Tracking LightSpy: Certificates as Windows into Adversary Behavior

Published: 2024-06-06 · Archived: 2026-04-05 16:27:49 UTC

TABLE OF CONTENTS

Introduction

In this post, we'll detail the infrastructure of the LightSpy spyware framework and highlight the unique TLS certificates that have been instrumental in identifying its servers.

We'll examine specific characteristics of the LightSpy network, such as commonly used ports, preferred hosting providers, registration details, and both existing and newly discovered certificates from our scans. This article aims to equip defenders with the information necessary to understand and anticipate the behaviors of the actors behind this operation.

A Quick Refresher

LightSpy is a sophisticated surveillance framework targeting iOS, Android, macOS, and Windows devices, focusing on the Asia-Pacific region. This framework is designed to exfiltrate a wide range of sensitive data from mobile devices, including files, screenshots, detailed location information (such as building floor numbers), voice recordings from WeChat calls, and payment information from WeChat Pay.

Additionally, LightSpy captures data from popular messaging apps like Telegram and QQ Messenger, highlighting its extensive capabilities and significant threat potential.

The following recent blog posts provide a more technical analysis of malware infiltrating networks.

Huntress – "LightSpy Malware Variant Targeting macOS"
ThreatFabric – "LightSpy: Implant for macOS"
Lookout – "Lookout Attributes Advanced Android Surveillanceware to Chinese Espionage Group APT41"

Overview of LightSpy's Infrastructure

According to our scans, most of LightSpy's infrastructure is located in China and Hong Kong, with a single server identified in Japan. **Topway Global Limited** and **ChinaNet** comprise most of the servers hosting the certificates associated with the framework. **Based on our visibility, figure 1** displays a graph highlighting the most popular hosting companies.

We didn't forget about **AndroidControl**, also known as **WyrmSpy**, LightSpy's reported successor. In the next section, we will cover the certificates behind both LightSpy and AndroidControl in detail.

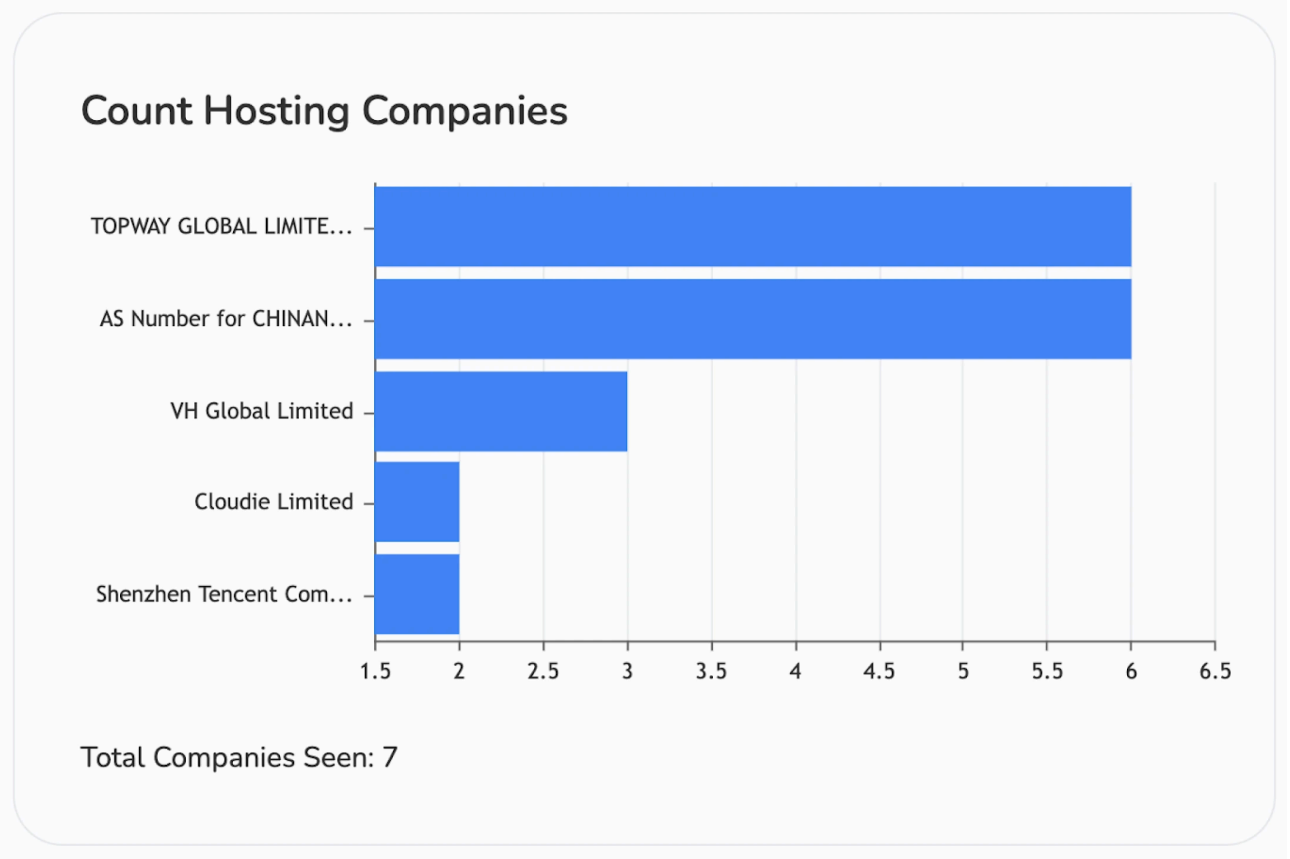

Figure 1: Common Hosting Companies in Hunt Platform

LightSpy uses a range of high ports for certificates, typically in the 50k+ range. In contrast, AndroidControl commonly uses port 443 for its control panel and port 3389 for Remote Desktop Protocol (RDP). Both frameworks leverage **Nginx** servers for their infrastructure, with LightSpy often seen using Nginx version **1.14.0** and AndroidControl using version **1.10.3**.

Hunt scans found that ports **51200** and **53501** are the most popular ports for LightSpy.

The top 10 ports are depicted below.

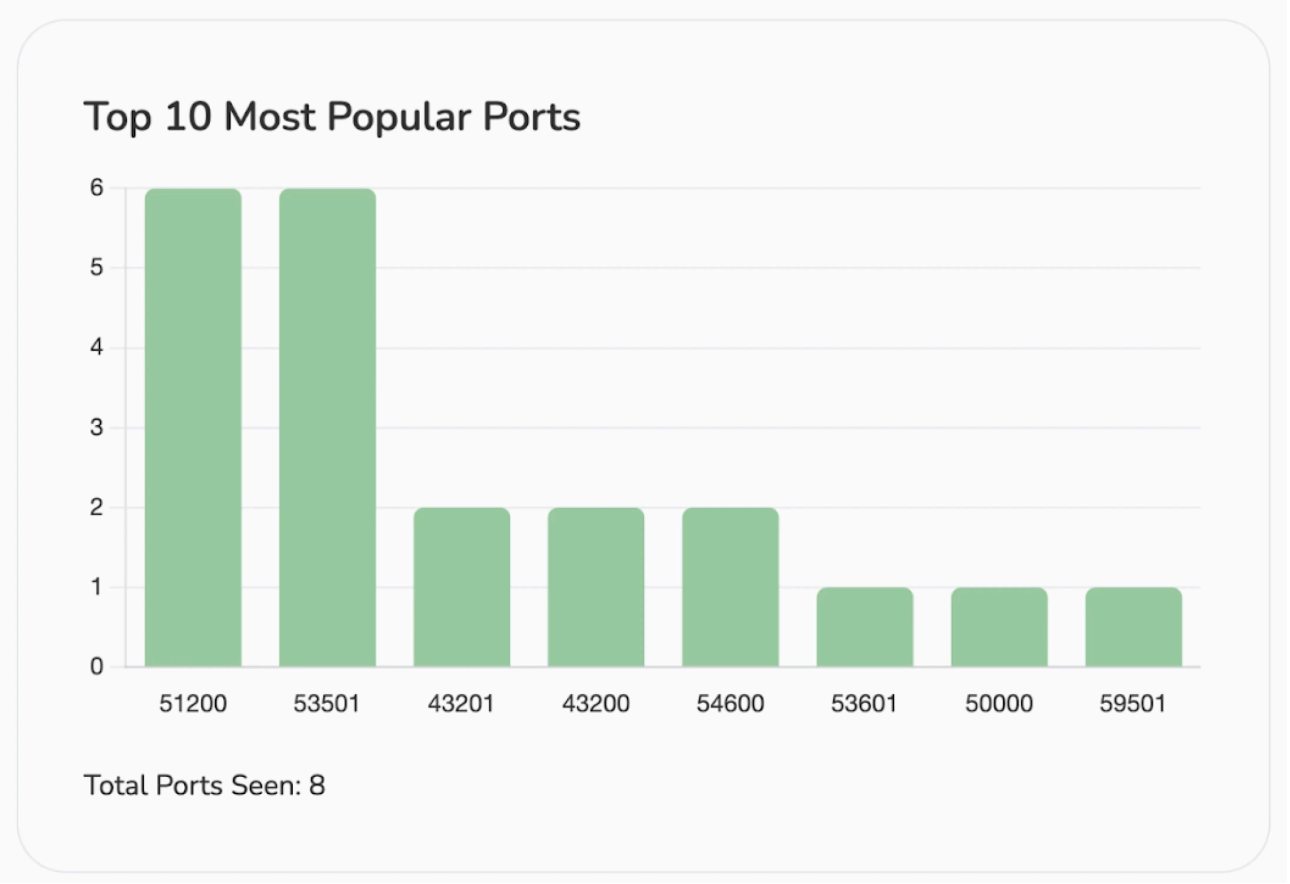

Figure 2: Most Popular Ports in Hunt

Detecting WyrmSpy was previously as straightforward as searching for web pages that display the HTML title ("**AndroidControl v1.0.4**"). However, this detection method is not foolproof and is easily changed by the actor(s) administering the server, rendering the query useless.

Like LightSpy, WyrmSpy uses a unique TLS certificate for its control panel. This procedure of using distinct certificates leads to a small number of IP addresses sharing it. While the title and certificate are easily changed, focusing on the latter allows researchers to identify related infrastructure, even if the page is altered or the actor has not yet started using the panel.

At the very least, we can get an idea of the certificate authority (if applicable) preferred by the attacker and the naming conventions used.

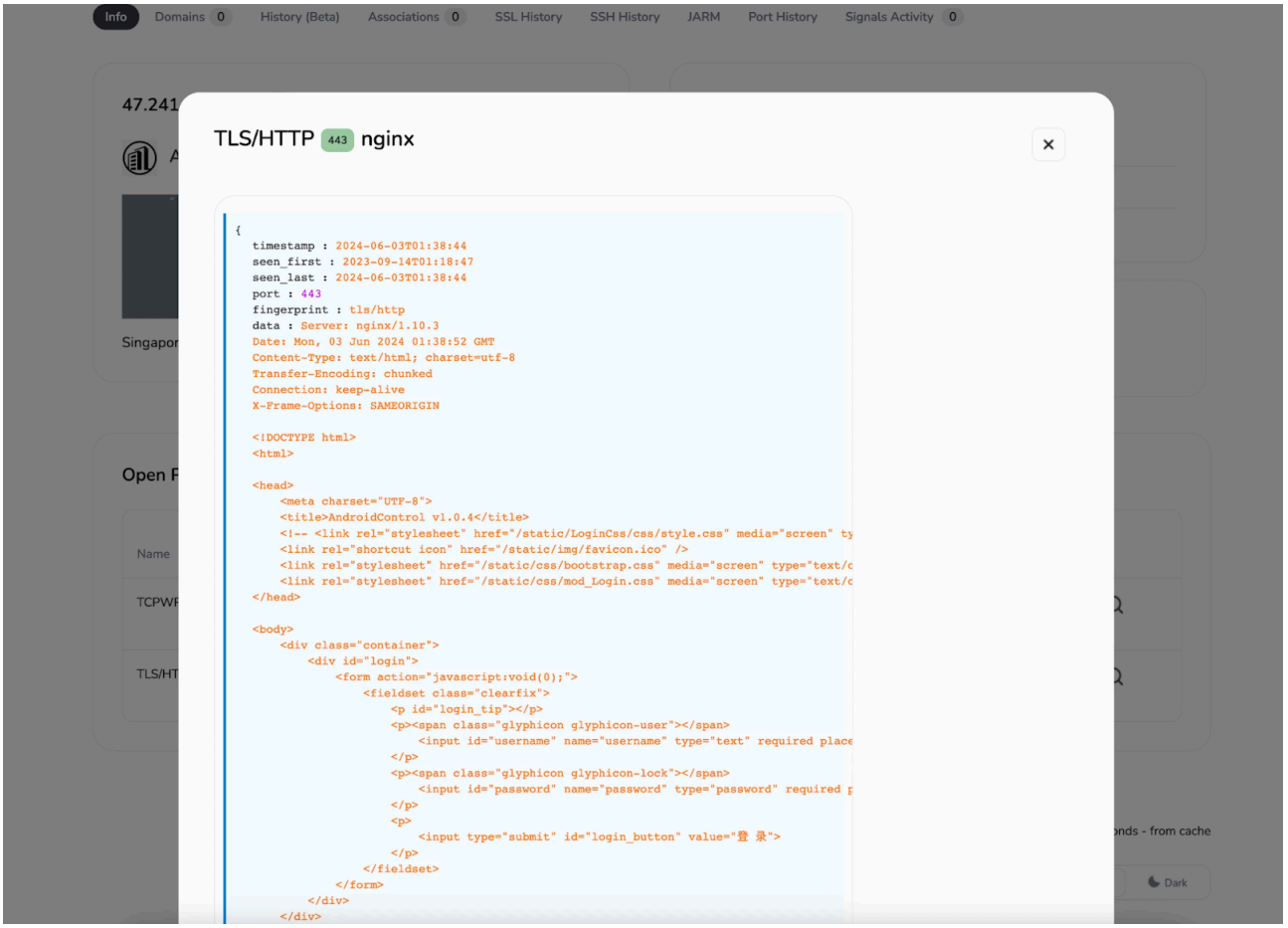

Figure 3: Screenshot of AndroidControl (WrymSpy) HTML Title Panel

Hunt is currently tracking 12 servers presenting the certificate we will discuss below.

Take a look for yourself using the Active C2 Servers feature here.

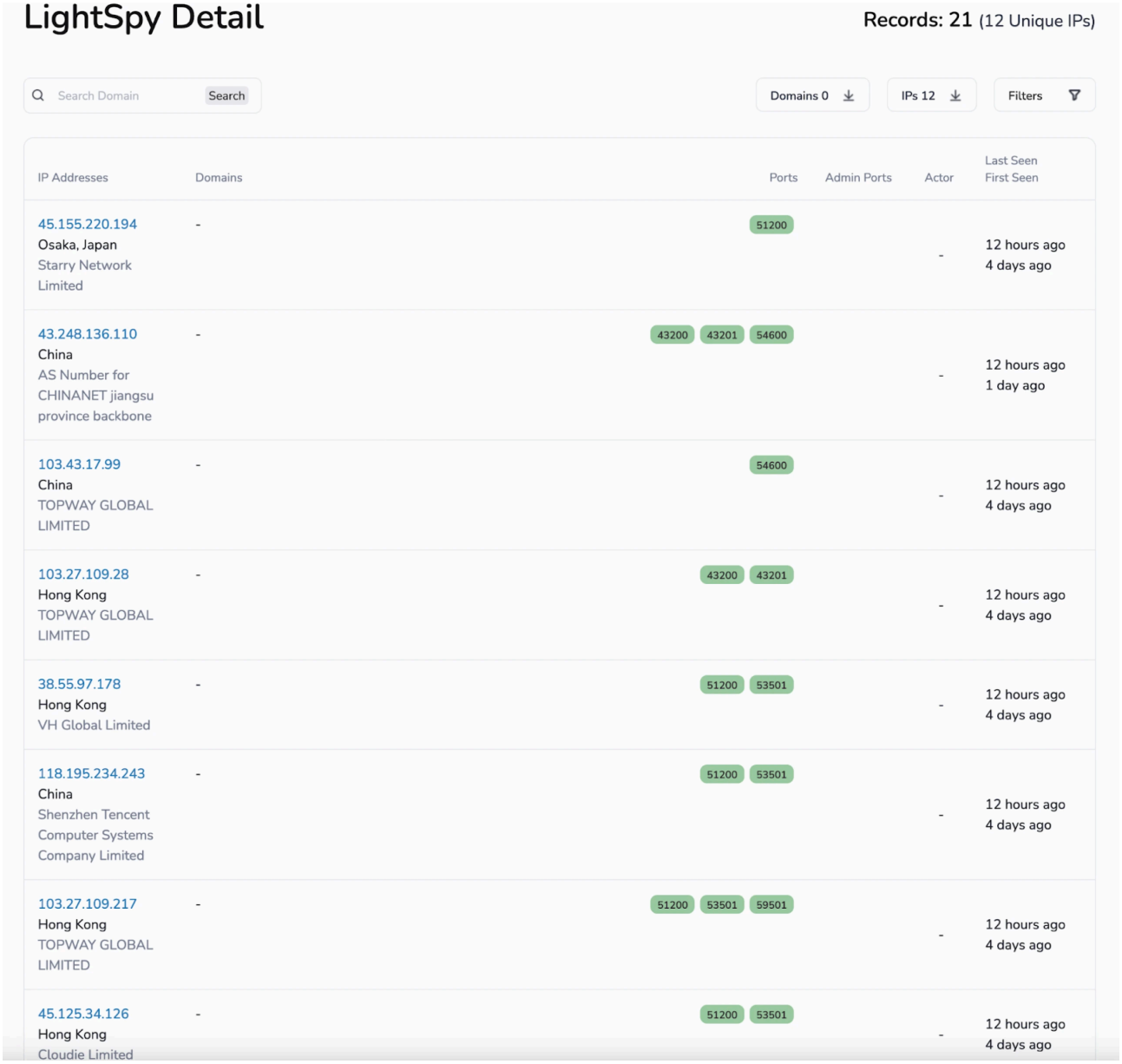

Figure 4: Just a Few of the LightSpy IP Addresses Available for Analysis in Hunt

Following the Certificates

We referenced the WyrmSpy certificate multiple times without displaying it. The full self-signed certificate is as follows:

- **C=US**
- **ST=State of California**
- **O=hxwa**
- **OU=John**
- **CN=X**

- **emailAddress=X3057@gmail.com**

If you've been following our blogs, you may recall our post on a cluster of **ShadowPad** infrastructure that used certificates spoofing the American technology company Dell. In that post, we highlighted several servers with RDP certificates following the "**iZ**[13 alphanumeric characters]" pattern. Notably, **47.241.218_217**, identified as WyrmSpy infrastructure, employs a similar naming convention, as illustrated in **Figure 5**.

ShadowPad blog post:
https://hunt.io/blog/tracking-shadowpad-infrastructure-via-non-standard-certificates

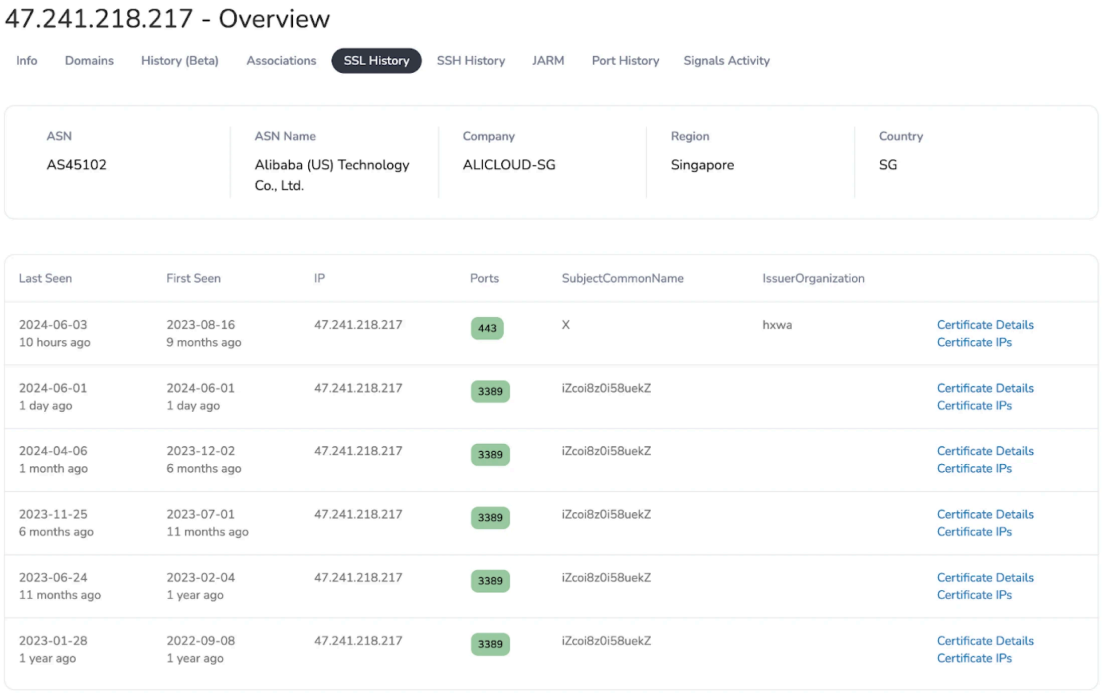

Figure 5: Certificates used on WrymSpy Server

Unfortunately, the trail ran cold on the above RDP certificate as we could not locate any additional servers using the above naming convention. However, we can pivot on the TLS certificate, which leads us to **5** additional servers worthy of a second look.

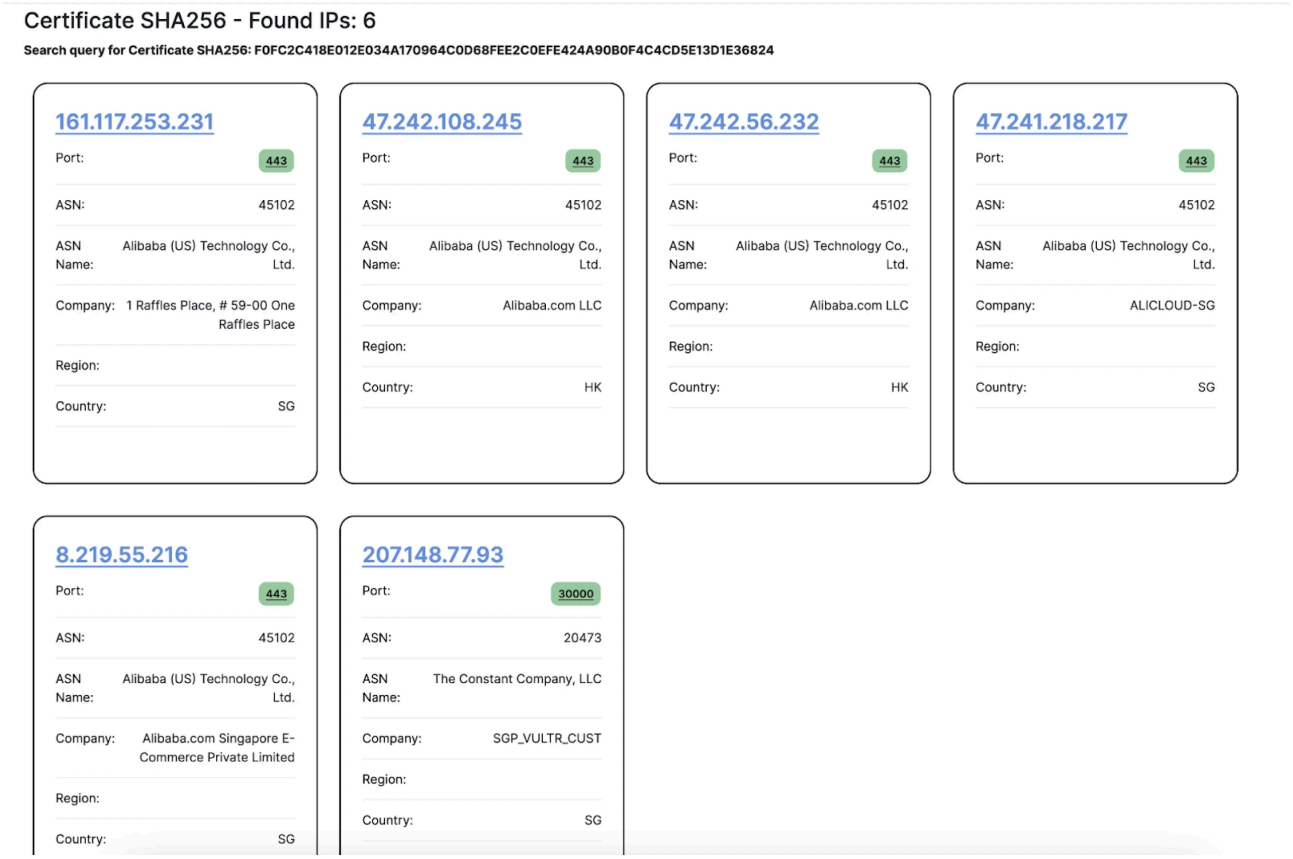

Figure 6: Pivot on AndroidControl TLS Certificate (Try it)

The certificates associated with LightSpy are reminiscent of the AndroidControl (WyrmSpy) names, with some notable differences:

LightSpy Certificate:

- **C=AU**
- **ST=SUN**
- **O=Kylin**
- **OU=base**
- **CN=admin1**
- **emailAddress=admin1@admin.com**

While both certificates follow a similar structure, the LightSpy certificate uses an **Australian** country code (C=AU) and generic organizational details. In contrast, the WyrmSpy certificate uses a **US** country code (C=US) and more specific, albeit fabricated, organizational information.

Despite these differences, the commonality in their structured format suggests a shared methodology or toolkit used by the threat actors behind both frameworks. This similarity can be a crucial indicator for defenders correlating and tracking related infrastructure more effectively.

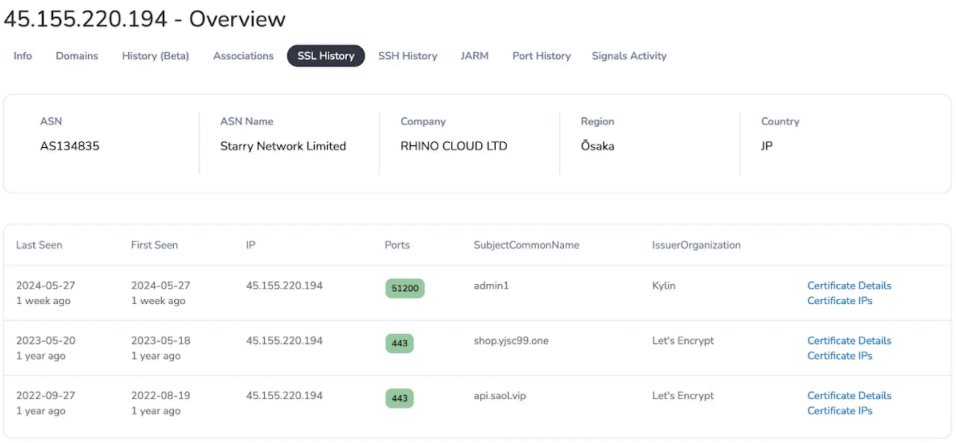

Figure 7: Example of a Short-lived LightSpy Certificate

Recently Seen Domains and Certificates

Once we establish a reliable query that consistently identifies malicious infrastructure, it's crucial not to rely solely on that detection method. Adversaries will likely make subtle server changes to evade detection or even transfer the IP address to another threat actor.

To counter this, we must periodically probe and reassess the identified servers (within reason), tracking changes over time. By doing so, we can proactively respond to these modifications and potentially differentiate between different threat actors using the same IP addresses or networks.

***It is crucial to be as discreet as possible when interacting directly with possible malicious infrastructure. Probing can tip off actors to your presence and expose your network to various attacks.**

While investigating these various IPs, we identified a server, **103.43.17_99**, that had recently started hosting the LightSpy certificate on port **54600**. Additionally, this server hosts another certificate on port 443 issued by **ZeroSSL** for the domain **yycclouds[.]com**, which also resolves to this IP address.

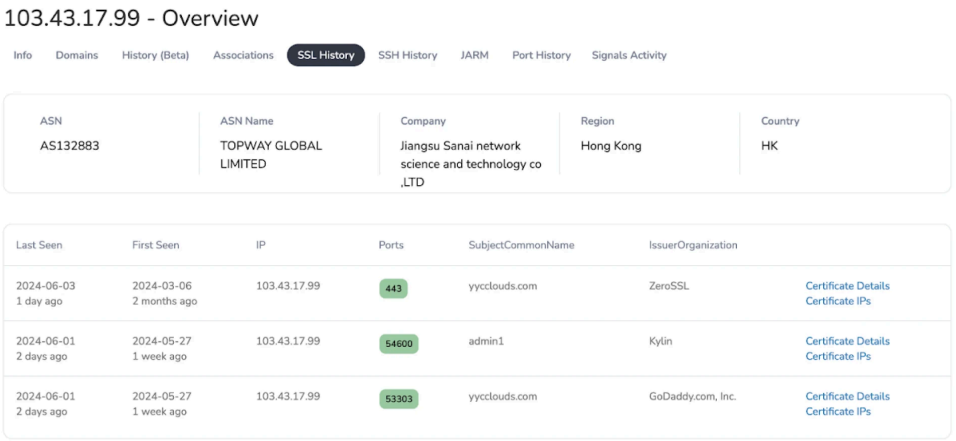

Figure 8: LightSpy Certificate Overlaps with ZeroSSL Certificate

The above domain is registered through GoDaddy and uses domaincontrol.com nameservers. As of the time of writing, there are no subdomains or web pages associated with the yycclouds domain.

Conclusion

In this post, we explored the intricate infrastructure of the LightSpy spyware framework and its successor, WyrmSpy. We highlighted the significance of focusing on TLS certificates and patterns in hosting providers, particularly in the Asia-Pacific region. Understanding these elements, along with critical infrastructure components such as ports, server software, hosting, domain registration, and certificates, allows us to better track and anticipate the evolving tactics of these threat actors.

Sign up for an account with Hunt to stay informed on the latest trends in malicious infrastructure and enhance your defensive capabilities.

Indicators

IP Address	**Notes**
103.27.109_217	LightSpy C2
43.248.136_110	LightSpy C2
103.27.109_28	LightSpy C2
38.55.97_178	LightSpy C2
103.43.17_99	LightSpy C2
43.248.136_104	LightSpy C2
45.125.34_126	LightSpy C2
45.155.220_194	LightSpy C2
154.91.196_185	LightSpy C2
222.219.183_84	LightSpy C2
47.241.218_217	WrymSpy C2
8.219.55.216	Shared certificate w/ WrymSpy
47.242.108_245	Shared certificate w/ WrymSpy
47.242.56_232	Shared certificate w/ WrymSpy
161.117.253_231	Shared certificate w/ WrymSpy

Certificate	**SHA-256**
LightSpy	efbfbd517e0727efbfbd48efbfbdd3b8efbfbdc69938efbfbd09efbfbd7cefbfbd3aefbfbd42417c
WrymSpy	efbfbd2c41efbfbd012e034a170964efbfbdd68fefbfbd2c0eefbfbd424aefbf bd5e13efbfbd6824

Source: https://hunt.io/blog/tracking-lightspy-certificates-as-windows-into-adversary-behavior