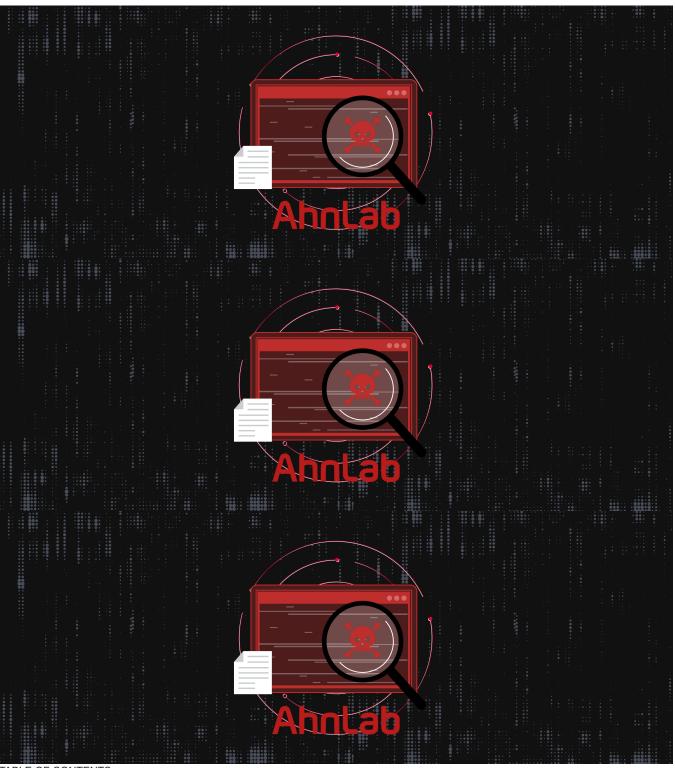
# Latrodectus Malware Masquerades as AhnLab Security Software to Infect Victims

kunt.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 <u>Brute Ratel C4</u>.

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.

44			$\mathrm C$ Reanalyze $$
/72	23546ec67474ed6788a14c9410f3fc458b5c5ff8bd13885100fb4f3e930a MeDExt.dll	130bf	Size Last Analysis Date 1.44 MB 19 days ago
Community Score	pedll detect-debug-environment self-delete 64bits long-sleep		
DETECTION D	ETAILS RELATIONS BEHAVIOR COMMUNITY		
Crowdsourced IDS ru	les O		
	4 0 LOW 1 INFO 0		
Matches rule ET P	DLICY OpenSSL Demo CA - Internet Widgits Pty (O) at Proofpoint Emerging. Traffic	Threats Open	
Dynamic Analysis Sa	ndbox Detections ①		
	box flags this file as: MALWARE TROJAN EVADER		
A The sandbox C2A	E flags this file as: MALWARE		
Popular threat label	trojan.latrodectus/kpgwm     Threat categories troj		Family labels latrodectus kpgwm r002c0xgo24
Popular threat label Security vendors' and			Family labels latrodectus kpgwm r002c0xgo24 Do you want to automate checks?
		an banker Alibaba	
Security vendors' and	ilysis ()		Do you want to automate checks?
Security vendors' and AhnLab-V3	Ilysis ① ① Trojan/Win.Evo-gen.C5652048	Alibaba	Do you want to automate checks?
Security vendors' and AhnLab-V3 ALYac	ilysis ① ① Trojan/Win.Evo-gen.C5652048 ① Trojan.Generic.36610729	Alibaba Antiy-AVL	Do you want to automate checks?           ① TrojanBanker:Win64/Latrodectus.9213e           ① Trojan[Banker]/Win64.Latrodectus
Security vendors' and AhnLab-V3 ALYac Avast	Invisis         O           ①         Trojan/Win.Evo-gen.C5652048           ①         Trojan.Generic.36610729           ①         Win64:Evo-gen (Trjj)	Alibaba Antiy-AVL AVG	Do you want to automate checks?  ① TrojanBanker:Win64/Latrodectus.9213e ① Trojan[Banker]/Win64.Latrodectus ② Win64:Evo-gen [Trj]
Security vendors' and AhnLab-V3 ALYac Avast Avira (no cloud)	t <b>lysis ①</b> ① Trojan/Win.Evo-gen.C5652048 ① Trojan.Generic.36610729 ② Win64:Evo-gen [Trj] ③ BDS/AVI.Latrodectus.kpgwm	Alibaba Antiy-AVL AVG BitDefender	Do you want to automate checks?  O TrojanBanker:Win64/Latrodectus.9213e  Trojan[Banker]/Win64.Latrodectus  Win64:Evo-gen [Trj]  Trojan.Generic.36610729

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.

Q 23546ec67474ed6788a14c9410f3fc458			± 🖵 🤉 🔅
	History ①	an a	
	Creation Time First Submission Last Submission Last Analysis	2024-03-14 06:11:52 UTC 2024-07-21 01:51:02 UTC 2024-07-21 01:51:02 UTC 2024-07-25 02:34:59 UTC	
	Names ①		
	MeDExt MeDExt.dll confrontation_1907ffc8.dll 306303576		
	Signature info ①		
	Signature Verification △ File is not signed File Version Information Copyright Product Description Original Name Internal Name File Version	Copyright (C) AhnLab, Inc. 1988-2012. All rights reserved AhnLab Smart Defense MeD Engine Estention MeDExt 2.23.0.12	

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				
1 MeDExtFinalize	000000180003580	1				
1 MeDExtGet	000000180003630	2				
1 MeDExtInitialize	000000180003570	3				
1 MeDExtSet	000000180003590	4				
1 DllEntryPoint	00000018000105D	[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 <u>Rapid7</u>.

Wireshark - Follow HTTP Stream (tcp.stream eq 17) - 23546ec67474ed6788814c9410f3fc458b5c5ff8bd13885100fb4f3e930a30bf_n	etwork.pcap _ 🗆 🗙
POST /live/HTTP/1.1 Accept: // Content-Typ: spplication/x-www-form-urlencoded Content-Typ: Voilla/A.0 (compatible; MSIE 7.6; Windows NT 5.1; Tob 1.1) Most: stripplassi.com Content-tength: 204 Cache-Control: no-cache	
<pre>ioPSESmic2CPDFXONtgMFMksx3Jnsxy2P9gMAHkuUUDbXvB4wemjamh2bExUT71+PakPenm+YAlleH8MAvpE/sej63A82YbVuBwmm26XcC56yPhYJ/rnDyAll2C5/F+s4Ns8FkoyfyM8e u3MM2277nkWFX2KYuMWFs68KXec12J1v+x2b6ku34m5hFfogXxFniRA==HTTP/1.1 463 Forbidden Date: Wed, 14 Aug 2024 12:28:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-allue CF-cache-Status: DVNAWTC Report-To: {endpoints' CF-cache-Status: DVNAWTC Report-To: {endpoints' Report-To: {endpoints' NetL: {"success_fraction":e, "report_to: "cf-net", "max_age":604800} Servor: cloudflare CF-RAY: B8/274118b2rdf-S-SIG</pre>	
alt-svc: h3=":443"; mm=86400 chtml> chead>stite2483 Forbidden cbody= ccente7>ch1>483 Forbidden ch1>ccente7>cl1>483 Forbidden ch2>ch1>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7>cente7> ch2>cente7> cent	
<pre></pre>	
n stand plet a stand and the stand	
Texan proc. Texan	Stream 17 🗘
Find:	Find Next
• Help	Filter Out This Stream Print Save as Back Sclose

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.

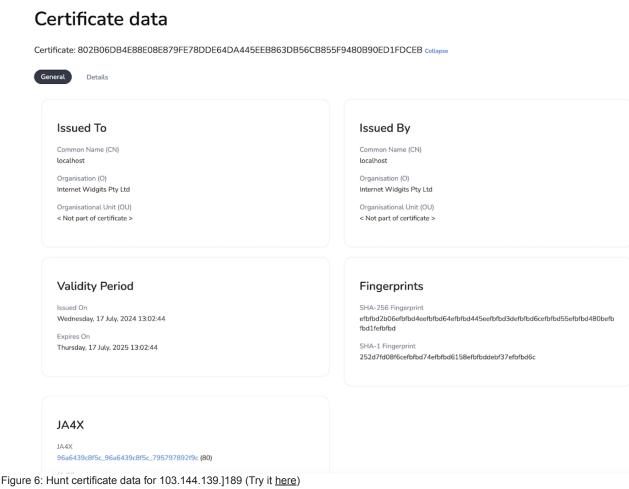
103.144.139.189	DNS	
Casbay Sdn. Bhd.	Reverse DNS	Unused
	Forward DNS	Not available
Kuala Lumpur	Tag	Not available
Shah Alam Kuala Lumpur, Kuala Lumpur, MY S	ASN	
	AS55720 103.144.139.0/24	Gigabit Hosting Sdn Bhd

Name	Port	Product	Version	Extra Info	Last Seen First Seen	
SSH	22	-	-	-	6 days ago 1 year ago	Q
НТТР	80 23	nginx	-		4 weeks ago 4 weeks ago	Q
TLS/HTTP	443	nginx	-		3 weeks ago 4 weeks ago	Q
HTTP	8080	nginx	-	-	4 weeks ago 4 weeks ago	Q

Figure 5: Initial IP that began our research (Link: here)

As reported by <u>ProofPoint</u> 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 <u>C2 servers</u> 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.



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"

# Advanced Search ③

Certificates 🗸

Q ja4x:"96a6439c8f5c\_96a6439c8f5c\_795797892f9c" AND subject.common\_name:"localhost"

Search

Examples: CobaltStrike in the past 7 days 💮

### Total count: 24

IP	Ports	Sha256 Hash	SeenFirst	SeenLast
<u>5.149.248.166</u>	443	83E005A015E5F4AC7E806AF9AF65CCE9B3CD629952A4AEC37583364F6CC15 708(1)	2024-07-28 00:32:58	2024-08-03 00:39:38
<u>190.211.254.112</u>	443	EBA731D4B5FAE11E4A4B47B860A8811249FC9291F0F7DCBA018ACCC922C9A4 5B(1)	2024-08-04 00:55:09	2024-08-12 04:13:39
<u>84.32.41.24</u>	443	9A3A3BB8C692E3567D9D25AE8DEFC454982C67FF358674010E59903B7FBAB7 39(1)	2024-08-09 05:54:03	2024-08-09 05:54:03
<u>5.255.101.33</u>	443	6DD7C9A302CF9AE97330C3205E7CC30AACDE5D518D2964FB34D09295BA4C 46CA(1)	2024-08-03 00:34:4 3	2024-08-03 00:34:4 3
<u>87.251.67.218</u>	443	2A2A8D624C128C067B32AD089E04C7ECB5FD9B9ED6E7BF8DCEE2CCE487011 FA0(1)	2024-08-09 06:56:55	2024-08-10 01:15:00
<u>85.239.61.165</u>	443	D5A4F59C3C98C80E2BC20072126286CD5482939104AE56F947135C8F1309F4 4A(1)	2024-06-27 12:46:05	2024-08-04 14:49:16
<u>87.121.61.160</u>	443	5D930F462C8B8ED2535AEC749204AA723C955B06FBED6C98B6A02C4D74A17 B4B(1)	2024-07-11 16:26:16	2024-08-01 12:55:17
<u>172.96.137.155</u>	443	E8D7A7D71C0AA5673943FC0580501C0219683E0797D6D88D52D18841DC58F2 6F(1)	2024-08-04 00:24:23	2024-08-04 00:24:23
<u>51.91.35.148</u>	443	27E336079CDFFB0CB3CA6B8125CA25FB1D8D97DB237F8FB39BE1626E3DC61C 5A(1)	2024-07-25 00:39:59	2024-08-09 01:15:10
<u>184.174.96.80</u>	443	E593CEDF37B5BADB0FDA1FF02894DC18D0B68F4143E09896971AAC0D52D4E4 EF(1)	2024-08-03 21:54:45	2024-08-04 02:19:50

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.

10	① 10/93 security	vendors flagged this IP	address as malicious		C'Reanalyze	ightarrow Similar $ee$	쁇 Graph 💠 API
(93) ⊗ Community Score ♥	103.144.139.182(10 AS 55720 (Gigabit H self-signed					MY	Last Analysis Date 18 days ago
DETECTION DET	TAILS RELATIONS	community					
Join our Community a	ind enjoy additional com	nmunity insights and cro	owdsourced detections, plus an API key	to <u>automate checks.</u>			
Passive DNS Replicatio	on (1) 🛈						Q
Date resolved 2024-07-12	Detections 17 / 93	<b>Resolver</b> VirusTotal	<b>Domain</b> spikeliftall.com				
Communicating Files (	(3) ①						Q
Scanned	Detections	Туре	Name				
2024-08-14	<mark>31</mark> / 74	Win32 EXE	GoogleAuthSetup.exe				
2024-08-13	53 / 75	Win32 EXE	confrontation_d140ec1a.exe				
2024-08-02	48 / 73	Win32 EXE	confrontation_79158f61.exe				
Historical Whois Looku	ıps (1) 🛈						
Last Updated + 2024-07-08	Organization					Em	ail
Historical SSL Certifica	ates (1) 🛈						
First seen + 2024-07-08	Subject localhost	Thumbpr 074171bf9e8	int 18f2a602aa15d16c1822647775c5e3				

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.

<u>94.232.46.205</u>	443	E831C0DF07470D07192E085028AACEA52B38279837A4C2D99A30BB0C78C014 7B(1)	2024-08-01 16:33:49	2024-08-14 04:38:52
<u>217.195.153.204</u>	443	2FF8B7D65F89735832391FD5C1C241FB8655B04BCAF20C3EF9EAE4DB402DF6 11(1)	2024-08-02 00:47:49	2024-08-03 10:08:11
<u>185.81.114.243</u>	443	ED8BA798679CC1CFE64D0E49AB6E8F9BFC030A1C320A55F5754787941B1A84	2024-08-04 23:56:45	2024-08-13 04:18:17
<u>89.251.22.26</u>	443	683A9753CF9DC19C044F5DD3DF8D269240811181814208A2EF7E0C0D182C33 A8(1)	2024-08-02 16:46:20	2024-08-04 20:53:16
<u>23.254.230.8</u>	443	51DDFD46A9AD37B1A1AFB5139FB34F26126F55F35DC8EF912F3CCB9062AAE3 32(1)	2024-08-03 00:47:05	2024-08-04 01:33:27
<u>185.196.11.28</u>	443	A8B3B1E8E7407F913F0A36AD21A39AC52CCF0D0C052BDC44438993492FBFD 95B(1)	2024-08-02 10:49:28	2024-08-10 20:45:41
<u>62.106.66.46</u>	443	06C630778E6F040E2B4ABD6CEB5E7277ACC08066F58557D8A0EA65F9469EB DFA(1)	2024-08-02 09:12:12	2024-08-12 23:40:15
<u>193.243.147.77</u>	443	9A8AE4AC8F7523DB551C5BFC24B4D52494D971F14ABEA1FE47D9385EF535B0 55(1)	2024-07-22 12:46:59	2024-08-04 14:46:11
<u>23.227.203.161</u>	443	94E9F0C4A286311C2A47ECF0B62453772365D2E1C1528EBAD3FC26B3214992 39(1)	2024-08-03 00:43:27	2024-08-04 20:47:45
45.129.199.25	443	CD661F5C4C823492004CB5C9E9301F5B1FF07D4CDB46F1568F777F60E28CB8 1A(1)	2024-07-07 14:56:12	2024-08-04 21:19:39
<u>45.143.166.190</u>	443	E31642A25040649A2C5ABFCC96806742D88884B5314AED1D93F3F6F2CAF8E4 81(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.

			C Reanalyze ≍ Similar ∨ 號 Graph Փ API
(93) → (93)	45.129.199.25 (45.129.199.0/24) AS 62005 ( BlueVPS OU ) self-signed		EE Last Analysis Date 10 days ago
DETECTION DET	AILS RELATIONS COMMUNITY		
Join our Community an	nd enjoy additional community insights and crowdsourced detections,	plus an API key to <b>automate checks.</b>	
Security vendors' analy	sis O		Do you want to automate checks?
AlphaSOC	() Malware	BitDefender	① Malware
CRDF	① Malicious	CyRadar	① Malware
Fortinet	() Malware	G-Data	① Malware
MalwareURL	() Malware	alphaMountain.ai	(i) Suspicious
Abusix	⊘ Clean	Acronis	🧭 Clean
ADMINUSLabs	⊘ Clean	AILabs (MONITORAPP)	🖉 Clean
AlienVault	⊘ Clean	Antiy-AVL	🧭 Clean
benkow.cc	⊘ Clean	Blueliv	🖉 Clean
Certego	⊘ Clean	Chong Lua Dao	🧭 Clean
CINS Army	⊘ Clean	CMC Threat Intelligence	🧭 Clean
Criminal IP	Clean	Cyble	⊘ Clean

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 <u>Brute Ratel C4</u>.

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.

			C Reanalyze $pprox$ Similar $arsim$ More $arsim$						
Community Score	23546ec67474ed6788a14c9410f3fc458b5c5ff8bd13885100fb4f3e930a30bf MeDExt.dll pedll detect-debug-environment self-delete 64bits long-sleeps	Size Last Analysis Date 1.44 MB 19 days ago							
Crowdsourced IDS rul	es ()								
	0 LOW 1 INFO 0								
Matches rule ET PO	LICY OpenSSL Demo CA - Internet Widgits Pty (0) at Proofpoint Emerging Threat traffic	ts Open							
Dynamic Analysis San	dbox Detections ①								
A The sandbox Zenb	ox flags this file as: MALWARE TROJAN EVADER								
A The sandbox C2AE	flags this file as: MALWARE								
Popular threat label (	D trojan.latrodectus/kpgwm Threat categories trojan		Family labels latrodectus kpgwm r002cDxgo24						
Security vendors' anal	ysis ①		Do you want to automate checks?						
AhnLab-V3	() Trojan/Win.Evo-gen.C5652048	Alibaba	() TrojanBanker:Win64/Latrodectus.9213e						
ALYac	() Trojan.Generic.36610729	Antiy-AVL	() Trojan[Banker]/Win64.Latrodectus						
Avast	() Win64:Evo-gen [Trj]	AVG	① Win64:Evo-gen [Trj]						
Avira (no cloud)	() BDS/AVI.Latrodectus.kpgwm	BitDefender	① Trojan.Generic.36610729						
Bkav Pro	() W32.Common.08325D2B	ClamAV	() Win.Trojan.Latrodectus-10031447-0						
CrowdStrike Falcon	() Win/malicious_confidence_100% (W)	Cylance	① Unsafe						
DrWeb	() BackDoor.Siggen2.4752	Emsisoft	() Trojan.Generic.36610729 (B)						

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.

23546ec67474ed6788a14c9410f3fc458			1 🗅 🖵 🕐 🔅
	History ©		
	Creation Time First Submission Last Submission Last Analysis	2024-03-14 06:11-52 UTC 2024-07-21 01:51:02 UTC 2024-07-21 01:51:02 UTC 2024-07-23 02:34:59 UTC	
	Names O		
	MeDExt MeDExt.dll confrontation_1907ffc8.dll 306303576		
	Signature info ①		
	Signature Verification △ File is not signed File Version Information Copyright Product Description Original Name Internal Name File Version	Copyright (C) AhnLab, Inc. 1988-2012. All rights reserved AhnLab Smart Defense MeD Engine Extention MeDExt. dll MeDExt	

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
1 MeDExtFinalize	000000180003580	1
1 MeDExtGet	000000180003630	2
1 MeDExtInitialize	000000180003570	3
🚺 MeDExtSet	000000180003590	4
1 DllEntryPoint	00000018000105D	[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 <u>Rapid7</u>.

Wireshark - Follow HTTP Stream (tcp.stream eq 17) - 23546ec67474ed6788814c9410f3fc458b5c5ff8bd13885100fb4f3e930a30bf_n	etwork.pcap _ 🗆 🗙
POST /lue/ HTTP/1.1 Accept: // Content-Type: application/x-www-form-urlencoded Content-Type: application/x-www-form-urlencoded Wost: stripplast.com Content-Length: Zod Cache-Control: no-cache	
<pre>j0PSTSslt2CPOFXOUGMFMksx3Jnsxqy2PgdH4Hku6UUDbKvB4wem_amh2DExU171+PaRPomm+X1LeH8MAvpE/sej63A82YbVuBwmm2GXCC56yPhY3/rnDyA11ZC5/F+s4Ns8FkoyfyM8e u3MW2C77nK4WSZKYUMUFs68KxeC121v=x2 Date: Wed, 14 Aug 2024 12:28:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-allue CF-cache-Status: DVMAWIC Report-To: {endpoints: [{"url":"https://va.net.cloudflare.com//report/v4?s=d1QY06qRxmUtrxr114bT16XVCqXMKxtwFma1Tp0yAEjE%2B03hPFcw34Dp87aaGFW wEL: {"success_fraction:s, "report_to:"cf-net", "max_age":604808} Server: cloudflare</pre>	
alt-svc:ha=":443"; ma=86400 <html> <head><title>403&lt;/pre&gt; Forbidden&lt;/fitle&gt;&lt;/head&gt; Conter&gt; Conter Cont&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;! a padding to disable MSIE and Chrome friendly error page&gt;&lt;br&gt;&lt;! a padding to disable MSIE and Chrome friendly error page&gt;&lt;br&gt;&lt;! a padding to disable MSIE and Chrome friendly error page&gt;&lt;br&gt;&lt;! a padding to disable MSIE and Chrome friendly error page&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;1 stores okt 1 stores okt 1 turn&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Entire conversation (1,611 bytes)    Show data as UTF-8&lt;/td&gt;&lt;td&gt;Stream 17 💠&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Find:&lt;/td&gt;&lt;td&gt;Find &lt;u&gt;N&lt;/u&gt;ext&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;• Help&lt;/td&gt;&lt;td&gt;Filter Out This Stream Print Save as Back Sclose&lt;/td&gt;&lt;/tr&gt;&lt;/tbody&gt;&lt;/table&gt;</title></head></html>	

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.

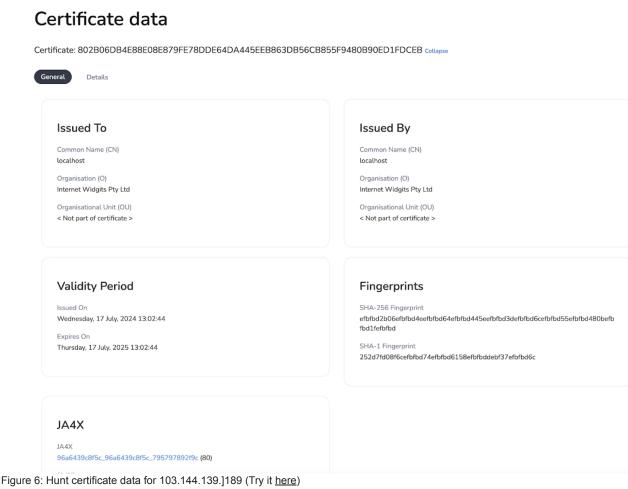
103.144.139.189 🗉	DNS	
Casbay Sdn. Bhd.	Reverse DNS	Unused
	Forward DNS	Not available
Kuala Lumpur	Tag	Not available
Shah Alam Kuala Lumpur, Kuala Lumpur, MY 🛇	ASN A555720 103.144.139.0/24	Gigabit Hosting Sdn Bhd

Name	Port	Product	Version	Extra Info	Last Seen First Seen	
SSH	22	-	-	-	6 days ago 1 year ago	Q
НТТР	80	nginx	-		4 weeks ago 4 weeks ago	Q
TLS/HTTP	443	nginx	-		3 weeks ago 4 weeks ago	Q
HTTP	8080	nginx	-	-	4 weeks ago 4 weeks ago	Q

Figure 5: Initial IP that began our research (Link: here)

As reported by <u>ProofPoint</u> 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 <u>C2 servers</u> 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.



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"

# Advanced Search ③

Certificates 🗸

Q ja4x:"96a6439c8f5c\_96a6439c8f5c\_795797892f9c" AND subject.common\_name:"localhost"

Search

Examples: CobaltStrike in the past 7 days

### Total count: 24

Image:					
111111111111111111111111111111111111	IP	Ports	Sha256 Hash	SeenFirst	SeenLast
110         58(1)           84.32.41.24         443         9A3A3BBBC692E3567D9D25AEBDEFC454982C67FF35867A010E59903B7FBAB7         2024-08-09 05:54:03         2024-08-09 05:54:03           5.255.101.33         443         6DD7C9A302CF9AE97330C3205E7CC30AACDE5D51BD2964FB34D09295BA4C         2024-08-03 00:34:4         3           5.255.101.33         443         6DD7C9A302CF9AE97330C3205E7CC30AACDE5D51BD2964FB34D09295BA4C         2024-08-03 00:34:4         3         3           87.251.67.218         443         2A2ABB624C128C067B32AD089E04C7ECB5FD9B9ED6E7BFBDCEE2CCE487011         2024-08-09 06:56:55         2024-08-10 01:15:00           85.239.61165         443         D5A4F59C3C98C80E2BC20072126286CD5482939104AE56F947135C8F1309F4         2024-06-27 12:46:05         2024-08-04 14:49:16           87.121.611.60         443         5D930F462C8B8ED2535AEC749204AA723C955B06FBEDBC98B6A02C4D74A17         2024-07-11 16:26:16         2024-08-04 12:55:17           172.96.137.155         443         EB07A7D71C0AA5673943FC0580501C0219683E0797D6D88D52D18641DC58F2         2024-08-04 00:24:23         2024-08-04 00:24:23           51.91.35.148         443         27E336079CDFFB0CB3CA6B8125CA25FB1D8D97DB237F8FB39BE1626E3DC61C         2024-07-25 00:39:59         2024-08-09 01:15:10           184.174.96.60         443         E593CEDF37B5BAD0FDA1FF02894DC18D095DB237F8FB39BE1626E3DC61C         2024-08-03 21:54:45         2024-08-09 01:15:10	<u>5.149.248.166</u>	443		2024-07-28 00:32:58	2024-08-03 00:39:38
111       39(1)         5.255.101.33       443       6DD7C9A302CF9AE97330C3205E7CC30AACDE5D518D2964FB34D09295BA4C 46CA(1)       2024-08-03 00:34:4 3       2024-08-03 00:34:4 3         87.251.67.218       443       2A2A80624C128C067B32AD089E04C7ECB5FD9B9ED6E7BF8DCEE2CCE487011 FA0(1)       2024-08-09 06:56:55       2024-08-10 01:15:00         85.239.61.165       443       D5A4F59C3C98C80E2BC20072126286CD5482939104AE56F947135C8F1309F4 4A(1)       2024-06-27 12:46:05       2024-08-04 14:49:16         87.121.61.160       443       5D930F462C8B8ED2535AEC749204AA723C955B06FBED6C98B6A02C4D74A17 84B(1)       2024-07-11 16:26:16       2024-08-01 12:55:17         172.96.137.155       443       EBD7A7D71C0AA5673943FC0580501C0219683E0797D6D88D52D18841DC58F2       2024-08-04 00:24:23       2024-08-04 00:24:23         51.91.35.148       443       27E336079CDFFB0CB3CA6B8125CA25FB1D8D97DB237F8FB39BE1826E3DC61C       2024-07-25 00:39:59       2024-08-04 01:15:10         184.174.96.80       443       E593CEDF37B5BAABD6FDA1FF02894DC18D0B68F4143E09896971AAC0D52D4E4       2024-08-03 21:54:45       2024-08-04 02:19:50	<u>190.211.254.112</u>	443		2024-08-04 00:55:09	2024-08-12 04:13:39
46CA(1)       3       3         87.251.67.218       443       2A2A8D624C128C067B32AD089E04C7ECB5FD9B9ED6E7BF8DCEE2CCE487011 FA0(1)       2024-08-09 06:56:55       2024-08-10 01:15:00         85.239.61.165       443       D5A4F59C3C98C80E2BC20072126286CD5482939104AE56F947135C8F1309F4 4A(1)       2024-06-27 12:46:05       2024-08-04 14:49:16         87.121.61.160       443       5D930F462C888ED2535AEC749204AA723C955B06FBED8C98B6A02C4D74A17 B4B(1)       2024-07-11 16:26:16       2024-08-01 12:55:17         172.96.137.155       443       E8D7A7D71C0AA5673943FC0580501C0219683E0797D6D88D52D18841DC58F2 6F(1)       2024-08-04 00:24:23       2024-08-04 00:24:23         51.91.35.148       443       27E336079CDFFB0CB3CA6B8125CA25FB1D8D97DB237F8F839BE1626E3DC61C 5A(1)       2024-07-25 00:39:59       2024-08-09 01:15:10         184.174.96.80       443       E593CEDF37B5BADB0FDA1FF02894DC18D0868F1413E09896971AAC0D52D4E4       2024-08-03 21:54:45       2024-08-04 02:19:50	84.32.41.24	443		2024-08-09 05:54:03	2024-08-09 05:54:03
Internation	<u>5.255.101.33</u>	443			
4A(1)         87.121.61.160       443       5D930F462C8B8ED2535AEC749204AA723C955B06FBED6C98B6A02C4D74A17 B4B(1)       2024-07-11 16:26:16       2024-08-01 12:55:17         172.96.137.155       443       E8D7A7D71C0AA5673943FC0580501C0219683E0797D6D88D52D18841DC58F2 6F(1)       2024-08-04 00:24:23       2024-08-04 00:24:23       2024-08-04 00:24:23         51.91.35.148       443       27E336079CDFFB0CB3CA6B8125CA25FB1D8D97DB237F8F839BE1626E3DC61C 5A(1)       2024-07-25 00:39:59       2024-08-09 01:15:10         184.174.96.80       443       E593CEDF37B5BADB0FDA1FF02894DC18D0B68F4143E09896971AAC0D52D4E4       2024-08-03 21:54:45       2024-08-04 02:19:50	<u>87.251.67.218</u>	443		2024-08-09 06:56:55	2024-08-10 01:15:00
International       International<	<u>85.239.61.165</u>	443		2024-06-27 12:46:05	2024-08-04 14:49:16
Example         GF(1)           51.91.35.148         27E336079CDFFB0CB3CA6B8125CA25FB1D8D97DB237F8F839BE1626E3DC61C         2024-07-25 00:39:59         2024-08-09 01:15:10           51.91.35.148         443         27E336079CDFFB0CB3CA6B8125CA25FB1D8D97DB237F8F839BE1626E3DC61C         2024-07-25 00:39:59         2024-08-09 01:15:10           184.174.96.80         443         E593CEDF37B5BADB0FDA1FF02894DC18D0B68F4143E09896971AAC0D52D4E4         2024-08-03 21:54:45         2024-08-04 02:19:50	<u>87.121.61.160</u>	443		2024-07-11 16:26:16	2024-08-01 12:55:17
184.174.96.80         443         E593CEDF37B5BADB0FDA1FF02894DC18D0B68F4143E09896971AAC0D52D4E4         2024-08-03 21:54:45         2024-08-04 02:19:50	<u>172.96.137.155</u>	443		2024-08-04 00:24:23	2024-08-04 00:24:23
440	<u>51.91.35.148</u>	443		2024-07-25 00:39:59	2024-08-09 01:15:10
	<u>184.174.96.80</u>	443		2024-08-03 21:54:45	2024-08-04 02:19:50

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.

10	① 10/93 security	vendors flagged this IP	address as malicious		C'Reanalyze	ightarrow Similar $ee$	쁇 Graph 💠 API
(93) ⊗ Community Score ♥	103.144.139.182(10 AS 55720 (Gigabit H self-signed					MY	Last Analysis Date 18 days ago
DETECTION DET	TAILS RELATIONS	community					
Join our Community a	ind enjoy additional com	nmunity insights and cro	owdsourced detections, plus an API key	to <u>automate checks.</u>			
Passive DNS Replicatio	on (1) 🛈						Q
Date resolved 2024-07-12	Detections 17 / 93	<b>Resolver</b> VirusTotal	<b>Domain</b> spikeliftall.com				
Communicating Files (	(3) ①						Q
Scanned	Detections	Туре	Name				
2024-08-14	<mark>31</mark> / 74	Win32 EXE	GoogleAuthSetup.exe				
2024-08-13	53 / 75	Win32 EXE	confrontation_d140ec1a.exe				
2024-08-02	48 / 73	Win32 EXE	confrontation_79158f61.exe				
Historical Whois Looku	ıps (1) 🛈						
Last Updated + 2024-07-08	Organization					Em	ail
Historical SSL Certifica	ates (1) 🛈						
First seen + 2024-07-08	Subject localhost	Thumbpr 074171bf9e8	int 18f2a602aa15d16c1822647775c5e3				

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.

<u>94.232.46.205</u>	443	E831C0DF07470D07192E085028AACEA52B38279837A4C2D99A30BB0C78C014 7B(1)	2024-08-01 16:33:49	2024-08-14 04:38:52
<u>217.195.153.204</u>	443	2FF8B7D65F89735832391FD5C1C241FB8655B04BCAF20C3EF9EAE4DB402DF6 11(1)	2024-08-02 00:47:49	2024-08-03 10:08:11
<u>185.81.114.243</u>	443	ED8BA798679CC1CFE64D0E49AB6E8F9BFC030A1C320A55F5754787941B1A84	2024-08-04 23:56:45	2024-08-13 04:18:17
<u>89.251.22.26</u>	443	683A9753CF9DC19C044F5DD3DF8D269240811181814208A2EF7E0C0D182C33 A8(1)	2024-08-02 16:46:20	2024-08-04 20:53:16
<u>23.254.230.8</u>	443	51DDFD46A9AD37B1A1AFB5139FB34F26126F55F35DC8EF912F3CCB9062AAE3 32(1)	2024-08-03 00:47:05	2024-08-04 01:33:27
<u>185.196.11.28</u>	443	A8B3B1E8E7407F913F0A36AD21A39AC52CCF0D0C052BDC44438993492FBFD 95B(1)	2024-08-02 10:49:28	2024-08-10 20:45:41
<u>62.106.66.46</u>	443	06C630778E6F040E2B4ABD6CEB5E7277ACC08066F58557D8A0EA65F9469EB DFA(1)	2024-08-02 09:12:12	2024-08-12 23:40:15
<u>193.243.147.77</u>	443	9A8AE4AC8F7523DB551C5BFC24B4D52494D971F14ABEA1FE47D9385EF535B0 55(1)	2024-07-22 12:46:59	2024-08-04 14:46:11
<u>23.227.203.161</u>	443	94E9F0C4A286311C2A47ECF0B62453772365D2E1C1528EBAD3FC26B3214992 39(1)	2024-08-03 00:43:27	2024-08-04 20:47:45
45.129.199.25	443	CD661F5C4C823492004CB5C9E9301F5B1FF07D4CDB46F1568F777F60E28CB8 1A(1)	2024-07-07 14:56:12	2024-08-04 21:19:39
<u>45.143.166.190</u>	443	E31642A25040649A2C5ABFCC96806742D88884B5314AED1D93F3F6F2CAF8E4 81(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.

			C' Reanalyze 🗢 Similar ∨ 🞇 Graph 🚸 API
(93 × Community Score ♥	45.129.199.25 (45.129.199.0/24) AS 62005 (BlueVPS OU ) self-signed		EE Last Analysis Date 10 days ago
DETECTION DET	AILS RELATIONS COMMUNITY		
Join our Community an	nd enjoy additional community insights and crowdsourced detections, plus an A	PI key to <b>automate checks.</b>	
Security vendors' analy	sis ()		Do you want to automate checks?
AlphaSOC	() Malware	BitDefender	() Malware
CRDF	① Malicious	CyRadar	① Malware
Fortinet	① Malware	G-Data	① Malware
MalwareURL	① Malware	alphaMountain.ai	() Suspicious
Abusix	⊘ Clean	Acronis	🕑 Clean
ADMINUSLabs	⊘ Clean	AILabs (MONITORAPP)	🕑 Clean
AlienVault	⊘ Clean	Antiy-AVL	🕑 Clean
benkow.cc	⊘ Clean	Blueliv	🕑 Clean
Certego	⊘ Clean	Chong Lua Dao	🕑 Clean
CINS Army	⊘ Clean	CMC Threat Intelligence	🕑 Clean
Criminal IP	⊘ Clean	Cyble	🕑 Clean

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/