

REPORT XLMRat Lab

Analyst: Ruslan

Date: 2026-01-19

1. Incident Summary

Network evidence indicates that an internal host 10.1.19.101 retrieved suspicious content over HTTP from an external endpoint 45.126.209.4 using port 222. The observed activity includes HTTP GET requests for the resources xlm.txt and mdm.jpg, with the stage-1 URL explicitly documented as <http://45.126.209.4:222/mdm.jpg>.

2. Detection Details

Detection was performed through packet and HTTP-layer review. Conversation statistics highlighted a high-volume exchange between 10.1.19.101 and 45.126.209.4, which prompted deeper inspection. Applying an HTTP request filter (http.request) surfaced GET activity to xlm.txt and mdm.jpg. The workflow also records that HTTP objects were exported/extracted and then checked for maliciousness, tying the network retrieval directly to the recovered payload artifacts.

3. Analysis

The collected artifacts describe a multi-stage chain consisting of a loader and a secondary executable. A SHA256 hash is provided for the malware executable:

1eb7b02e18f67420f42b1d94e74f3b6289d92672a0fb1786c30c03d68e81d798. The sample is labeled by Alibaba as asynrat, and the file creation timestamp documented in the artifact set is 2023-10-30 15:08.

Execution tradecraft includes the use of a Windows LOLBin for stealthy process execution:

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe. This is relevant because it indicates an attempt to blend malicious execution into legitimate system tooling.

The artifact set also enumerates dropped files associated with the activity: Conted.vbs, Conted.ps1, and Conted.bat. These filenames provide concrete host-level pivots for validation and scoping on endpoints beyond the initially observed system.

4. Impact Assessment

From the available evidence, the confirmed impact is limited to demonstrated retrieval of stage content from 45.126.209.4:222 by 10.1.19.101 and the presence of indicators consistent with follow-on execution via RegSvcs.exe and referenced dropped scripts. This supports a conclusion of likely host compromise on the victim system, but the provided materials do not contain endpoint telemetry sufficient to confirm persistence, privilege changes, credential access, lateral movement, or data exfiltration. Therefore, the impact assessment is restricted to what is explicitly observable in the network and extracted-object artifacts.

5. Indicators of Compromise

Network indicators include communication between 10.1.19.101 and 45.126.209.4 and HTTP activity on port 222, including requests for mdm.jpg and xlm.txt, with the documented stage-1 URL <http://45.126.209.4:222/mdm.jpg>.

Host and file indicators include the LOLBin path

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvc.exe, the dropped filenames Conted.vbs, Conted.ps1, and Conted.bat, the malware executable hash 1eb7b02e18f67420f42b1d94e74f3b6289d92672a0fb1786c30c03d68e81d798, the malware label asynrat, and the documented timestamp 2023-10-30 15:08.

Conclusion

The evidence set supports a clear chain of events: an internal host (10.1.19.101) contacted an external server (45.126.209.4:222) and retrieved stage content via HTTP, including the documented stage-1 object mdm.jpg. Extracted artifacts describe a loader and a secondary executable associated with the activity, provide a concrete SHA256 for the malware executable, and label it as asynrat. The inclusion of RegSvc.exe as an execution mechanism and the referenced dropped scripts (Conted.*) provide specific pivots for endpoint validation and incident scoping, but no additional claims about persistence or data loss are made because such evidence is not present in the provided materials.

Analysys

1. The attacker successfully executed a command to download the first stage of the malware. What is the URL from which the first malware stage was installed?

Statistics → Conversations shows that the victim host 10.1.19.101 was sending a lot of packets to host 45.126.209.4

Ethernet · 1		IPv4 · 2		IPv6	TCP · 3		UDP · 1							
Address A	Address B	Packets	Bytes		Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A		
10.1.9.101	45.126.209.4	1,548	586 k		576	75 k	972	510 k	0.000000	766.3712		787		
10.1.9.101	10.1.9.1	2	478		1	78	1	400	141.351709	0.3346		1,864		

Let's check in the http.request filter:

http.request							
No.	Time	Source	Destination	Protocol	Length	Host	Info
4	2024-01-09 17:27:27.871218	10.1.9.101	45.126.209.4	HTTP	357	45.126.209.4:222	GET /xlm.txt HTTP/1.1
12	2024-01-09 17:27:29.161649	10.1.9.101	45.126.209.4	HTTP	127	45.126.209.4:222	GET /mdm.jpg HTTP/1.1

You can see get requests xlm.txt, mdm.jpg.

File → Export Objects → HTTP:

Text Filter:

Packet	Hostname	Content Type	Size	Filename
7	45.126.209.4:222	text/plain	1,974 bytes	xlm.txt
344	45.126.209.4:222	image/jpeg	431 kB	mdm.jpg

Download both files and check them in VirusTotal.

28

/ 61

Community Score

28/61 security vendors flagged this file as malicious

Reanalyze

Similar

More

1e9c29d7af6011ca9d5609cb93b554965c61105a42df9e0c36274e60db71b1d

Size

1.93 KB

Last Analysis Date

5 days ago

xlm.txt

vba

detect-debug-environment

malware

checks-cpu-name

macro-powershell

checks-network-adapters

calls-wmi

exe-pattern

powershell

long-sleeps

run-file

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 14

Join our Community

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

Code insights

The code defines an array of strings (LZeWX) and then concatenates them into a single string (OodJR). It then uses the WScript.Shell object to execute a PowerShell command with the following options:

-NOP: Do not display the PowerShell console window.

-WIND HIDE: Hide the PowerShell console window.

Show more

Popular threat label

trojan.runner/ac1b

Threat categories

trojan

Family labels

runner

ac1b

alien

Security vendors' analysis

Do you want to automate checks?

AliCloud	Trojan.Win/Runner.A	ALYac	Trojan.Script.Agent
Arcabit	Trojan.Generic.D4937A69	Avast	Script:SNH-gen [PUP]
AVG	Script:SNH-gen [PUP]	BitDefender	Trojan.GenericKD.76773993
CTX	Vba.trojan.runner	Cynet	Malicious (score: 99)
DrWeb	Trojan.DownLoader46.46363	Emsisoft	Trojan.GenericKD.76773993 (B)
eScan	Trojan.GenericKD.76773993	ESET-NOD32	PowerShell/Runner.A Suspicious Applica...

31

/ 62

Community Score

-12

31/62 security vendors flagged this file as malicious

Reanalyze

Similar

More

83babee77db36512c0eab8ea6b35e981aa4288a4095985d69b3841f8b684fe11

mdm.jpg

Size

421.10 KB

Last Analysis Date

20 days ago

powershell

run-file

long-sleeps

enum-windows

detect-debug-environment

exe-pattern

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 13+

Join our Community

and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Code insights

The script decodes two embedded hexadecimal strings into byte arrays. One byte array is then loaded into memory as a .NET assembly using reflection. A specific method within this in-memory assembly is subsequently invoked, and the other decoded byte array along with a path to a system executable is passed as arguments to this method.

The initial PowerShell code is written to a file named 'Conted.ps1' in the 'C:\Users\Public\' directory. A batch file named 'Conted.bat' is then created in the same directory. This batch file is configured to execute [Show more](#)

Popular threat label

trojan.powershell/runner

Threat categories

trojan

dropper

Family labels

powershell

runner

psdrop

Security vendors' analysis

Do you want to automate checks?

AliCloud	Trojan(dropper);Win/Runner.Gen	ALYac	Trojan.GenericKDZ.105650
Arcabit	Trojan.Generic.D19CB2	Avast	Script:SNH-gen [Trj]
AVG	Script:SNH-gen [Trj]	BitDefender	Trojan.GenericKDZ.105650
Bkav Pro	W32.Common.BC097C02	CTX	Powershell.trojan.runner
Cynet	Malicious (score: 99)	DrWeb	PowerShell.Inject.128
Emsisoft	Trojan.GenericKDZ.105650 (8)	eScan	Trojan.GenericKDZ.105650

We're sure the files are indeed malicious and can safely view the URL:

```

Transmission Control Protocol, Src Port: 49709, Dst Port: 222, Seq: 1, Ack: 1, Len: 73
Hypertext Transfer Protocol
  GET /mdm.jpg HTTP/1.1\r\n
  Host: 45.126.209.4:222\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://45.126.209.4:222/mdm.jpg]
  [HTTP request 1/1]

```

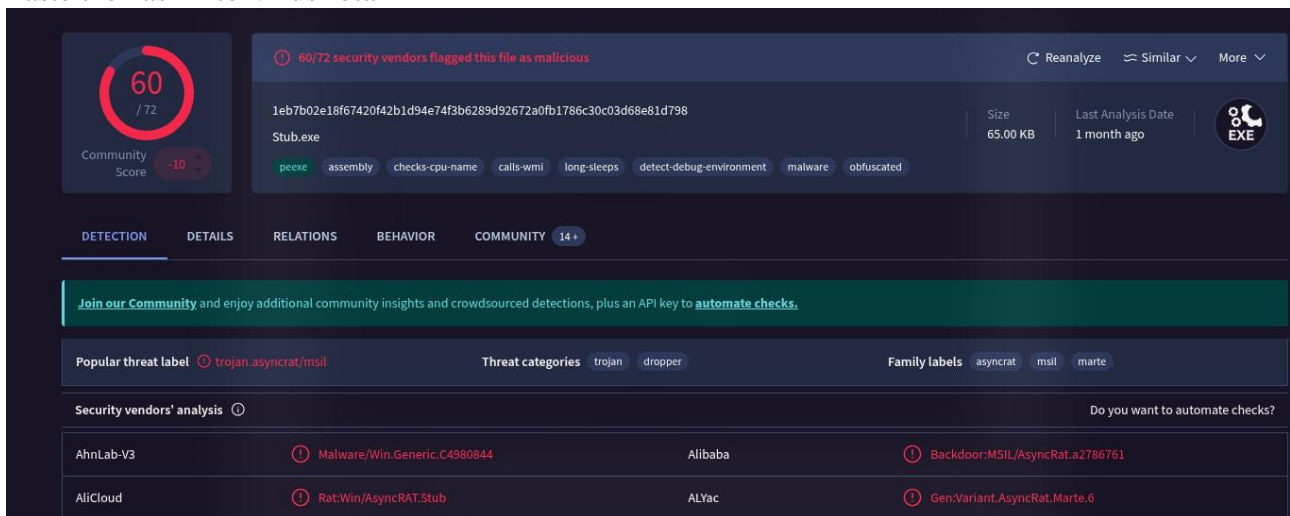
Answer: <http://45.126.209.4:222/mdm.jpg>

2. Which hosting provider owns the associated IP address?

Using WHOIS, we enter the IP address 45.126.204.4. We see the URL: <https://www.reliablesite.net>

4. What is the malware family label based on Alibaba?

Paste the hash into VirusTotal



The screenshot shows the VirusTotal analysis page for a file named 'Stub.exe' with SHA256 hash '1eb7b02e18f67420f42b1d94e74f3b6289d92672a0fb1786c30c03d68e81d798'. The file size is 65.00 KB and it was last analyzed 1 month ago. The community score is 60/72, with 60/72 security vendors flagging it as malicious. The file is categorized as 'malware' and 'obfuscated'. The popular threat label is 'trojan.asyncrat/msil'. The threat categories are 'trojan' and 'dropper'. The family labels are 'asyncrat', 'msil', and 'marte'. The security vendors' analysis table shows detections from AhnLab-V3, AliCloud, and others.

Security vendors' analysis	Malware name	Vendor	Malware name
AhnLab-V3	Malware/Win.Generic.C4980844	Alibaba	Backdoor:MSIL/AsyncRat.a2786761
AliCloud	Rat:Win/AsyncRAT.Stub	ALYac	Gen:Variant.AsyncRat.Marte.6

Answer: asyncrat

5. What is the timestamp of the malware's creation?

In details we can find History

History ⓘ	
Creation Time	2023-10-30 15:08:44 UTC
First Seen In The Wild	2024-01-11 18:17:54 UTC
First Submission	2024-01-11 16:36:37 UTC
Last Submission	2026-01-16 12:55:51 UTC
Last Analysis	2025-11-27 08:41:15 UTC

Answer: 2023-10-30 15:08

6. Which LOLBin is leveraged for stealthy process execution in this script? Provide the full path.

Open with a text editor or via nano jpg:

```
$NK = $Fu.GetType('N#ew#PE#2.P#E'-replace '#', '')
$MZ = $NK.GetMethod('Execute')
$NA = 'C:\W#####indow#####s\Mi####cr'-replace '#', ''
$AC = $NA + 'osof#####t.NET\Fra####mework\v4.0.303###19\R##egSvc#####s.exe'-replace '#', ''
$VA = @($AC, $NKbb)
```

We remove all the # symbols: \$NA = 'C:\W#####indow#####s\Mi####cr'-replace '#', ''

We get:

C:\Windows\Micr
rosoft.NET\Framework\v4.0.30319\RegSvc.exe

Склеиваем с \$NA:

C:\Windows\Micr + osoft.NET\Framework\v4.0.30319\RegSvc.exe =
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvc.exe

Answer: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvc.exe

7. The script is designed to drop several files. List the names of the files dropped by the script.

В txt file можно увидеть:

Conted.vbs

Conted.ps1

Conted.bat