Derailing the Raptor Train

blog.lumen.com/derailing-the-raptor-train/

Black Lotus Labs Posted On September 18, 2024

0
35.1K Views

Executive Summary

In mid-2023, Black Lotus Labs began an investigation into compromised routers that led to the discovery of a large, multi-tiered botnet consisting of small office/home office (SOHO) and IoT devices that we assess is likely operated by the nation-state Chinese threat actors known as Flax Typhoon. We call this botnet "Raptor Train," and it has been over four years in the making.

At its peak in June 2023, the Raptor Train botnet consisted of over 60,000 actively compromised devices. Since that time, there have been more than 200,000 SOHO routers, NVR/DVR devices, network attached storage (NAS) servers, and IP cameras; all conscripted into the Raptor Train botnet, making it one of the largest Chinese state-sponsored IoT botnets discovered to-date. In fact, a command and control (C2) domain in the most recent campaign cracked both the Cloudflare Radar and Cisco Umbrella “top 1 million” popularity lists. Based on the recent scale of device exploitation, we suspect hundreds of thousands of devices have been entangled by this network since its formation in May 2020.

The botnet operators manage this large and varied network through a series of distributed payload and C2 servers, a centralized Node.js backend, and a cross-platform Electron application front-end that the actors have dubbed “Sparrow.” This is a robust, enterprise-grade control system used to manage upwards of 60 C2 servers and their infected nodes at any given time. This service enables an entire suite of activities, including scalable exploitation of bots, vulnerability and exploit management, remote management of C2 infrastructure, file uploads and downloads, remote command execution, and the ability to tailor IoT-based distributed denial of service (DDoS) attacks at-scale. The botnet operators can automate certain tasks for the C2 network and allow for the steady collection of logs and bot information to increase the operators’ situational awareness. Using an advanced control system frees up time for hands-on exploitation, streamlines the management process and allows more threat actors to contribute to operations.

While Black Lotus Labs has yet to see any DDoS attacks originating from Raptor Train, we suspect this is an ability the China-based operators preserve for future use. Black Lotus Labs has discovered activity from this network targeting U.S. and Taiwanese entities in the military, government, higher education, telecommunications, defense industrial base (DIB) and information technology (IT) sectors. In addition, possible exploitation attempts against Atlassian Confluence servers and Ivanti Connect Secure appliances have sprung from nodes associated with this botnet.

We will break down this large, complex botnet into two parts – this blog and a longer, downloadable report. Here we will walk through a high-level overview of the network architecture of Raptor Train, describe exploitation campaigns, add a brief analysis of the C2 controller software, and conclude with the potential operational use of this network, based on our visibility. For the malware analysis, extended details of each campaign and full scope of research into this four-year operation, please download the full Raptor Train report.

Lumen Technologies would like to commend the FBI and DOJ 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. In addition, we have null-routed traffic to the known points of infrastructure used by the Raptor Train operators including their distributed botnet management, C2, payload and exploitation infrastructure.

Technical Details

The Raptor Train botnet is a complex, multi-tiered network that has been evolving over the last four years. Black Lotus Labs has observed at least three tiers of activity, and several categories within each tier. During operations, bot tasks are initiated from Tier 3 “Sparrow” management nodes, which are then routed through the appropriate Tier 2 C2s and then sent to the bots themselves in Tier 1. Like the base of a pyramid, the first tier is the largest in size, while Tiers 2 and 3 form the control, exploitation and management segments. Each tier has varying lifecycles, some due to the nature and use of the physical device as with Tier 1, where bots last an average of 17 days. Most Tier 2 and Teir 3 nodes are procured Virtual Private Servers (VPSs) allowing them to have greater longevity averaging around 77 days. The Tier 2 VPSs are located throughout the world, while Tier 3 servers are largely based in Hong Kong or the PRC.

The primary implant seen on most of the Tier 1 nodes, which Black Lotus Labs calls “Nosedive”, is a custom variation of the Mirai implant that is supported on all major SOHO and IoT architectures (e.g. MIPS, ARM, SuperH, PowerPC, etc.). Nosedive implants are typically deployed from Tier 2 payload servers through a unique URL encoding scheme and domain injection method. Nosedive droppers use this method to request payloads for specific C2s by encoding the requested C2 domain and joining it with a unique “key” that identifies the bot and the target architecture of the compromised device (e.g. MIPS, ARM, etc.), which is then injected into the Nosedive implant payload that is deployed to the Tier 1 node. Once deployed, Nosedive runs in-memory only and allows the operators to execute commands, upload and download files, and run DDoS attacks on compromised devices.

All samples Black Lotus Labs found of Nosedive and its associated droppers were memory-resident only and deleted from disk. This, in addition to anti-forensics techniques employed on these devices including the obfuscation of running process names, compromising devices through a multi-stage infection chain, and killing remote management processes, makes detection and forensics much more difficult.

The breakdown of the Raptor Train network by tier is as follows:

- Tier 1
  - Compromised SOHO/IoT devices
- Tier 2
  - Exploitation servers
  - Payload servers
  - C2 servers

Tier 3

- Management nodes
- “Sparrow” nodes

Network Architecture

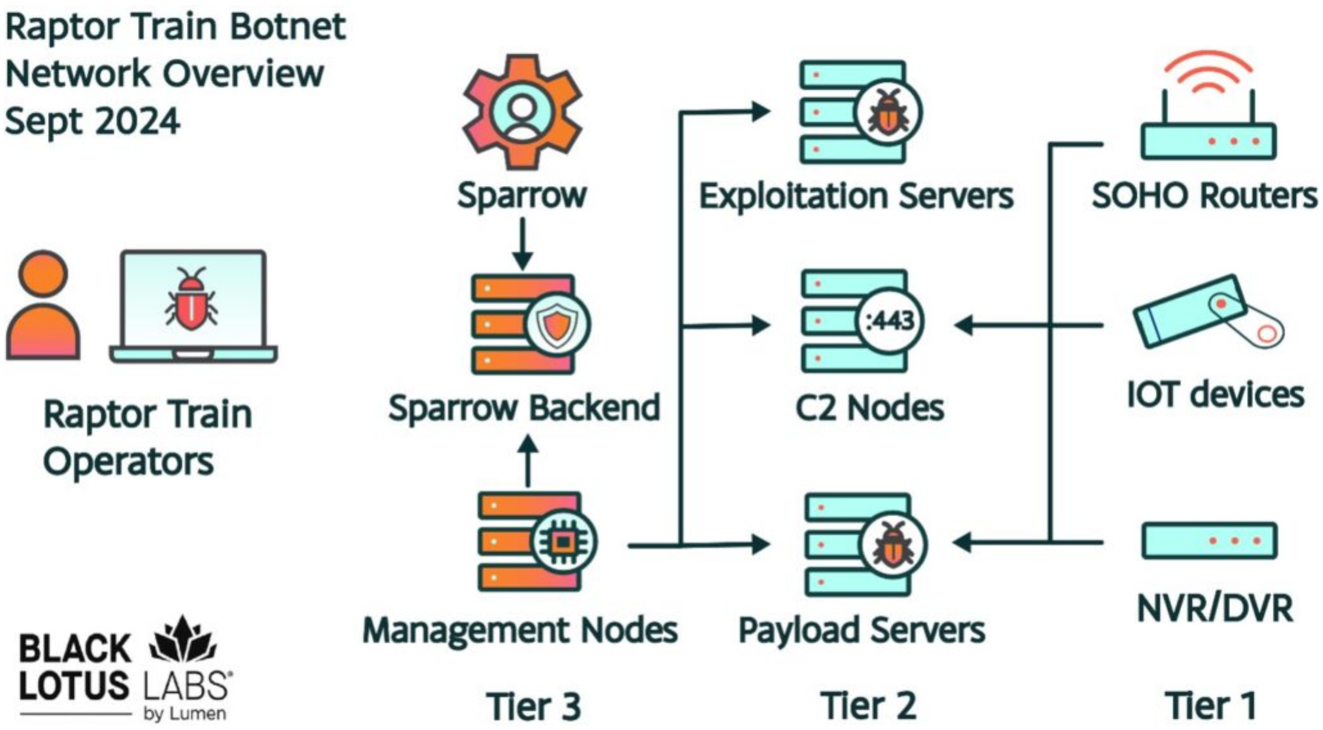


Figure 1: Overview of the Raptor Train network architecture and tiering structure.

Tier 1

This tier consists of the compromised SOHO and IoT devices, including modems, routers, IP cameras, NVR/DVR devices, and NAS devices. The operators are likely exploiting more than 20 different device types with both 0-day and n-day (known) vulnerabilities for inclusion as Tier 1 nodes. These include, but may not be limited to, the following:

Modems/Routers

ActionTec PK5000

ASUS RT-*/GT-*/ZenWifi

TP-LINK

DrayTek Vigor

Tenda Wireless

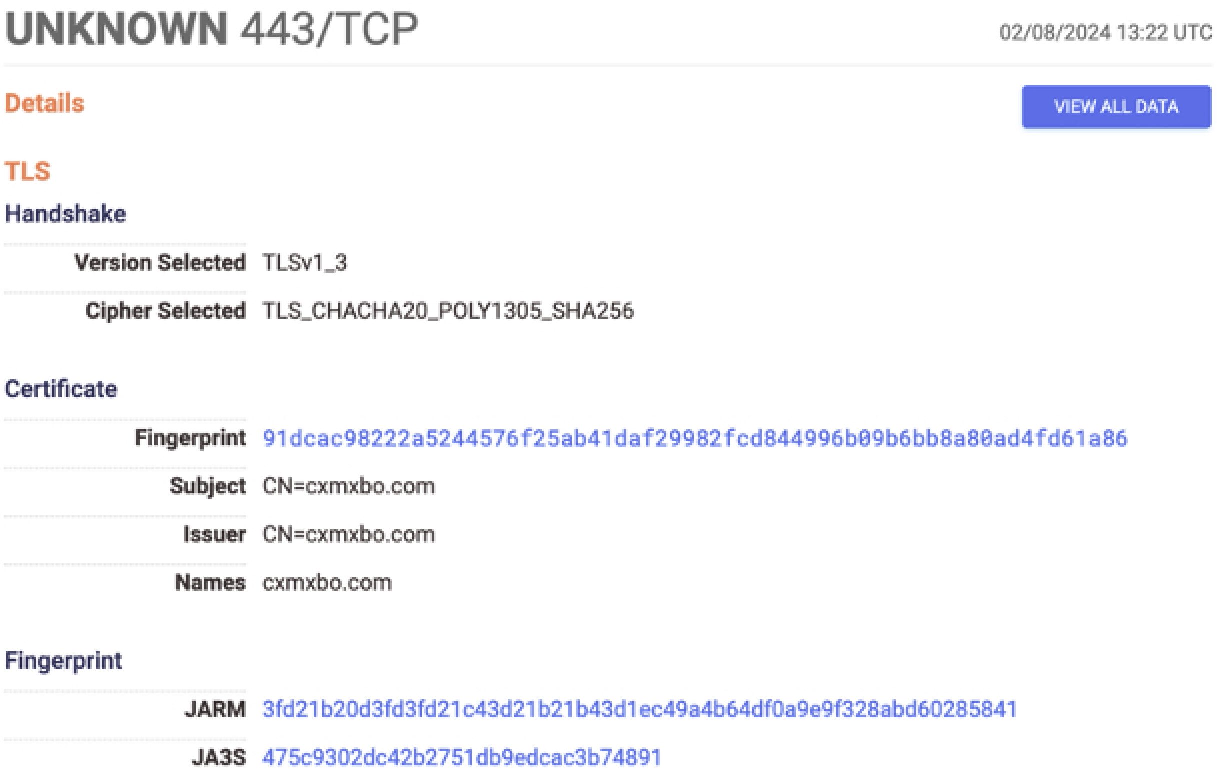
  - Ruijie
  - Zyxel USG*
  - Ruckus Wireless
  - VNPT iGate
  - Mikrotik
  - TOTOLINK
- IP Cameras
  - D-LINK DCS-*
  - Hikvision
  - Mobotix
  - NUUO
  - AXIS
  - Panasonic
- NVR/DVR
  - Shenzhen TVT NVRs/DVRs
- NAS
  - QNAP (TS Series)
  - Fujitsu
  - Synology
  - Zyxel

The number of active Tier 1 nodes is constantly fluctuating; tens of thousands of actively compromised devices check into the Tier 2 C2 servers at any given time. The average lifespan of an active Tier 1 node (compromised device) is approximately 17 days and most of the Nosedive implants do not have a method of persistence, which is a sign the operators are not concerned with the regular rotation of compromised devices. The massive scale of vulnerable devices on the internet allows the actors to forgo persistence mechanisms and regularly exploit new devices to meet operational needs.

Tier 2

This tier consists of procured, dedicated virtual servers and serves as the C2, exploitation and payload delivery framework to the Tier 1 nodes. The payload servers can be further broken down into two types: first stage and second stage. The more generic “first-stage” payload servers are longer-running and provide the payload retrieval capability for most of the compromised Tier 1 nodes. The “second stage” servers often host their payloads on high, random ephemeral ports (e.g. 32123, 38525, etc.) and are used in multi-stage droppers. We have observed these “second stage” payload servers in more targeted efforts against specific device types, possibly to better obfuscate 0-day vulnerabilities in the target devices.

The C2 servers in Tier 2 receive the callbacks from compromised devices in Tier 1 over port 443. A signature feature of the Tier 2 C2 servers is the exposed C2 port, 443, with a TLS certificate displaying a random alphanumeric domain in the subject and issuer fields, as seen below:



UNKNOWN 443/TCP

02/08/2024 13:22 UTC

Details

TLS

Handshake

Version Selected TLSv1_3

Cipher Selected TLS_CHACHA20_POLY1305_SHA256

Certificate

Fingerprint 91dcac98222a5244576f25ab41daf29982fcd844996b09b6bb8a80ad4fd61a86

Subject CN=cxmxbo.com

Issuer CN=cxmxbo.com

Names cxmxbo.com

Fingerprint

JARM 3fd21b20d3fd3fd21c43d21b21b43d1ec49a4b64df0a9e9f328abd60285841

JA3S 475c9302dc42b2751db9edcac3b74891

Figure 2: Censys screenshot taken on February 08, 2024, showing an example of a TLS certificate on port 443 of a Tier 2 C2 node, with a random alphanumeric domain name, cxmxbo.com, as the subject and issuer DN.

The Tier 2 C2 nodes are most often managed by Tier 3 management nodes over port 34125, which has its own unique TLS certificate. The growth of Tier 2 C2 nodes has been significant over the past four years. For example, Black Lotus Labs tracked approximately 1-5 C2 nodes between 2020 and 2022, 11 C2 nodes in mid-2023, 30 C2 nodes between February 2024 and March 2024, and upwards of 60 C2 nodes between June 2024 and August 2024. Each time we identified a growth in C2 nodes, we observed an increase in Tier 1 nodes (bots).

Tier 3

Tier 3 is the management tier of the botnet. The botnet operators can manually manage Tier 2 nodes via SSH over port 22 from the Tier 3 nodes and, for the Tier 2 C2 nodes specifically, automatically via TLS connections over port 34125. These management nodes relay commands and collect data for the Sparrow controller.

For manual Tier 2 management, the Tier 3 nodes were observed with sustained sessions to Tier 2 nodes over SSH port 22 exclusively during Chinese working hours, Monday through Friday:

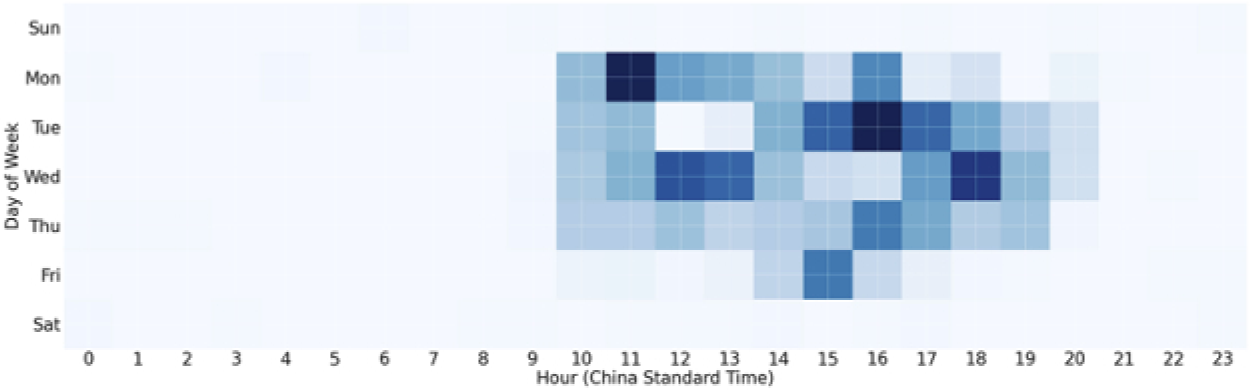


Figure 3: Heatmap showing days and times of Tier 3 node SSH sessions over port 22 to Tier 2 payload and C2 servers aligned with Chinese working hours, Monday through Friday (China Standard Time).

In addition, Tier 3 nodes were found with consistent, recurring connections over TLS over port 34125. These connections are part of the Sparrow C2 controller process where the Tier 3 management nodes are regularly collecting logs and bot information and issuing commands to the C2s that originate from the Sparrow front-end controller. In contrast to the manual management over port 22, the Sparrow connections over port 34125 are more regular and consistent at all hours of the day, every day of the week:

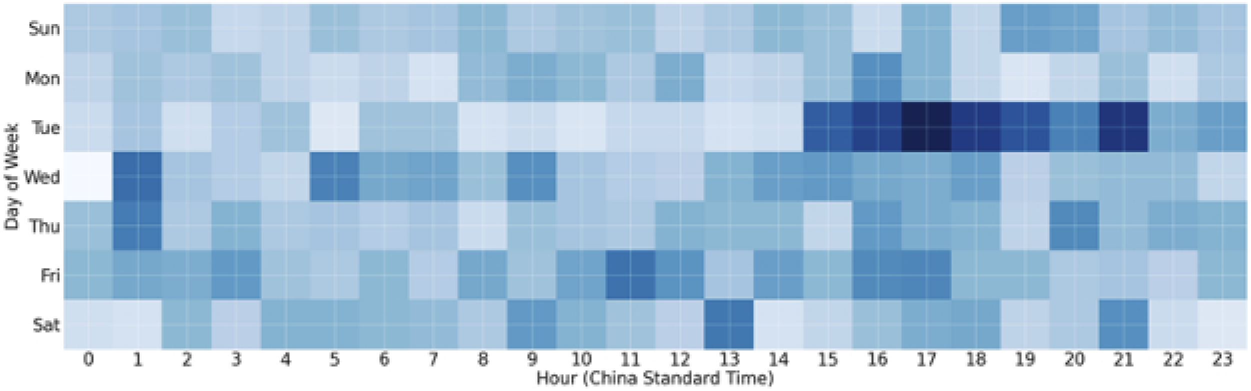


Figure 4: Heatmap showing days and times of Tier 3 node TLS sessions over port 34125 to Tier 2 C2 servers aligned with all hours of the day (China Standard Time).

The Sparrow controller falls into another set of Tier 3 management nodes that we call “Sparrow” nodes. The Sparrow nodes provide the front-end (web interface), backend (database) and auxiliary functions (e.g. payload/exploit generator) needed for management and continued growth of the expansive Raptor Train network.

The primary Sparrow web interface is named “节点综合控制工具v1.0.7” which translates to “Node Comprehensive Control Tool v1.0.7” (NCCT). The botnet operators named this NCCT management application “Sparrow,” and it is a full-featured, scalable botnet controller in the form of a cross-platform Electron application. Sparrow provides a permission-based management system enabling a team of botnet operators to execute commands, upload or download files, collect data on or run DDoS attacks on compromised devices. The operators can also manage and control a broad set of exploits, vulnerabilities, distributed C2 servers, and infected nodes from a central platform.

Figure 5: Screenshot of the interactive Sparrow "Node Comprehensive Control Tool" (NCCT).

Black Lotus Labs identified another Tier 3 Sparrow management node we call "Condor." Condor is a web service built to enable an array of vulnerability exploitation elements of the botnet including payload generation, exploit attempts, verification, and logging. Condor assists in the discovery of new vulnerabilities (e.g. 0-days), verifying active payloads and testing exploits.

More details on the multi-tiered network architecture, malware analysis (including Nosedive and its various droppers) and management infrastructure capabilities (including Sparrow and Condor) can be found in the full Raptor Train report here.

Campaign Overview

The Raptor Train botnet has been constantly evolving since mid-2020. The initial campaign, Crossbill, began with a single C2 callback and 4 subdomains. By the middle of the botnet's lifecycle, the naming scheme of the C2 domains had shifted to include random alphanumeric subdomains, which led to a diversified and expanded Tier 2 infrastructure and the introduction of a unique URL encoding scheme. While some of the naming patterns and even certificates were repeated, each campaign showed distinctions in size, targeting, or rotating C2 root domains. Black Lotus Labs has detected several bands of effort since Raptor Train's inception over four years ago, and has divided them into four campaigns: Crossbill, Finch, Canary and Oriole.

Crossbill Campaign (May 2020 to April 2022)

The earliest identified campaign began in May 2020. During this campaign, the operators deployed the very first iteration of the Mirai-based, customized implant we call Nosedive on compromised devices. Initially, the root domain k3121.com was used as the sole C2 domain, but by mid-2021, the operators began using encoded random alphanumeric C2 subdomains (e.g. wsxe.k3121.com, dfgh.k3121.com, etc.).

Finch Campaign (July 2022 to June 2023)

The Finch campaign began in July 2022 and is signified by the root domain b2047.com. Despite the campaign not starting until July 2022, the b2047.com domain was first registered in September 2019 and resolved to parked Alibaba Cloud IP space. It is possible the preparation phase of the Raptor Train botnet was already underway by late 2019.

The C2 subdomains of b2047.com followed a similar format to those in the Crossbill campaign in 2020 (e.g. abpi.b2047.com, oklm.b2047.com, etc.). However, in June 2023 the C2 subdomain length expanded to a longer pattern (e.g. amushuvfikjas.b2047.com, acgtjkiufde.b2047.com, etc.) and the Finch campaign ramped up. By mid-June 2023, at least 10,000 distinct devices were infected.

Canary Campaign (May 2023 to August 2023)

Starting in late May 2023, Raptor Train operators began a more tailored campaign in terms of types of devices in Tier 1, heavily targeting ActionTec PK5000 modems, Hikvision IP cameras, Shenzhen TVT NVRs and ASUS RT-* and GT-* routers (among others). While this campaign did continue the use of the b2047.com C2 domain (and associated subdomains), it was the first time Black Lotus Labs observed the use of multi-stage droppers and some degree of in-memory “persistence” for the Nosedive implant. There was also a notable increase, compared to earlier campaigns, in the number of Tier 2 C2 servers (from approximately 1-3 active to over 10 active) and in Tier 1 nodes (from approximately 10,000 to over 60,000) during the Canary campaign.

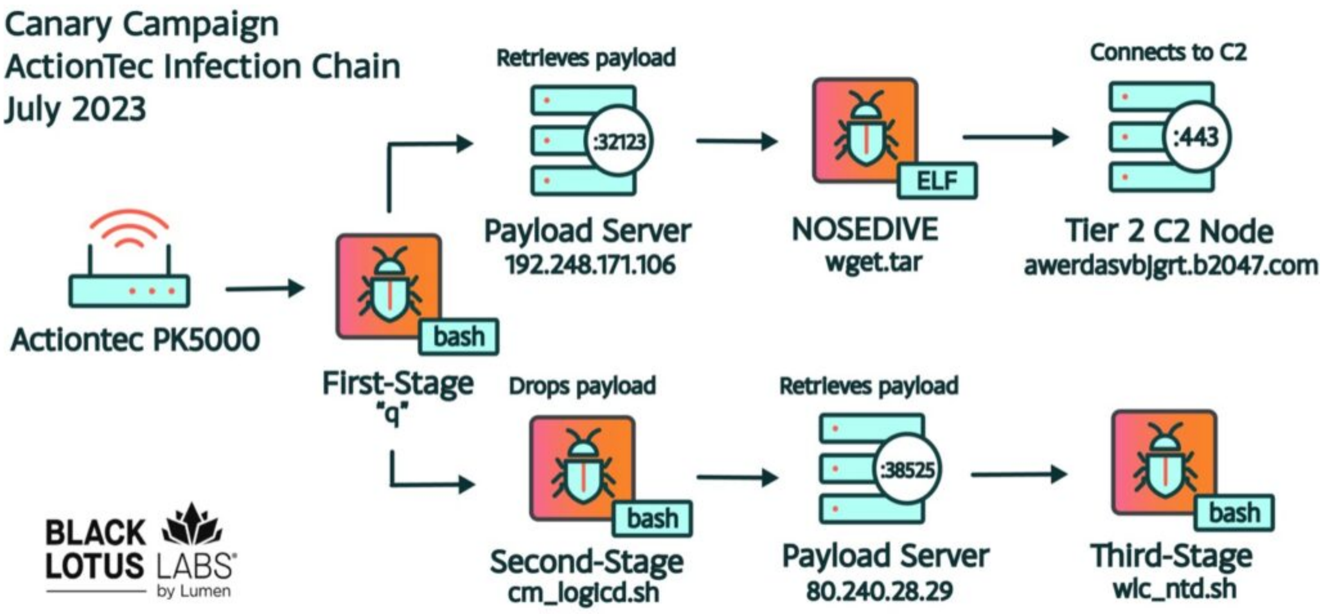


Figure 6: Overview of a Canary campaign infection chain showing multi-stage droppers/loaders and Nosedive samples, as well as second and third-stage bash scripts, as seen on an infected Actiontec PK5000 device.

Oriole Campaign (June 2023 to Present)

Beginning in June 2023, another large exploitation campaign kicked off, sharing a few months’ overlap with the more tailored Canary campaign. The Oriole campaign is signified primarily by the root domain w8510.com and associated C2 subdomains (e.g. qacassdfawemp.w8510.com, dftiscasdwe.w8510.com, etc.).

Between April 2024 and August 2024, Black Lotus Labs saw an expansion of exploited device types including VNPT iGate routers, AXIS IP cameras and compromised NAS devices such as QNAP NAS, Zyxel NAS, Fujitsu NAS and Synology NAS. By August 2024, Raptor Train maintained an *average* of approximately 30,000 compromised devices in Tier 1, which is a testament to its size and scale given how quickly the devices power cycle and rotate (as mentioned earlier, cycling on average every 17 days).

The w8510.com C2 domain for this campaign became so prominent in compromised IoT devices that, in June 2024, it was included in the Cisco Umbrella domain rankings, and by August 2024 it was included in Cloudflare Radar's top 1 million domains, as it became one of the top million most resolved domains on the internet. This is a concerning feat because domains reported in these popularity lists often circumvent security tools via domain whitelisting, enabling the botnet operators to maintain access and further avoid detection.

These campaigns highlight the evolving tactics, techniques, and procedures (TTPs) of the Raptor Train botnet operators, as well as the resources that continuously feed into the development, maintenance and growth of the botnet.

Attribution and Operational Use

Based on management and operational timeframes favored by Raptor Train, the targeting of sectors aligned with Chinese interests, Chinese language use, and other TTP overlaps; Black Lotus Labs assesses the botnet operators of Raptor Train are likely the nation-state Chinese threat actors known as Flax Typhoon.

Analysis of Tier 3 management node sessions in which the nodes are connecting to Tier 2 C2 servers for management activity shows almost exclusively Chinese working hours, Monday through Friday:

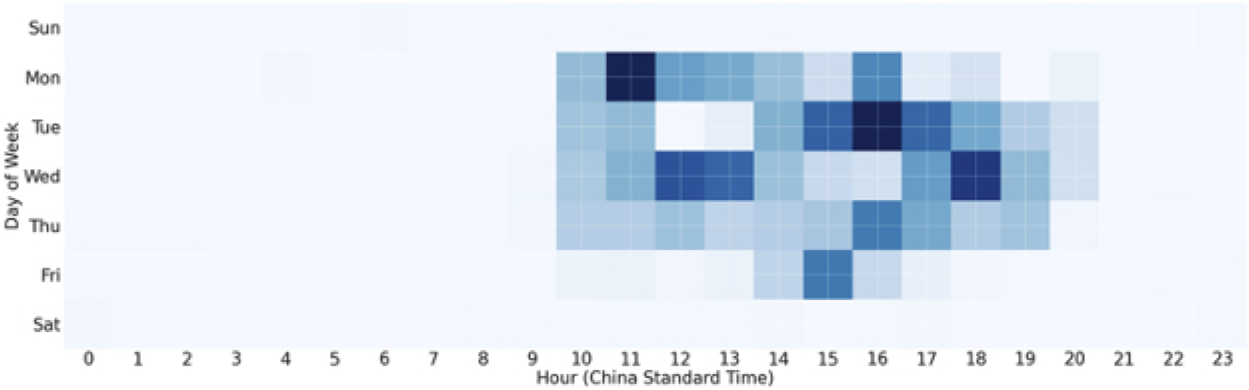


Figure 7: Heatmap showing days and times of Tier 3 node SSH sessions over port 22 to Tier 2 payload and C2 servers aligned with China Standard Time (as shown in Fig. 3).

Black Lotus Labs uncovered targeting activities through this network that appeared to be concentrated on the military, government, higher education, telecommunications, defense industrial base (DIB), and information technology (IT) sectors in the U.S. and Taiwan. For instance, in late December 2023, the botnet operators conducted extensive scanning efforts targeting the U.S. military, U.S. government, IT providers, and DIBs. There was also widespread, global targeting, such as a government agency in Kazakhstan, along with more targeted scanning and likely exploitation attempts against vulnerable software including Atlassian Confluence servers and Ivanti Connect Secure appliances (likely via CVE-2024-21887) in the same sectors.

Conclusion

Black Lotus Labs' investigation into the Raptor Train botnet has revealed a highly sophisticated and large-scale operation likely managed by the Chinese nation-state threat actors known as Flax Typhoon. The botnet, which has been active for over four years, has compromised hundreds of thousands of SOHO devices making it one of the largest Chinese state-sponsored IoT botnets seen to date. The botnet operators manage this extensive network with a custom-built, cross-platform application through a multi-tiered distributed payload and C2 architecture that allows them to manage hundreds of thousands of devices worldwide.

This botnet has targeted entities in the U.S. and Taiwan across various sectors, including military, government, higher education, telecommunications, defense industrial base, and IT. The investigation has yielded insights into the botnet's network architecture, exploitation campaigns, malware components, and operational use, illuminating the evolving tactics and techniques employed by the threat actors. A major concern of the Raptor Train botnet is the DDoS capability that we have not yet observed actively deployed, but we suspect is being maintained for future use.

Our findings underscore the importance of continued vigilance and collaboration among cybersecurity professionals to detect, analyze, and mitigate such sophisticated threats. Black Lotus Labs remains committed to monitoring and disrupting the activities of the Raptor Train botnet and other similar threats to ensure the security and integrity of global digital infrastructure.

To protect their networks from compromises by advanced threat actors and others who may leverage sophisticated networks such as Raptor Train:

> 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 use properly configured and updated EDR solutions on hosts and regularly update software consistent with vendor patches where applicable.

All users of networking equipment: Remain mindful of devices at or near “end-of-life” and aging out of vendor support. So-called “EoL” devices are an attack surface that draws the attention of an ever-growing field of attackers.

The details above are a summarized version of the full Raptor Train report. You can download the full Raptor Train report to dive deeper into the network architecture, malware analysis, exploitation campaigns, targeting and attribution of this expansive botnet. We have added the indicators of compromise (IoCs) from this campaign into the threat intelligence feed that fuels the Lumen Connected Security portfolio and are blocking all traffic to or from the known infrastructure of this botnet.

Analysis of the Raptor Train botnet was performed by Michael Horka and Steve Rudd. Technical editing by Ryan English and Danny Adamitis.

For additional IoCs associated with this campaign, please download the full Raptor Train report or 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: 35,136