"Checking all the Boxes"
LapDogs, The New ORB in Town

Executive Summary

SecurityScorecard's STRIKE research team has identified a new suspected China-Nexus network of Operational Relay Boxes (ORB) called "LapDogs" targeting primarily Linux-based Small Office/Home Office (SOHO) devices around the globe. The LapDogs network has a high concentration of victims across the United States and Southeast Asia, and is slowly but steadily growing in size.

LapDogs employs a custom backdoor we named "ShortLeash," which establishes a foothold on compromised devices and connects them within the network. ShortLeash generates unique, self-signed TLS certificates with spoofed metadata for each node.

Our analysis traces these certificates to over 1,000 actively infected nodes globally, revealing geographical targeting patterns indicative of structured tasking. ShortLeash enables unnoticed operation with high-level privileges, creating backups for persistence. Forensic evidence, including Mandarin developer notes within the startup script, tools, techniques, and procedures (TTPs), and victimology supports attribution to China-Nexus Advanced Persistent Threats (APTs) and similar ORBs. The research further identifies targeted operations based on certificate issuance dates and port assignments, which enables us to pinpoint distinct intrusion sets with geographical clusters.

A similar ORB, "PolarEdge," was found to share some infrastructure characteristics but differs in TTPs and certificate management.

Victimology analysis reveals affected ISPs, hardware vendors, and specific organizations in several sectors, including IT, networking, real estate, and media. SecurityScorecard STRIKE assesses LapDogs to be a gradually growing, methodically operated China-Nexus ORB with prolonged intrusion operations, distinct from opportunistic botnets.

Key Takeaways

- Over 1,000 actively infected nodes

- Targets are highly localized in the United States and Southeast Asia, particularly Japan, South Korea, Hong Kong, and Taiwan

- Victims in real estate, IT, networking, and media

- A custom backdoor named "ShortLeash," which establishes a foothold on compromised devices and enables the hackers to act covertly

- Small Office/Home Office (SOHO) devices are mainly targeted

- Campaign growth is deliberate, beginning in September 2023 and expanding with methodical tasking

- LapDogs shares commonalities with some prolific China-Nexus ORB networks, most notably PolarEdge, while conclusively standing out as an independent ORB

Table of Contents

Background

ORB Networks: An emerging threat

Before we dive deeper into the details and the inner workings of LapDogs, we'd like to provide a baseline understanding of Operational Relay Boxes (ORB) Networks, which will be instrumental to understanding our findings.

Research into ORB Networks first emerged in 2020, showcasing threat actors that have used—and often shared—ORB Networks to conduct covert operations. ORB Networks are made up of Virtual Private Servers (VPSs) and a series of compromised devices, such as Internet of Things (IoT) devices or routers, which operators use in concert to conduct espionage.

Hackers that use ORB Networks use the various devices as their proxies and rely on them for obfuscation. In essence, bad actors can maintain plausible deniability by using ORB Networks (see Google's Mandiant blog on the historical development of ORBs as a threat vector **here**).

China-Nexus threat actors are increasingly using ORB Networks, as demonstrated by the rising numbers of research teams uncovering ORB Networks and intrusion operations traced back to them (one recent example is SentinelLABS' **report** on the PurpleHaze activity cluster). The rise of ORB Networks as a main TTP for China-nexus APTs poses a significant challenge to traditional security best-practices by eroding the importance of Indicators of Compromise (IOC) tracking, due to the sheer number of nodes and the rapid pace at which they change.

While commonly compared with (or mistaken for) Botnets—which leverage a series of compromised and remotely-controlled devices—ORB Networks tend to be used more covertly and their functionalities and capabilities usually emphasize espionage-oriented campaigns. While both ORBs and Botnets commonly consist of a large set of compromised, legitimate internet-facing devices or virtual services, ORB Networks are more like swiss army knives, and can contribute to any stage of the intrusion lifecycle, from reconnaissance, anonymized actor browsing, and netflow collection to port and vulnerability scanning, initiating intrusion cycles by reconfiguring nodes into staging or even C2 servers, and relaying exfiltrated data up the stream.

While ORBs are certainly capable of performing "noisy" activities such as Distributed Denial-of-Service (DDoS) attacks or Brute Force attacks, they rarely ever do so. All the while, legitimate internet traffic continues to traverse the nodes, which further obfuscates malicious activities by drowning them out in the noise of benign traffic.

Initiating the research

SecurityScorecard's STRIKE team conducted an analysis of a series of reports concerning a prolonged espionage campaign targeting multiple organizations in Taiwan over the span of at least two years. One such report is Cisco Talos' blog regarding an unidentified threat actor, designated as UAT-5918, which was targeting critical infrastructure in Taiwan (see Talos report **here**).

The report describes a threat actor that achieves initial access by exploiting unpatched vulnerabilities in internet-exposed web and application servers, and continues to employ various open-source tools commonly associated with China-Nexus threat actors. Among the tools listed in the IOC section is the PE file svchost.exe (SHA256: 02ab315e4e3cf71c1632c91d4914c21b9f6e0b9aa0263f2400d6381aab759a61).

The aforementioned PE was available on the VirusTotal platform. Sandbox data collected on the sample, recorded attempts to establish encrypted communication with a hardcoded domain at www[.]northumbra[.]com, supposedly its C2 server, via numerous HTTPS POST requests with various added parameters. Around the original report's publication time, this domain was hosted on the IP address, 103.106.230[.]31, located geographically in Taiwan.



The IP address has since transitioned to host another subdomain under the same domain: ns[.]northumbra[.]com, thus implicating the entire domain of northumbria[.]com as potentially actor-controlled infrastructure. At that point in time, IP 103.106.230[.]31 had also presented a distinct, self-signed TLS certificate that later proved instrumental in our identification of the entire ORB network.

TLS Certificate based hunting

We investigated the TLS certificate hosted on IP 103.106.230[.]31 and found it to be captured by netflow sniffing modules of two different sandboxes on the VirusTotal platform (thumbprint:7267c503291cd69efe109a32f5ef090f73268353). This finding revealed some eye-catching metadata, presented as signed by the City of Los Angeles Police Department (LAPD), which indicates the hackers are potentially attempting to masquerade as a legitimate LAPD network device. It is based on this finding that we have decided to dub this ORB Network as "LapDogs."

We also observed the certificate being used to establish a TLS session with IP 103.106.230[.]31 as the hosting IP for the hardcoded C2 domain www[.]northumbra[.]com, as it was captured in VirusTotal's Dynamic analysis sandboxes. This further implicates the certificate as a crucial piece of this intrusion set puzzle, since it is directly connected to the malicious service running on the server side.
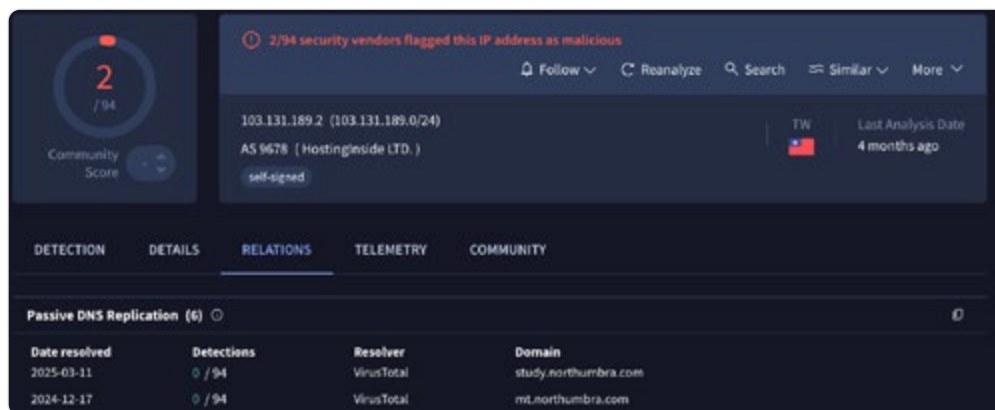
After analyzing scan data on VirusTotal, we found that this specific certificate is unique to this IP alone, setting it apart from recycled certificates commonly found in use by threat actors over various campaigns and tools. However, certificates with similar metadata (albeit different serial numbers) appeared on other subdomains under northumbra[.]com, and all of which were on IPs local to Taiwan.

One said IP, 103.131.189[.]2, uses a certificate with matching issuer and subject data, but with a different thumbprint (c2445738f130062559a758ad5cad85efbdab2417) and different validity and expiration dates. SecurityScorecard assesses with a high level of confidence that this indicates one threat actor is likely behind this set of domain and subdomains, part of which involves crafting self-signed certificates. Certificates found with similar metadata should be examined in an attempt to trace them back to this threat actor and infrastructure under its control.

In addition to the shared certificate metadata, the two IPs showed a similar JARM fingerprint (3fd3fd16d3fd3fd22c3fd3fd3fd3fdf20014c17cd0943e6d9e2fb9cd59862b) potentially indicating similarities in network configuration of the running services at the specific ports presenting the certificates. SecurityScorecard's STRIKE threat intelligence team hunted for the JARM fingerprint and the certificate metadata on open source tools as well as SecurityScorecard's proprietary scanners, enabling us to identify over 1,000 actively infected nodes around the globe. These effectively form the ORB Network.

From here, the ORB Network has been used to facilitate intrusion operations, demonstrated by the unfolding campaigns against critical infrastructure in Taiwan. And we have reason to believe the operators are running a highly targeted operation: Unlike a Botnet, which would compromise a large sweep of devices around the globe without much concern to their location, we observe clear preferences for five specific locations around the globe, which we detail further in this report.

ShortLeash: The LapDogs backdoor

The startup Bash script

Using the aforementioned network indicators of compromise, and with assistance from the threat intelligence team of an involved third party, STRIKE team was able to recover and investigate an a malicious payload and a startup Bash script to execute it. This startup script came coupled (naturally) with the Linux version of ShortLeash. After a static analysis of the payload we were able to determine that this sample and the sample originally discovered in the activity targeting critical infrastructure in Taiwan (as also mentioned by Cisco Talos' report) are indeed two variants of the same malware. The accompanying Bash script is very straightforward in its function:

- The script begins by assessing the privileges of the local user, insisting on being a root level user to run the script.

- It then checks whether the operating system is Ubuntu or CentOS, which enables it to target the relevant folder in the directory based on each architecture - /etc/systemd/system/ in Ubuntu and /lib/systemd/system/ in CentOS.

- If the operating system does not match either, the script will print a message in Mandarin, which is roughly translated to "Unknown System."

- Immediately after defining the OS, the script will create a backup of the existing malicious .service file within the same directory, naming the new one ""ff-agent-pi.service" and the backup ""ff-agent-pi.service_bak."

- This service is then interpreted by the system daemon.

- It is enabled to run in the background, with root level privileges and to be reloaded on a reboot, ensuring persistence and startup survivability.

The core payload

The payload has embedded an encrypted configuration. It is compressed with a UCL-looking compression algorithm and then encrypted in two layers. The decryption is the same for both layers, but the decryption key is different.

```
id __fastcall decrypt(BYTE *ciphertext, __int64 size, char ke

__int64 i; // rdx01
BYTE ciphertext_byte; // al@2

for ( i = size - 1; i != -1; --i )
{
  ciphertext_byte = ciphertext[i] - key;
  ciphertext[i] = ciphertext_byte;
  if ( i )
    ciphertext[i] = ciphertext_byte - ciphertext[i - 1];
}
```

- The first decryption layer uses the last byte as the decryption key, while the second decryption layer uses a key that is computed by adding the bytes of a buffer composed of 20 bytes.

- The second decryption layer doesn't decrypt the entire content resulting from the first decryption layer, but only the amount specified in the last two bytes of the content resulting from the first decryption layer.

The plaintext resulting after both decryption layers consists of:

- DWORD CRC32 value of the compressed content

- DWORD size of the decompressed content

- DWORD CRC32 value of the decompressed content

Compressed content

The decrypted and decompressed configuration contains, among other things, two certificates, two private keys, and a URL. The following is an example of a decrypted configuration:

It runs a server on the infected system and simulates Nginx responses:

```
date_format      db '%a, %d %b %Y %H:%M:%S GMT',0
                                          ; DATA XREF: get_date_header+44↑o
aDate            db 'Date',0             ; DATA XREF: get_date_header+78↑o
aNginx           db 'nginx',0            ; DATA XREF: get_server_header+2↑o
aServer          db 'Server',0           ; DATA XREF: get_server_header+23↑o
```

When contacting the C2, it randomly chooses the query parameter among a list of hardcoded words:

```
url_params       dq offset asc_4B6741+21h
                                          ; DATA XREF:
                                          ; "id"
                 dq offset asc_4BCF4F+25h ; "value"
                 dq offset asc_4BE3B2+6   ; "name"
                 dq offset asc_4B717A     ; "where"
                 dq offset asc_4B7180     ; "which"
                 dq offset asc_4BB6A1+38h ; "key"
                 dq offset asc_4B7186     ; "word"
                 dq 0
```

These preliminary findings, which we gained from analyzing the ShortLeash Backdoor, enabled us to assess the functionality of it as the core connective tissue that holds the LapDogs ORB Network together. More research is required to further understand the capabilities and embedded mechanisms of this payload, which we will continue to analyze and will report on in the future.

LapDogs ORB Profile

As we collated the different devices operating as nodes within this network, we identified certain commonalities in the data, enabling us to paint a more cohesive picture as to the unique profile of the network, from targeted devices to victims and vulnerabilities. The following are the most prominent of these commonalities that enabled us to narrow down the profile of victim devices, and therefore information about the malicious actors behind the ORB operation.

Focus on Linux-based SOHO Devices

While our research found separate samples of ShortLeash aimed for Linux and Microsoft Windows based systems, the vast majority of devices we were able to observe in the network are Linux-based, Small Office/ Home Office (SOHO) routers. This type of compromised device appeared more than any other device type in the network.

Other examples of compromised devices/nodes in the ORB Network include, but are not limited to, various types of IP cameras, smart IoT devices and virtual servers operating on different versions of Linux or Windows. In cases where the operating system was not explicitly stated in the metadata, we were, to some extent, able to infer the operating system from running services, device vendor information, and model data.

The small minority of Microsoft Windows-based systems that our scan was able to recover were also running additional Linux-based services in conjunction with Windows, such as OpenSSH or mini_httpd for Linux (a small HTTP server), thus leaving an inconclusive ruling as to the nature of these unique incidents. Overall, LapDogs operators appear to favor targeting Linux-based systems in their operations.

Country-based targeting

Through Geolocating IPs within the network, we found that although the LapDogs operator is conducting their operation around the globe, it is highly localized to the United States and Southeast Asian countries, with some exceptions.

The network targeted numerous victims in Japan, South Korea, Taiwan, and Hong Kong in particular. Altogether these five targets—United States, Japan, South Korea, Taiwan, and Hong Kong—comprise nearly 90% of the entire network.

Top 5 Countries

Country	Value
United States	352
Japan	256
South Korea	226
Taiwan	80
Hong Kong	37
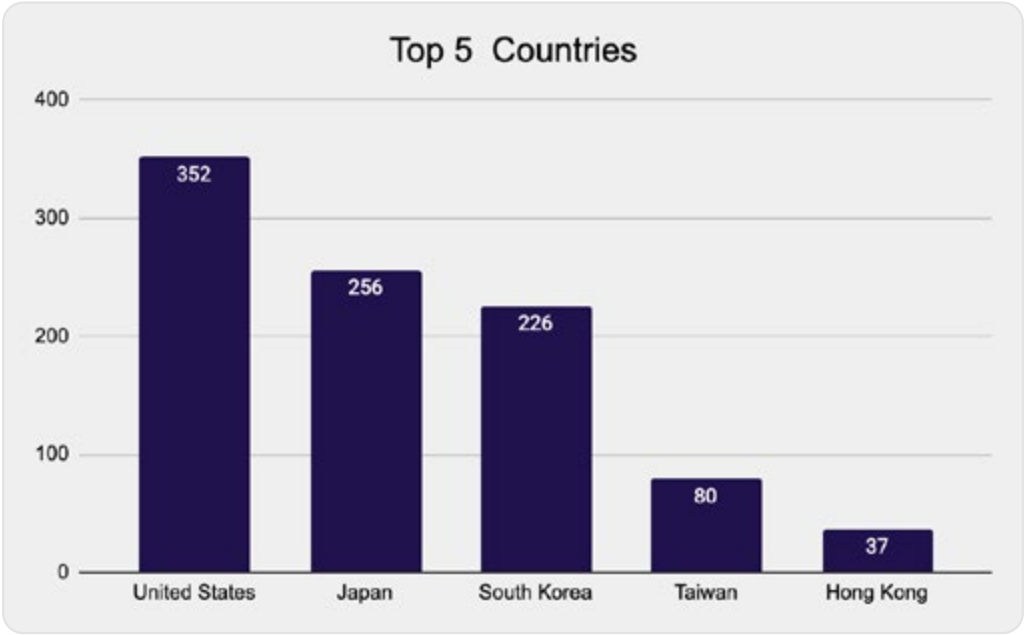
High vendor specialization

We assess that nearly 55% (or 587) of all observed compromised devices are Ruckus Wireless access point devices based on running services and TLS certificates configured for each device. While they share common risk factors with other vendors' embedded devices, the sheer numbers might indicate initial focus on this vendor or higher success rate with it.

Another device brand that received particular attention from LapDogs is the Buffalo Technology AirStation wireless routers, with 107 infected devices. Each of these uses an IP located in Japan, with most located in Tokyo.

Lacking device management

Our proprietary CVE scanning capabilities at SecurityScorecard indicate that a large proportion of the IPs within the network are specifically vulnerable to CVE-2015-1548 and CVE-2017-17663, two vulnerabilities associated with ACME mini_httpd of older versions.

Among nearly all compromised nodes within LapDogs, some version of a lightweight web server is present (such as lighttpd or mini_httpd), befitting embedded devices profiles. In many cases, light web servers are preinstalled from the factory, and are used as a web based interface for management and configuration. In the case of Ruckus devices, old versions of "EmbedThis GoAhead" web applications are a built-in user interface web application for device configuration. Ruckus wireless devices will also commonly run old versions of DropBearSSH. Devices from other vendors were using ACME mini_httpd1.19, a version from 2003. Devices commonly run old and unpatched SSH services.

Intrusion campaign design and execution

Mapping the timeline and tasking of LapDogs intrusions

When we delved into the TLS certificates and their metadata, we were able to uncover specific details that suggest the operators are methodical and operate with specific tasking. Our analysis was able to discern specific TLS certificate issue dates, patterns, and which countries the hackers intended to target, indicating careful planning, surging interest in Japan, and steady interest in other targets around the globe.

A unique element of LapDogs is that compromised nodes generate their own TLS certificates locally. While certificate metadata can be tampered with and thus is not always reliable, correlation analysis between (1) certificate issue dates (2) port numbers the operator assigned to the malicious service, and (3) the targeted country, revealed a unique, triangular, relationship.

For example, when we examine the certificate issue date, it appears that certificates for the LapDogs service were generated in batches, commonly with seconds between each certificate. The timeline of all known issue dates in the ORB Network can be seen here:
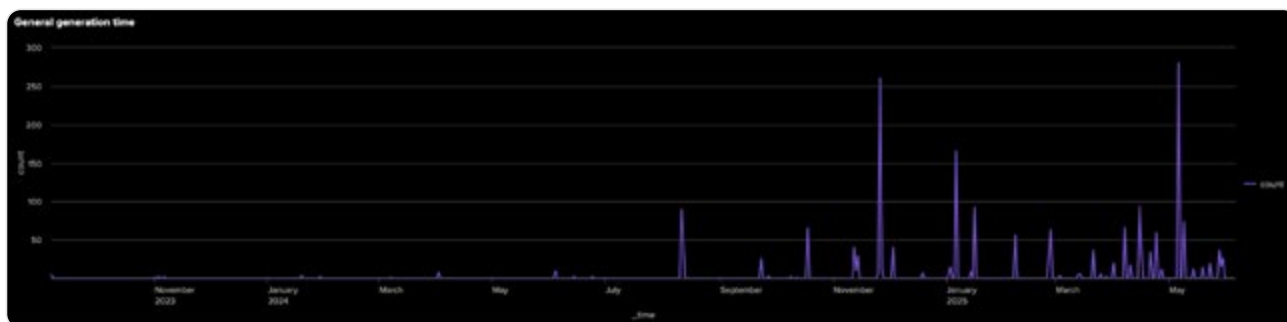
The earliest observed certificate within the network was issued in September of 2023—on 2023-09-06 at 07:00:19 (GMT).

- Interestingly enough, this certificate is one of two unique instances in which the same certificate is shared by two IP addresses.

- It is plausible that this instance is a case where one device uses two external IP addresses simultaneously.

- Indeed, in this instance, the certificate was used by two IPs, both of which were located in Taiwan and hosting two different subdomains of "Northumbra[.]com," which we found to be related to Cisco Talos' previously mentioned research (103.131.189[.]36 and 103.131.189[.]2).

In the second instance where two IPs shared a certificate—which were issued in November of 2024 (on 2024-11-26 at 02:27:19 GMT), the two IPs are part of the same C class and share the same main domain.

- Their subdomains are "pc1" and "pc2." In this specific incident, the LapDogs operator targeted a Buffalo Technology AirStation device.

- Other TLS encrypted services running on both of these IPs shared the exact same certificate, including the "Buffalo setup" certificate, commonly generated as a default local certificate per individual device.

- We therefore assess the compromised device in this incident is the Buffalo AirStation router itself—one device used as a gateway for two different internal endpoints, with two separate external IPs and subdomains.

From this we hypothesize that certificates are generated per instance of ShortLeash installation and not per unique IP.

Following our hypothesis that unique certificates are generated per ShortLeash instance, we then assessed whether certificate issue and expiration dates can be used to determine when devices had been compromised.

As seen before, LapDogs' operator appears to batch create certificates on specific dates (within one batch, certificates will portray issue dates and time with seconds apart from one to the next). Correlating the issue date with countries of the targeted devices (based on geolocating IPs) showed interesting results that indicate this threat actor is likely acting methodically and has specific tasking:
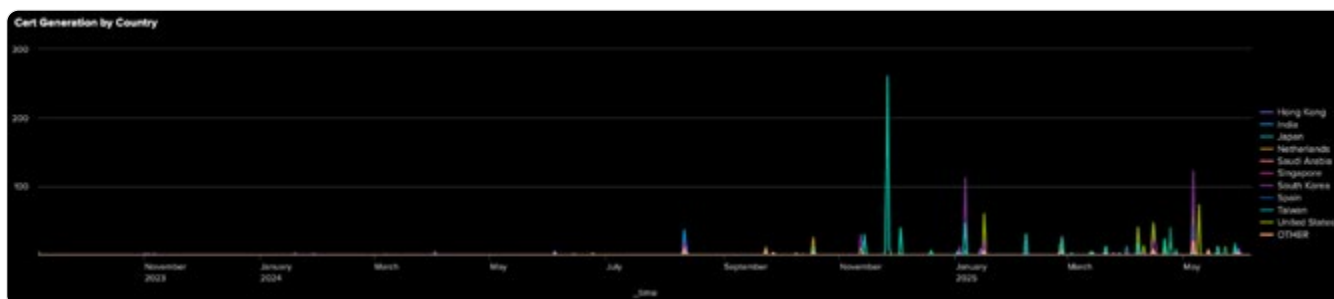
As seen in the timechart above, in many instances, within a defined, short span of time, LapDog's operators would limit the scope of their operations to specific targeting of a single country. In other cases, they would target multiple countries simultaneously. That initially led us to believe that LapDogs operators would conduct campaigns with a target country in mind, and when more than one country seems to sprout new LapDogs nodes at the same time, that can be simply explained as different operations occurring simultaneously.

Our assessment shifted slightly when we attempted to then correlate certificates' issue dates with the port assigned for the malicious web service
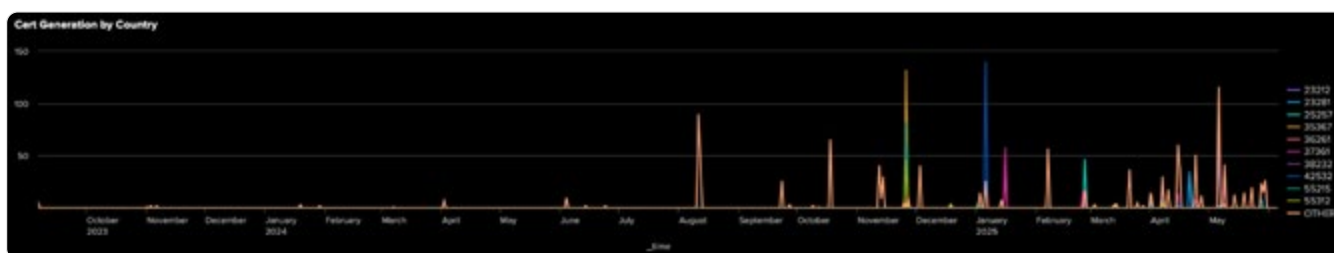
The correlation between port number and dates at first seemed like an inverted image of the date and country correlation. For instance, our analysis found that all certificates from November 26th, 2024, were tied to compromised devices in Japan—essentially confirming that Japan was the only country targeted on that day, with over 123 infected devices. At the same time, the compromised devices in Japan had the malicious certificates appear on one of three different ports, effectively dividing them into three distinct groups.

On the other hand, on January 6th, 2025, over 166 certificates were generated by compromised devices, spanning three different countries (Japan, South Korea, and Taiwan) but 140 of them (including devices from all three countries) shared the same port for the malicious service (42532).

When examining the exact time of issuance more closely, however, the picture became clearer: Certificates can be grouped by batches of issuance, lasting a few seconds and up to two hours at a time. All certificates that are issued within the same "batch" will then be served on the same port by the malicious web service, regardless of its geographic location. We therefore arrived at the following hypotheses to analyze expansion campaigns of LapDogs:

1. **"Certificates are issued locally per instance of ShortLeash, and are generated in a time relative to the activation of the malicious web service by ShortLeash"**

Once ShortLeash is executed, it immediately springs the malicious web service into action, triggering the generation of the certificate. In addition, from the handful of instances where two different IPs served the exact same ShortLeash certificate, we infer that ShortLeash may operate more than one malicious web server per instance, but will use the same certificate it generated for both. This ultimately means that the certificate issue date is a useful indicator to assess local infection time.

2. **"Port number is assigned by the operator of the network, per intrusion set, and not by the local instance of ShortLeash"**

This is somewhat confirmed by the shared port numbers on all the devices within the same certificate batch, regardless of the device type, geographic location or ISP. That isn't to say that the specific port number holds any unique significance, but simply that it is probably given to the node and not decided by it, along with all the same targets within the same intrusion set. Since some expansion operations of LapDogs seem to unfold in tandem, port assignment by the operator may allude to the perceived different sets of targets.

When aiming to analyze threat actors' motivations and goals for intrusion campaigns, being able to differentiate between different sets of targets for each individual intrusion is key. Going back to the example of November 26th, 2024 when the operators targeted over 120 devices in Japan with three different ports assigned, by tracking down the owners of each compromised device, and analyzing commonalities among them, we can also try to infer what was the threat actor's aim, based on shared commonalities among the group.

In addition, knowing that within the span of a single targeted operation, all successfully compromised devices will consequently run the malicious web service on the same port may enable threat hunters, SOC analysts and first responders to track affected infrastructure faster and more efficiently

3. **"Commonly, but not always, the operator focuses on one region or country at a time"**

This assessment is explained by the country data correlating with issue date as a statistical artifact. This specific hypothesis highlights the uniqueness of LapDogs as an ORB, most likely operated by a task-driven and goal-oriented threat actor, unlike a Botnet that spreads itself autonomously or guided opportunistically based on all available vulnerable devices.

4. **"The first (visible) intrusion set occurred on September 6th, 2023, in Taiwan. From there, the next instance appeared only four months later, on January 19th, 2024"**

Derived directly from the certificate issue dates, we can see that expansion campaigns of LapDogs did not start with a large set of targets, but rather slowly (but steadily) grew in numbers, all the while maintaining persistent control over older nodes in the network. (The nodes with certificates issued in September 2023 maintain them and the malicious service to this day.) This pattern of gradual expansion by itself is yet another indication to a methodical and strategic operational planning, not at all the explosive eruption of nodes in an opportunistic-natured Botnet.

Interestingly enough, the original IP we found to communicate with the ShortLeash sample from Cisco Talos' report (103.106.230[.]31) is currently not presenting the LapDogs certificate (shown in the VirusTotal platform only as historical data). We can therefore surmise that historical nodes over the years could have been tracked and taken down individually based on their suspicious activity.

This caveat is exactly the reason we prefer to approach LapDogs as a unified phenomenon and not as individual instances of the same malware and behavior: Not only is it supported by our data that nodes use the malicious service to communicate with each other and thus create a de facto network, but we also believe that this new approach to threat modulation and perception may enable us to develop better mitigation strategies to tackle emerging threats of this caliber.

Identifying intrusion sets across the ORB Network

As we've established, looking at individual certificate generation dates and unique port numbers assigned to the malicious service enabled us to uncover discrete groups that emerged from the data. For some groups, distinct commonalities or patterned themes became clearer.

In order to test this hypothesis against the bulk dataset at our disposal, we utilized commercially available artificial intelligence (AI) and large language models (LLMs) for large data analysis. We performed IP grouping and then assessed group commonalities based on pre-determined parameters. With this, we were able to group the entire set of identified devices into 162 distinct intrusion sets or groups representing short-term intrusion sets.

Statistical analysis of the certificate generation intervals found a 1.8 second interval expectancy between consecutive certificates within a group. This very obviously points to an automated process and not a manual one-by-one infection process—notwithstanding having 53 groups (out of 162) consisting of a single targeted device, which in a different setting, might have alluded to "hands-on" infection operations.

It is imperative to remember that the certificates that we were able to examine, represent the successfully targeted devices, while the actual list of targets is presumably larger. This can also account for the differentiation in certificate generation intervals, where presumably other targeted devices could fit in between two certificates with a longer interval.

IP Group Sizes Over Time by Common Country Targeting
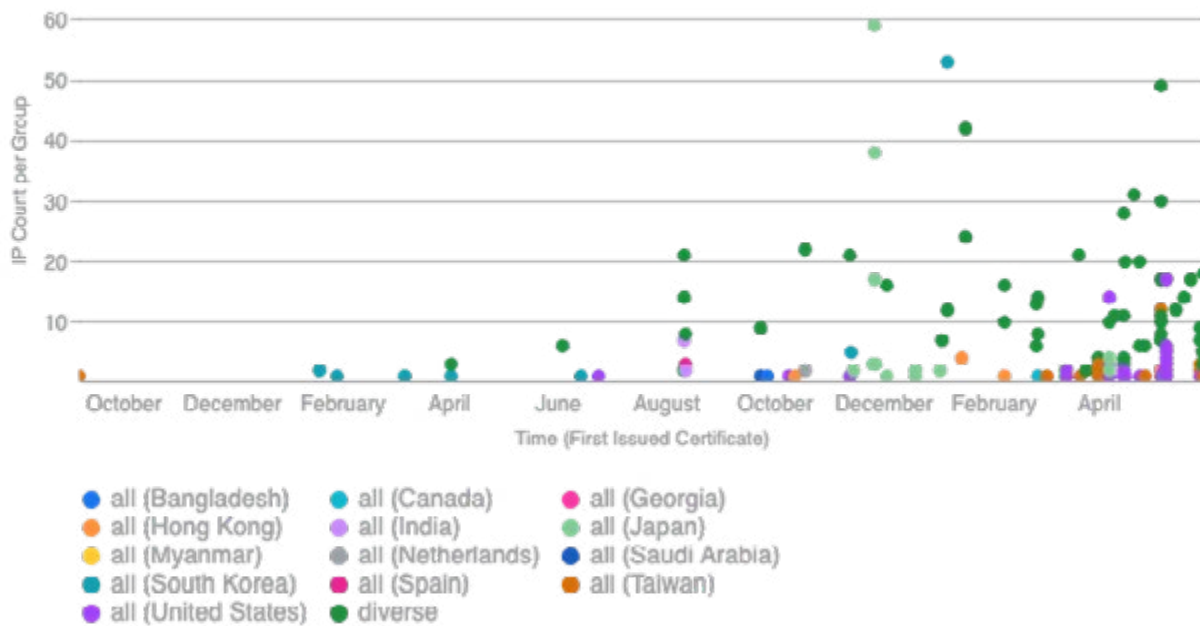
When analyzing group commonalities among these 162 intrusion sets, the structured and targeted element of intrusion sets grew more distinct. As shown in the chart above, many intrusion sets had a sole country focus, many of which were limited to targets within the same city.

While many groups are diverse in geographic location, we found that in some instances, geographic disjointment concurred with ISP focus, where targets share an international internet provider. To fully explore this notion of ISP versus geographic targeting, we performed a Pearson correlation analysis to assess just how independent these two variables really are.

- As can be seen in the scatter plot graph to the right, ISPs and geolocation targeting are very strongly correlated within our entire data set (Pearson correlation coefficient 0.859, $\alpha<0.00000\sim$) and thus are heavily intertwined (as can be expected).

- We therefore decided to unify ISP and geographical commonalities into one workframe, simply asking the question "is there a localized unifying theme within a given intrusion set?".

- Since every intrusion set with only a single target would be mistaken for a "targeted group" due to no differentiation, we sampled intrusion sets with two or more IP addresses within a given group to assess how many can be considered to share commonalities.
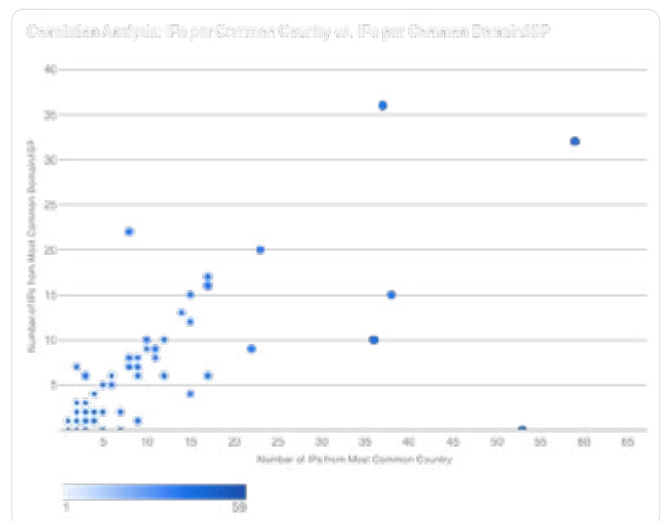
109 Groups (out of 162) in total consisted of two or more IPs, representing approximately 94% out of all IPs within the ORB. 37 out of 109 groups (and 346 IPs in total, or 34.7%), showed to have a shared commonality between group members, based on a common geographical location or an ISP provider (we defined >95% of the entire group as the threshold to match the commonality criteria), as summarized by the following chart:
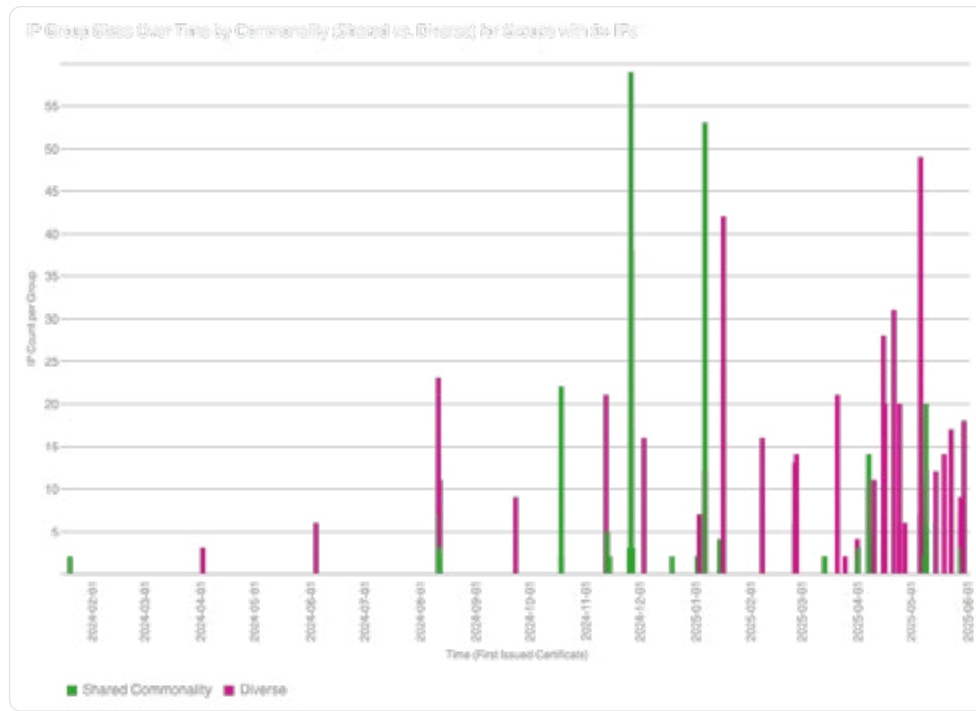
We summarize our conclusions from examining expansion operations of the LapDogs as follows:

- LapDogs is a gradually growing network of (mostly) compromised devices, serving as operational nodes, with the earliest available nodes dating back to September, 2023.

- Since then, it has expanded in methodical and small scale operations, effectively infecting no more than 60 devices per intrusion set.

- While it is difficult to extract the operators' goals and motivations from the available data, we can surmise that the hackers prioritize certain countries and geographical locations within a broader goals' hierarchy.

- This conclusion is supported not only by the overall prevalence of infected devices in the United States and Southeast Asia, but also when a case by case perspective on intrusion sets is applied:Over a third of all of the ORB operation revolve around a geographical focal point, occasionally even localized down to the city level.

- In sum, the LapDogs ORB shows signs of a vast and prolonged intrusion operation that is carried out with intent and planning for both the overarching picture and the finer details.

PolarEdge: A separate, sister ORB

Among known ORB Networks, which our colleagues in the industry have previously researched and reported on, one ORB stands out as noticeably similar to LapDogs: PolarEdge (see Sekoia's blogpost **here**).

Sekoia's Threat Detection & Research team uncovered PolarEdge, an Internet of Things (IoT) ORB Network active since late 2023. It exploits N-day vulnerabilities to target routers and other IoT devices. Compromising a device will introduce it into the network and will enable its abuse as a multifunctional node.

This description nearly matches our observations of LapDogs' targets, and there are similarities observed on the infrastructure level as well. At the moment, however, our conclusion from examining the correlation between the two is that LapDogs and PolarEdge are separate entities.

During our research into LapDogs, we have found six instances in which a router device was showing signs of infection by both LapDogs and PolarEdge simultaneously, each running on a different service, and so, we were able to closely examine the commonalities and differences. A router device infected with either the PolarEdge malware or with ShortLeash will begin running a new web service, presenting as a light web application, and will commonly operate from a high and uncommon port, presenting the incriminating TLS certificate as indication.

Overall network operators of the two ORBs seem to favor Southeast Asia and the United States as their main areas of operation. In both instances, the malicious service running on the compromised device will show the following JARM TLS fingerprint: 3fd3fd16d3fd3fd22c3fd3fd3fd3fdf20014c17cd0943e6d9e2fb9cd59862b. As mentioned before, this JARM is overall indicative of lightweight web servers.

There are several key differences between the two networks, however:

TTP comparison:
While ShortLeash and PolarEdge malware functionally serve a very similar purpose, a Diff comparison between the two payloads found very little code commonalities shared between them. The infection process, which is aimed toward the same set of embedded devices and architecture, is still in different locations within the device's directory (PolarEdge operates from the /tmp/ folder, while ShortLeash is dropped into the /etc/systemd/system directory).

Persistence is also achieved differently: While PolarEdge backdoor replaces the CGI script of the devices with the operator's designated webshell, ShortLeash merely inserts itself into the system directory as a .service file, ensuring the persistence of the service upon reboot, with root level privileges.

While PolarEdge has only reportedly targeted router devices or similar embedded devices, we have observed ShortLeash with a Linux variant that is capable of running on virtual private servers (VPSs), routers and IoT devices by adjusting the installation process to native OS in the compromised environment. We have also observed a Microsoft Windows variant, of which our scanners were able to find examples of active nodes running a Windows server (and even Windows XP).

Network indicators and behavior:

Compromised nodes within either ORB will run a unique service that's indicative of the malicious service operating in the background, each presenting its own corresponding unique TLS certificate. However, while PolarEdge nodes use the exact same set of certificates (including the expiration date and serial number), each node in LapDogs will generate its own TLS certificate, all the while sharing the exact same subject and issuer data. We also assess that these certificates are generated locally by ShortLeash.

In addition to that, the malicious web service activated by ShortLeash will attempt to masquerade itself as a versionless Nginx web server, while PolarEdge does not respond to http requests with banners, and does not seem to attempt to present itself as a legitimate service

Commonalities and differences between the networks can be quickly summarized with the following table:

Feature	LapDogs	PolarEdge
JARM TLS Fingerprint	3fd3fd16d3fd3fd-22c3fd3fd3fd3fdf20014c17cd-0943e6d9e2fb9cd59862b	3fd3fd16d3fd3fd-22c3fd3fd3fd3fdf20014c17cd-0943e6d9e2fb9cd59862b
Geographic spread	SouthEast Asia and the U.S.	SouthEast Asia, Latin-America and the U.S.
Installation Location	Drops in '/etc/systemd/system/' in Ubuntu, and '/lib/systemd/system/' in CentOS	Operates from the `/tmp/` folder.
Persistence	Inserts itself as a `.service` file, autoruns and creates a backup copy with every device reboot.	Replaces the CGI script with the operator's designated webshell.
Target Devices	Linux variant for VPSs, routers, IoT devices. Also has a Microsoft Windows variant (found on Windows Server, Windows XP).	Primarily targets router devices or similar embedded devices.
TLS Certificate Issuance	Each node generates its own TLS certificate with the same subject and issuer data.	Nodes use the exact same set of certificates (including expiration date and serial number).
HTTP Banner Service Data	Responds to HTTP requests with a fake Nginx web server banner.	Does not respond to HTTP requests with a banner.

Victimology

Associated ISPs

The attackers mostly targeted SOHO routers with static IPs, so the most common domain names we encountered were placeholder domains from the internet service provider. Through this we were able to easily compile a list of internet providers that were vicariously affected by LapDogs.

Having that said, some routing devices might be of direct use and ownership of the ISPs themselves. This poses a potential risk to the internet providers' internal networks and systems, depending on networking services, network architecture and other infrastructure that might rely on an infected device. Thus there could still be a potential threat imposed on the ISP itself, and we suggest mitigating it. We suggest investigating compromised devices and applying the network and behavioural fingerprints we've laid out in this report to hunt for future LapDogs targeting.

The chart below shows the top ten most prolific ISPs appearing in observed LapDogs nodes we were able to detect.

Resolved Domain Names

Domain	Count
res.spectrum.com	283
asahi-net.or.jp	63
bn.2iij.net	23
ucom.ne.jp	20
ap.nuro.jp	16
ocn.ne.jp	15
dion.ne.jp	13
mesh.ad.jp	13
hinet-ip.hinet.net	12
biz.spectrum.com	9
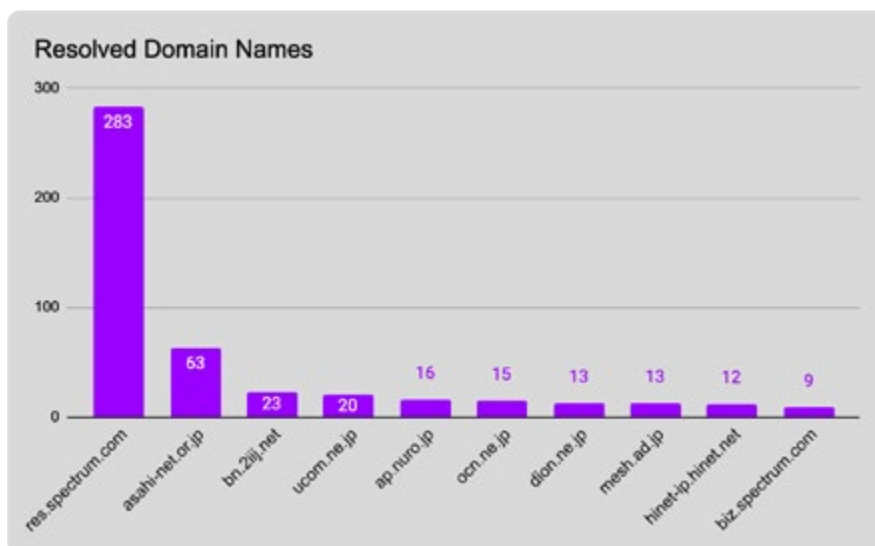
SecurityScorecard's STRIKE are coordinating with affected parties and 3rd parties we were able to detect, including ISPs, to aid in investigation and mitigation efforts. If you fear that you were impacted by LapDogs, you may reach out to STRIKE for information and assistance (STRIKE's contact information is provided at the bottom of the IOC section).

Targeted hardware and firmware vendors:

Based on concurring services and TLS certificates observed on other services, aside from the malicious one, we were able to uncover a set of device models and vendors that were targeted and successfully compromised. We have not observed a limitation within ShortLeash regarding hardware types or vendors, so long that the operating system of the device fits the available ShortLeash version. Here is a list of observed hardware models that are actively infected—and which can likely be targeted by LapDogs in the future:

Vendor	Metadata associated with devices
Ruckus Wireless	Ruckus Wireless (based on running EmbedThis GoAhead webapp)
ASUS	Asus wanduck WAN monitor httpd, ASUS WRT http admin
Buffalo Technology	Buffalo AirStation http config
Cisco-Linksys	Cisco-Linksys E4200 WAP upnpd
Cross Digital Video Recorders (DVRs)	Cross DVR httpd
D-Link Corporation	D-Link WRPD
Microsoft	Microsoft HTTPAPI httpd, Microsoft ftpd, Microsoft Windows XP telnetd, Microsoft IIS httpd, Microsoft Terminal Service
Panasonic	Panasonic webcam http config
Synology	Synology DSM Snapshot Replication iSCSI LUN

Directly affected organizations:

Based on resolved domains and direct IP location tracing, we were able to uncover some potential victims of LapDogs. It is imperative to first define the three3 types of potential victims that might arise in the LapDogs campaign:

1. **ORB victims:** The owner of the device that operators compromise in order to add it to the LapDogs network. These devices turn into operational nodes to be used by a potential "client" of the ORB. The nodes may serve as an obfuscation layer to mask the threat actors' backend infrastructure.

2. **Targeted victims:** The individuals or organizations that the hacker or network operator uses the ORB against. These victims need not be connected by any means to the compromised devices (which are used as nodes in the network to facilitate targeting).

3. **Hybrid victims:** A compromised device is used as an attack vector, allowing access into the internal network it is serving. In these cases, the hackers can compromise the device and use it as the initial access vector into the local network.

In the following cases we have assessed targets to be "ORB victims," as defined in our first category, although they could potentially become a "Hybrid victim" if they are not already:

ORB victims in Japan:

- A Municipal Services office

- IT and networking solution companies

- A construction and real estate company

ORB victims in UK:

- A media company.

Every node in the LapDogs ORB can be used by a threat actor to further access the internal network the node is connected to, therefore each owner of a compromised device might be further victimised and should take preventative measures.

Attribution

As with other ORB Networks, it can be difficult to determine the exact threat actor operating the network, as ORB Networks can be—and historically have been—shared by more than one threat actor for separate campaigns and intrusion sets. In Cisco Talos' report, it is assessed that UAT-5918 is a China-Nexus espionage threat actor, due to similarities in tactics and targeting to other prolific actors. This assessment is further supported by LapDogs, as we were able to find Mandarin code notes within the startup script for ShortLeash. The focus on Southeast Asian countries and the United States is circumstantial yet noteworthy evidence as well, given the heightened focus of China-Nexus APTs on these regions.

We therefore assess with moderate confidence that LapDogs is an Operational Relay Box Network that China-Nexus threat actors use. Based on Cisco Talos' previous assessment regarding UAT-5918, we also assess UAT-5918 used the LapDogs ORB Network at least once in its operations in Taiwan. We cannot yet confirm whether UAT-5918 is the operator or just a client of the network. We also cannot yet confirm whether other threat actors have or will have access to leverage LapDogs as well.

Conclusion

LapDogs is a gradually growing Operational Relay Box (ORB) Network, which we assess China-Nexus threat actors are using to conduct a targeted operation around the globe. This campaign shows a surging interest from China-Nexus threat actors in using ORB Networks to conduct covert intrusion campaigns both around the globe and tailored to specific victims of interest. With an increasing interest in this approach, security teams should be on alert that China-Nexus threat actors are disrupting traditional playbooks for IOC tracking, response, and remediation.

The LapDogs ORB Network began operating as of September 2023 at the latest and has been performing expansion operations ever since. It has infected no more than 60 devices at a time, targeting primarily embedded devices in and around the United States and Southeast Asia. The operator appears to have strategically planned expansion campaigns, which occur in small intrusion sets over time.

The attackers leverage ShortLeash, a custom backdoor malware, to compromise devices and maintain an interconnected network. When executed on a given device, ShortLeash creates a fake Nginx web server and locally generates a unique, self-signed, TLS certificate presenting as "LAPD" (which appears to be an attempt to imitate the Los Angeles Police Department).

Analysis shows 162 distinct intrusion sets, with about a third sharing a common geographical location or ISP, suggesting the operators are highly focused on several specific locations and further distinguishing LapDogs as a goal-oriented actor. Overall, LapDogs is a vast, prolonged intrusion operation with clear intent and planning, emphasizing the need for vigilance in securing embedded devices.

Contact STRIKE for Incident Response

SecurityScorecard's STRIKE Team has access to one of the world's largest databases of cybersecurity signals, dedicated to identifying threats that evade conventional defenses. With proactive risk management and a rapid response approach, SecurityScorecard offers companies protection against third-party risks and the ability to counter active threats like LapDogs.

Discover how SecurityScorecard and its STRIKE Team can strengthen your enterprise's security. For STRIKE media inquiries, contact us **here**.

IOCs

ShortLeash - the LapDogs ORB payload

Description	Type	Indicator
ShortLeash Bash startup script	SHA256	75618401b64046d970df49fcfdfcc36174b0aae27ac4e1c178dc75219992080a
ShortLeash - Linux variant	SHA256	9b954bfc2949d07eb41446225592eaa65ed3954cd2b93a13c574bb89147a4465
ShortLeash - Linux variant	SHA256	33ff77940436498a50bbb05391324964063cd3c93f2e66b07d1cb31442bb1513
ShortLeash - Linux variant	SHA256	073133298e5cca0833354be754f5d14358c0dbc24ba5f70e5b5eceec1d6726e6
ShortLeash - Windows variant	SHA256	02ab315e4e3cf71c1632c91d4914c21b9f6e0b9aa0263f2400d6381aab759a61
ShortLeash - Windows variant	SHA256	1a180186e6fbaf6fa88f934965290235e8418976d6f3546dbf100217d1752db4

Network fingerprints

Description	Type	Indicator
Certificate metadata - subject and issuer	TLS certificate	CN=ROOT, O=LAPD, ST=California, C=US, L=LA, OU=Police department
Certificate metadata - subject and issuer (appears in different order)	TLS certificate	CN=ROOT, O=LAPD, ST=California, C=US, OU=Police department, L=LA
JARM fingerprint for the malicious service	JARM	3fd3fd16d3fd3fd22c3fd3fd3fd3fdf20014c17cd0943e6d9e2fb9cd59862b

Network indicators

Description	Type	Indicator
LapDogs related domain	Domain	northumbra[.]com
LapDogs related domain	Domain	ns.northumbra[.]com
LapDogs C2 domain	Domain	www.northumbra[.]com
LapDogs C2 domain	Domain	study.northumbra[.]com
LapDogs node IP	IPv4	119.31.186[.]253
LapDogs node IP	IPv4	103.131.189[.]36
LapDogs node IP	IPv4	103.131.189[.]2
Suspected LapDogs VPS node	IPv4	64.176.228[.]227
Suspected LapDogs VPS node	IPv4	103.117.100[.]77
Suspected LapDogs VPS node	IPv4	103.117.100[.]79
Suspected LapDogs VPS node	IPv4	103.117.100[.]117
Suspected LapDogs VPS node	IPv4	103.135.248[.]52
Suspected LapDogs VPS node	IPv4	141.164.44[.]183
Suspected LapDogs VPS node	IPv4	141.164.50[.]206
Suspected LapDogs VPS node	IPv4	141.164.51[.]99
Suspected LapDogs VPS node	IPv4	141.164.63[.]253
Suspected LapDogs VPS node	IPv4	158.247.201[.]36
Suspected LapDogs VPS node	IPv4	158.247.208[.]113
Suspected LapDogs VPS node	IPv4	158.247.216[.]244
Suspected LapDogs VPS node	IPv4	158.247.244[.]8
Suspected LapDogs VPS node	IPv4	158.247.250[.]190
Suspected LapDogs VPS node	IPv4	180.210.220[.]148

For the full IOC list or more information - please contact SecurityScorecard's STRIKE **here**.

References

- Cisco Talos, "UAT-5918 targets critical infrastructure entities in Taiwan," Talos Intelligence Blog, **https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/**.

- Sekoia, "PolarEdge: Unveiling an uncovered ORB network," Sekoia Blog, **https://blog.sekoia.io/polaredge-unveiling-an-uncovered-iot-botnet/**.

- Google's Mandiant, "China Nexus Espionage ORB Networks," Google Cloud Blog, **https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks**.

- SentinelLABS, "Follow the Smoke: China Nexus Threat Actors Hammer at the Doors of Top-Tier Targets," SentinelOne Labs, **https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/**.