumen null-routed three Proxy Router C2 & previously identified payload server; 144.202.49[.]189, 159.203.113[.]25 and 216.128.179[.]235.
December 13, 2023	17:00 UTC	Lumen released the public KV-botnet blog

January 3, 2024	15:10 UTC	Last observed beacon to the new 152.32.138[.]247 callback server
January 8, 2024	17:14 UTC	Lumen null-routed the payload server and callback server; 152.32.138[.]247, 45.159.209[.]228.
January 12, 2024	18:34 UTC	The router proxy IP addresses were null-routed; 45.63.60[.]39 & 45.32.174[.]131

Mitigations and Recommendations

Black Lotus Labs has added the IoCs from this campaign into the threat intelligence feed that fuels the Lumen Connected Security portfolio, and we continue to monitor for new infrastructure, targeting activity and expanding TTPs. In addition, we have null-routed traffic to the known points of infrastructure used by the KV-botnet.

We will continue to collaborate with the security research community to share findings related to this activity and ensure the public is informed. We encourage the community to monitor for and alert on these and any similar IoCs.

Further, to protect networks from compromises by Volt Typhoon and others who may leverage sophisticated obfuscation networks such as KV-botnet:

- Network defenders: 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.
- Consumers with SOHO routers: Users should follow best practices of regularly rebooting routers and installing security updates and patches. Users should leverage properly configured and updated EDR solutions on hosts and regularly update software consistent with vendor patches where applicable.

Analysis of the KV-botnet was performed by Danny Adamitis, Steve Rudd and Michael Horka. 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: 18,882

Black Lotus Labs

Author

Black Lotus Labs

The mission of Black Lotus Labs is to leverage our network visibility to help protect customers and keep the internet clean.

Trending Now

You may also like

Services not available everywhere. ©2022 Lumen Technologies. All Rights Reserved.