First Shift CTF Writeup
Author: Ernest Nyabayo Osindo

The first SOC shift won't be that challenging, right?

Probably Just Fine

Welcome to your first shift! You are greeted by an internal alert on the SOC dashboard titled "Unusual VPN login of susan.martin@probablyfine.thm from 37.19.201.132 (Singapore)."

The SOC handover notes did indeed mention that Susan from Marketing is in Singapore, attending a security vendor conference. It is probably just fine, but the SOC procedure tells us to verify each IP in our threat intel platform TryDetectThis. Answer the first two questions to gather more information and determine the threat level.

TryDetectThis

TryDetectThis is a threat intelligence database to check the reputation and other details of IP addresses, domains, and file hashes. To access this platform, please navigate to the following URL in your own browser:https://static-labs.tryhackme.cloud/apps/trydetectthis/

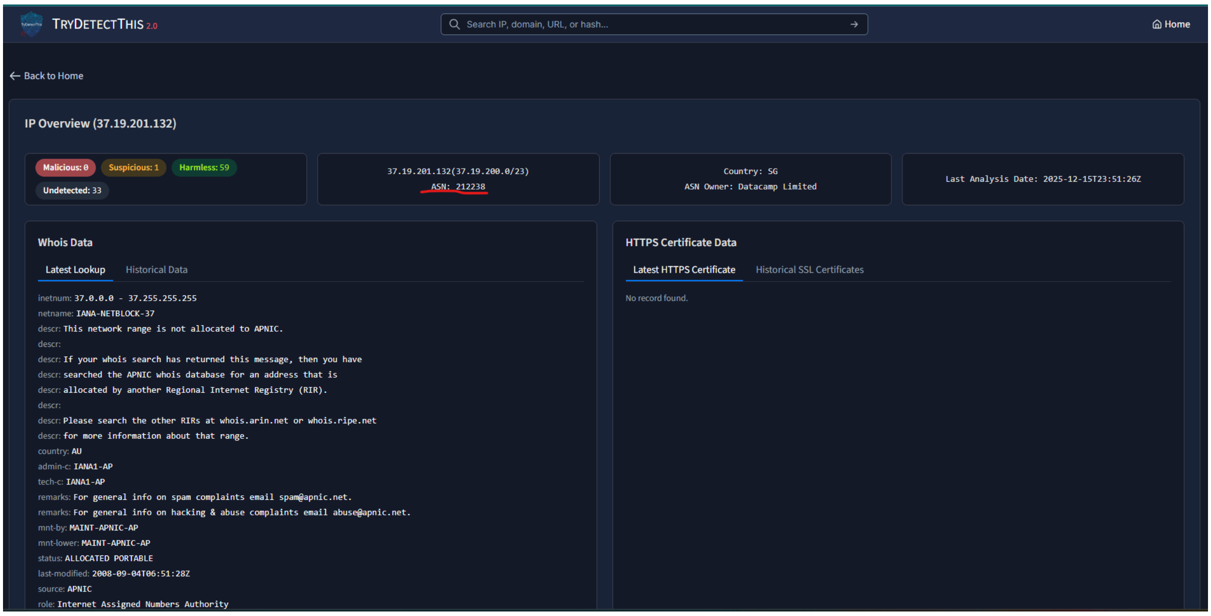
VirusTotal

Another Threat Intelligence database:https://www.virustotal.com/

Is It Really Fine

That login IP looks suspicious, doesn't it? Your teammates reached out to Susan, and she confirmed she did not log in to the company VPN. She also mentioned that while using a public Wi-Fi hotspot at a cafe, she was suddenly prompted to install a "security check" tool, which she did. The host telemetry reveals a suspicious binary with the hash b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630. Can you help us figure out what this binary exactly does and answer the remaining questions?

What is the ASN number related to the IP?



IP Overview (37.19.201.132)

Malicious: 0 Suspicious: 1 Harmless: 59
Undetected: 33

37.19.201.132(37.19.200.0/23)
ASN: 212238

Country: SG
ASN Owner: Datacamp Limited

Last Analysis Date: 2025-12-15T23:51:26Z

Whois Data

Latest Lookup | Historical Data

```
inetnum: 37.0.0.0 - 37.255.255.255
netname: IANA-NETBLOCK-37
descr: This network range is not allocated to APNIC.
descr:
descr: If your whois search has returned this message, then you have
descr: searched the APNIC whois database for an address that is
descr: allocated by another Regional Internet Registry (RIR).
descr:
descr: Please search the other RIRs at whois.arin.net or whois.ripe.net
descr: for more information about that range.
country: AU
admin-c: IANA1-AP
tech-c: IANA1-AP
remarks: For general info on spam complaints email spam@apnic.net.
remarks: For general info on hacking & abuse complaints email abuse@apnic.net.
mnt-by: MAINT-APNIC-AP
mnt-lower: MAINT-APNIC-AP
status: ALLOCATED PORTABLE
last-modified: 2008-09-04T06:51:28Z
source: APNIC
role: Internet Assigned Numbers Authority
```

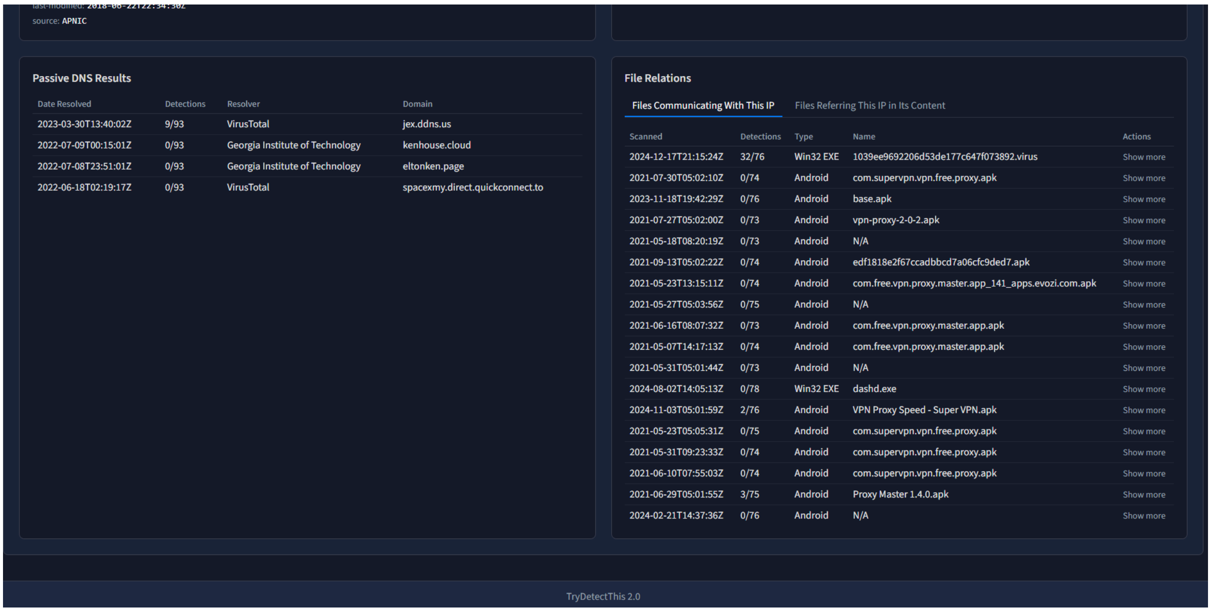
HTTPS Certificate Data

Latest HTTPS Certificate | Historical SSL Certificates

No record found.

Answer: 212238

Which service is offered from this IP?



last-modified: 2018-08-22T22:34:30Z
source: APNIC

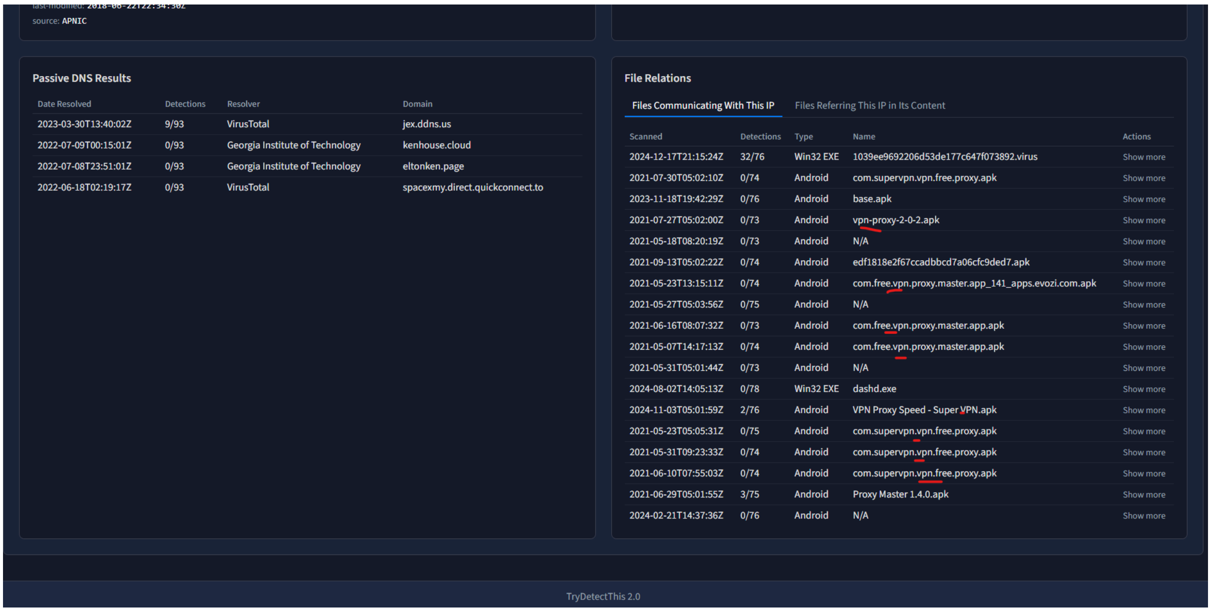
Passive DNS Results

Date Resolved	Detections	Resolver	Domain
2023-03-30T13:40:02Z	9/93	VirusTotal	jex.ddns.us
2022-07-09T00:15:01Z	0/93	Georgia Institute of Technology	kenhouse.cloud
2022-07-08T23:51:01Z	0/93	Georgia Institute of Technology	eltonken.page
2022-06-18T02:19:17Z	0/93	VirusTotal	spacexmy.direct.quickconnect.to

File Relations

Scanned	Detections	Type	Name	Actions
2024-12-17T21:15:24Z	32/76	Win32 EXE	1039ee9692206d53de177c647f073892.virus	Show more
2021-07-30T05:02:10Z	0/74	Android	com.supervpn.vpn.free.proxy.apk	Show more
2023-11-18T19:42:29Z	0/76	Android	base.apk	Show more
2021-07-27T05:02:00Z	0/73	Android	vpn-proxy-2-0-2.apk	Show more
2021-05-18T08:20:19Z	0/73	Android	N/A	Show more
2021-09-13T05:02:22Z	0/74	Android	edf1818e2f67ccadbbcd7a06cfc9ded7.apk	Show more
2021-05-23T13:15:11Z	0/74	Android	com.free.vpn.proxy.master.app_141_apps.evozi.com.apk	Show more
2021-05-27T05:03:56Z	0/75	Android	N/A	Show more
2021-06-16T08:07:32Z	0/73	Android	com.free.vpn.proxy.master.app.apk	Show more
2021-05-07T14:17:13Z	0/74	Android	com.free.vpn.proxy.master.app.apk	Show more
2021-05-31T05:01:44Z	0/73	Android	N/A	Show more
2024-08-02T14:05:13Z	0/78	Win32 EXE	dashd.exe	Show more
2024-11-03T05:01:59Z	2/76	Android	VPN Proxy Speed - Super VPN.apk	Show more
2021-05-23T05:05:31Z	0/75	Android	com.supervpn.vpn.free.proxy.apk	Show more
2021-05-31T09:23:33Z	0/74	Android	com.supervpn.vpn.free.proxy.apk	Show more
2021-06-10T07:55:03Z	0/74	Android	com.supervpn.vpn.free.proxy.apk	Show more
2021-06-29T05:01:55Z	3/75	Android	Proxy Master 1.4.0.apk	Show more
2024-02-21T14:37:36Z	0/76	Android	N/A	Show more

TryDetectThis 2.0



last-modified: 2018-08-22T22:34:30Z
source: APNIC

Passive DNS Results

Date Resolved	Detections	Resolver	Domain
2023-03-30T13:40:02Z	9/93	VirusTotal	jex.ddns.us
2022-07-09T00:15:01Z	0/93	Georgia Institute of Technology	kenhouse.cloud
2022-07-08T23:51:01Z	0/93	Georgia Institute of Technology	eltonken.page
2022-06-18T02:19:17Z	0/93	VirusTotal	spacexmy.direct.quickconnect.to

File Relations

Files Communicating With This IP
Files Referring This IP in Its Content

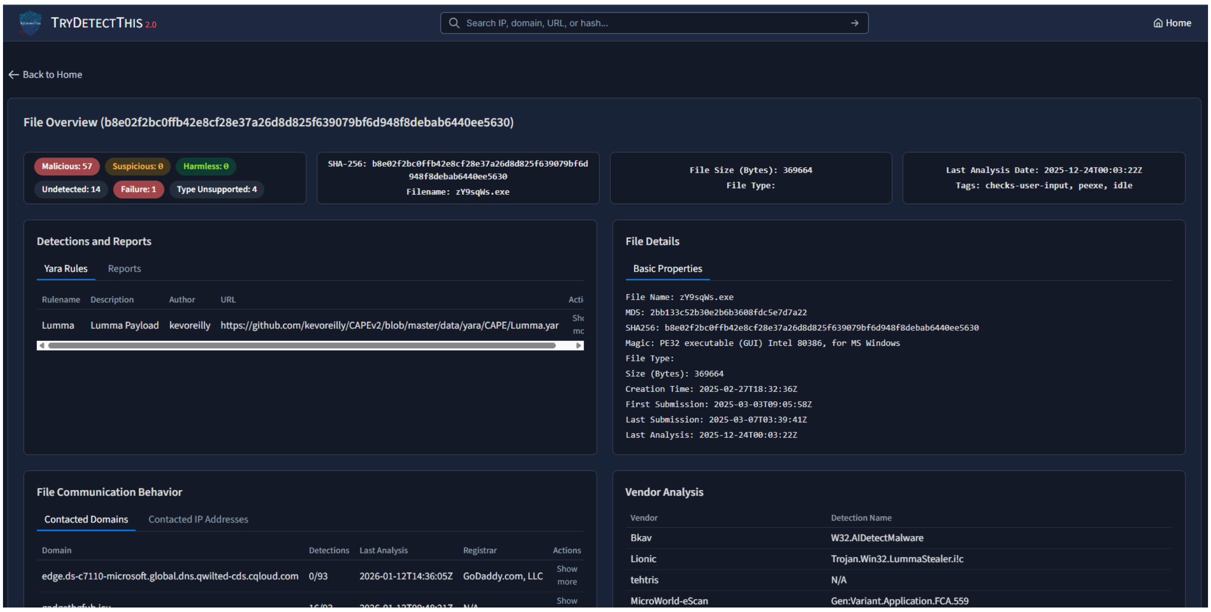
Scanned	Detections	Type	Name	Actions
2024-12-17T21:15:24Z	32/76	Win32 EXE	1039ee9692206d53de177c647f073892.virus	Show more
2021-07-30T05:02:10Z	0/74	Android	com.supervpn.vpn.free.proxy.apk	Show more
2023-11-18T19:42:29Z	0/76	Android	base.apk	Show more
2021-07-27T05:02:00Z	0/73	Android	vpn-proxy-2-0-2.apk	Show more
2021-05-18T08:20:19Z	0/73	Android	N/A	Show more
2021-09-13T05:02:22Z	0/74	Android	edf1818e2f67ccadbbcd7a06cfc9ded7.apk	Show more
2021-05-23T13:15:11Z	0/74	Android	com.free.vpn.proxy.master.app_141_apps.evozi.com.apk	Show more
2021-05-27T05:03:56Z	0/75	Android	N/A	Show more
2021-06-16T08:07:32Z	0/73	Android	com.free.vpn.proxy.master.app.apk	Show more
2021-05-07T14:17:13Z	0/74	Android	com.free.vpn.proxy.master.app.apk	Show more
2021-05-31T05:01:44Z	0/73	Android	N/A	Show more
2024-08-02T14:05:13Z	0/78	Win32 EXE	dashd.exe	Show more
2024-11-03T05:01:59Z	2/76	Android	VPN Proxy Speed - Super VPN.apk	Show more
2021-05-23T05:05:31Z	0/75	Android	com.supervpn.vpn.free.proxy.apk	Show more
2021-05-31T09:23:33Z	0/74	Android	com.supervpn.vpn.free.proxy.apk	Show more
2021-06-10T07:55:03Z	0/74	Android	com.supervpn.vpn.free.proxy.apk	Show more
2021-06-29T05:01:55Z	3/75	Android	Proxy Master 1.4.0.apk	Show more
2024-02-21T14:37:36Z	0/76	Android	N/A	Show more

TryDetectThis 2.0

Answer: VPN

What is the filename of the file related to the hash?

B8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630



File Overview (b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630)

Malicious: 57 Suspicious: 0 Harmless: 0 Undetected: 14 Failure: 1 Type Unsupported: 4

```
SHA-256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d
948f8debab6440ee5630
Filename: zY9sqWs.exe
```

```
File Size (Bytes): 369664
File Type:
```

```
Last Analysis Date: 2025-12-24T00:03:22Z
Tags: checks-user-input, peexe, idle
```

Detections and Reports

Rulename	Description	Author	URL	Acti
Lumma	Lumma Payload	kevoreilly	https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/Lumma.yar	Sho mo

File Details

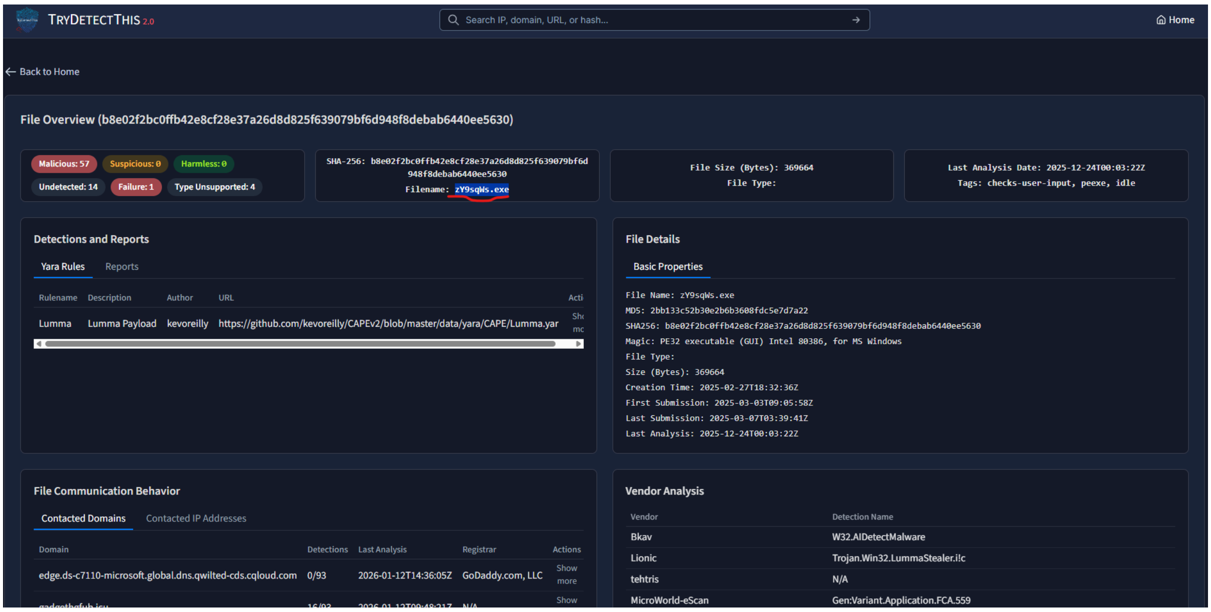
```
File Name: zY9sqWs.exe
MD5: 2bb133c52b30e2b6b3608fdc5e7d7a22
SHA256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630
Magic: PE32 executable (GUI) Intel 80386, for MS Windows
File Type:
Size (Bytes): 369664
Creation Time: 2025-02-27T18:32:36Z
First Submission: 2025-03-03T09:05:58Z
Last Submission: 2025-03-07T03:39:41Z
Last Analysis: 2025-12-24T00:03:22Z
```

File Communication Behavior

Domain	Detections	Last Analysis	Registrar	Actions
edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com	0/93	2026-01-12T14:36:05Z	GoDaddy.com, LLC	Show more
gadgethfub.icu	16/93	2026-01-12T09:48:21Z	N/A	Show

Vendor Analysis

Vendor	Detection Name
Bkav	W32.AIDetectMalware
Lionic	Trojan.Win32.LummaStealer.i!c
tehtris	N/A
MicroWorld-eScan	Gen:Variant.Application.FCA.559



TRYDETECTTHIS 2.0
Search IP, domain, URL, or hash...
Home
Back to Home

File Overview (b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630)

Malicious: 57 Suspicious: 0 Harmless: 0 Undetected: 14 Failure: 1 Type Unsupported: 4

SHA-256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d
948f8debab6440ee5630
Filename: zY9sqWs.exe

File Size (Bytes): 369664
File Type:

Last Analysis Date: 2025-12-24T00:03:22Z
Tags: checks-user-input, peexe, idle

Detections and Reports
Yara Rules Reports

Rulename	Description	Author	URL	Acti
Lumma	Lumma Payload	kevoreilly	https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/Lumma.yar	Sho mo

File Details
Basic Properties

File Name: zY9sqWs.exe
MD5: 2bb133c52b30e2b6b3608fdc5e7d7a22
SHA256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630
Magic: PE32 executable (GUI) Intel 80386, for MS Windows
File Type:
Size (Bytes): 369664
Creation Time: 2025-02-27T18:32:36Z
First Submission: 2025-03-03T09:05:58Z
Last Submission: 2025-03-07T03:39:41Z
Last Analysis: 2025-12-24T00:03:22Z

File Communication Behavior
Contacted Domains Contacted IP Addresses

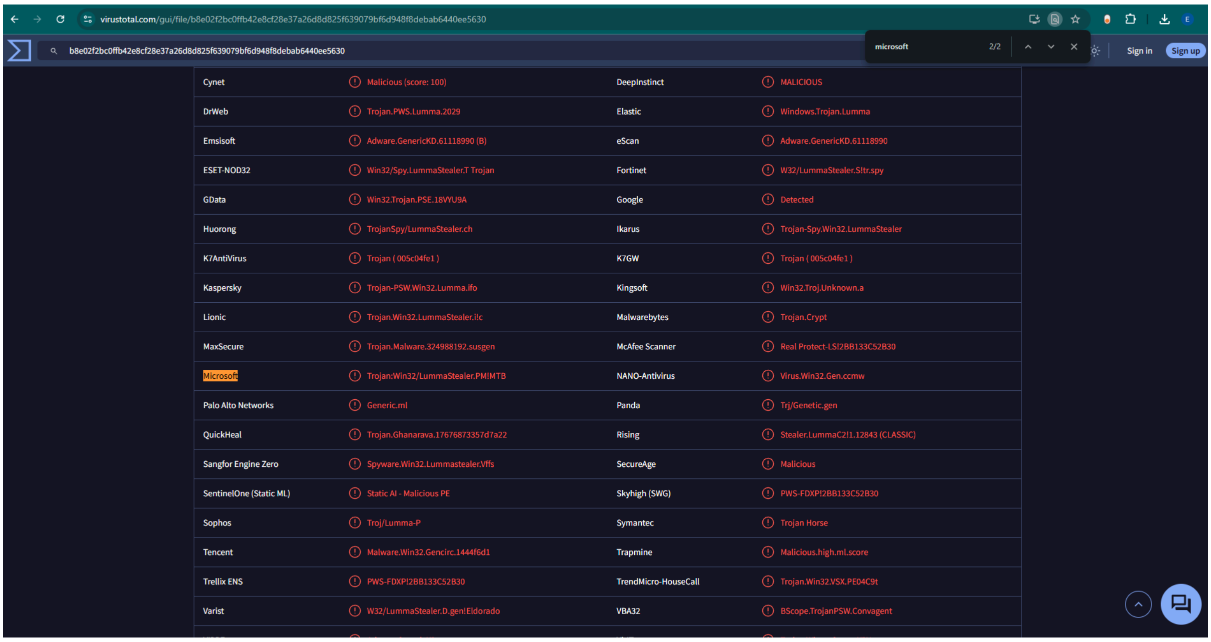
Domain	Detections	Last Analysis	Registrar	Actions
edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com	0/93	2026-01-12T14:36:05Z	GoDaddy.com, LLC	Show more
gadgethfub.icu	16/93	2026-01-12T09:48:21Z	N/A	Show

Vendor Analysis

Vendor	Detection Name
Bkav	W32.AIDetectMalware
Lionic	Trojan.Win32.LummaStealer.i!c
tehtris	N/A
MicroWorld-eScan	Gen:Variant.Application.FCA.559

Answer: zY9sqWs.exe

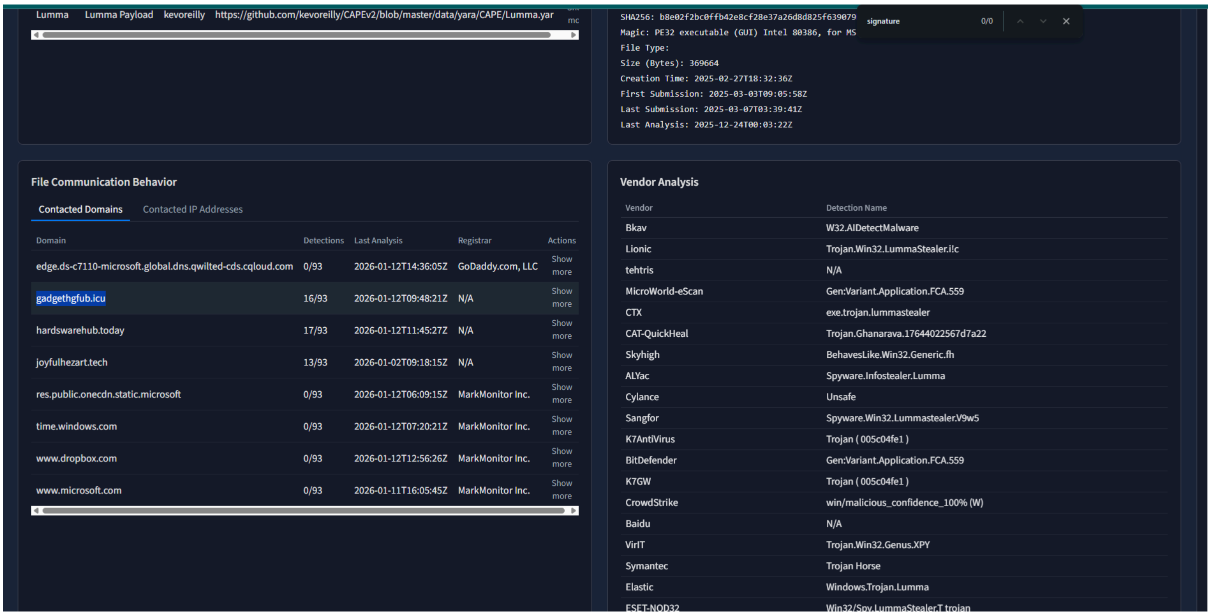
What is the threat signature that Microsoft assigned to the file?


virustotal.com/gui/file/b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630
b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630
microsoft 2/2
Sign in
Sign up

Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	Trojan.PWS.Lumma.2029	Elastic	Windows.Trojan.Lumma
Emsisoft	Adware.GenericKD.61118990 (B)	eScan	Adware.GenericKD.61118990
ESET-NOD32	Win32/Spy.LummaStealer.T Trojan	Fortinet	W32/LummaStealer.S!tr.spy
GData	Win32.Trojan.PSE.18VYU9A	Google	Detected
Huorong	TrojanSpy/LummaStealer.ch	Ikarus	Trojan-Spy.Win32.LummaStealer
K7AntiVirus	Trojan (005c04fe1)	K7GW	Trojan (005c04fe1)
Kaspersky	Trojan-PSW.Win32.Lumma.ifo	Kingsoft	Win32.Troj.Unknown.a
Lionic	Trojan.Win32.LummaStealer.i!c	Malwarebytes	Trojan.Crypt
MaxSecure	Trojan.Malware.324988192.susgen	McAfee Scanner	Real Protect-LS!2BB133C52B30
Microsoft	Trojan:Win32/LummaStealer.PM!MTB	NANO-Antivirus	Virus.Win32.Gen.ccmw
Palo Alto Networks	Generic.ml	Panda	Trj/Genetic.gen
QuickHeal	Trojan.Ghanarava.17676873357d7a22	Rising	Stealer.LummaC2!1.12843 (CLASSIC)
Sangfor Engine Zero	Spyware.Win32.Lummastealer.Vffs	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE	Skyhigh (SWG)	PWS-FDXP!2BB133C52B30
Sophos	Troj/Lumma-P	Symantec	Trojan Horse
Tencent	Malware.Win32.Gencirc.1444f6d1	Trapmine	Malicious.high.ml.score
Trellix ENS	PWS-FDXP!2BB133C52B30	TrendMicro-HouseCall	Trojan.Win32.VSX.PE04C9t
Varist	W32/LummaStealer.D.gen!Eldorado	VBA32	BScope.TrojanPSW.Convagent

Answer: Trojan:Win32/LummaStealer.PM!MTB

One of the contacted domains is part of a large malicious infrastructure cluster.
Based on its HTTPS certificate, how many domains are linked to the same campaign?


Lumma Lumma Payload kevoreilly https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/Lumma.yar

```
SHA256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079
Magic: PE32 executable (GUI) Intel 80386, for MS
File Type:
Size (Bytes): 369664
Creation Time: 2025-02-27T18:32:36Z
First Submission: 2025-03-03T09:05:58Z
Last Submission: 2025-03-07T03:39:41Z
Last Analysis: 2025-12-24T00:03:22Z
```

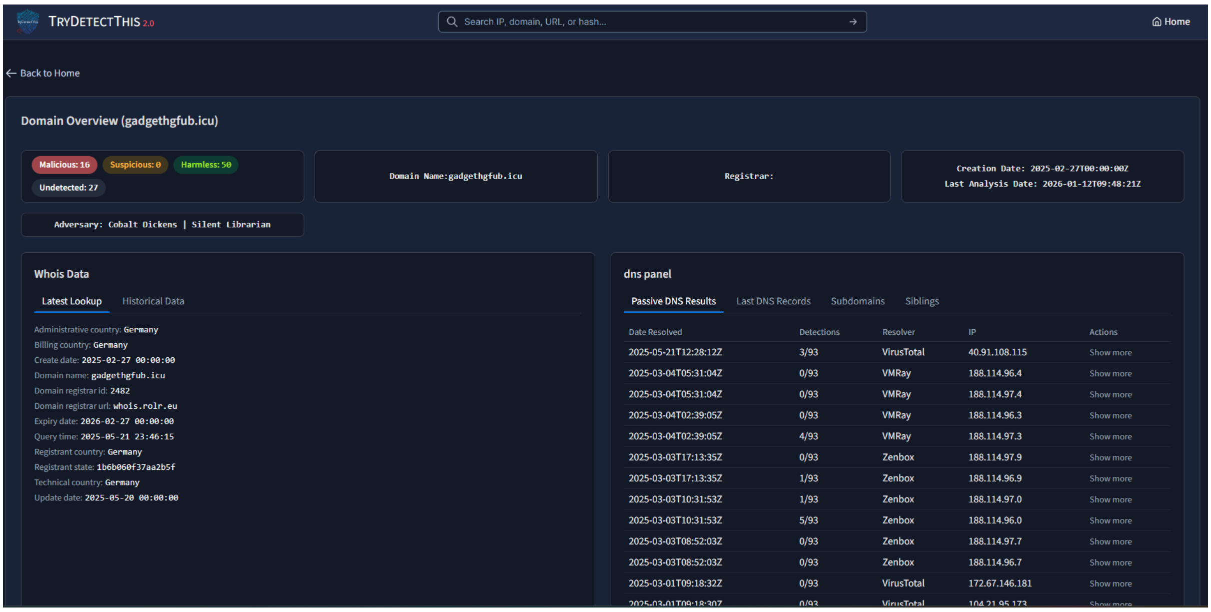
File Communication Behavior

Domain	Detections	Last Analysis	Registrar	Actions
edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com	0/93	2026-01-12T14:36:05Z	GoDaddy.com, LLC	Show more
gadgethgfub.icu	16/93	2026-01-12T09:48:21Z	N/A	Show more
hardswarehub.today	17/93	2026-01-12T11:45:27Z	N/A	Show more
joyfulhezart.tech	13/93	2026-01-02T09:18:15Z	N/A	Show more
res.public.onecdn.static.microsoft	0/93	2026-01-12T06:09:15Z	MarkMonitor Inc.	Show more
time.windows.com	0/93	2026-01-12T07:20:21Z	MarkMonitor Inc.	Show more
www.dropbox.com	0/93	2026-01-12T12:56:26Z	MarkMonitor Inc.	Show more
www.microsoft.com	0/93	2026-01-11T16:05:45Z	MarkMonitor Inc.	Show more

Vendor Analysis

Vendor	Detection Name
Bkav	W32.AIDetectMalware
Lionic	Trojan.Win32.LummaStealer.i!c
tehtris	N/A
MicroWorld-eScan	Gen:Variant.Application.FCA.559
CTX	exe.trojan.lummastealer
CAT-QuickHeal	Trojan.Ghanarava.17644022567d7a22
Skyhigh	BehavesLike.Win32.Generic.fh
ALYac	Spyware.Infostealer.Lumma
Cylance	Unsafe
Sangfor	Spyware.Win32.Lummastealer.V9w5
K7AntiVirus	Trojan (005c04fe1)
BitDefender	Gen:Variant.Application.FCA.559
K7GW	Trojan (005c04fe1)
CrowdStrike	win/malicious_confidence_100% (W)
Baidu	N/A
VirIT	Trojan.Win32.Genus.XPY
Symantec	Trojan Horse
Elastic	Windows.Trojan.Lumma
ESET-NOD32	Win32/Spy.LummaStealer.T trojan

One of the contacted domains: **gadgethgfub.icu**
Search this domain on TryDetect this



Domain Overview (gadgethgfub.icu)

Malicious: 16 Suspicious: 0 Harmless: 50 Undetected: 27

Domain Name:gadgethgfub.icu

Registrar:

Creation Date: 2025-02-27T00:00:00Z
Last Analysis Date: 2026-01-12T09:48:21Z

Adversary: Cobalt Dickens | Silent Librarian

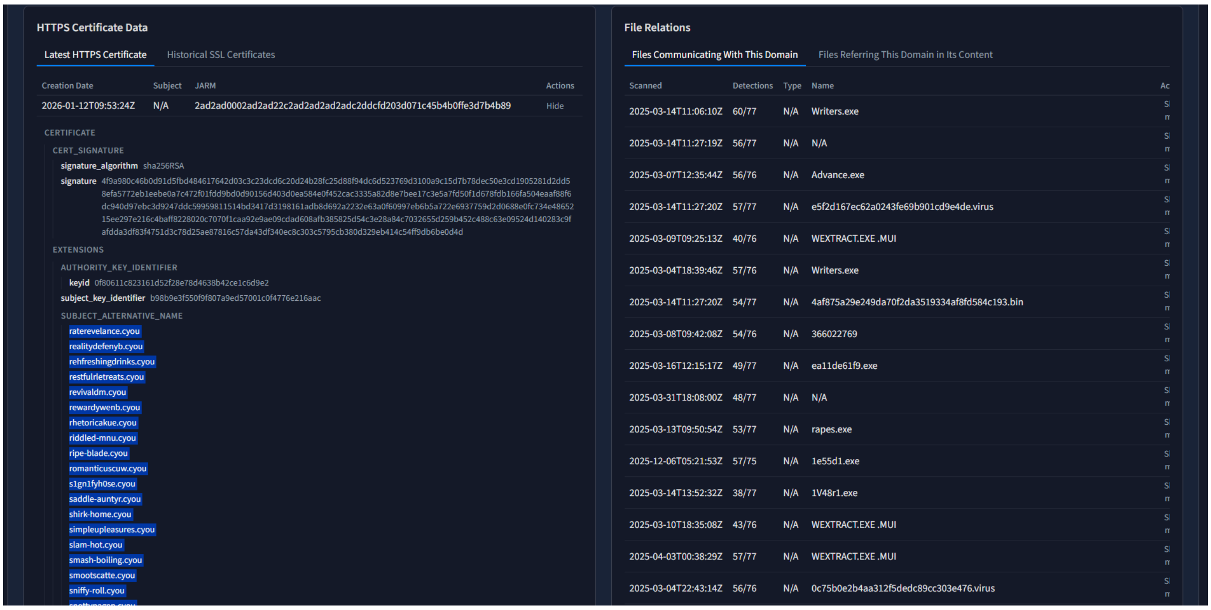
Whois Data

Administrative country: Germany
Billing country: Germany
Create date: 2025-02-27 00:00:00
Domain name: gadgethgfub.icu
Domain registrar id: 2482
Domain registrar url: whois.rolr.eu
Expiry date: 2026-02-27 00:00:00
Query time: 2025-05-21 23:46:15
Registrant country: Germany
Registrant state: 1b6b060f37aa2b5f
Technical country: Germany
Update date: 2025-05-20 00:00:00

dns panel

Date Resolved	Detections	Resolver	IP	Actions
2025-05-21T12:28:12Z	3/93	VirusTotal	40.91.108.115	Show more
2025-03-04T05:31:04Z	0/93	VMRay	188.114.96.4	Show more
2025-03-04T05:31:04Z	0/93	VMRay	188.114.97.4	Show more
2025-03-04T02:39:05Z	0/93	VMRay	188.114.96.3	Show more
2025-03-04T02:39:05Z	4/93	VMRay	188.114.97.3	Show more
2025-03-03T17:13:35Z	0/93	Zenbox	188.114.97.9	Show more
2025-03-03T17:13:35Z	1/93	Zenbox	188.114.96.9	Show more
2025-03-03T10:31:53Z	1/93	Zenbox	188.114.97.0	Show more
2025-03-03T10:31:53Z	5/93	Zenbox	188.114.96.0	Show more
2025-03-03T08:52:03Z	0/93	Zenbox	188.114.97.7	Show more
2025-03-03T08:52:03Z	0/93	Zenbox	188.114.96.7	Show more
2025-03-01T09:18:32Z	0/93	VirusTotal	172.67.146.181	Show more
2025-03-01T09:18:30Z	0/93	VirusTotal	104.21.95.173	Show more

Scroll down to the HTTPS Certificate Data and copy the list of the domains as shown below



HTTPS Certificate Data

Creation Date	Subject	JARM	Actions
2026-01-12T09:53:24Z	N/A	2ad2ad0002ad2ad22c2ad2ad2ad2adc2ddcfd203d071c45b4b0ffe3d7b4b89	Hide

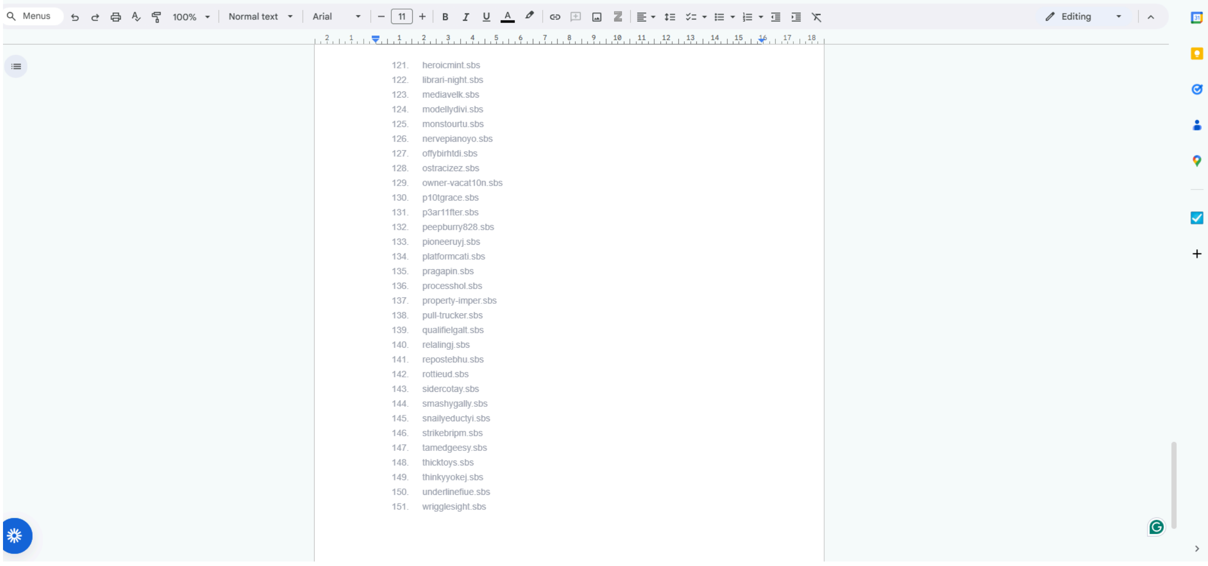
```
CERTIFICATE
  CERT_SIGNATURE
    signature_algorithm sha256RSA
    signature 4f9a980c46b0d91d5fbd484617642d03c3c23dcd6c20d24b28fc25d88f94dc6d523769d3100a9c15d7b78dec50e3cd1905281d2dd5
              8efa5772eb1eebe0a7c472f01fdd9bd0d90156d403d0ea584e0f452cac3335a82d8e7bee17c3e5a7fd50f1d678fdb166fa504eaaf88f6
              dc940d97ebc3d9247ddc59959811514bd3417d3198161adb8d692a2232e63a0f60997eb6b5a722e6937759d2d0688e0fc734e48652
              15ee297e216c4baff8228020c7070f1caa92e9ae09cdad608afb385825d54c3e28a84c7032655d259b452c488c63e09524d140283c9f
              afdda3df83f4751d3c78d25ae87816c57da43df340ec8c303c5795cb380d329eb414c54ff9db6be0d4d
  EXTENSIONS
    AUTHORITY_KEY_IDENTIFIER
      keyid 0f80611c823161d52f28e78d4638b42ce1c6d9e2
    subject_key_identifier b98b9e3f550f9f807a9ed57001c0f4776e216aac
    SUBJECT_ALTERNATIVE_NAME
      raterevelance.cyou
      realitydefenyb.cyou
      rehfreshingdrinks.cyou
      restfulrletreats.cyou
      revivaldm.cyou
      rewardywenb.cyou
      rhetoricakue.cyou
      riddled-mnu.cyou
      ripe-blade.cyou
      romanticuscuw.cyou
      s1gn1fyh0se.cyou
      saddle-auntyr.cyou
      shirk-home.cyou
      simpleupleasures.cyou
      slam-hot.cyou
      smash-boiling.cyou
      smootscatte.cyou
      sniffy-roll.cyou
```

File Relations

Files Communicating With This Domain
Files Referring This Domain in Its Content

Scanned	Detections	Type	Name	Ac
2025-03-14T11:06:10Z	60/77	N/A	Writers.exe	S n
2025-03-14T11:27:19Z	56/77	N/A	N/A	S n
2025-03-07T12:35:44Z	56/76	N/A	Advance.exe	S n
2025-03-14T11:27:20Z	57/77	N/A	e5f2d167ec62a0243fe69b901cd9e4de.virus	S n
2025-03-09T09:25:13Z	40/76	N/A	WEXTRACT.EXE .MUI	S n
2025-03-04T18:39:46Z	57/76	N/A	Writers.exe	S n
2025-03-14T11:27:20Z	54/77	N/A	4af875a29e249da70f2da3519334af8fd584c193.bin	S n
2025-03-08T09:42:08Z	54/76	N/A	366022769	S n
2025-03-16T12:15:17Z	49/77	N/A	ea11de61f9.exe	S n
2025-03-31T18:08:00Z	48/77	N/A	N/A	S n
2025-03-13T09:50:54Z	53/77	N/A	rapes.exe	S n
2025-12-06T05:21:53Z	57/75	N/A	1e55d1.exe	S n
2025-03-14T13:52:32Z	38/77	N/A	1V48r1.exe	S n
2025-03-10T18:35:08Z	43/76	N/A	WEXTRACT.EXE .MUI	S n
2025-04-03T00:38:29Z	57/77	N/A	WEXTRACT.EXE .MUI	S n
2025-03-04T22:43:14Z	56/76	N/A	0c75b0e2b4aa312f5dedc89cc303e476.virus	S n

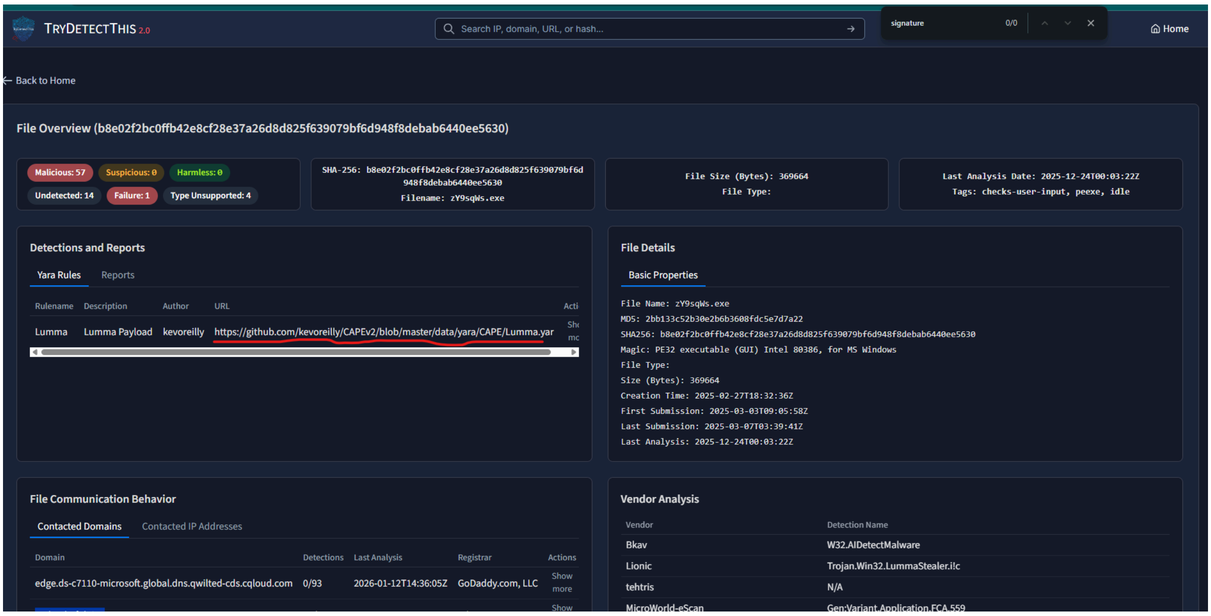
Paste the list in a document to count using the automatic numbering



121. heroicmint.sbs
122. librari-night.sbs
123. mediavelk.sbs
124. modellydivi.sbs
125. monstourtu.sbs
126. nervepianoyo.sbs
127. offybirhtdi.sbs
128. ostracizez.sbs
129. owner-vacat10n.sbs
130. p10tgrace.sbs
131. p3ar11fter.sbs
132. peepburry828.sbs
133. pioneeruyj.sbs
134. platformcati.sbs
135. pragapin.sbs
136. processhol.sbs
137. property-imper.sbs
138. pull-trucker.sbs
139. qualifielgalt.sbs
140. relalingj.sbs
141. repostebhu.sbs
142. rottieud.sbs
143. sidercotay.sbs
144. smashygally.sbs
145. snailyeductyi.sbs
146. strikebripm.sbs
147. tamedgeesy.sbs
148. thicktoys.sbs
149. thinkyyokej.sbs
150. underlinefiue.sbs
151. wrigglesight.sbs

Answer: 151

The file matches one of the YARA rules made by "kevoreilly". What line is present in the rule's "condition" field?



File Overview (b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630)

Malicious: 57 Suspicious: 0 Harmless: 0
Undetected: 14 Failure: 1 Type Unsupported: 4

```
SHA-256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d
948f8debab6440ee5630
Filename: zY9sqWs.exe
```

```
File Size (Bytes): 369664
File Type:
```

```
Last Analysis Date: 2025-12-24T00:03:22Z
Tags: checks-user-input, peexe, idle
```

Detections and Reports

Yara Rules | Reports

Rulename	Description	Author	URL	Acti
Lumma	Lumma Payload	kevoreilly	https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/Lumma.yar	Sh mc

File Details

Basic Properties

```
File Name: zY9sqWs.exe
MD5: 2bb133c52b30e2b6b3608fdc5e7d7a22
SHA256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630
Magic: PE32 executable (GUI) Intel 80386, for MS Windows
File Type:
Size (Bytes): 369664
Creation Time: 2025-02-27T18:32:36Z
First Submission: 2025-03-03T09:05:58Z
Last Submission: 2025-03-07T03:39:41Z
Last Analysis: 2025-12-24T00:03:22Z
```

File Communication Behavior

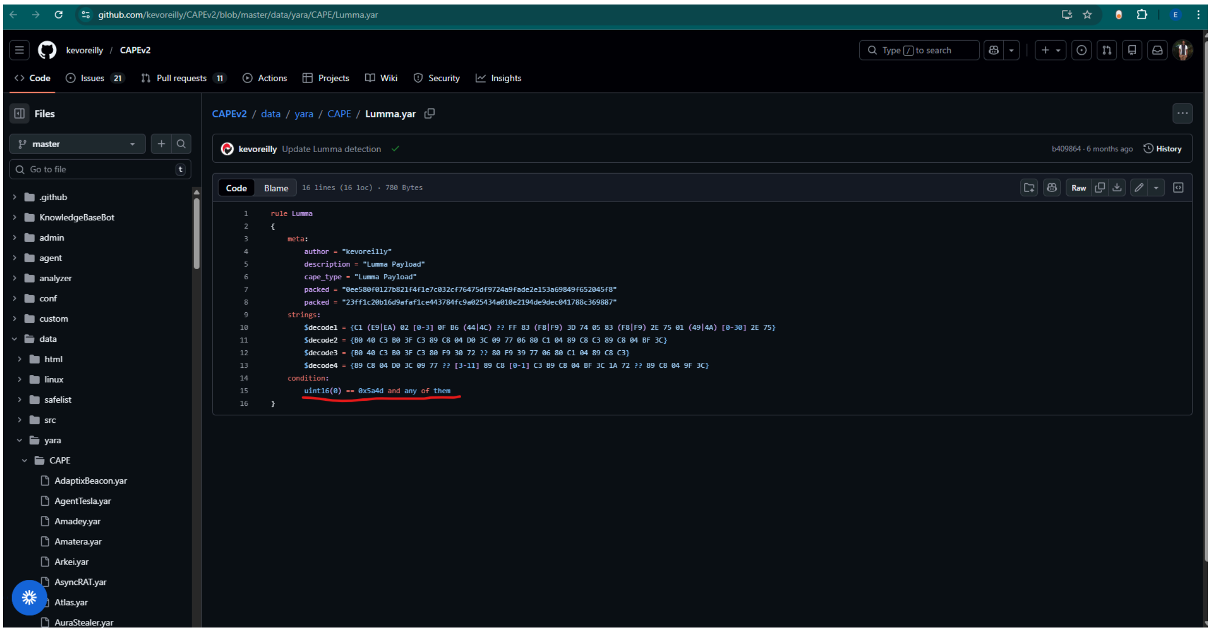
Contacted Domains | Contacted IP Addresses

Domain	Detections	Last Analysis	Registrar	Actions
edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com	0/93	2026-01-12T14:36:05Z	GoDaddy.com, LLC	Show more
				Show

Vendor Analysis

Vendor	Detection Name
Bkav	W32.AIDetectMalware
Lionic	Trojan.Win32.LummaStealer.i!c
tehtris	N/A
MicroWorld-eScan	Gen:Variant.Application.FCA.559

Copy the link and browse it:
https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/Lumma.yar



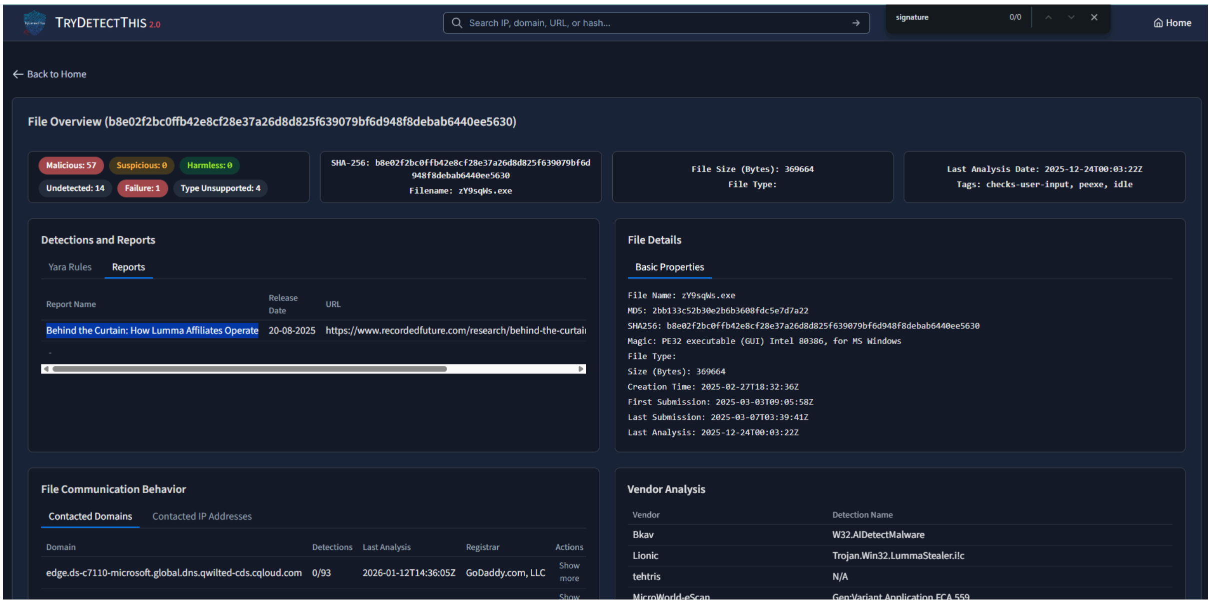
kevoreilly Update Lumma detection ✓

16 lines (16 loc) · 780 Bytes

```
rule Lumma
{
    meta:
        author = "kevoreilly"
        description = "Lumma Payload"
        cape_type = "Lumma Payload"
        packed = "0ee580f0127b821f4f1e7c032cf76475df9724a9fade2e153a69849f652045f8"
        packed = "23ff1c20b16d9afaf1ce443784fc9a025434a010e2194de9dec041788c369887"
    strings:
        $decode1 = {C1 (E9|EA) 02 [0-3] 0F B6 (44|4C) ?? FF 83 (F8|F9) 3D 74 05 83 (F8|F9) 2E 75 01 (49|4A) [0-30] 2E 75}
        $decode2 = {B0 40 C3 B0 3F C3 89 C8 04 D0 3C 09 77 06 80 C1 04 89 C8 C3 89 C8 04 BF 3C}
        $decode3 = {B0 40 C3 B0 3F C3 80 F9 30 72 ?? 80 F9 39 77 06 80 C1 04 89 C8 C3}
        $decode4 = {89 C8 04 D0 3C 09 77 ?? [3-11] 89 C8 [0-1] C3 89 C8 04 BF 3C 1A 72 ?? 89 C8 04 9F 3C}
    condition:
        uint16(0) == 0x5a4d and any of them
}
```

Answer: uint16(0) == 0x5a4d and any of them

The file is also mentioned in one of the TI reports. What is the title of the report mentioning this hash?



File Overview (b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630)

Malicious: 57 Suspicious: 0 Harmless: 0
Undetected: 14 Failure: 1 Type Unsupported: 4

SHA-256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630
Filename: zY9sqWs.exe

File Size (Bytes): 369664
File Type:

Last Analysis Date: 2025-12-24T00:03:22Z
Tags: checks-user-input, peexe, idle

Detections and Reports

Yara Rules | Reports

Report Name	Release Date	URL
Behind the Curtain: How Lumma Affiliates Operate	20-08-2025	https://www.recordedfuture.com/research/behind-the-curtai
-		

File Details

Basic Properties

```
File Name: zY9sqWs.exe
MD5: 2bb133c52b30e2b6b3608fdc5e7d7a22
SHA256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630
Magic: PE32 executable (GUI) Intel 80386, for MS Windows
File Type:
Size (Bytes): 369664
Creation Time: 2025-02-27T18:32:36Z
First Submission: 2025-03-03T09:05:58Z
Last Submission: 2025-03-07T03:39:41Z
Last Analysis: 2025-12-24T00:03:22Z
```

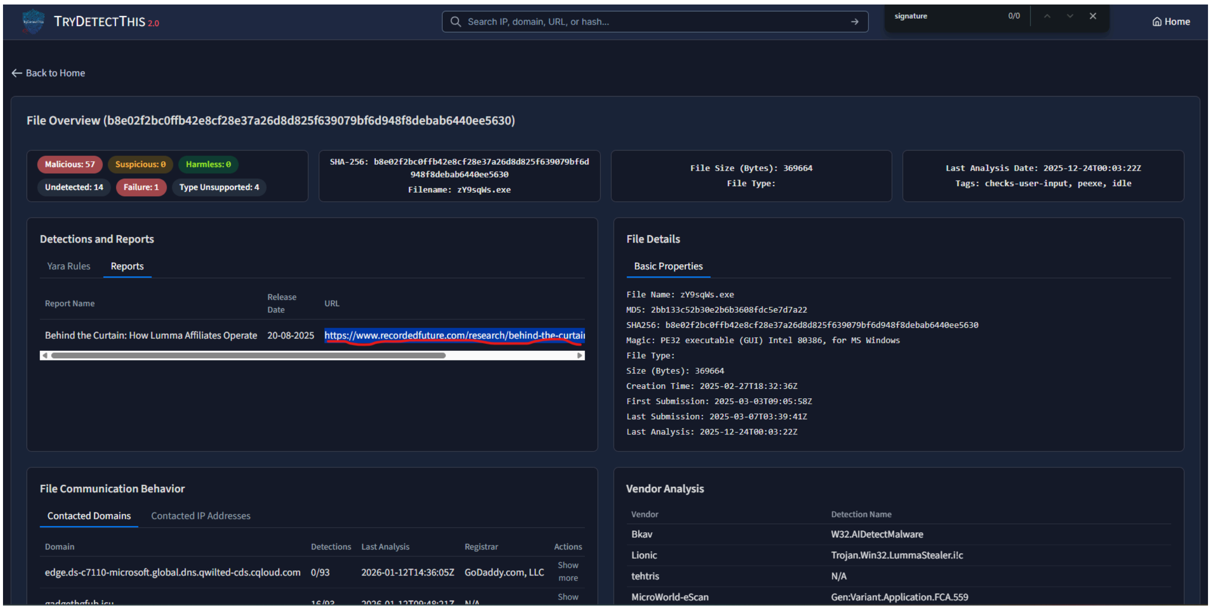
File Communication Behavior

Contacted Domains | Contacted IP Addresses

Domain	Detections	Last Analysis	Registrar	Actions
edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com	0/93	2026-01-12T14:36:05Z	GoDaddy.com, LLC	Show more
				Show

Vendor Analysis

Vendor	Detection Name
Bkav	W32.AIDetectMalware
Lionic	Trojan.Win32.LummaStealer.i!c
tehtris	N/A
MicroWorld-eScan	Gen:Variant.Application.FCA.559



File Overview (b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630)

Malicious: 57 Suspicious: 0 Harmless: 0
Undetected: 14 Failure: 1 Type Unsupported: 4

SHA-256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630
Filename: zY9sqWs.exe

File Size (Bytes): 369664
File Type:

Last Analysis Date: 2025-12-24T00:03:22Z
Tags: checks-user-input, peexe, idle

Detections and Reports

Yara Rules | Reports

Report Name	Release Date	URL
Behind the Curtain: How Lumma Affiliates Operate	20-08-2025	https://www.recordedfuture.com/research/behind-the-curtai

File Details

Basic Properties

```
File Name: zY9sqWs.exe
MD5: 2bb133c52b30e2b6b3608fdc5e7d7a22
SHA256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630
Magic: PE32 executable (GUI) Intel 80386, for MS Windows
File Type:
Size (Bytes): 369664
Creation Time: 2025-02-27T18:32:36Z
First Submission: 2025-03-03T09:05:58Z
Last Submission: 2025-03-07T03:39:41Z
Last Analysis: 2025-12-24T00:03:22Z
```

File Communication Behavior

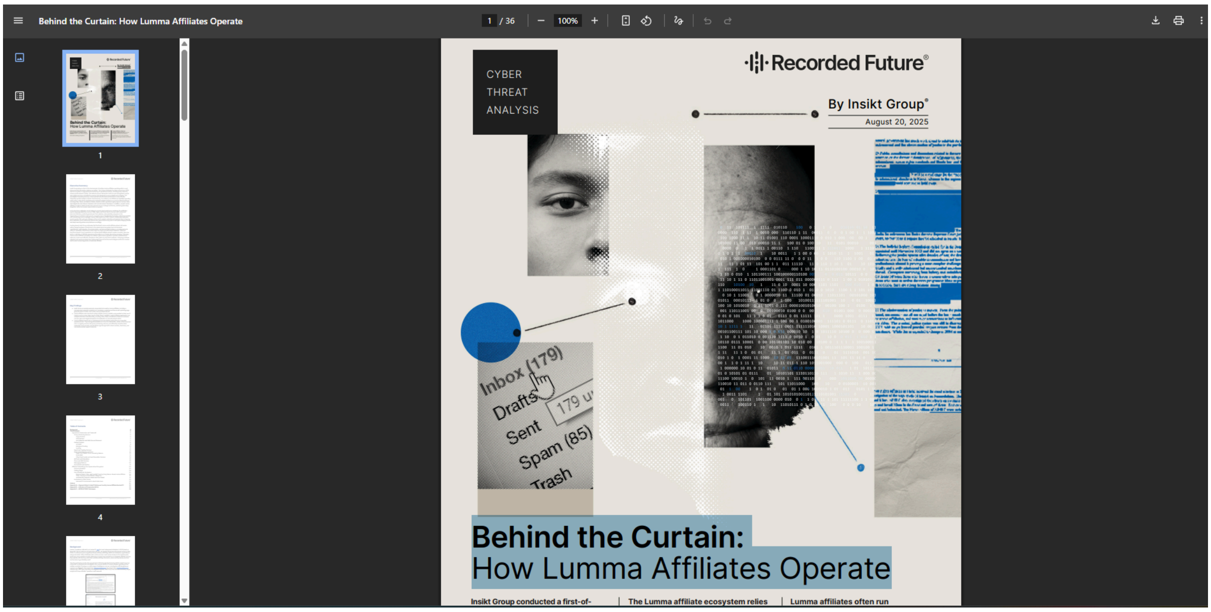
Contacted Domains | Contacted IP Addresses

Domain	Detections	Last Analysis	Registrar	Actions
edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com	0/93	2026-01-12T14:36:05Z	GoDaddy.com, LLC	Show more
gadgethgfub.icu	16/93	2026-01-12T09:48:21Z	N/A	Show

Vendor Analysis

Vendor	Detection Name
Bkav	W32.AIDetectMalware
Lionic	Trojan.Win32.LummaStealer.i!c
tehtris	N/A
MicroWorld-eScan	Gen:Variant.Application.FCA.559

https://www.recordedfuture.com/research/behind-the-curtain-how-lumma-affiliates-operate



CYBER THREAT ANALYSIS

Recorded Future®

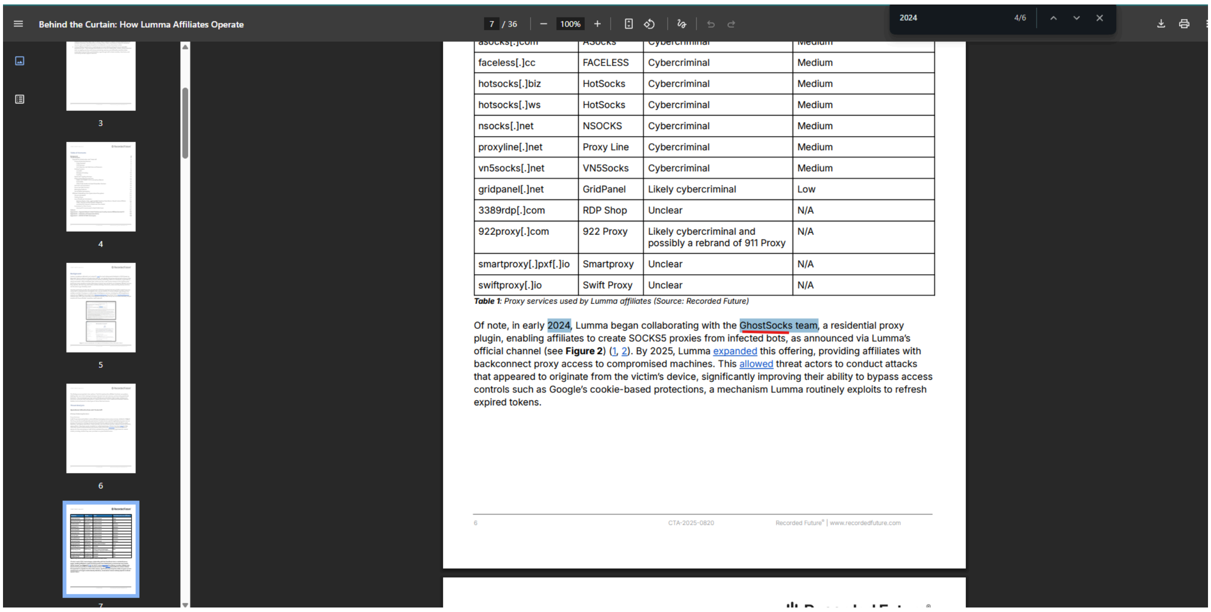
By Insikt Group®
August 20, 2025

Behind the Curtain:
How Lumma Affiliates Operate

Insikt Group conducted a first-of- | The Lumma affiliate ecosystem relies | Lumma affiliates often run

Answer: Behind the Curtain: How Lumma Affiliates Operate

Which team did the author of the malware start collaborating with in early 2024?



asocks[.]com	ASocks	Cybercriminal	Medium
faceless[.]cc	FACELESS	Cybercriminal	Medium
hotsocks[.]biz	HotSocks	Cybercriminal	Medium
hotsocks[.]ws	HotSocks	Cybercriminal	Medium
nsocks[.]net	NSOCKS	Cybercriminal	Medium
proxyline[.]net	Proxy Line	Cybercriminal	Medium
vn5socks[.]net	VN5Socks	Cybercriminal	Medium
gridpanel[.]net	GridPanel	Likely cybercriminal	Low
3389rdp[.]com	RDP Shop	Unclear	N/A
922proxy[.]com	922 Proxy	Likely cybercriminal and possibly a rebrand of 911 Proxy	N/A
smartproxy[.]pxf[.]io	Smartproxy	Unclear	N/A
swiftproxy[.]io	Swift Proxy	Unclear	N/A

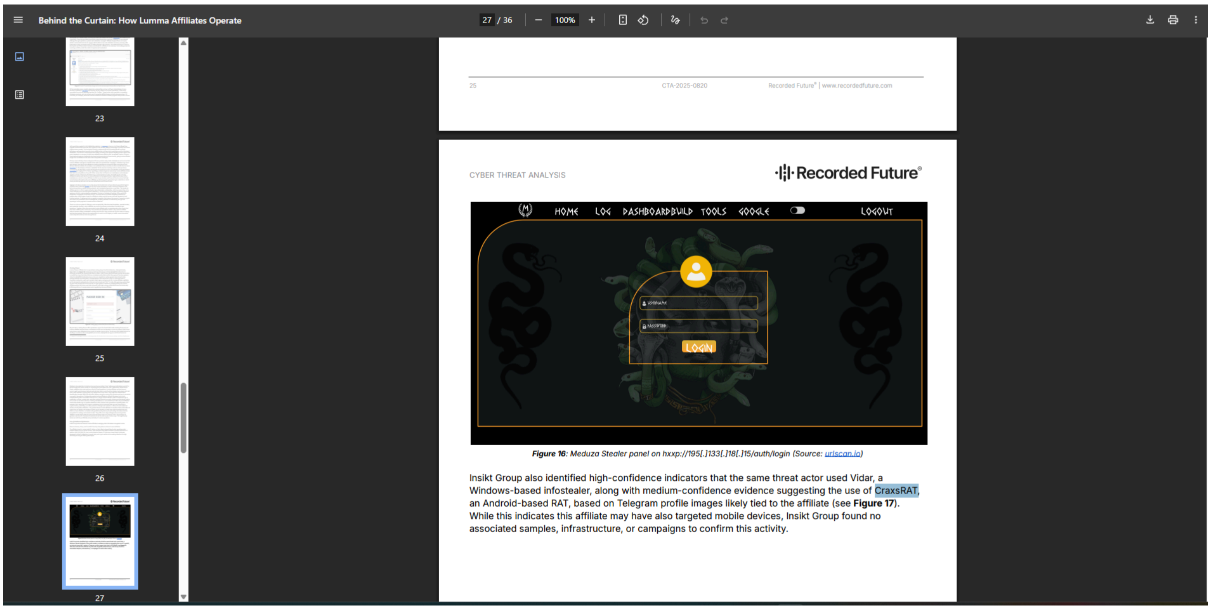
***Table 1**: Proxy services used by Lumma affiliates (Source: Recorded Future)*

Of note, in early 2024, Lumma began collaborating with the GhostSocks team, a residential proxy plugin, enabling affiliates to create SOCKS5 proxies from infected bots, as announced via Lumma's official channel (see **Figure 2**) (1, 2). By 2025, Lumma expanded this offering, providing affiliates with backconnect proxy access to compromised machines. This allowed threat actors to conduct attacks that appeared to originate from the victim's device, significantly improving their ability to bypass access controls such as Google's cookie-based protections, a mechanism Lumma routinely exploits to refresh expired tokens.

6 CTA-2025-0820 Recorded Future® | www.recordedfuture.com

Answer: GhostSocks

A Mexican-based affiliate related to the malware family also uses other infostealers.
Which mentioned infostealer targets Android systems?



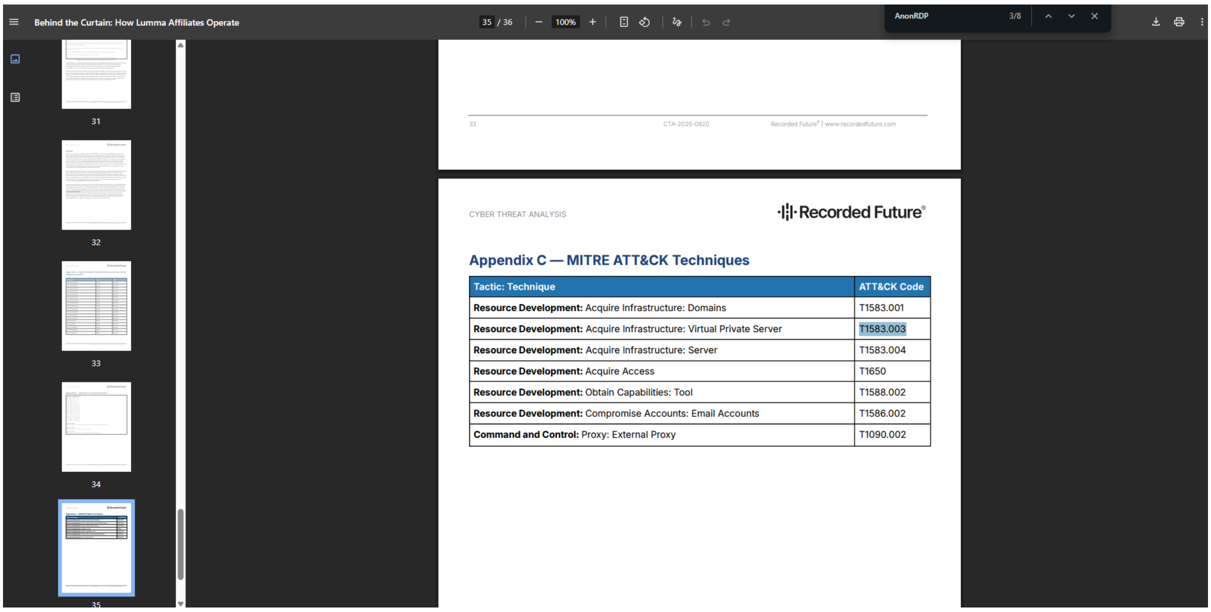
Behind the Curtain: How Lumma Affiliates Operate
27 / 36
100%
25 CTA-2025-0820 Recorded Future® | www.recordedfuture.com
CYBER THREAT ANALYSIS
Recorded Future®
HOME
LOG
DASHBOARD
BUILD
TOOLS
GOOGLE
LOGOUT
LOGIN

***Figure 16**: Meduza Stealer panel on hxxp://195[.]133[.]18[.]15/auth/login (Source: urlscan.io)*

Insikt Group also identified high-confidence indicators that the same threat actor used Vidar, a Windows-based infostealer, along with medium-confidence evidence suggesting the use of CraxsRAT, an Android-based RAT, based on Telegram profile images likely tied to the affiliate (see **Figure 17**). While this indicates this affiliate may have also targeted mobile devices, Insikt Group found no associated samples, infrastructure, or campaigns to confirm this activity.

Answer: CraxsRAT

The report states that the affiliates behind the malware use the services of AnonRDP.
Which MITRE ATT&CK sub-technique does this align with?



33 CTA-2025-0820 Recorded Future® | www.recordedfuture.com

CYBER THREAT ANALYSIS

Recorded Future®

Appendix C — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Resource Development: Acquire Infrastructure: Server	T1583.004
Resource Development: Acquire Access	T1650
Resource Development: Obtain Capabilities: Tool	T1588.002
Resource Development: Compromise Accounts: Email Accounts	T1586.002
Command and Control: Proxy: External Proxy	T1090.002

Answer: T1583.003