Network Forensics Incident Report

Case ID: 2026-LUMMA-001

Investigator: Mohamed Farah

Date: January 23, 2026

Subject: Analysis of Lumma Stealer Infection on Host 160.9.3.101

Executive Summary

On September 3, 2025, a security incident was identified involving host **160.9.3.101**. Forensic analysis of network traffic (PCAP) confirmed a multi-stage infection starting with a malicious ZIP file download, followed by automated Command and Control (C2) beaconing via Windows PowerShell. The attack concluded with the successful exfiltration of system metadata to an external server.

Indicators of Compromise (IOCs)

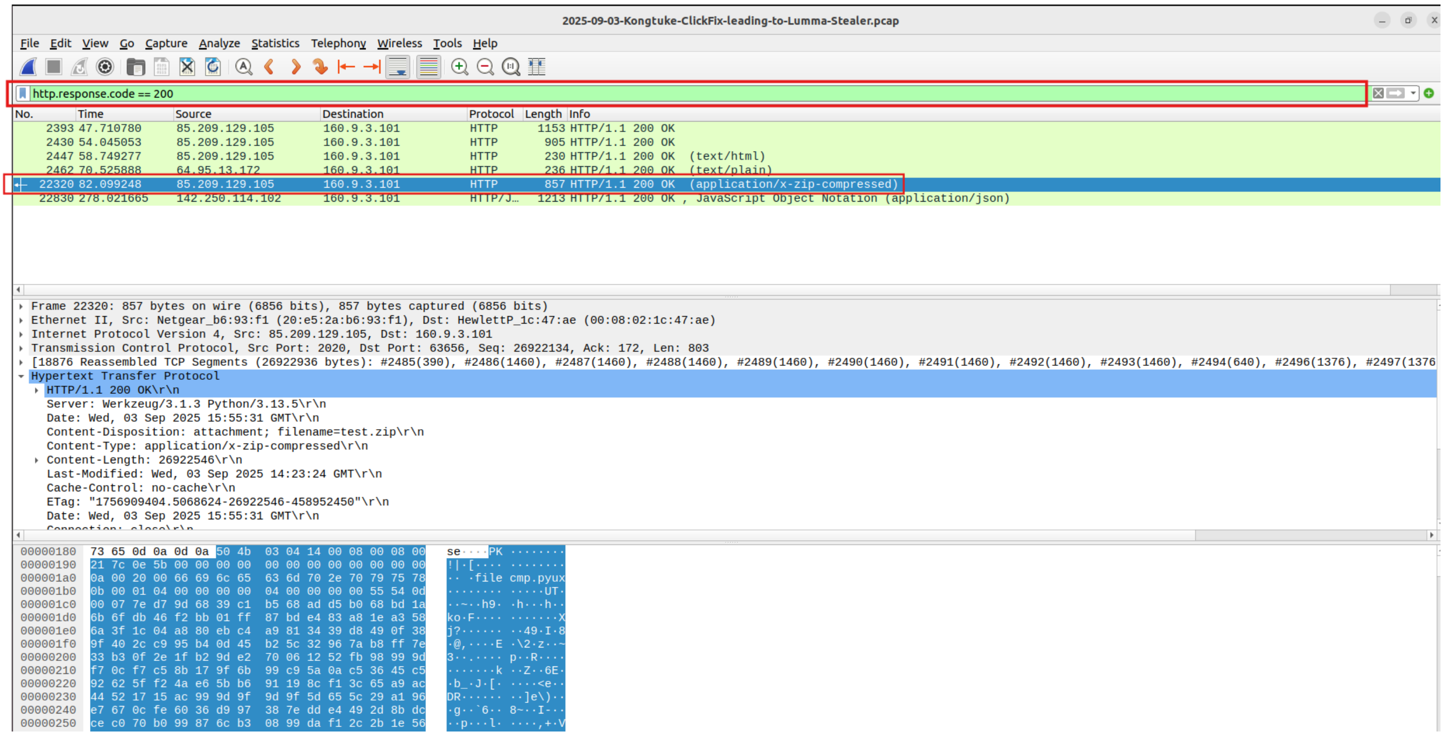
The following forensic artifacts were identified during the investigation:

- **Victim IP:** 160.9.3.101
- **Malicious Delivery IP:** 85.209.129.105 (Port 2020)
- **C2 / Exfiltration IP:** 104.16.231.132
- **Malware Hash (SHA-256):** e2c0390d80410e4358435c10cfc3d27b788d2299daa9d052d9c16526ee4635ad
- **User-Agent:** WindowsPowerShell/5.1.26100.4768

Technical Analysis & Evidence

1. Delivery Vector (The Download)

The initial infection began with a DNS query for a suspicious domain, leading to a GET request for a resource named /19. Despite the obfuscated naming convention, HTTP metadata confirmed the delivery of a compressed payload.


2025-09-03-Kongtuke-ClickFix-leading-to-Lumma-Stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.response.code == 200
```

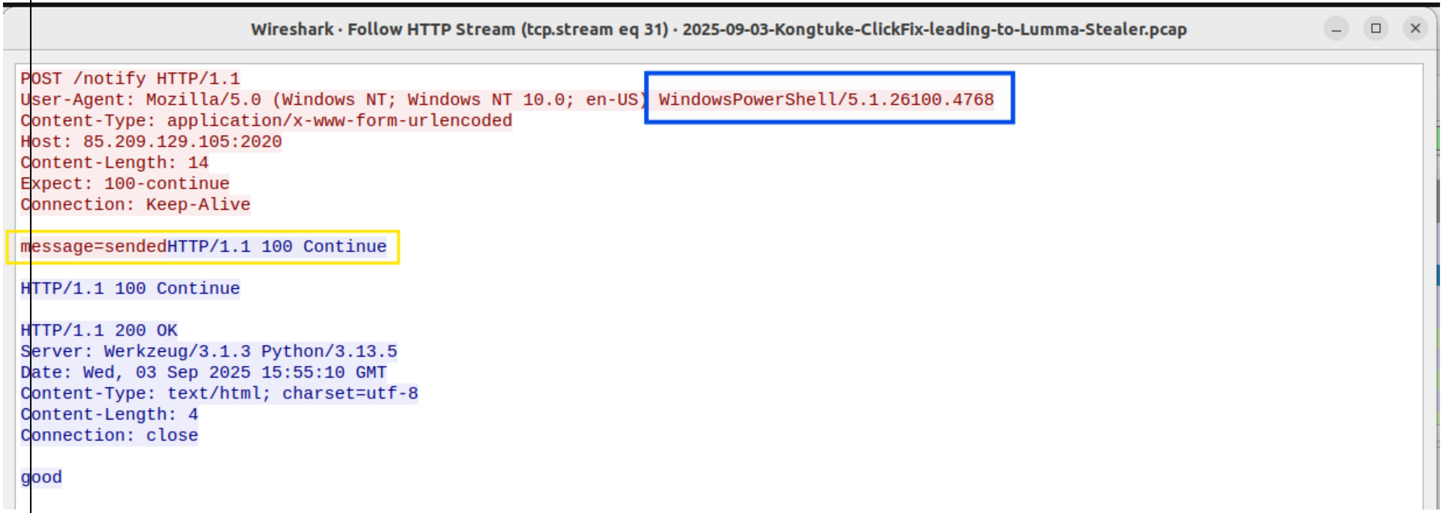
```
No.   Time          Source            Destination    Protocol  Length Info
 2393 47.710780     85.209.129.105    160.9.3.101    HTTP        1153 HTTP/1.1 200 OK
 2430 54.045053     85.209.129.105    160.9.3.101    HTTP         905 HTTP/1.1 200 OK
 2447 58.749277     85.209.129.105    160.9.3.101    HTTP         230 HTTP/1.1 200 OK  (text/html)
 2462 70.525888     64.95.13.172      160.9.3.101    HTTP         236 HTTP/1.1 200 OK  (text/plain)
22320 82.099248     85.209.129.105    160.9.3.101    HTTP         857 HTTP/1.1 200 OK  (application/x-zip-compressed)
22830 278.021665    142.250.114.102   160.9.3.101    HTTP/J…     1213 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
```

```
Frame 22320: 857 bytes on wire (6856 bits), 857 bytes captured (6856 bits)
Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
Internet Protocol Version 4, Src: 85.209.129.105, Dst: 160.9.3.101
Transmission Control Protocol, Src Port: 2020, Dst Port: 63656, Seq: 26922134, Ack: 172, Len: 803
[18876 Reassembled TCP Segments (26922936 bytes): #2485(390), #2486(1460), #2487(1460), #2488(1460), #2489(1460), #2490(1460), #2491(1460), #2492(1460), #2493(1460), #2494(640), #2496(1376), #2497(1376
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Server: Werkzeug/3.1.3 Python/3.13.5\r\n
  Date: Wed, 03 Sep 2025 15:55:31 GMT\r\n
  Content-Disposition: attachment; filename=test.zip\r\n
  Content-Type: application/x-zip-compressed\r\n
  Content-Length: 26922546\r\n
  Last-Modified: Wed, 03 Sep 2025 14:23:24 GMT\r\n
  Cache-Control: no-cache\r\n
  ETag: "1756909404.5068624-26922546-458952450"\r\n
  Date: Wed, 03 Sep 2025 15:55:31 GMT\r\n
  Connection: close\r\n
```

```
00000180  73 65 0d 0a 0d 0a 50 4b  03 04 14 00 08 00 08 00   se····PK ········
00000190  21 7c 0e 5b 00 00 00 00  00 00 00 00 00 00 00 00   !|·[···· ········
000001a0  0a 00 20 00 66 69 6c 65  63 6d 70 2e 70 79 75 78   ·· ·file cmp.pyux
000001b0  0b 00 01 04 00 00 00 00  04 00 00 00 00 55 54 0d   ········ ·····UT·
000001c0  00 07 7e d7 9d 68 39 c1  b5 68 ad d5 b0 68 bd 1a   ··~··h9· ·h···h··
000001d0  6b 6f db 46 f2 bb 01 ff  87 bd e4 83 a8 1e a3 58   ko·F···· ·······X
000001e0  6a 3f 1c 04 a8 80 eb c4  a9 81 34 39 d8 49 0f 38   j?······ ··49·I·8
000001f0  9f 40 2c c9 95 b4 0d 45  b2 5c 32 96 7a b8 ff 7e   ·@,····E ·\2·z··~
00000200  33 b3 0f 2e 1f b2 9d e2  70 06 12 52 fb 98 99 9d   3··.···· p··R····
00000210  f7 0c f7 c5 8b 17 9f 6b  99 c9 5a 0a c5 36 45 c5   ·······k ··Z··6E·
00000220  92 62 5f f2 4a e6 5b b6  91 19 8c f1 3c 65 a9 ac   ·b_·J·[· ····<e··
00000230  44 52 17 15 ac 99 9d 9f  9d 9f 5d 65 5c 29 a1 96   DR······ ··]e\)··
00000240  e7 67 0c fe 60 36 d9 97  38 7e dd e4 49 2d 8b dc   ·g··`6·· 8~··I-··
00000250  ce c0 70 b0 99 87 6c b3  08 99 da f1 2c 2b 1e 56   ··p···l· ····,+·V
```

2. Execution Analysis (The Actor)

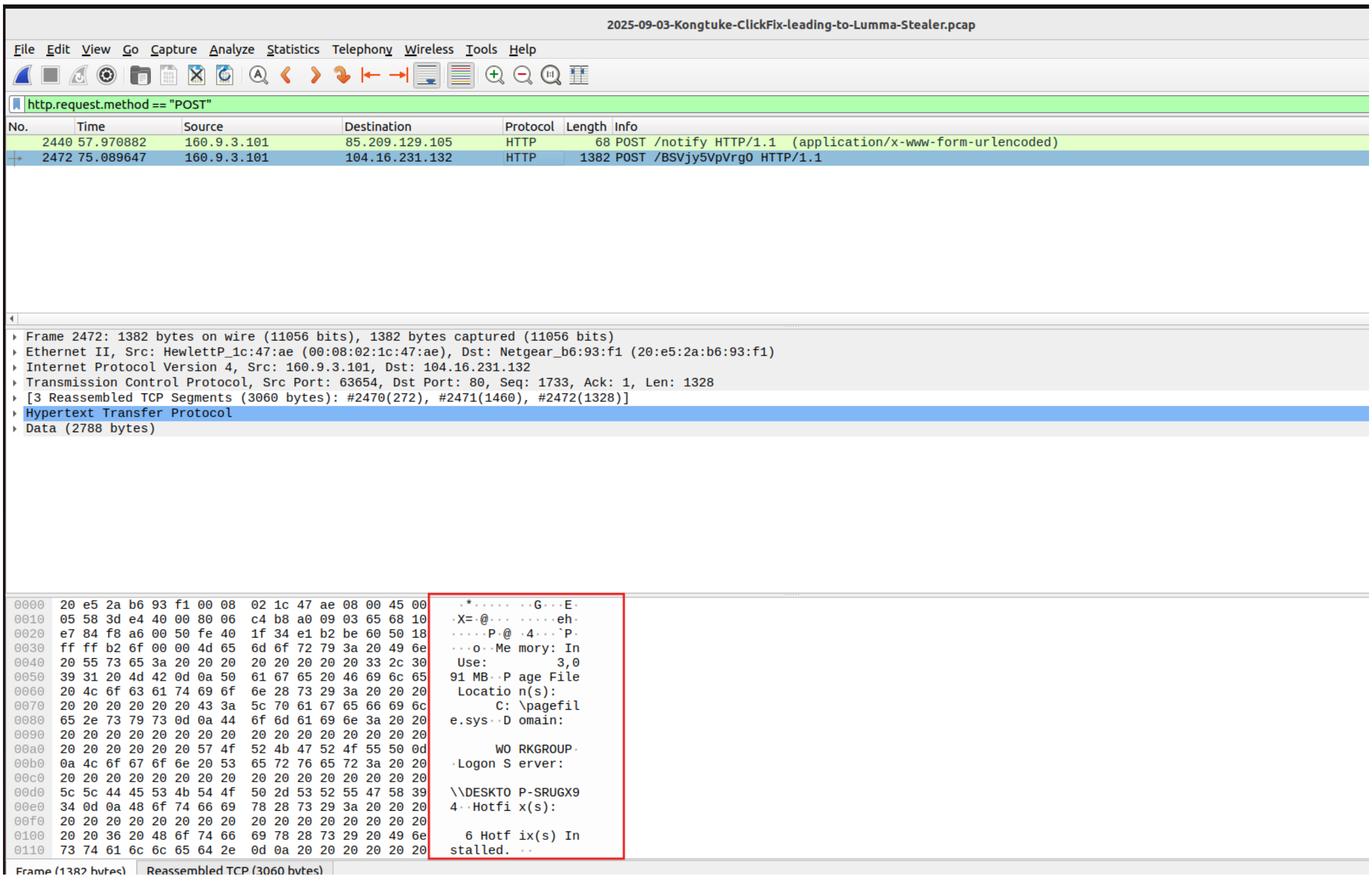
By following the HTTP stream for the /notify endpoint, it was determined that the requests were initiated by **Windows PowerShell** rather than a standard web browser. The host performed a check-in by sending message=sended, which was acknowledged by the server with a good response.


Wireshark · Follow HTTP Stream (tcp.stream eq 31) · 2025-09-03-Kongtuke-ClickFix-leading-to-Lumma-Stealer.pcap

```
POST /notify HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.26100.4768
Content-Type: application/x-www-form-urlencoded
Host: 85.209.129.105:2020
Content-Length: 14
Expect: 100-continue
Connection: Keep-Alive

message=sendedHTTP/1.1 100 Continue

HTTP/1.1 100 Continue

HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.13.5
Date: Wed, 03 Sep 2025 15:55:10 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4
Connection: close

good
```

3. Exfiltration Analysis (The Theft)

The final stage involved the theft of host-specific information. A POST request to 104.16.231.132 contained clear-text strings detailing the victim's hardware and network environment.

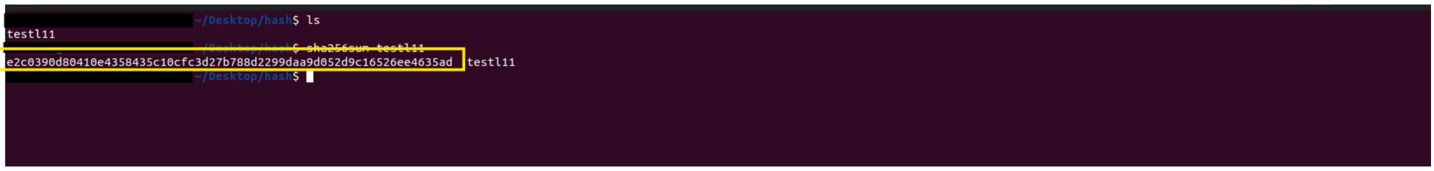


2025-09-03-Kongtuke-ClickFix-leading-to-Lumma-Stealer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == "POST"

No.  Time      Source       Destination     Protocol Length Info
2440 57.970882 160.9.3.101  85.209.129.105  HTTP       68 POST /notify HTTP/1.1  (application/x-www-form-urlencoded)
2472 75.089647 160.9.3.101  104.16.231.132  HTTP     1382 POST /BSVjy5VpVrg0 HTTP/1.1

› Frame 2472: 1382 bytes on wire (11056 bits), 1382 bytes captured (11056 bits)
› Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
› Internet Protocol Version 4, Src: 160.9.3.101, Dst: 104.16.231.132
› Transmission Control Protocol, Src Port: 63654, Dst Port: 80, Seq: 1733, Ack: 1, Len: 1328
› [3 Reassembled TCP Segments (3060 bytes): #2470(272), #2471(1460), #2472(1328)]
› Hypertext Transfer Protocol
› Data (2788 bytes)

0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00    ·*·····  ··G···E·
0010  05 58 3d e4 40 00 80 06  c4 b8 a0 09 03 65 68 10   ·X=·@···  ·····eh·
0020  e7 84 f8 a6 00 50 fe 40  1f 34 e1 b2 be 60 50 18   ·····P·@  ·4···`P·
0030  ff ff b2 6f 00 00 4d 65  6d 6f 72 79 3a 20 49 6e   ···o··Me  mory: In
0040  20 55 73 65 3a 20 20 20  20 20 20 20 20 33 2c 30    Use:           3,0
0050  39 31 20 4d 42 0d 0a 50  61 67 65 20 46 69 6c 65   91 MB··P  age File
0060  20 4c 6f 63 61 74 69 6f  6e 28 73 29 3a 20 20 20    Locatio  n(s):
0070  20 20 20 20 20 20 43 3a  5c 70 61 67 65 66 69 6c         C:  \pagefil
0080  65 2e 73 79 73 0d 0a 44  6f 6d 61 69 6e 3a 20 20   e.sys··D  omain:
0090  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00a0  20 20 20 20 20 20 57 4f  52 4b 47 52 4f 55 50 0d         WO  RKGROUP·
00b0  0a 4c 6f 67 6f 6e 20 53  65 72 76 65 72 3a 20 20   ·Logon S  erver:
00c0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00d0  5c 5c 44 45 53 4b 54 4f  50 2d 53 52 55 47 58 39   \\DESKTO  P-SRUGX9
00e0  34 0d 0a 48 6f 74 66 69  78 28 73 29 3a 20 20 20   4··Hotfi  x(s):
00f0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0100  20 20 36 20 48 6f 74 66  69 78 28 73 29 20 49 6e     6 Hotf  ix(s) In
0110  73 74 61 6c 6c 65 64 2e  0d 0a 20 20 20 20 20 20   stalled.  ··
```

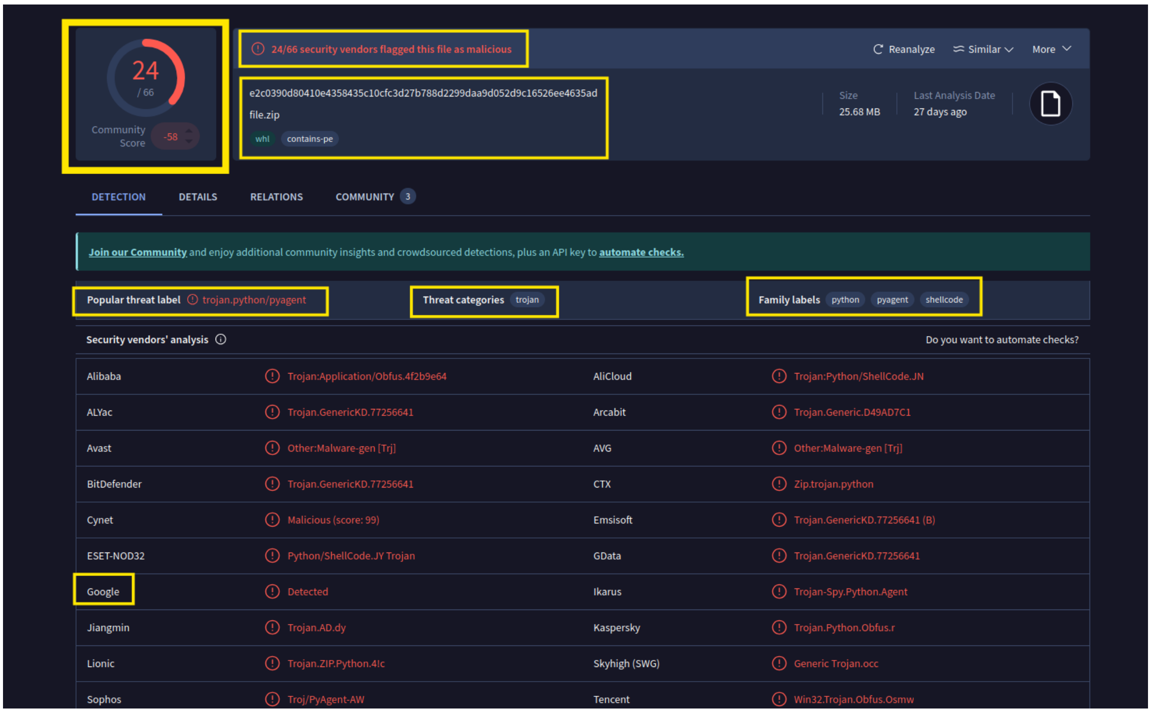
4. Forensic Verification

The malicious ZIP file was exported from the traffic and hashed using SHA-256.



```
[redacted]~/Desktop/hash$ ls
testl11
[redacted]~/Desktop/hash$ sha256sum testl11
e2c0390d80410e4358435c10cfc3d27b788d2299daa9d052d9c16526ee4635ad  testl11
[redacted]~/Desktop/hash$ █
```

Verification via VirusTotal confirmed the file as a Trojan-type malware belonging to the **Lumma Stealer** family, with a detection rate of 24/66 vendors.



24/66 security vendors flagged this file as malicious

e2c0390d80410e4358435c10cfc3d27b788d2299daa9d052d9c16526ee4635ad
file.zip
whl contains-pe

Size 25.68 MB

Last Analysis Date 27 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.python/pyagent

Threat categories trojan

Family labels python pyagent shellcode

Security vendors' analysis

Do you want to automate checks?

Alibaba	Trojan:Application/Obfus.4f2b9e64	AliCloud	Trojan:Python/ShellCode.JN
ALYac	Trojan.GenericKD.77256641	Arcabit	Trojan.Generic.D49AD7C1
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
BitDefender	Trojan.GenericKD.77256641	CTX	Zip.trojan.python
Cynet	Malicious (score: 99)	Emsisoft	Trojan.GenericKD.77256641 (B)
ESET-NOD32	Python/ShellCode.JY Trojan	GData	Trojan.GenericKD.77256641
Google	Detected	Ikarus	Trojan-Spy.Python.Agent
Jiangmin	Trojan.AD.dy	Kaspersky	Trojan.Python.Obfus.r
Lionic	Trojan.ZIP.Python.4!c	Skyhigh (SWG)	Generic Trojan.occ
Sophos	Troj/PyAgent-AW	Tencent	Win32.Trojan.Obfus.Osmw

5. Conclusion

The investigation confirms that host **160.9.3.101** was compromised by Lumma Stealer. It is recommended to isolate the host, wipe and re-image the machine, and reset all user credentials that may have been stored in browser memory.