

# Exploring Splashtop RMM and Relays

 [blog.axelator.net/close-those-ports-exploring-splashtop-rmm-and-relays](https://blog.axelator.net/close-those-ports-exploring-splashtop-rmm-and-relays)

axelator

November 6, 2025



When looking for suspicious network connectivity, it's important to understand what other services might be running on the destination IP. It could be a harmless Python server with an open directory hosting files but additional analysis revealed it's running Empire at the same time. That open directory may not seem so benign now.

**HTTP 6001 / TCP**
🔗 DEFAULT\_LANDING\_PAGE

🕒 LAST OBSERVED
NOV 05, 2025
| 07:19 UTC
• 🔄 Live Rescan

Cache-Control: no-cache, no-store, must-revalidate

Response Body

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">...

**FINGERPRINT**

JA4TScan
65160\_2-4-8-1-3\_1460\_71-2-4-8-16

**CVES (2)**

⚠️ CVE-2008-1446
⚠️ CVE-2009-2521

**THREAT (1)**

🚩 Empire

**HTTP 8000 / TCP**
🔗 OPEN\_DIRECTORY

🕒 LAST OBSERVED
NOV 05, 2025
| 10:37 UTC
• 🔄 Live Rescan

SOFTWARE
Python 3.8.10
Python Software Foundation Simplehttp 0.6

**DETAILS**

URI
http://123.56.43.176:8000/
Go
Status
200 OK
Path
/
Body Hash
64670d17768d6acf1c4dcba1be895e2cf9c75a1e06a13af47f3964c0ef9d1608
HTML Title
Directory listing for /
Headers
HTTP/1.0 200 OK
Content-Length: 627..
Response Body
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>...

**OPEN DIRECTORY**
5 files, 1 folder
| 0 B

Name

/.git/
Exploit.class
Exploit.java
jndi\_marshalsec.py
marshalsec-0.0.3-SNAPSHOT-all.jar
README.md

Now what about less suspicious indicators like a residential IP hosting Plex, Grafana, and SSH for one of those servers because why not? In some cases, this could be a simple instance of UPnP forwarding ports on the user's behalf so they don't have to manually port forward products they want accessible outside of their home. With remote access services open to the internet though, this creates unwanted attention towards your network. It'll most likely be benign scanners but of

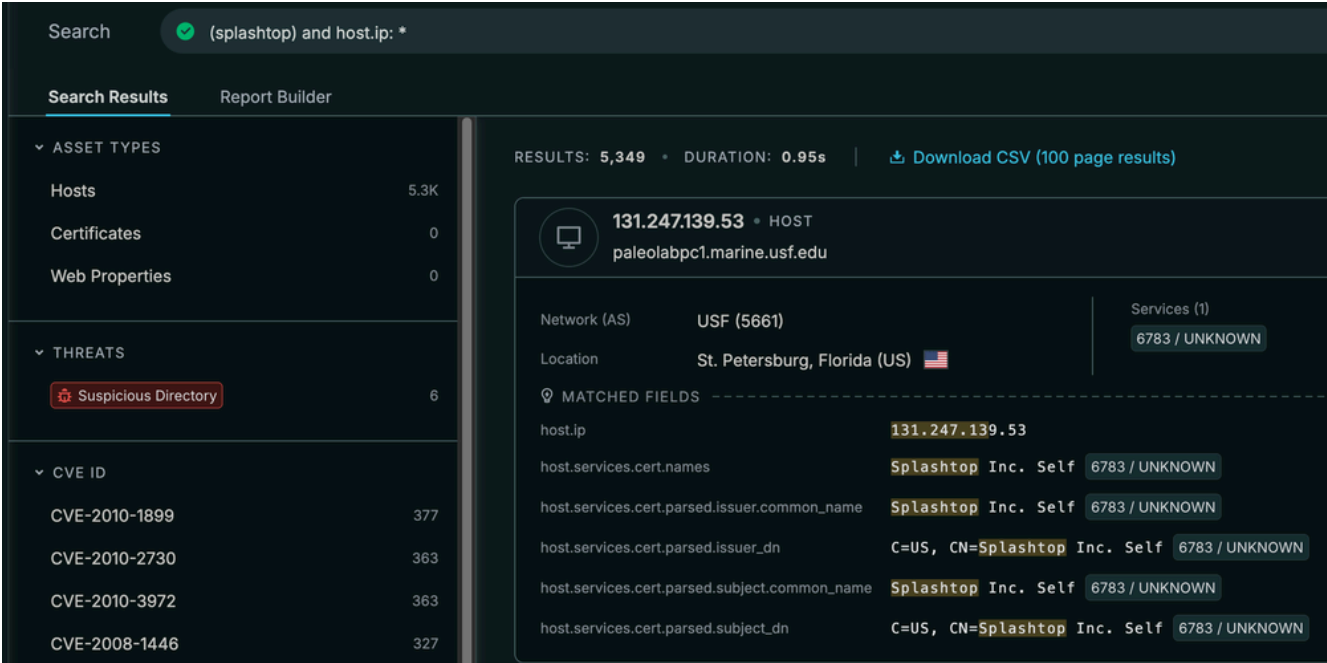
course the internet isn't all safe. It can also attract scanners attempting to exploit vulnerable services or brute force login prompts with default configurations. See Zensec's latest [report](#) on Medusa/DragonForce abusing RMM tools.

In any case, I wanted to explore RMM tools since leaving remote access ports open to the internet poses some serious risks of unwanted users gaining access to not just the network but remote management of desktops/laptops. One of those risks is exemplified in an earlier [post](#) showing how an exposed Docker API port can result in crypto miners and botnet activity.

Looking back at some intel reporting, one RMM tool I didn't know much about was Splashtop. It has been used by [Medusa Group](#), [APT44](#), and [Scattered Spider](#) so it has a notorious history of being used for nefarious activities. In the case of APT44:

The use of RMM software allowed the threat actor to retain critical C2 functions while masquerading as a legitimate utility, which made it less likely to be detected than a remote access trojan (RAT).

Not knowing much about the tool beforehand besides it being for remote management, I did a simple keyword search in Censys to uncover any hosts exposing a Splashtop connection.



(splashtop) and host.ip: \*

There are over 5,000 results and surely not *all* of them are Splashtop services. Right? Looking at the ports list, the most common is 6783 / UNKNOWN with 443 / HTTP in close second. Yes 443 is HTTPS but Censys protocol labels don't separate HTTP from HTTPS. Since 6783 isn't tied to any protocol, it most likely isn't related to a login portal.

Search ✓ ((splashtop) and host.ip: \*) and host.services.port = "6783"

Search Results Report Builder

Download the current page of results as a CSV

RESULTS: 2,796 • DURATION: 1.33s | [Download CSV \(100 page results\)](#)

131.247.139.53 • HOST  
paleolabpc1.marine.usf.edu

Network (AS) USF (5661) Location St. Petersburg, Florida (US)

Services (1) 6783 / UNKNOWN

MATCHED FIELDS

host.ip	131.247.139.53
host.services.cert.names	Splashtop Inc. Self 6783 / UNKNOWN
host.services.cert.parsed.issuer.common_name	Splashtop Inc. Self 6783 / UNKNOWN
host.services.cert.parsed.issuer_dn	C=US, CN=Splashtop Inc. Self 6783 / UNKNOWN
host.services.cert.parsed.subject.common_name	Splashtop Inc. Self 6783 / UNKNOWN
host.services.cert.parsed.subject_dn	C=US, CN=Splashtop Inc. Self 6783 / UNKNOWN
host.services.port	6783 6783 / UNKNOWN

ASSET TYPES

Hosts	2.8K
Certificates	0
Web Properties	0

CVE ID

CVE-2010-1899	376
CVE-2010-2730	363
CVE-2010-3972	363
CVE-2008-1446	326
CVE-2009-2521	326

More ▾

KNOWN EXPLOITED

((splashtop) and host.ip: \*) and host.services.port = "6783"

Looking at any host matching that query, the certificate name seems very common. So common in fact that I generated a report to group all events by `host.services.cert.names` and found the assumption to be true.

- 99% of hosts have a cert name "Splashtop Inc. Self CA"
- 0.5% have "SRS"
- 0.07% have "\*.relay.splashtop.com"

This still doesn't explain "what" port 6783 is though. Time to find some documentation.

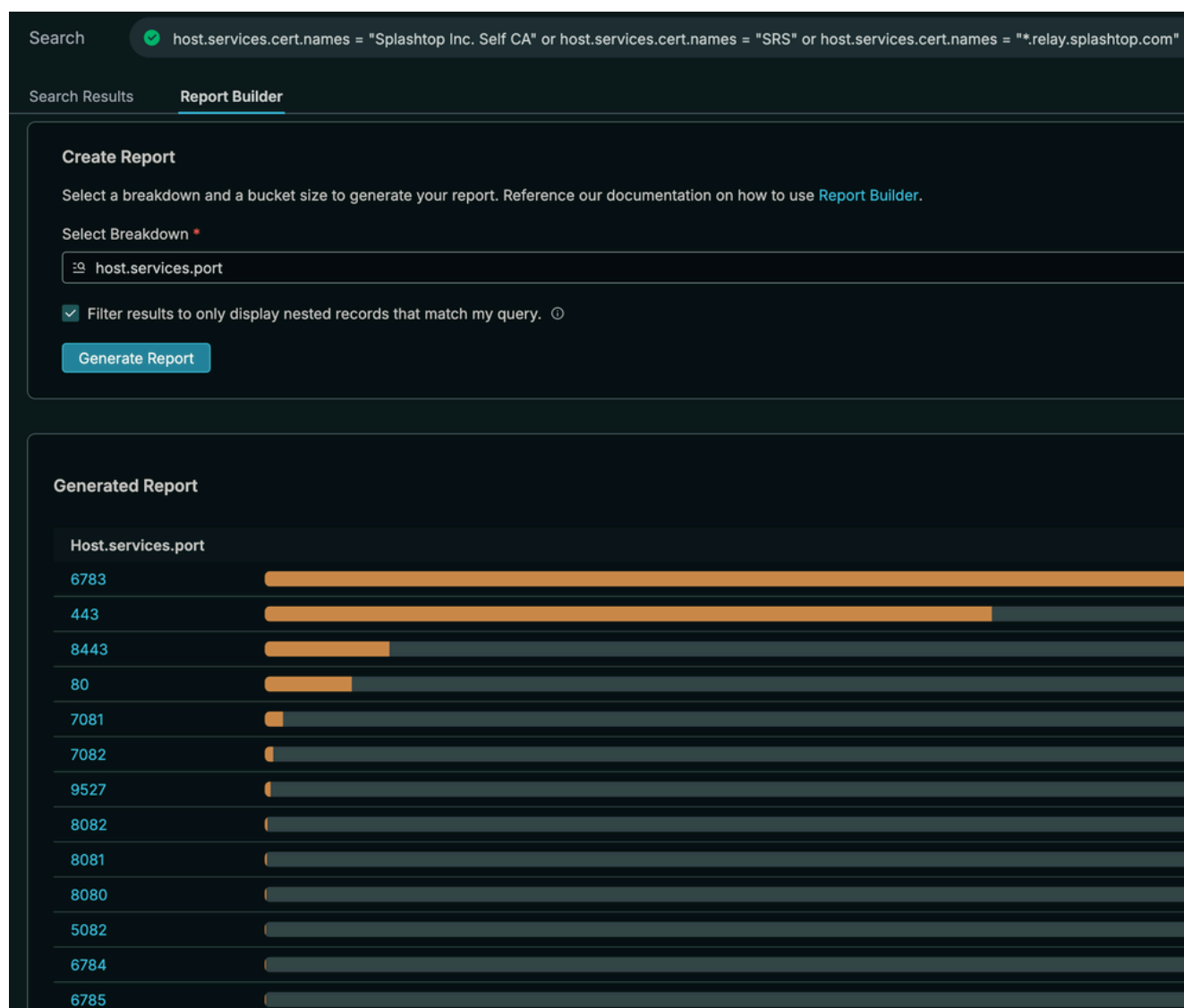
- <https://support-splashtopbusiness.splashtop.com/hc/en-us/articles/360038221472-Enabling-Direct-connection-Local-Connections>
- <https://support-splashtoponprem.splashtop.com/hc/en-us/articles/900000397406-Splashtop-Streamer-settings>

Splashtop remote connections can be local (peer to peer) or remote through Splashtop relay servers. Local connections, by default, use port TCP 6783.

That guide answers a few questions:

- This documentation deals with Splashtop Streamer. "Install the Splashtop Streamer on any Windows, Mac, or Linux computers that you want to remotely access, view, and control from another device using the Splashtop app."
- Splashtop remote connections are handled by Splashtop relay servers.
- The default (although configurable) port is 6783.

- The other two SSL certificate names make sense. SRS is most likely short for Splashtop Relay Service and they also use wildcard relay certs.
- The default port isn't a specific filter anymore after doing the inverse of combining the three certificate names and pivoting on port.



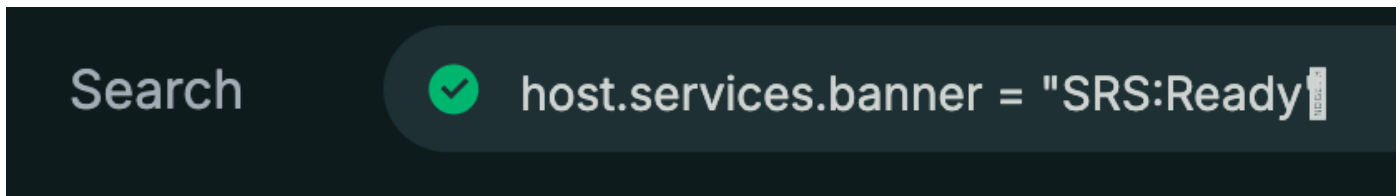
The list keeps going

## Banner Hash & Port

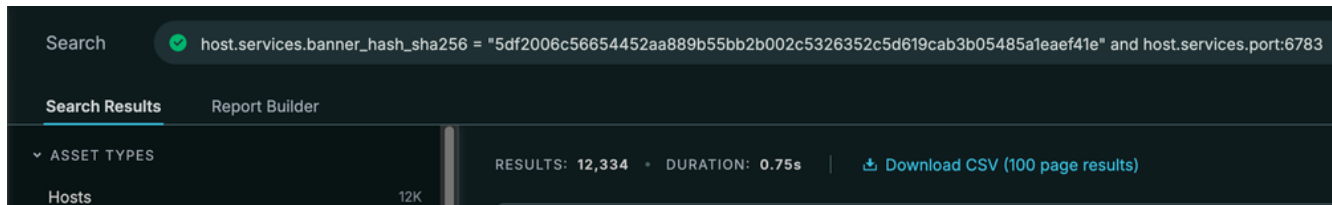
The first query really only covered any service on port 6783 and had the keyword Splashtop. That's not very specific and with thousands of results, it's prone to false positives.

I decided to pivot on another common value but included the port again to add some level of confidence. Even though the port can be changed, there are plenty of results to help find more commonalities across a host running Splashtop Streamer. That common value is the banner header for each response: `SRS:Ready\u0000`

The last few characters represent null value. Even though in search it just appends a blank space, it's not very user friendly to type in and can also be easy to forget.



Instead, I opted to use the banner hash of that value.

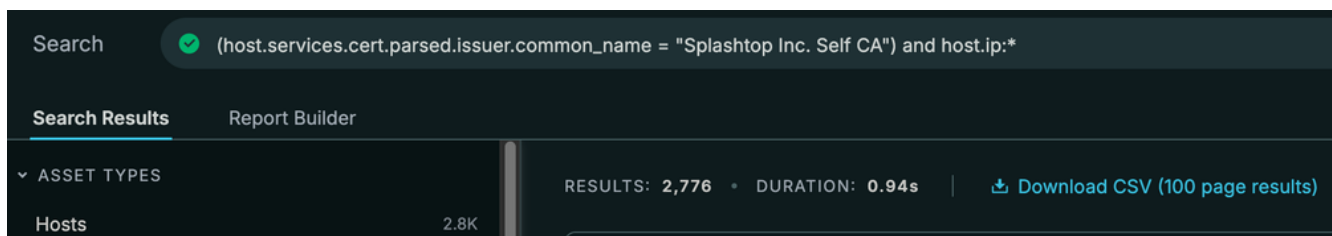


With over 12k results, this query was not much better but it could possibly be used in conjunction with another query in the future.

## SSL

Next is to focus on SSL content. From the first query, there were 3 common certificate names shared amongst these results.

The first being the most common certificate name "Splashtop Inc. Self CA". Based on a majority of operating systems and other services being related to desktops, this is a self-signed certificate by Splashtop for the Streamer software.



This second certificate is a bit more interesting. I included more in the screenshot because what stood out to me is there are only two ASNs. All but one are tied to CELLCO-PART which operates as Verizon Business. Even when I removed the port number from the filter, the results stayed the same.



Search ✓ (((splashtop) and host.ip: \*) and host.services.port = "6783") and host.services.cert.names = "SRS"

**Search Results** | Report Builder

ASSET TYPES	Count
Hosts	16
Certificates	0
Web Properties	0


PROTOCOLS	Count
UNKNOWN	16


TRANSPORT PROTOCOLS	Count
TCP	16

PORTS	Count
6783	16

NETWORKS (AS)	Count
CELLCO-PART	15
AS-WAVE-1	1


RESULTS: 16 • DURATION: 0.35s | [Download CSV \(16 page results\)](#)


**166.139.163.71 • HOST**

Network (AS)	CELLCO-PART (6167)	Services	6783 / U
Location	Euleless, Texas (US) 		

MATCHED FIELDS

host.ip	166.139.163.71
host.services.cert.names	SRS 6783 / UNKNOWN
host.services.cert.parsed.issuer.organization	Splashtop Inc. 6783 / UNKNOWN
host.services.cert.parsed.issuer_dn	n Jose, O=Splashtop Inc., OU= 67
host.services.cert.parsed.subject.organization	Splashtop Inc. 6783 / UNKNOWN
host.services.cert.parsed.subject_dn	n Jose, O=Splashtop Inc., OU= 67
host.services.port	6783 6783 / UNKNOWN


**166.139.163.72 • HOST**

(((splashtop) and host.ip: \*) and host.services.port = "6783") and host.services.cert.names = "SRS"

## Cellco Partnership

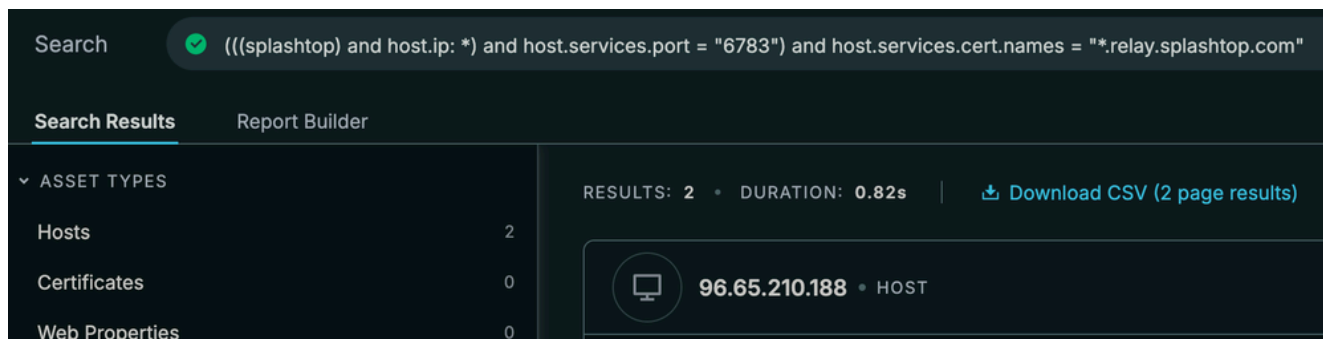


The certificate also has "Android" as the Organizational Unit which indicates these are for mobile systems. My guess here based on some more documentation is the Android signature is used for the Android Remote Control service for Splashtop Enterprise and Remote Support.

- <https://www.splashtop.com/blog/remote-access-view-control-android-phones-tablets>
- <https://www.splashtop.com/solutions/remote-desktop/android>

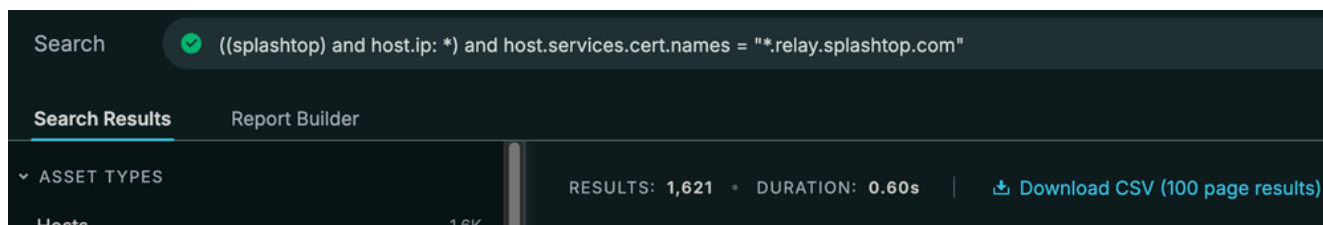
SRS is most likely the mobile Splashtop Relay Service which leads to the next question. Why is there another certificate called "\*.relay.splashtop.com"?

The last certificate only has two results. Knowing that port 6783 is default and enough documentation has showed me that other services use different ports, I removed it and the data became a lot more interesting.



`(((splashtop) and host.ip: ) and host.services.port = "6783") and host.services.cert.names =  
".relay.splashtop.com"`

Most of the results here are on 443.



`(((splashtop) and host.ip: ) and host.services.cert.names = ".relay.splashtop.com"`

Looking for [more information](#) on relay servers, this certificate seems to be used for the wider range of data relays while the previous cert focused just on mobile relay connectivity. So all hosts in this query operate as relay servers.

## Allowing Communication with Splashtop Servers

If firewall restrictions are affecting Splashtop, and your firewall supports domain-based rules, you can allow the following domains to restore connectivity:

Service Region	Domains	Purpose
All	*.api.splashtop.com	API and session services
All	*.relay.splashtop.com	Data relay
All	update.splashtop.com update-g3.splashtop.com	Streamer and app auto-updates
EU	*.api.splashtop.eu	API and session services
OC	*.api.splashtop.nr	API and session services

The asterisk (\*) represents a wildcard — it covers all subdomains under the root domain.

[How to find your Splashtop service region](#)

## Cleaning Up

I just showed a bunch of queries so I'll do my best to organize them in a way that can be used for tagging. If you weren't aware, the new Censys Platform includes Collections which allow you to store queries in the platform and monitor them over time.



## Splashtop Streamer

This query provides a good list of hosts using the identified Splashtop Streamer certificate with the hash of the banner response `SRS:Ready\u0000`. It doesn't include the default port since that was proven to not be the case for every host. At the time of writing, there are 2,610 active hosts. The `host.ip:*` option at the end isn't required. I just like to include it to look for only hosts and not web properties.

```
(host.services.cert.parsed.issuer.common_name = "Splashtop Inc. Self CA" and  
host.services.banner_hash_sha256 =  
"5df2006c56654452aa889b55bb2b002c5326352c5d619cab3b05485a1eaf41e") and host.ip:*
```

Splashtop Streamer Query

## Splashtop Relay

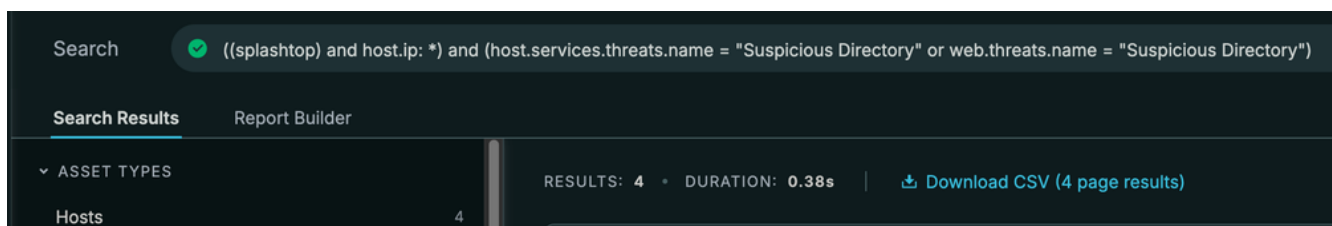
The certificates seemed to be the more important assets when looking at relays. I included both the mobile and general data relays into one since they both play a similar role. The `splashtop` keyword at the end helps reduce the false positive rate since I noticed unrelated services also having a certificate name `SRS`.

```
(host.services.cert.names = "SRS" or host.services.cert.names = "*.relay.splashtop.com") and  
splashtop
```

Splashtop Relay Query

## The Malware

From the first Splashtop query, you may have noticed a "Suspicious Directory" threat label. If not, surprise! Suspicious directories are open directories but hosting possibly malicious files. In this query, I'm just filtering on anything with the Suspicious Directory threat name.



```
((splashtop) and host.ip: *) and (host.services.threats.name = "Suspicious Directory" or web.threats.name  
= "Suspicious Directory")
```

From the results, none of the hosts are actually running Splashtop but they are hosting files where the filename *contains* Splashtop, among other things.



With 4 hosts, I'll pick one that really stands out.

**2600:3c02::f03c:91ff:fe91:b370** • HOST

Suspicious Directory

12 CVEs

OPEN\_DIRECTORY

REMOTE\_ACCESS

OS

Canonical Linux

Network (AS)

AKAMAI-LINODE-AP Akamai Connected Cloud (63949)

Location

Atlanta, Georgia (US)

Services (4)

21 / FTP 22 / SSH 80 / HTTP 443 / HTTP

Software (3)

Vsftpd Project Vsftpd 3.0.5 Openbsd Openssh 8.2 Apache Httpd 2.4.41

MATCHED FIELDS

-----

host.ip

2600:3c02::f03c:91ff

host.services.endpoints.open\_directory.files.name

Splashtop\_Personal\_ 80 / HTTP 443 / HTTP

host.services.endpoints.open\_directory.files.path

/Splashtop\_Personal\_ 80 / HTTP 443 / HTTP

host.services.threats.name

Suspicious Directory 80 / HTTP 443 / HTTP

IPv6, FTP, SSH, and HTTP. Not weird at all.

To see just how suspicious this IP is, I wanted to query it in VirusTotal but IPv6 isn't really something we can query, so what's next?

SSH key pivot! This revealed the IPv4 equivalent host.

Search

host.services.ssh.server\_host\_key.fingerprint\_sha256 = "2a4c3084ab5554e8111fd48af142e2fafc96611f339cec09e8dc7dd930044fc"

Search Results

Report Builder

ASSET TYPES

Hosts

2

Certificates

0

Web Properties

0

THREATS

Suspicious Directory

4

CVE ID

CVE-2016-20012

2

CVE-2020-12062

2

CVE-2020-14145

2

CVE-2020-15778

2

CVE-2021-28041

2

More

KNOWN EXPLOITED

THIRD\_PARTY

4

SOFTWARE VENDORS

apache

4

RESULTS: 2 • DURATION: 0.19s | Download CSV (2 page results)

**45.79.214.229** • HOST

www.wirsz.com

Suspicious Directory

12 CVEs

OPEN\_DIRECTORY

REMOTE\_ACCESS

OS

Canonical Linux

Network (AS)

AKAMAI-LINODE-AP Akamai Connected Cloud (63949)

Location

Atlanta, Georgia (US)

Services (4)

21 / FTP 22 / SSH 80 / HTTP 443 / HTTP

Software (3)

Vsftpd Project Vsftpd 3.0.5 Openbsd Openssh 8.2 Apache Httpd 2.4.41

MATCHED FIELDS

-----

host.services.ssh.server\_host\_key.fingerprint\_sha256

2a4c3084ab5554e8111fd48af142e2fafc96611f339cec09e8dc7dd930044fc 22 / SSH

**2600:3c02::f03c:91ff:fe91:b370** • HOST

Suspicious Directory

12 CVEs

OPEN\_DIRECTORY

REMOTE\_ACCESS

OS

Canonical Linux

Network (AS)

AKAMAI-LINODE-AP Akamai Connected Cloud (63949)

Location

Atlanta, Georgia (US)

Services (4)

21 / FTP 22 / SSH 80 / HTTP 443 / HTTP

Software (3)

Vsftpd Project Vsftpd 3.0.5 Openbsd Openssh 8.2 Apache Httpd 2.4.41

MATCHED FIELDS

-----

host.services.ssh.server\_host\_key.fingerprint\_sha256

2a4c3084ab5554e8111fd48af142e2fafc96611f339cec09e8dc7dd930044fc 22 / SSH

host.services.ssh.server\_host\_key.fingerprint\_sha256 =  
 "2a4c3084ab5554e8111fd48af142e2fafc96611f339cec09e8dc7dd930044fc"

11/13

Looking for some files in this directory on VirusTotal, a ZIP file actually contains some WinVNC malware. Other files not found on VirusTotal but present inside the open directory were other remote access tools like TeamViewer, AnyDesk, Remote Assistant Setup, Splashtop Streamer, and Splashtop Personal.

8 / 66

Community Score

8/66 security vendors flagged this file as malicious

0d43037c88cca3566f171a19469cd09664d84906a91c248db7e18261d73c677f

PC%20Lean%20Tools.zip

Size5.87 MB

Last Analysis Date5 months ago

ZIP

zip checks-usb-bus contains-pe detect-debug-environment long-sleeps checks-user-input

DETECTION

DETAILS

RELATIONS

BEHAVIOR

CONTENT

TELEMETRY

COMMUNITY

Crowdsourced Sigma Rules

CRITICAL 0

HIGH 0

MEDIUM 0

LOW 3

Matches rule Stop Windows Service by Jakob Weinzettl, oscd.community, Nasreddine Bencherchali at Sigma Integrated Rule Set (GitHub)

↳ Detects a windows service to be stopped

Matches rule Creation of an Executable by an Executable by frack113 at Sigma Integrated Rule Set (GitHub)

↳ Detects the creation of an executable by another executable

Matches rule Net.exe Execution by Michael Haag, Mark Woan (improvements), James Pemberton / @4A616D6573 / oscd.community (improvements) at Sigma Integrated Rule Set (GitHub)

↳ Detects execution of Net.exe, whether suspicious or benign.

Security vendors' analysis on 2025-05-16T16:44:15 UTC

Popular threat label

trojan.winvnc

Threat categories

trojan hacktool

Family labels

winvnc

Alibaba	RiskWare:Win32/WinVNC.cf061225	AliCloud	Backdoor[rat]:Win/WinVNC.cd4a062b
GData	Win32.Application.Piriform.A	Jiangmin	RemoteAdmin.WinVNC.fz
Kaspersky	Not-a-virus:RemoteAdmin.Win32.WinVN...	Kingsoft	Malware.kb.a.973
NANO-Antivirus	Trojan.Win32.Generic.ktdauh	Rising	Trojan.Avkiller!8.FAD (CLOUD)

To reiterate two key points at the beginning:

- Medusa installed AnyDesk *after* exploiting a SimpleHelp vulnerability.
- From the APT44 report:

The use of RMM software allowed the threat actor to retain critical C2 functions while masquerading as a legitimate utility, which made it less likely to be detected than a remote access trojan (RAT).

RMM tools left open to the public aren't only susceptible to exploitation and remote access from unwanted users. They are also used as a persistence mechanism to maintain access after getting into an environment which can be gleamed from the VirusTotal screenshot above.

## Conclusion

This post shows just how prevalent RMM tooling is for threat actors and how important it is to secure your devices at home. Just like how you can check HavelBeenPwned for your email address in data breaches, I'd recommend querying a service like Censys or Shodan to figure out if

there are any public services being hosted on your WAN. If you're unsure what that IP might be, you can visit <https://www.whatsmyip.org/> or if the CLI is more your speed, `curl ipinfo.io/ip`. If your IP is hosting any services, ensure you know why, then find a better way to make them accessible from outside. Maybe setup a Wireguard tunnel, Tailscale if you want a mesh Wireguard network, or host them through a reverse proxy like Traefik or Nginx.

## References

---

- <https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/>
- <https://attack.mitre.org/groups/G1051/>
- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>

### [Hunting for EDR-Freeze](#)

[EDR bypassing has become a technique of choice for threat actors and has enabled a market of tools being sold on cybercrime forums: \\* Unit42 uncovered a variant of EDRSandBlast being sold on XSS and Exploit. \\* CheckPoint Research uncovered the use of a vulnerable driver, Truesight.sys, which evaded the Microsoft](#)

### [Homelabs Don't End, They Improve](#)

[There's a never ending list of homelab projects, ways to build one, hardware requirements, goals for running one, single server or 24U rack, the list goes on. I started my journey long ago when I thought VirtualBox and an external HDD was all I needed. Fast forward to](#)

### [LNK Stomping](#)

[This PoC provided by Elastic is about LNK Stomping. Currently Microsoft has not provided a CVE for this method; however, they did release CVE-2024-38212, a MotW bypass vulnerability, but only included SmartScreen, not Smart App Control \(SAC\). As this testing is done on Windows 10 with build number 19045, I](#)

[Axelarator's Blog](#) © 2025