Latrodectus Malware Masquerades as AhnLab Security Software to Infect Victims

hunt.io/blog/latrodectus-malware-masquerades-as-ahnlab-security-software-to-infect-victims

TABLE OF CONTENTS

During a recent analysis of known Latrodectus infrastructure, our research team encountered a command-and-control (C2) server at **103.144.139.]189** after pivoting on the TLS certificates. Communicating with this server was a **file named MeDExt.dll**, detected as the downloader by multiple vendors in VirusTotal.

Leveraging this discovery, we were able to identify additional IP addresses and domains associated with the distribution of Latrodectus malware.

Latrodectus is a downloader that functions as a backdoor, allowing threat actors to execute remote commands, gather information from compromised machines, and deploy additional malicious payloads, the most recent being Brute Ratel C4.

In this blog post, we will examine the malicious DLL and then dive into the C2 infrastructure we uncovered, including the certificate pivot and the associated domains identified during our research.

MeDExt.dll

Unfortunately, we don't have the initial access method for this attack campaign, but as past reports suggest, phishing and malicious ads are likely entry points into networks.

The DLL file that caught our attention, "MeDExt.dll," mimics the legitimate MeD Engine Extension from **AhnLab Smart Defense**. Given that this malicious file is a DLL, it's plausible that the legitimate parent executable was bundled with the Latrodectus malware or that this was a targeted attack aimed at a victim known to use AhnLab's services.

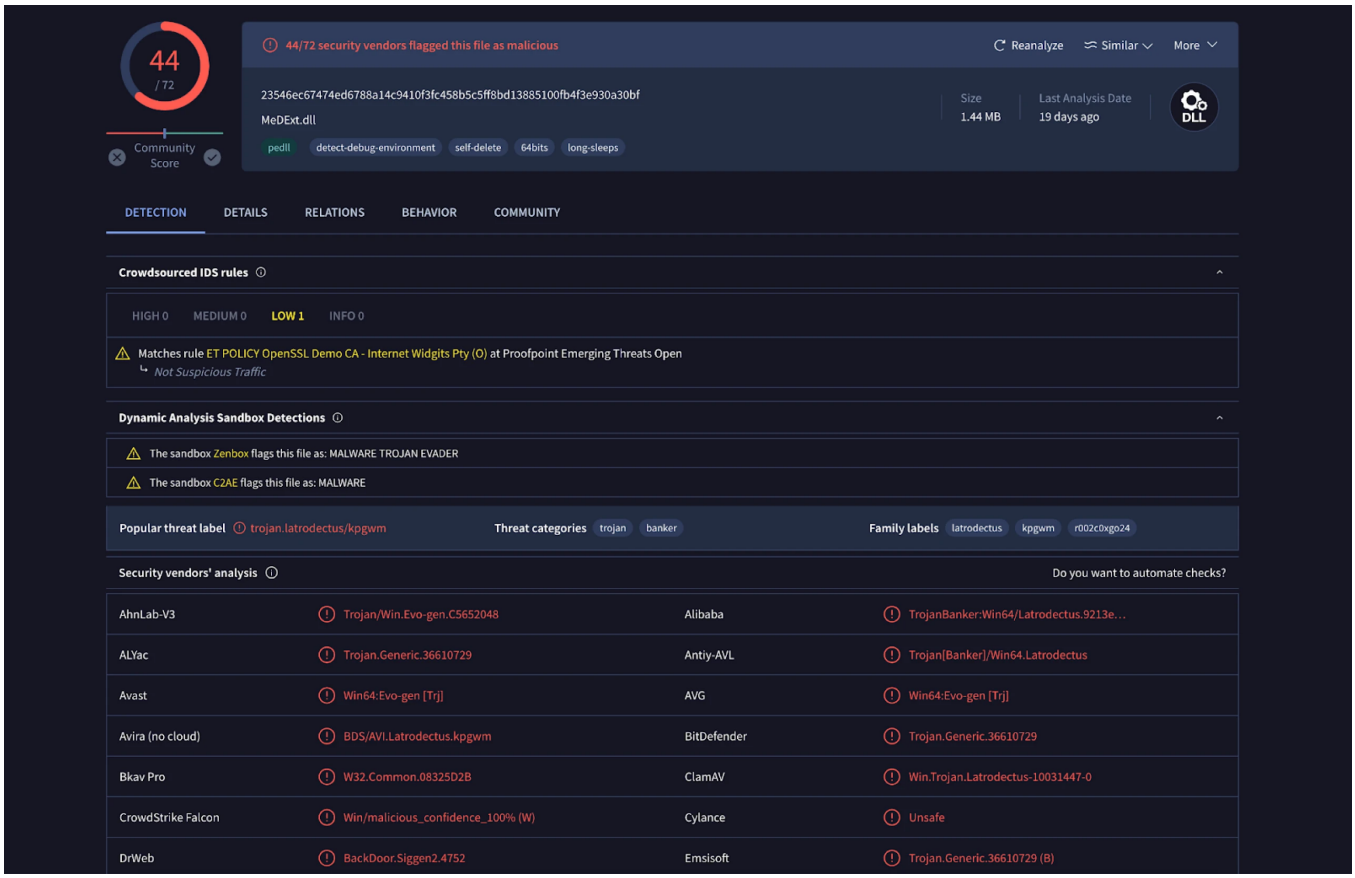


Figure 1: VirusTotal results for MeDExt.dll (Source: VirusTotal)
Spoofing a well-known anti-virus vendor increases the malware's stealth and the likelihood of bypassing security measures, reinforcing the importance of scrutinizing renamed files.

Below is the file signature info. Note the DLL is not signed.

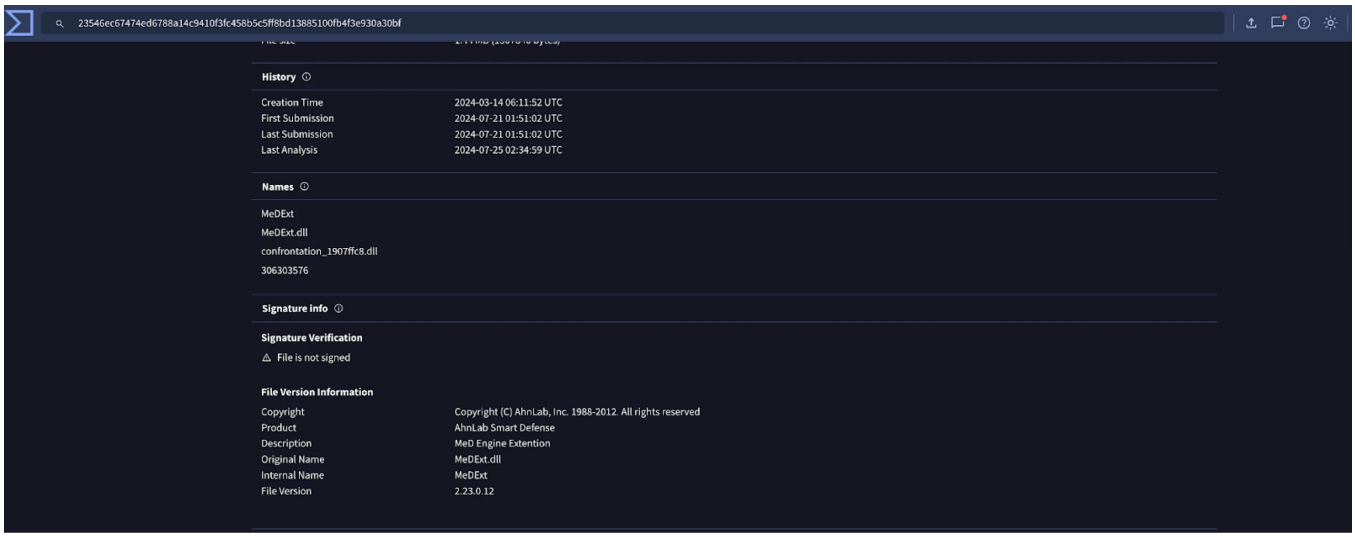


Figure 2: VirusTotal Signature Info for the suspect DLL

The PDB path (provided below) within the MeDExt.dll file offers a glimpse into the environment used by the threat actor(s)

C:\Build\Project\Medicine\Engine\2.0_MainTrunk\building\build\Project\Medicine\Engine\2.0\Trunk\Build\AMD64\free\MeDExt.pdb

The DLL has four exports with differing addresses, all following similar naming paths beginning with “MeDExt..”

Name	Address	Ordinal
MeDExtFinalize	0000000180003580	1
MeDExtGet	0000000180003630	2
MeDExtInitialize	0000000180003570	3
MeDExtSet	0000000180003590	4
DllEntryPoint	000000018000105D	[main entry]

Figure 3: Obligatory IDA screenshot showing the DLL’s exports

We could not identify any new TTPs during the analysis of the malicious file. This sample of Latrodectus employed familiar techniques, such as using the Windows Component Object Model (COM) to set a scheduled task for persistence.

Next, we'll examine the communication with the command and control infrastructure.

Command & Control Infrastructure Analysis

After running the file through multiple sandboxes, we observed Lactrodecuts attempting to communicate with the following domains + URLs:

- **stripplasst.]com/live/**
- **coolarition.]com/live/**

stripplasst.]com was registered through the OwnRegistrar, Inc. registrar, and coolarition[.]com through PDR Ltd. This consistent use of a single registrar should be used as a low-confidence indicator in tracking and attributing related malicious activity.

Both domains were unavailable during analysis, though we captured the first POST request to the C2 registering the victim's details in a PCAP, as seen below.

The IP address, 103.144.139.]189 for a short period resolved to the domain **riscoarchez[.]com**, also identified in a Latrodecuts attack paired with Brute Ratel C4 by Rapid7.

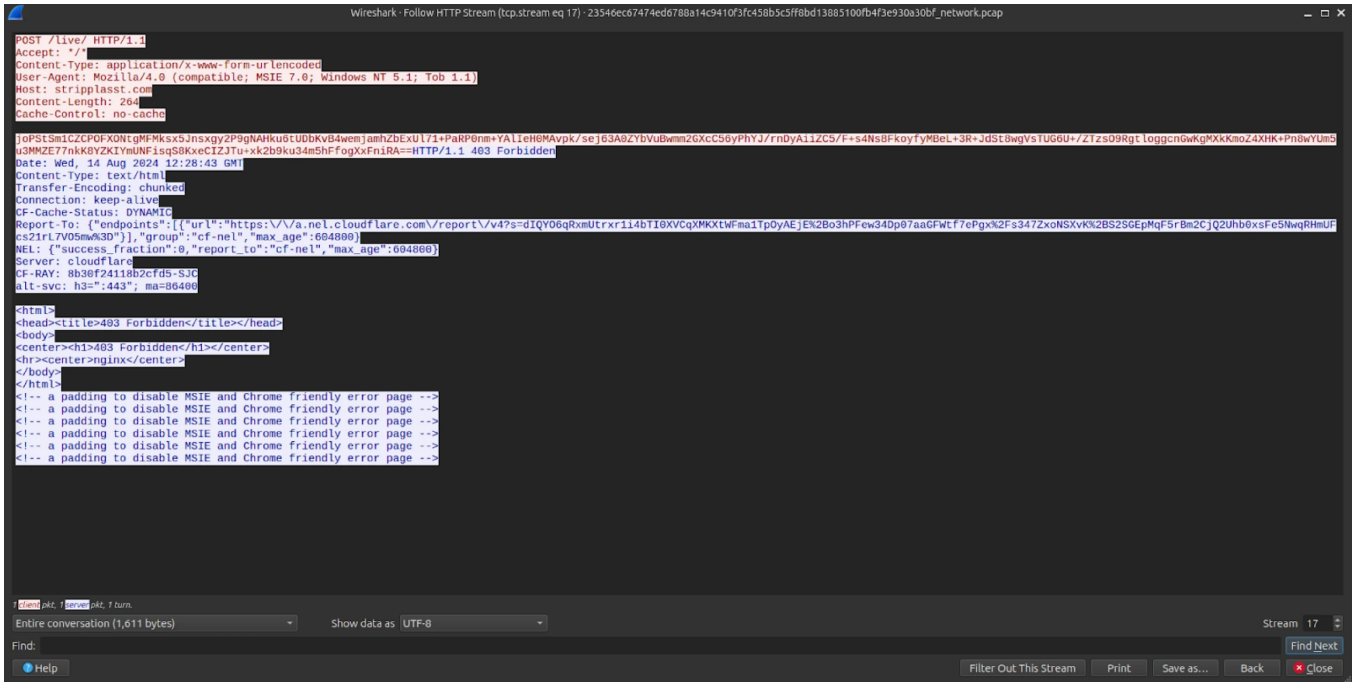


Figure 4: PCAP showing the initial registration request to one of the C2 domains.

The server that initiated our investigation is hosted on the Gigabit Hosting Sdn Bhd ASN.

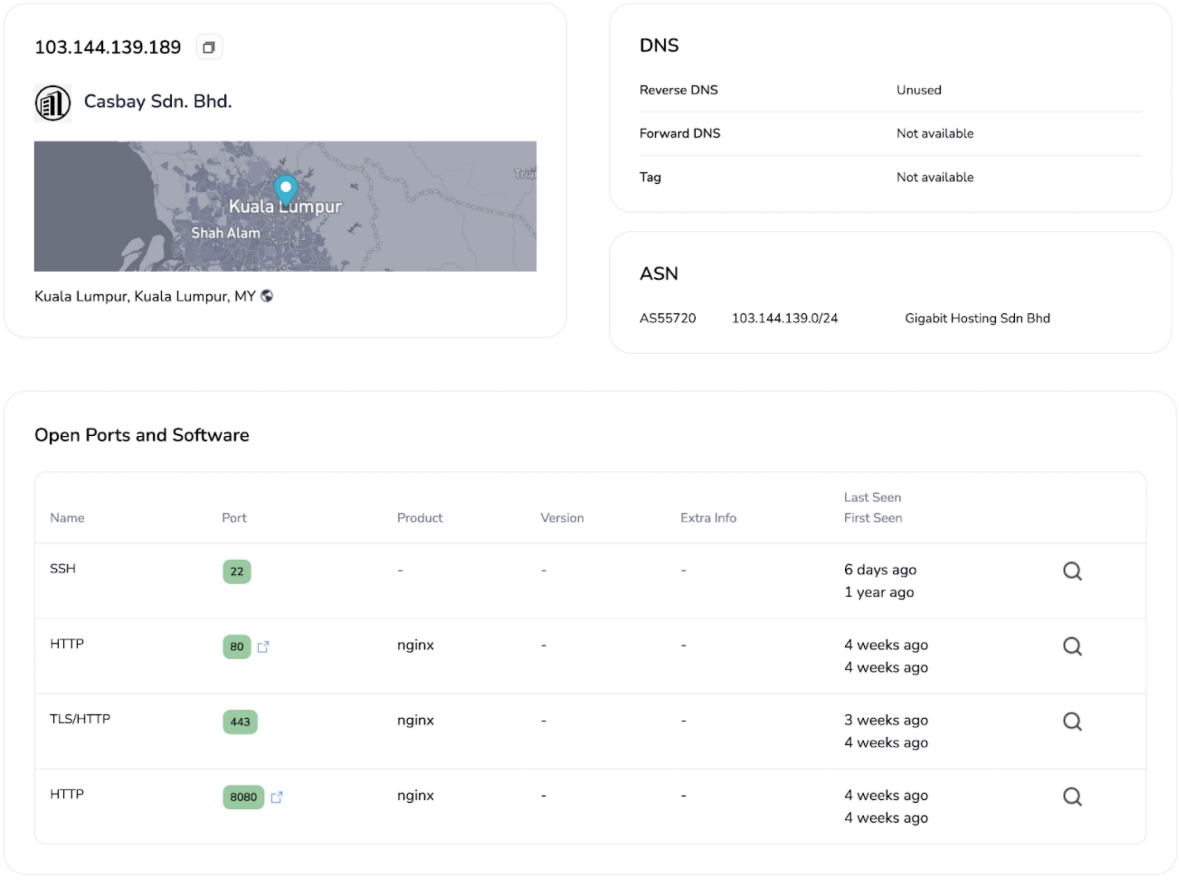


Figure 5: Initial IP that began our research (Link: here)
As reported by ProofPoint in their joint blog post with Team Cymru, we can see the server also has ports 443 and 8080 open, which were one of the criteria used to search for additional C2 servers in the article.

Moving to the SSL History, we noticed a semi-unique certificate on port 443. We say “semi” because many malware families use the “**Internet Widgits Pty Ltd**” Issuer Organization name in their self-signed certificates.

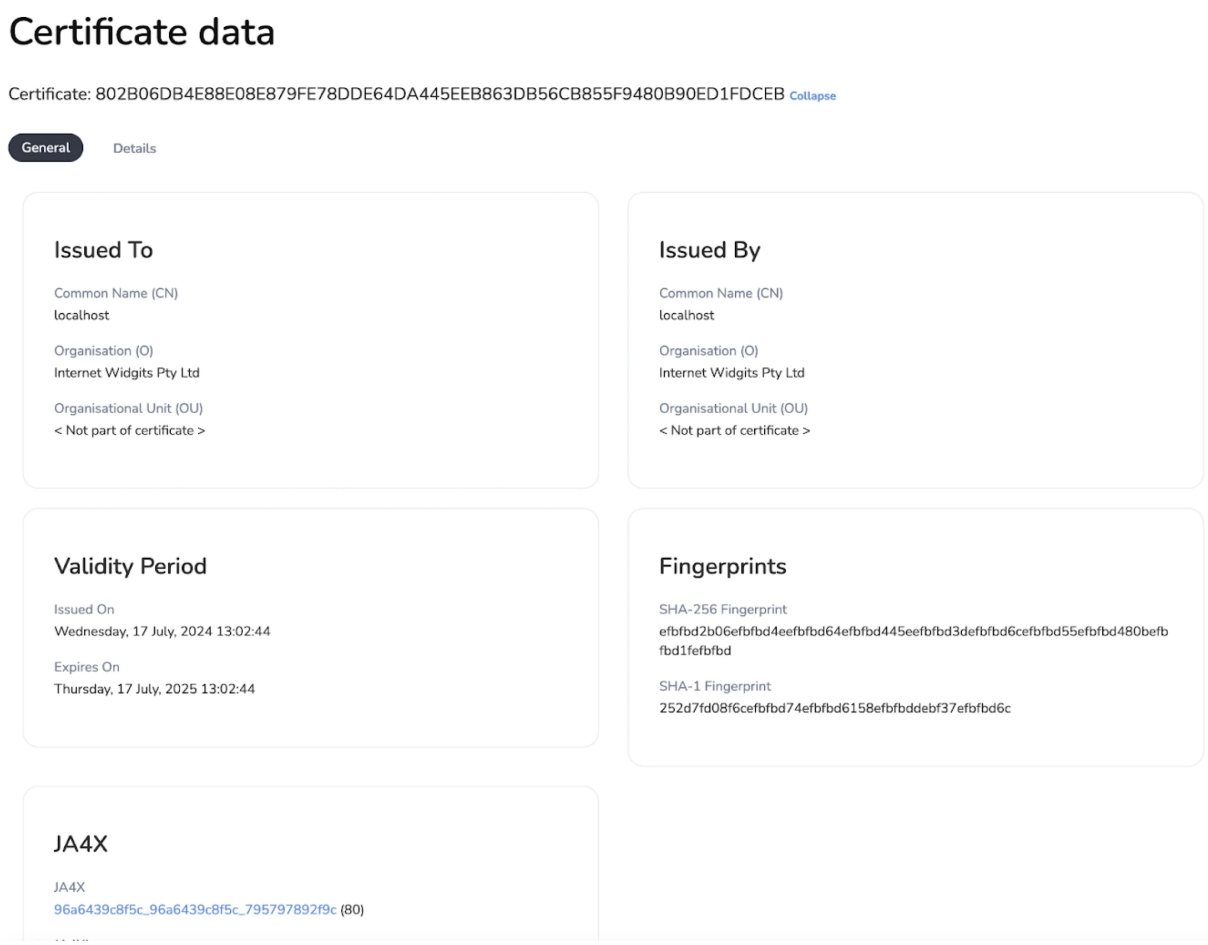


Figure 6: Hunt certificate data for 103.144.139.]189 (Try it here)
The complete certificate fields are below:

- Subject Common Name: localhost
- Subject Country: AU
- Subject Organization: Internet Widgits Pty Ltd
- Subject Organisational Unit: N/A
- Subject Locality: N/A
- Subject State: Some-State

We can use Hunt's Advanced Search feature to craft a query that will assist us in identifying servers using similar certificates as the above.

In the case of the Latrodectus C2 certs, we came up with the following query based on the JA4X hash and Subject Common Name:

ja4x:"96a6439c8f5c_96a6439c8f5c_795797892f9c" AND subject.common_name:"localhost"

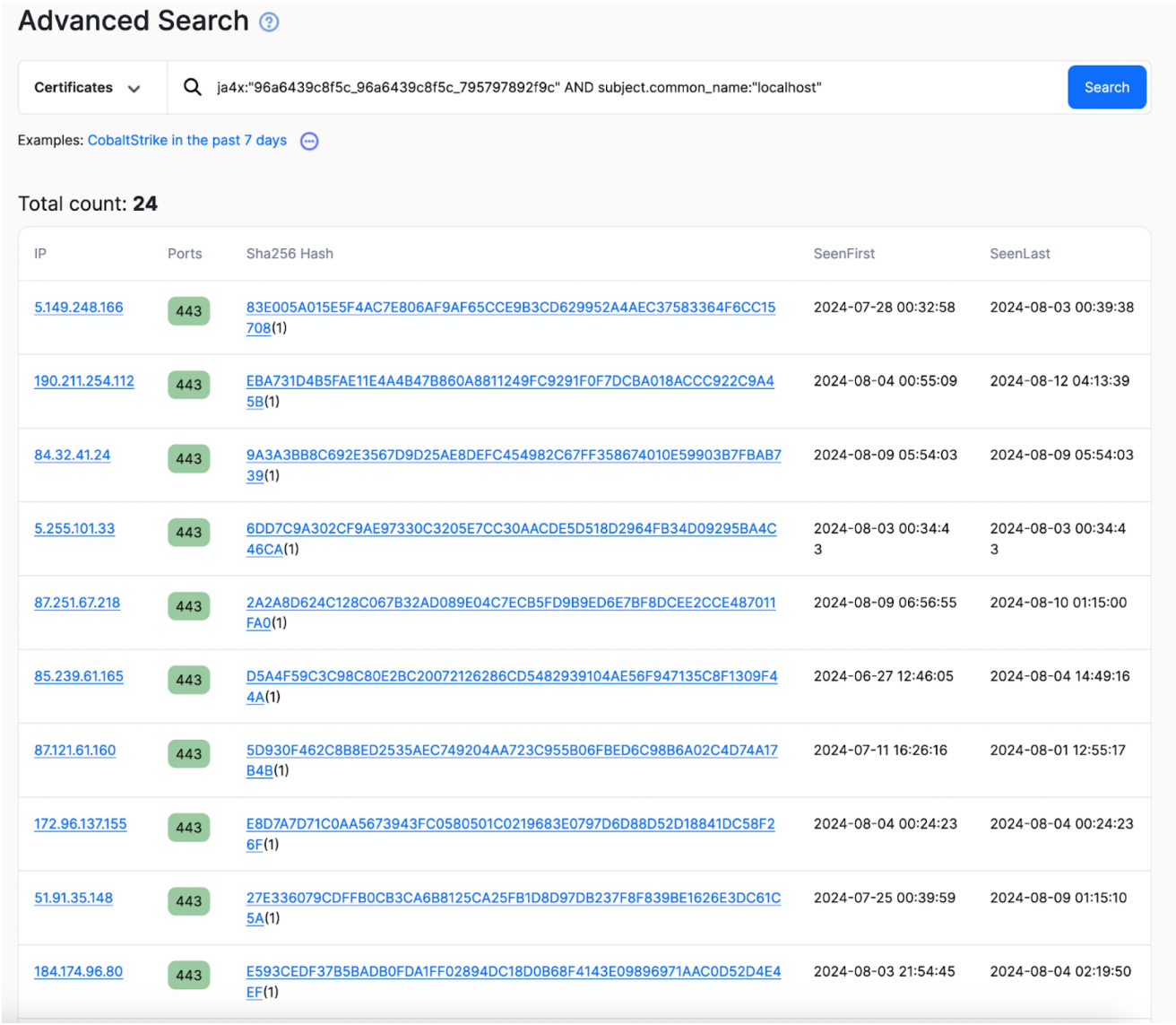


Figure 7: Hunt Advanced Search Results for the suspicious Latrodectus linked certificate (Try it out here)
The query returns just 24 results, suggesting we're on the right track in identifying Latrodectus servers. However, it's important to note that the certificate fields we're analyzing are commonly used for legitimate purposes and by other threat actors.

We cannot confirm that all results are linked to the malware; further investigation is required.

Poking around for similar server + certificate combinations on the same ASN as our initial IP, we found a malicious file mimicking the Google Authenticator app, also associated with Latrodectus communicating with **103.144.139.]182**.

The domain **spikeliftall.]com** resolves to the IP mentioned above, registered through **PDR Ltd**.

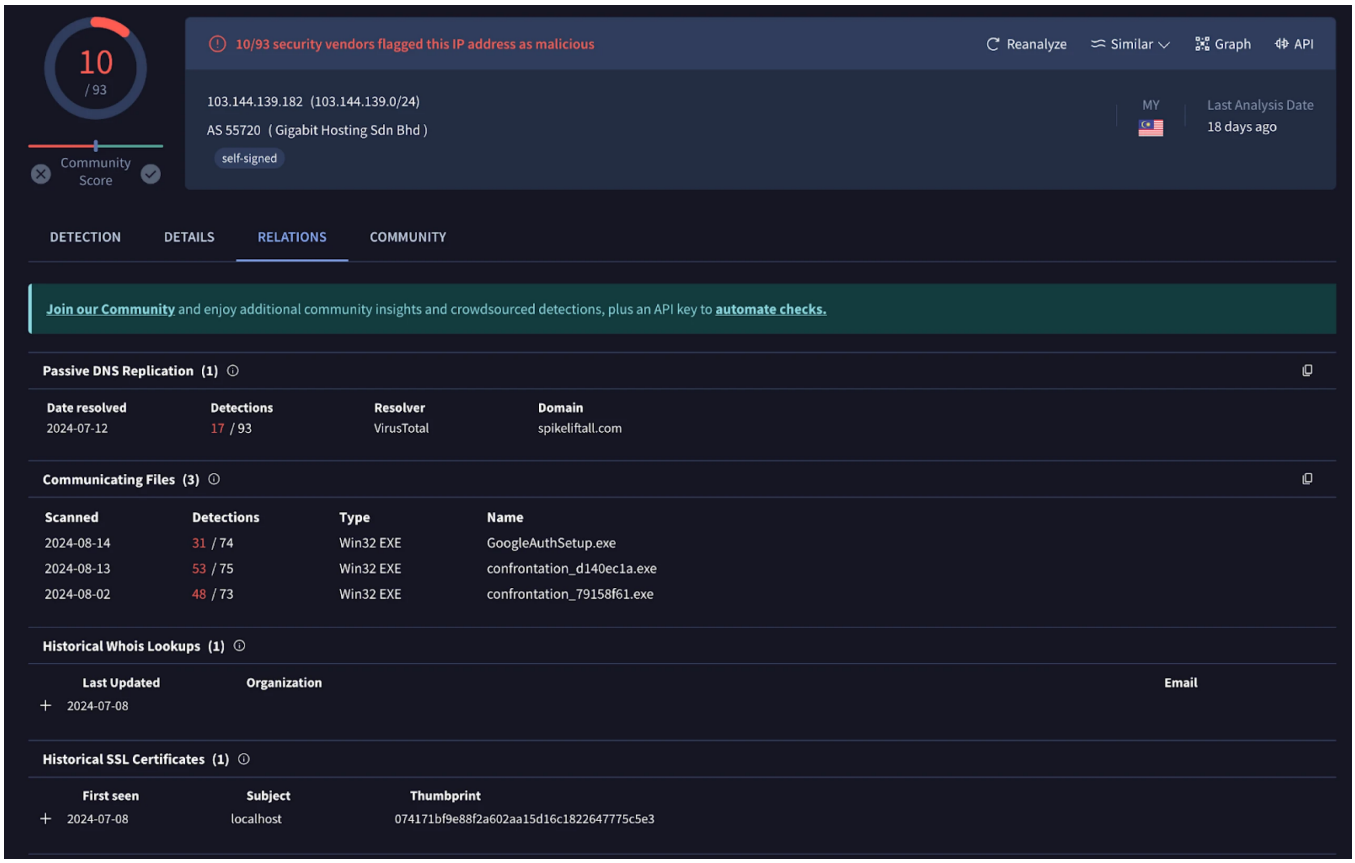
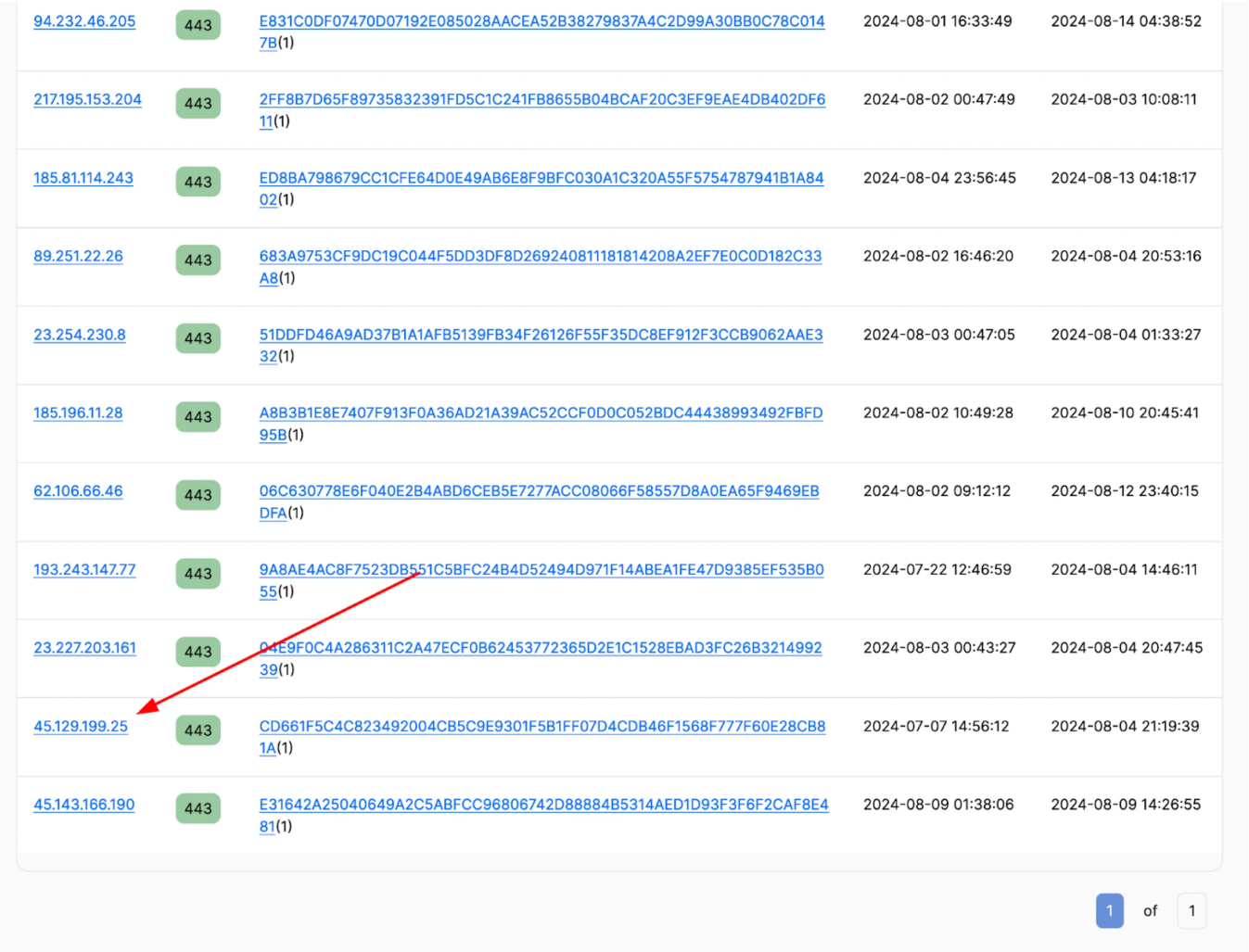


Figure 8: Another Lactrodectus C2 on the same ASN (Source: VirusTotal)
Again, this server also had port characteristics (443 & 8080) and a matching certificate seen with other command and control infrastructure.

On Aug 13, 2024, Symantec also noticed this campaign releasing a Protection Bulletin identifying the initial access vector as phishing.

After submitting a few IP addresses to VirusTotal for analysis, another server with a file detected as Latrodectus caught our attention.



94.232.46.205	443	E831C0DF07470D07192E085028AACEA52B38279837A4C2D99A30BB0C78C0147B(1)	2024-08-01 16:33:49	2024-08-14 04:38:52
217.195.153.204	443	2FF8B7D65F89735832391FD5C1C241FB8655B04BCAF20C3EF9EAE4DB402DF611(1)	2024-08-02 00:47:49	2024-08-03 10:08:11
185.81.114.243	443	ED8BA798679CC1CFE64D0E49AB6E8F9BFC030A1C320A55F5754787941B1A8402(1)	2024-08-04 23:56:45	2024-08-13 04:18:17
89.251.22.26	443	683A9753CF9DC19C044F5DD3DF8D2692408111818142 08A2EF7E0C0D182C33A8(1)	2024-08-02 16:46:20	2024-08-04 20:53:16
23.254.230.8	443	51DDFD46A9AD37B1A1AFB5139FB34F26126F55F35DC8EF912F3CCB9062AAE332(1)	2024-08-03 00:47:05	2024-08-04 01:33:27
185.196.11.28	443	A8B3B1E8E7407F913F0A36AD21A39AC52CCF0D0C052BDC44438993492FBFD95B(1)	2024-08-02 10:49:28	2024-08-10 20:45:41
62.106.66.46	443	06C630778E6F040E2B4ABD6CEB5E7277ACC08066F58557D8A0EA65F9469EBDFA(1)	2024-08-02 09:12:12	2024-08-12 23:40:15
193.243.147.77	443	9A8AE4AC8F7523DB551C5BFC24B4D52494D971F14ABEA1FE47D9385EF535B055(1)	2024-07-22 12:46:59	2024-08-04 14:46:11
23.227.203.161	443	04E9F0C4A286311C2A47ECF0B62453772365D2E1C1528EBAD3FC26B321499239(1)	2024-08-03 00:43:27	2024-08-04 20:47:45
45.129.199.25	443	CD661F5C4C823492004CB5C9E9301F5B1FF07D4CDB46F1568F777F60E28CB81A(1)	2024-07-07 14:56:12	2024-08-04 21:19:39
45.143.166.190	443	E31642A25040649A2C5ABFCC96806742D88884B5314AED1D93F3F6F2CAF8E481(1)	2024-08-09 01:38:06	2024-08-09 14:26:55

1 of 1

Figure 9: Additional suspicious IP associated with Latrodetus

The IP, hosted on BlueVPS OU, resolves to a single domain, **worlpquano.]com** registered through HOSTINGER, and used CloudFlare services in mid-July 2024.

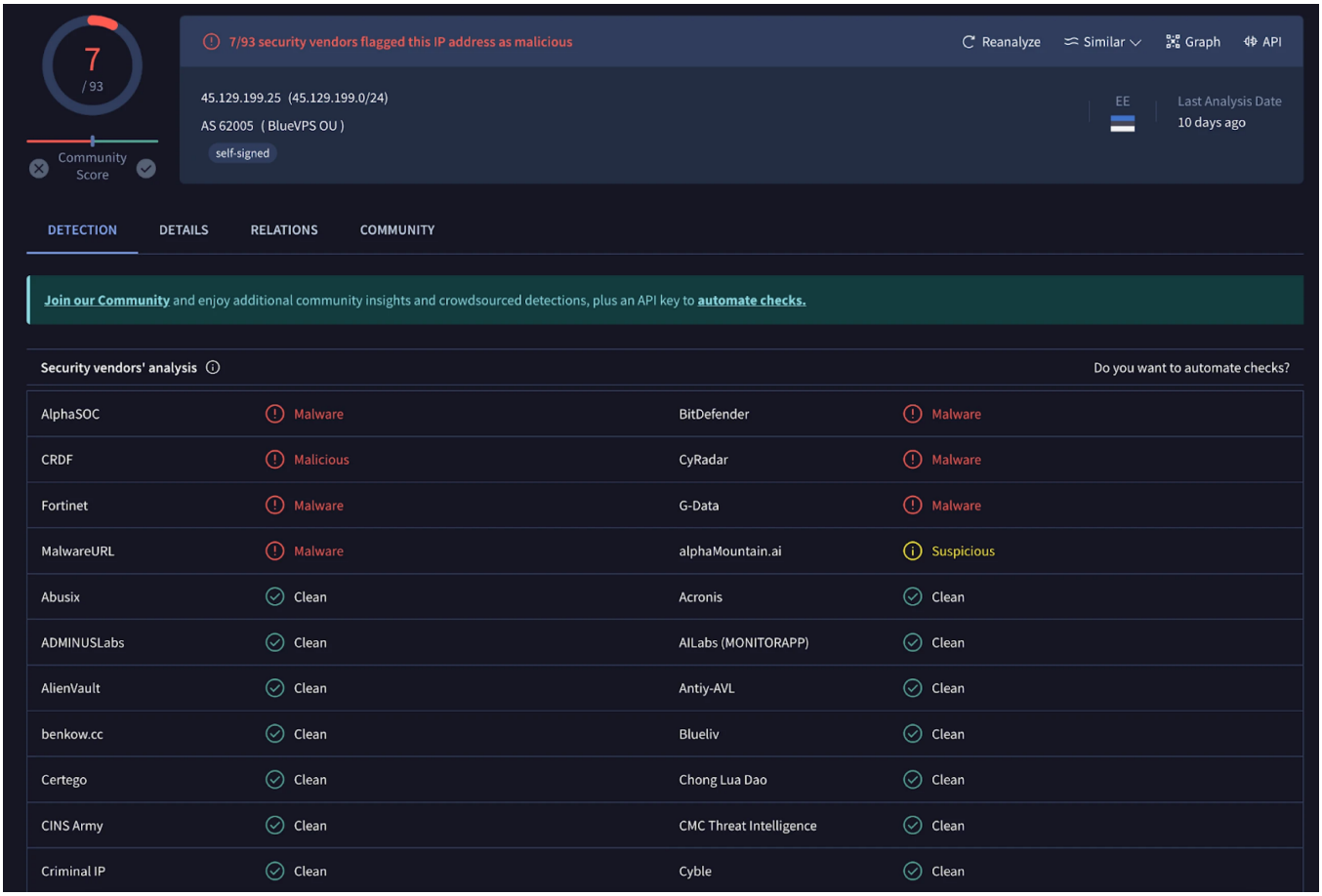


Figure 10: Third IP/domain associated with Latrodecuts scan results (Source: VirusTotal)

Conclusion

Latrodectus' tactic of impersonating legitimate security software highlights the persistent challenge of distinguishing between trusted and malicious files. Effective defense against such threats requires continuous monitoring and detailed analysis of network activity.

Request a demo today to get a closer look at how the Hunt platform can strengthen your defenses.

Network Observables

IP Address	Domain(s)	Domain Registrar	ASN	Notes
103.144.139.]189:443	riscoarchez.]com	Own Registrar	Gigabit Hosting Sdn Bhd	Initial IP that started investigation.
188.114.97.]7:443	stripplasst.]com	Own Registrar	CloudFlare	C2 for MeDExt.dll
188.114.97.]7:443, 84.32.41.]12:443	coolarition.]com	PDR Ltd.	CloudFlare, Hostgnome Ltd	C2 for MeDExt.dll
103.144.139.]182:443	spikeliftall.]com	PDR Ltd.	Gigabit Hosting Sdn Bhd	Jarm fingerprint + HTML response hash
45.129.199.]25:443	worlpquano.]com	HOSTINGER	BlueVPS OU	Identified as a possible Latrodectus C2 by Symantec

Host Observables

File Name	SHA-256 Hash	Notes
MeDExt.dll	23546ec67474ed6788a14c9410f3fc458b5c5ff8bd13885100fb4f3e930a30bf	Seen communicating with riscoarchez.]com/live/ stripplasst.]com/live/ coolartiion.]com/live/

File Name	SHA-256 Hash	Notes
GoogleAuthSetup.ex	62536e1486be7e31df6c111ed96777b9e3f2a912a2d7111253ae6a5519e71830	Seen communicating with steamcommunity.]com/profiles/76 godfaetret.]com/live/ spikeliftall.]com/live/
confrontation_d46a184c.exe	a459ce4bfb5d649410231bd4776c194b0891c8c5328bafc22184fe3111c0b3e7	Seen communicating with worlpquano.]com/live/ carflotyup.]com/live/

TABLE OF CONTENTS

During a recent analysis of known Latrodectus infrastructure, our research team encountered a command-and-control (C2) server at **103.144.139.]189** after pivoting on the TLS certificates. Communicating with this server was a **file named MeDExt.dll**, detected as the downloader by multiple vendors in VirusTotal.

Leveraging this discovery, we were able to identify additional IP addresses and domains associated with the distribution of Latrodectus malware.

Latrodectus is a downloader that functions as a backdoor, allowing threat actors to execute remote commands, gather information from compromised machines, and deploy additional malicious payloads, the most recent being Brute Ratel C4.

In this blog post, we will examine the malicious DLL and then dive into the C2 infrastructure we uncovered, including the certificate pivot and the associated domains identified during our research.

MeDExt.dll

Unfortunately, we don't have the initial access method for this attack campaign, but as past reports suggest, phishing and malicious ads are likely entry points into networks.

The DLL file that caught our attention, "MeDExt.dll," mimics the legitimate MeD Engine Extension from **AhnLab Smart Defense**. Given that this malicious file is a DLL, it's plausible that the legitimate parent executable was bundled with the Latrodectus malware or that this was a targeted attack aimed at a victim known to use AhnLab's services.

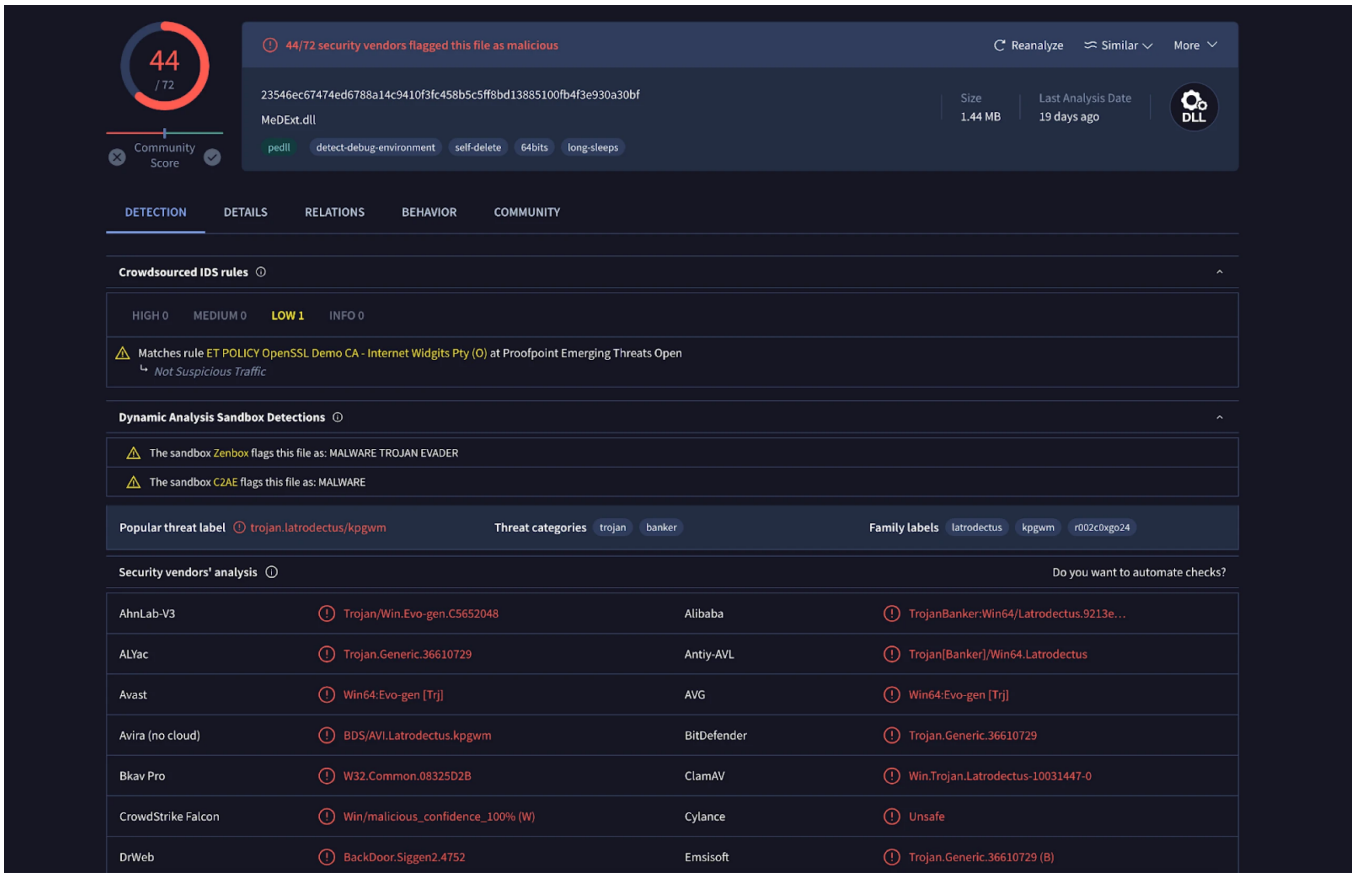


Figure 1: VirusTotal results for MeDExt.dll (Source: VirusTotal)

Spoofing a well-known anti-virus vendor increases the malware's stealth and the likelihood of bypassing security measures, reinforcing the importance of scrutinizing renamed files.

Below is the file signature info. Note the DLL is not signed.

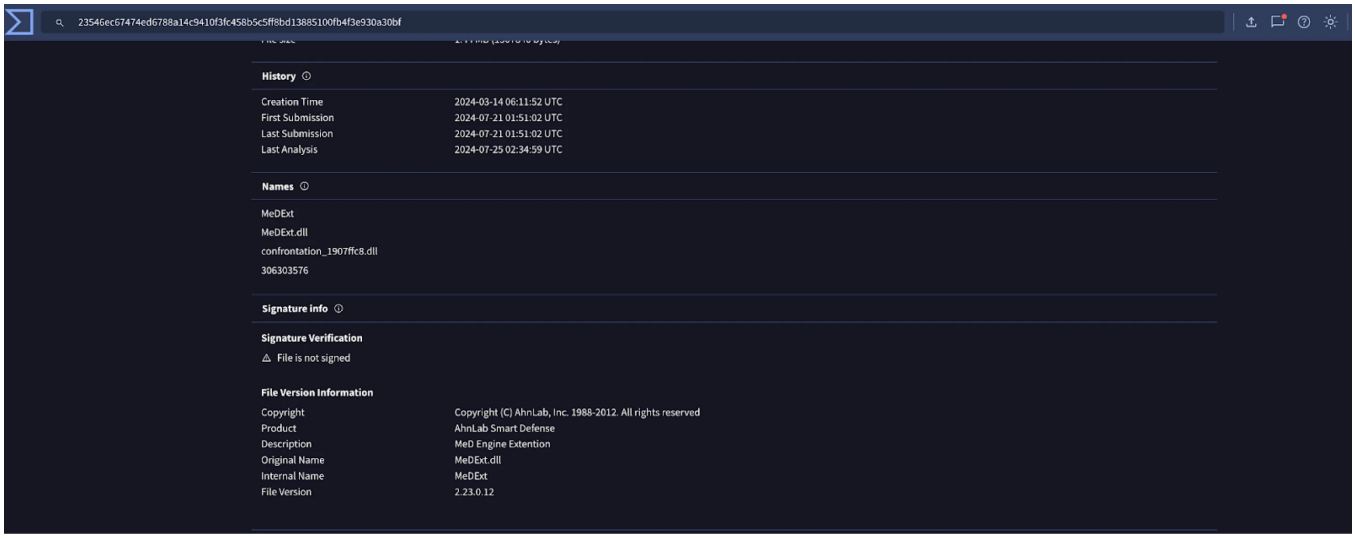


Figure 2: VirusTotal Signature Info for the suspect DLL

The PDB path (provided below) within the MeDExt.dll file offers a glimpse into the environment used by the threat actor(s)

C:\Build\Project\Medicine\Engine\2.0_MainTrunk\building\build\Project\Medicine\Engine\2.0\Trunk\Build\AMD64\free\MeDExt.pdb

The DLL has four exports with differing addresses, all following similar naming paths beginning with "MeDExt.."

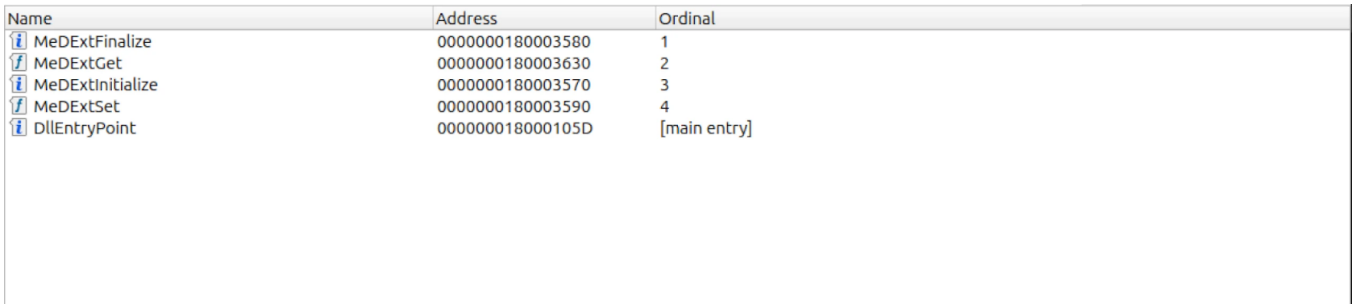


Figure 3: Obligatory IDA screenshot showing the DLL's exports

We could not identify any new TTPs during the analysis of the malicious file. This sample of Latrodectus employed familiar techniques, such as using the Windows Component Object Model (COM) to set a scheduled task for persistence.

Next, we'll examine the communication with the command and control infrastructure.

Command & Control Infrastructure Analysis

After running the file through multiple sandboxes, we observed Lactrodecuts attempting to communicate with the following domains + URLs:

- **stripplasst.]com/live/**
- **coolarition.]com/live/**

stripplasst.]com was registered through the OwnRegistrar, Inc. registrar, and coolarition[.]com through PDR Ltd. This consistent use of a single registrar should be used as a low-confidence indicator in tracking and attributing related malicious activity.

Both domains were unavailable during analysis, though we captured the first POST request to the C2 registering the victim's details in a PCAP, as seen below.

The IP address, 103.144.139.]189 for a short period resolved to the domain **riscoarchez[.]com**, also identified in a Latrodecuts attack paired with Brute Ratel C4 by Rapid7.

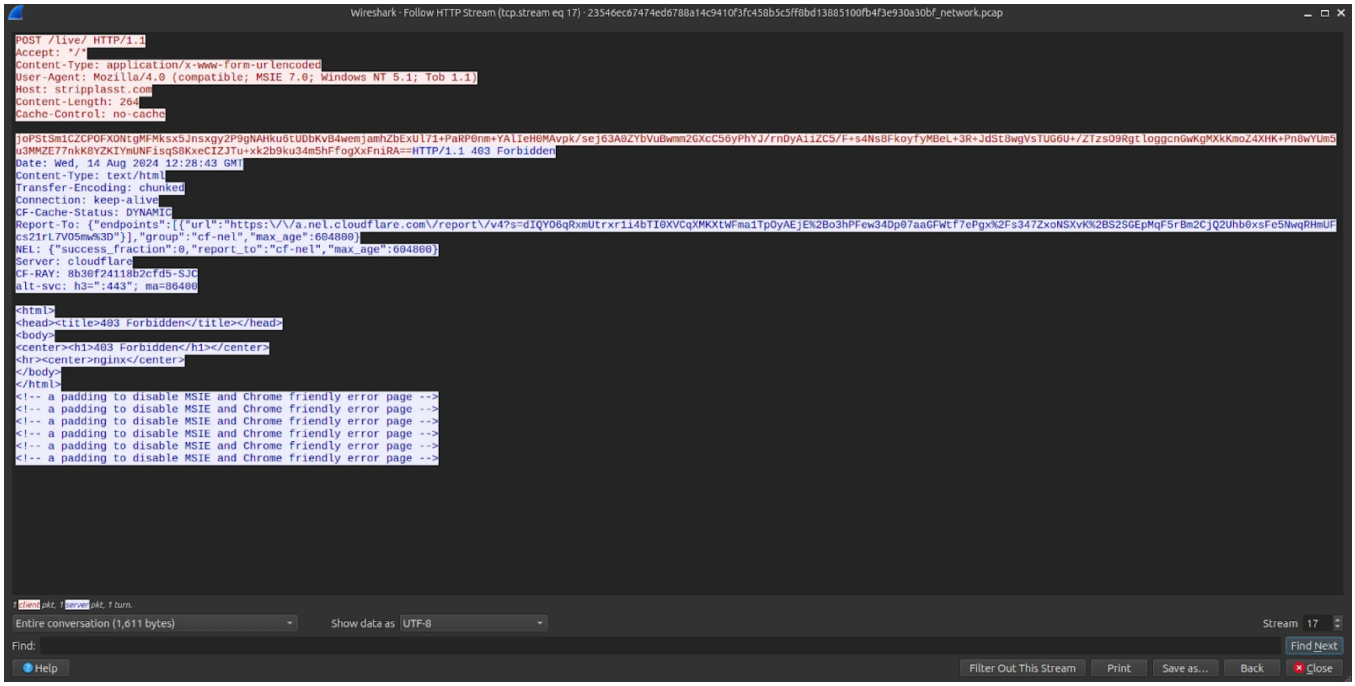


Figure 4: PCAP showing the initial registration request to one of the C2 domains.

The server that initiated our investigation is hosted on the Gigabit Hosting Sdn Bhd ASN.

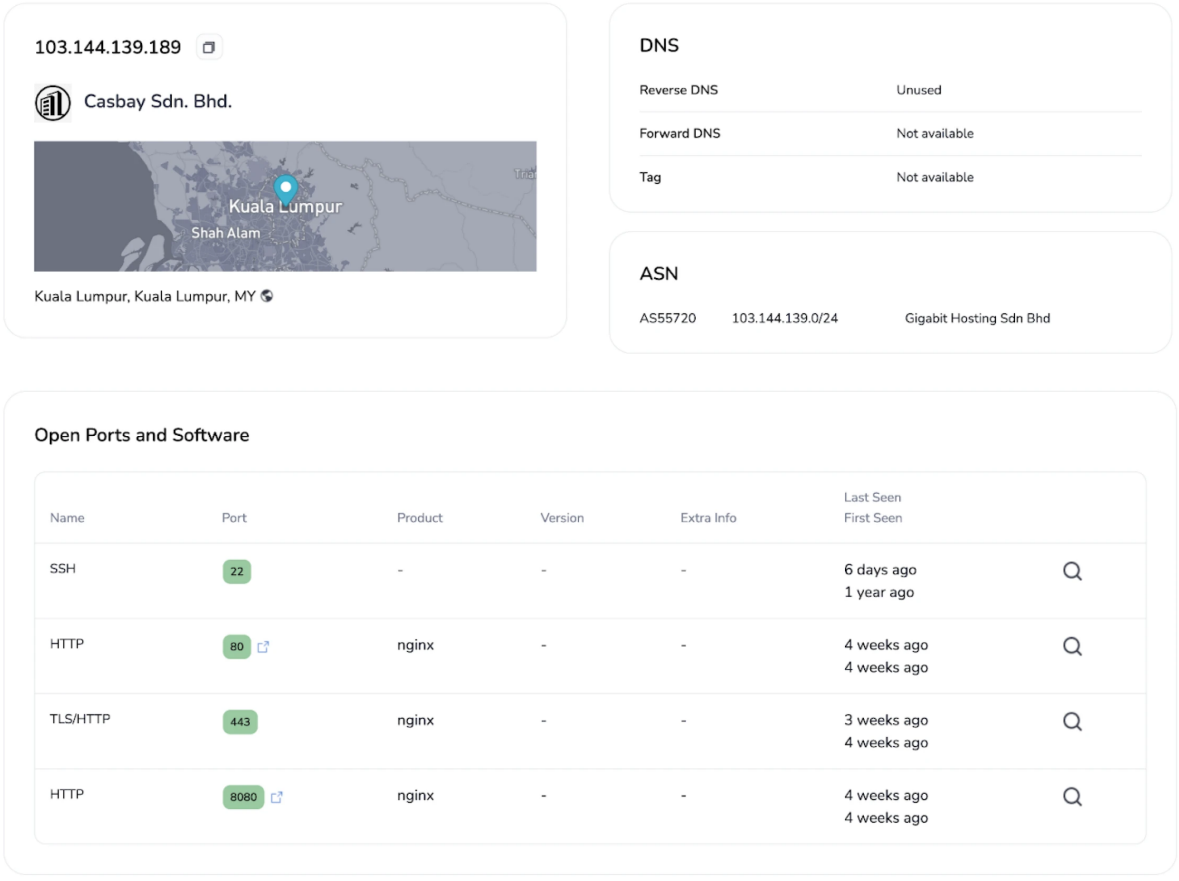


Figure 5: Initial IP that began our research (Link: here)
As reported by ProofPoint in their joint blog post with Team Cymru, we can see the server also has ports 443 and 8080 open, which were one of the criteria used to search for additional C2 servers in the article.

Moving to the SSL History, we noticed a semi-unique certificate on port 443. We say “semi” because many malware families use the “**Internet Widgits Pty Ltd**” Issuer Organization name in their self-signed certificates.

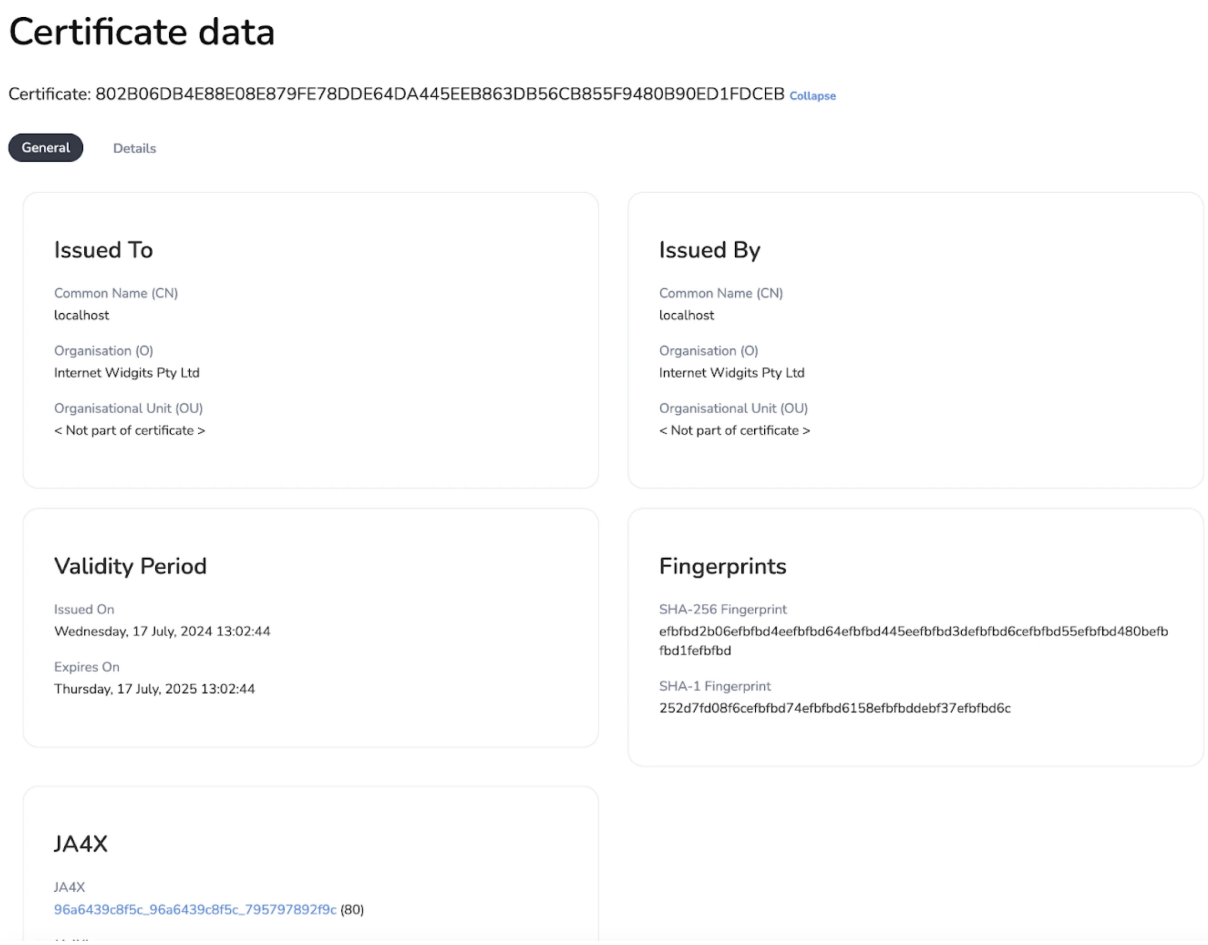


Figure 6: Hunt certificate data for 103.144.139.]189 (Try it here)
The complete certificate fields are below:

- Subject Common Name: localhost
- Subject Country: AU
- Subject Organization: Internet Widgits Pty Ltd
- Subject Organisational Unit: N/A
- Subject Locality: N/A
- Subject State: Some-State

We can use Hunt's Advanced Search feature to craft a query that will assist us in identifying servers using similar certificates as the above.

In the case of the Latrodectus C2 certs, we came up with the following query based on the JA4X hash and Subject Common Name:

ja4x:"96a6439c8f5c_96a6439c8f5c_795797892f9c" AND subject.common_name:"localhost"

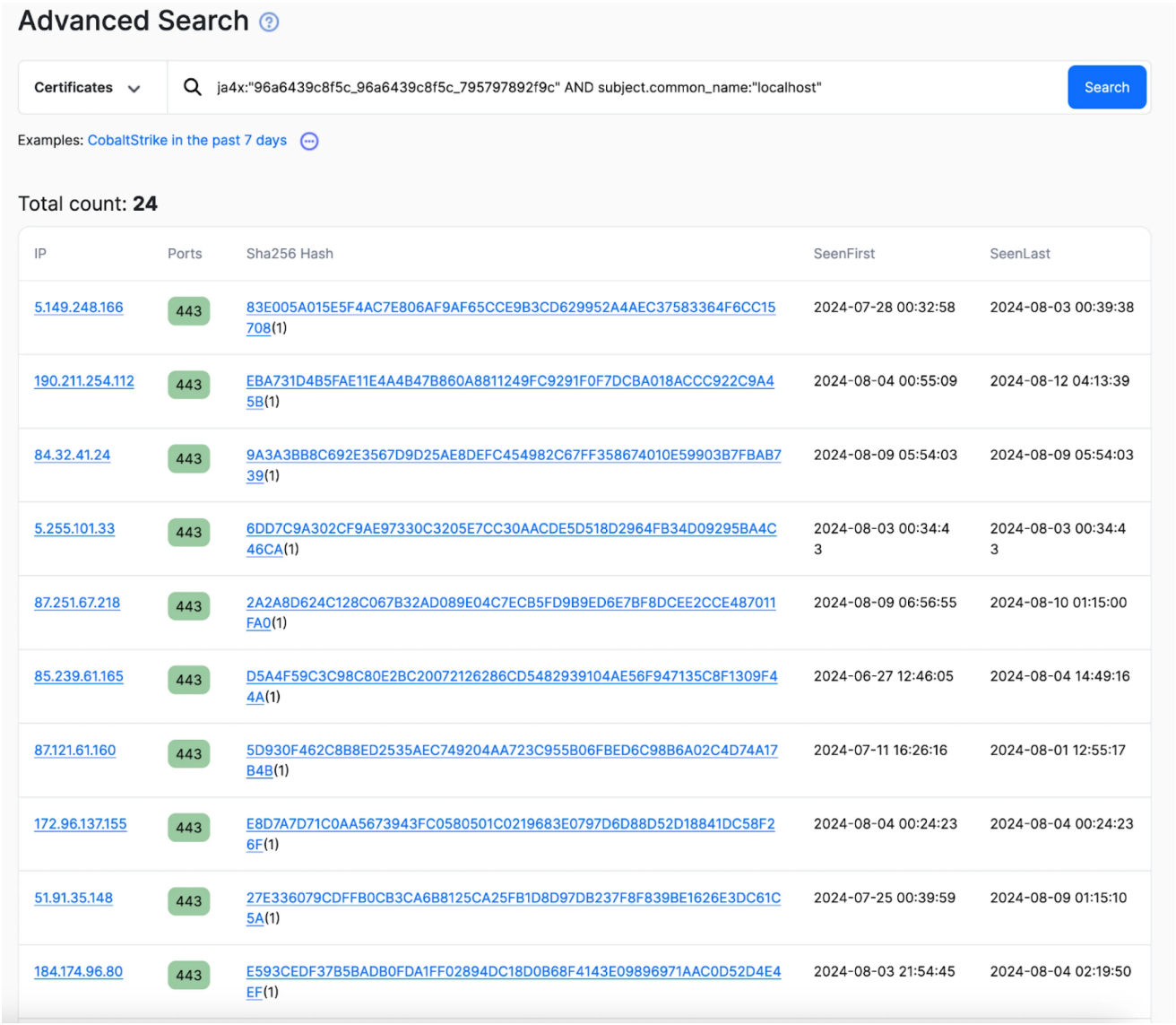


Figure 7: Hunt Advanced Search Results for the suspicious Latrodectus linked certificate (Try it out here)
The query returns just 24 results, suggesting we're on the right track in identifying Latrodectus servers. However, it's important to note that the certificate fields we're analyzing are commonly used for legitimate purposes and by other threat actors.

We cannot confirm that all results are linked to the malware; further investigation is required.

Poking around for similar server + certificate combinations on the same ASN as our initial IP, we found a malicious file mimicking the Google Authenticator app, also associated with Latrodectus communicating with **103.144.139.]182**.

The domain **spikeliftall.]com** resolves to the IP mentioned above, registered through **PDR Ltd**.

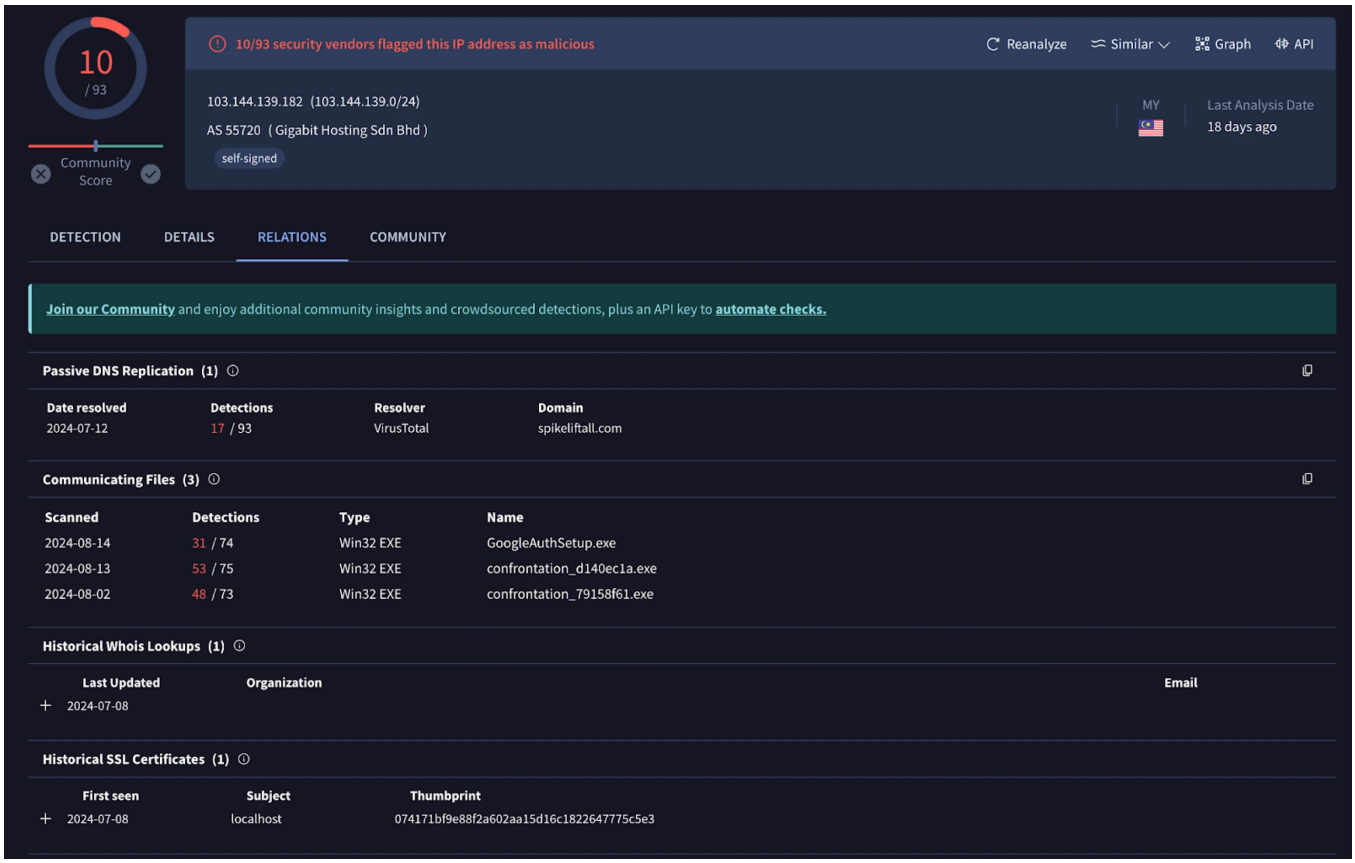


Figure 8: Another Lactrodectus C2 on the same ASN (Source: VirusTotal)
Again, this server also had port characteristics (443 & 8080) and a matching certificate seen with other command and control infrastructure.

On Aug 13, 2024, Symantec also noticed this campaign releasing a Protection Bulletin identifying the initial access vector as phishing.

After submitting a few IP addresses to VirusTotal for analysis, another server with a file detected as Latrodectus caught our attention.

94.232.46.205	443	E831C0DF07470D07192E085028AACEA52B38279837A4C2D99A30BB0C78C0147B(1)	2024-08-01 16:33:49	2024-08-14 04:38:52
217.195.153.204	443	2FF8B7D65F89735832391FD5C1C241FB8655B04BCAF20C3EF9EAE4DB402DF611(1)	2024-08-02 00:47:49	2024-08-03 10:08:11
185.81.114.243	443	ED8BA798679CC1CFE64D0E49AB6E8F9BFC030A1C320A55F5754787941B1A8402(1)	2024-08-04 23:56:45	2024-08-13 04:18:17
89.251.22.26	443	683A9753CF9DC19C044F5DD3DF8D2692408111818142 08A2EF7E0C0D182C33A8(1)	2024-08-02 16:46:20	2024-08-04 20:53:16
23.254.230.8	443	51DDFD46A9AD37B1A1AFB5139FB34F26126F55F35DC8EF912F3CCB9062AAE332(1)	2024-08-03 00:47:05	2024-08-04 01:33:27
185.196.11.28	443	A8B3B1E8E7407F913F0A36AD21A39AC52CCF0D0C052BDC44438993492FBFD95B(1)	2024-08-02 10:49:28	2024-08-10 20:45:41
62.106.66.46	443	06C630778E6F040E2B4ABD6CEB5E7277ACC08066F58557D8A0EA65F9469EBDFA(1)	2024-08-02 09:12:12	2024-08-12 23:40:15
193.243.147.77	443	9A8AE4AC8F7523DB551C5BFC24B4D52494D971F14ABEA1FE47D9385EF535B055(1)	2024-07-22 12:46:59	2024-08-04 14:46:11
23.227.203.161	443	04E9F0C4A286311C2A47ECF0B62453772365D2E1C1528EBAD3FC26B321499239(1)	2024-08-03 00:43:27	2024-08-04 20:47:45
45.129.199.25	443	CD661F5C4C823492004CB5C9E9301F5B1FF07D4CDB46F1568F777F60E28CB81A(1)	2024-07-07 14:56:12	2024-08-04 21:19:39
45.143.166.190	443	E31642A25040649A2C5ABFCC96806742D88884B5314AED1D93F3F6F2CAF8E481(1)	2024-08-09 01:38:06	2024-08-09 14:26:55

1 of 1

Figure 9: Additional suspicious IP associated with Latrodetus

The IP, hosted on BlueVPS OU, resolves to a single domain, **worlpquano.]com** registered through HOSTINGER, and used CloudFlare services in mid-July 2024.

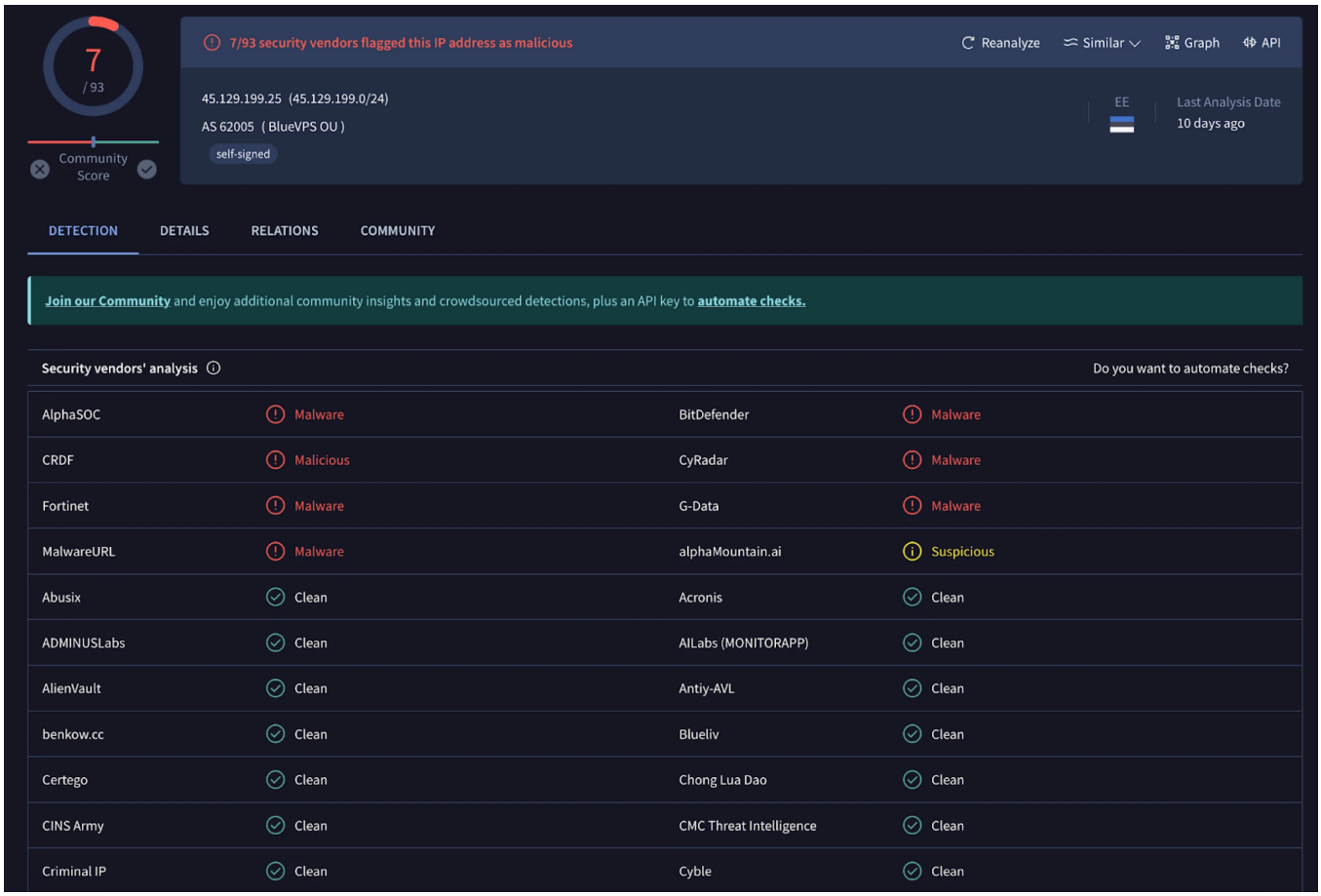


Figure 10: Third IP/domain associated with Latrodecuts scan results (Source: VirusTotal)

Conclusion

Latrodectus' tactic of impersonating legitimate security software highlights the persistent challenge of distinguishing between trusted and malicious files. Effective defense against such threats requires continuous monitoring and detailed analysis of network activity.

Request a demo today to get a closer look at how the Hunt platform can strengthen your defenses.

Network Observables

IP Address	Domain(s)	Domain Registrar	ASN	Notes
103.144.139.]189:443	riscoarchez.]com	Own Registrar	Gigabit Hosting Sdn Bhd	Initial IP that started investigation.
188.114.97.]7:443	stripplasst.]com	Own Registrar	CloudFlare	C2 for MeDExt.dll
188.114.97.]7:443, 84.32.41.]12:443	coolarition.]com	PDR Ltd.	CloudFlare, Hostgnome Ltd	C2 for MeDExt.dll
103.144.139.]182:443	spikeliftall.]com	PDR Ltd.	Gigabit Hosting Sdn Bhd	Jarm fingerprint + HTML response hash
45.129.199.]25:443	worlpquano.]com	HOSTINGER	BlueVPS OU	Identified as a possible Latrodectus C2 by Symantec

Host Observables

File Name	SHA-256 Hash	Notes
MeDExt.dll	23546ec67474ed6788a14c9410f3fc458b5c5ff8bd13885100fb4f3e930a30bf	Seen communicating with riscoarchez.]com/live/ stripplasst.]com/live/ coolartiion.]com/live/

File Name	SHA-256 Hash	Notes
GoogleAuthSetup.ex	62536e1486be7e31df6c111ed96777b9e3f2a912a2d7111253ae6a5519e71830	Seen communicating with steamcommunity.]com/profiles/76 godfaetret.]com/live/ spikeliftall.]com/live/
confrontation_d46a184c.exe	a459ce4bfb5d649410231bd4776c194b0891c8c5328bafc22184fe3111c0b3e7	Seen communicating with worlpquano.]com/live/ carflotyup.]com/live/