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 asyncrat, 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\RegSvcs.exe, the dropped filenames Conted.vbs, Conted.ps1, and Conted.bat, the malware executable hash 1eb7b02e18f67420f42b1d94e74f3b6289d92672a0fb1786c30c03d68e81d798, the malware label asyncrat, and the documented timestamp 2023-10-30 15:08.

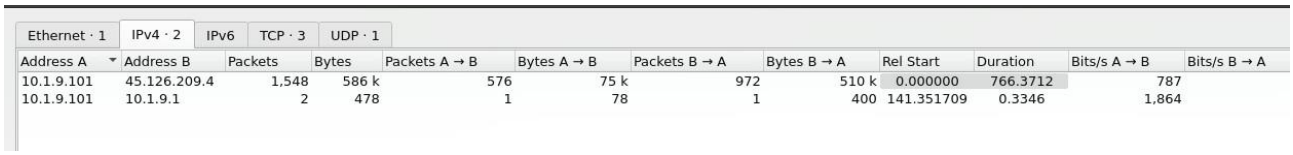
Conclusion

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 asyncrat. The inclusion of RegSvcs.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.

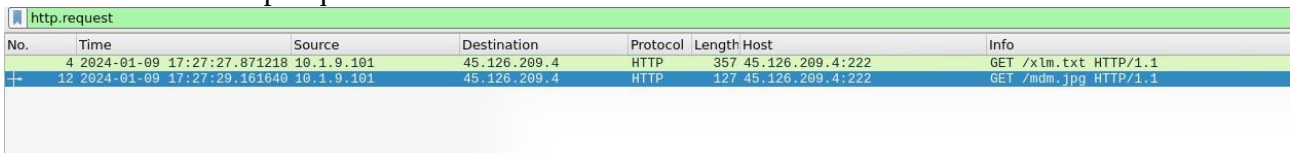
Analysys

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

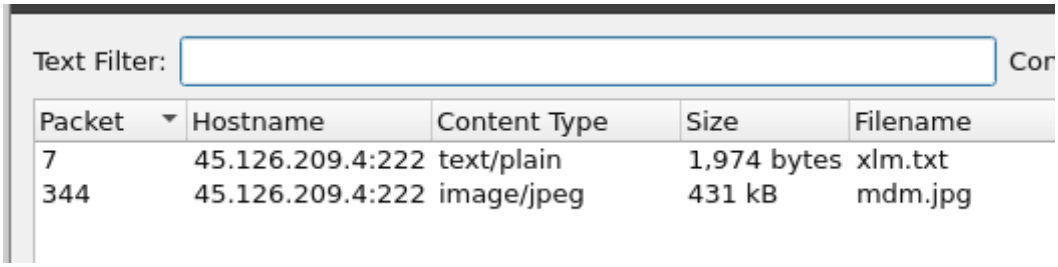


Let's check in the http.request filter:

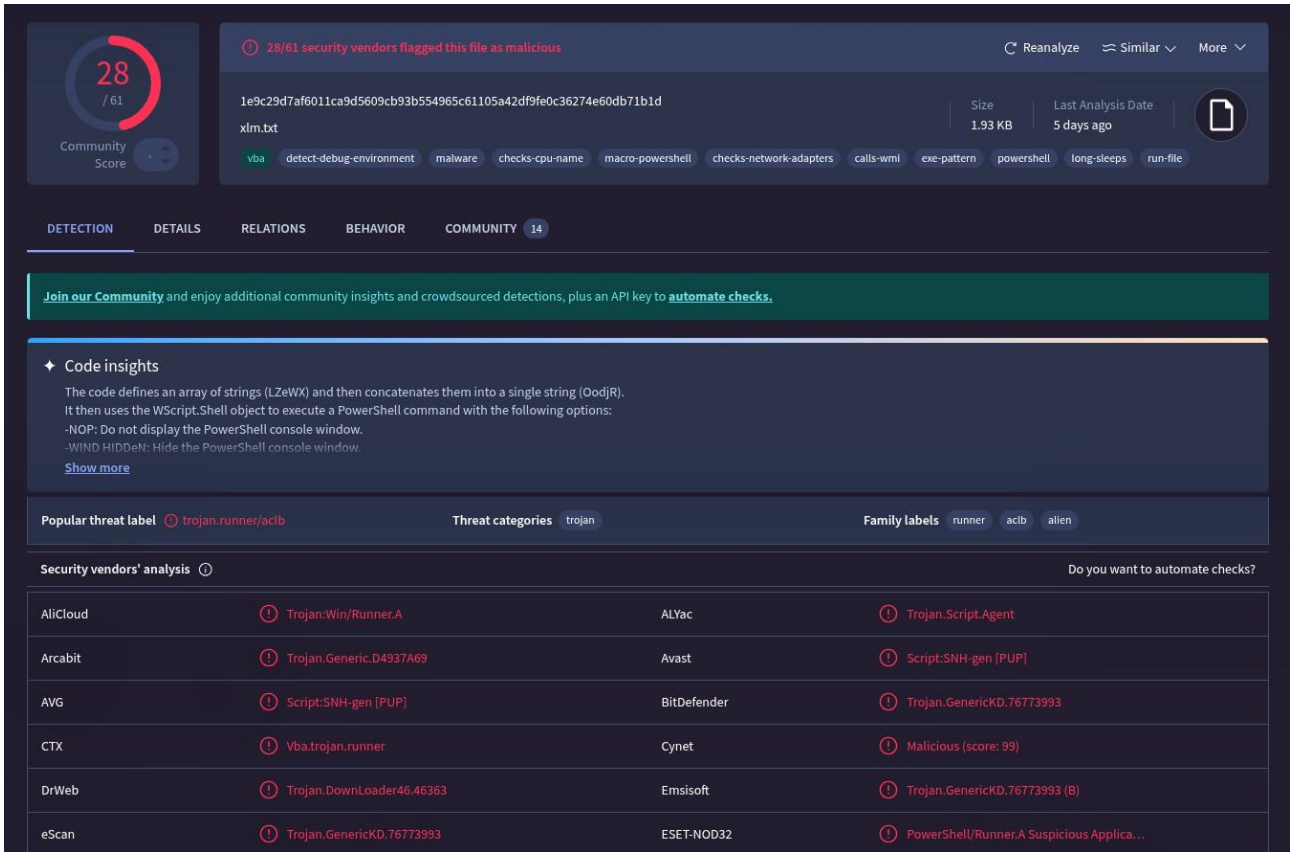


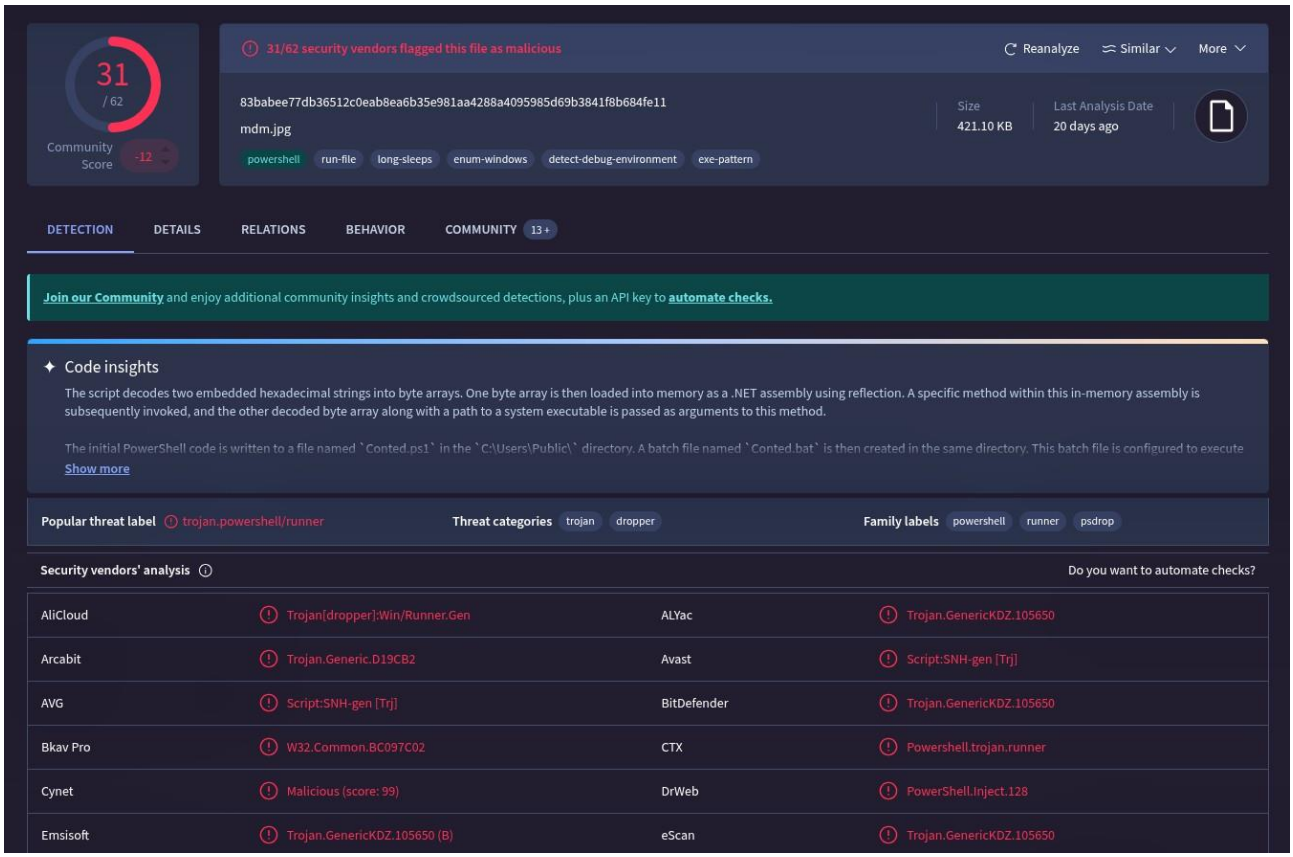
You can see get requests xlm.txt, mdm.jpg.

File → Export Objects → HTTP:



Download both files and check them in VirusTotal.





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

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

2. Which hosting provider owns the associated IP address?

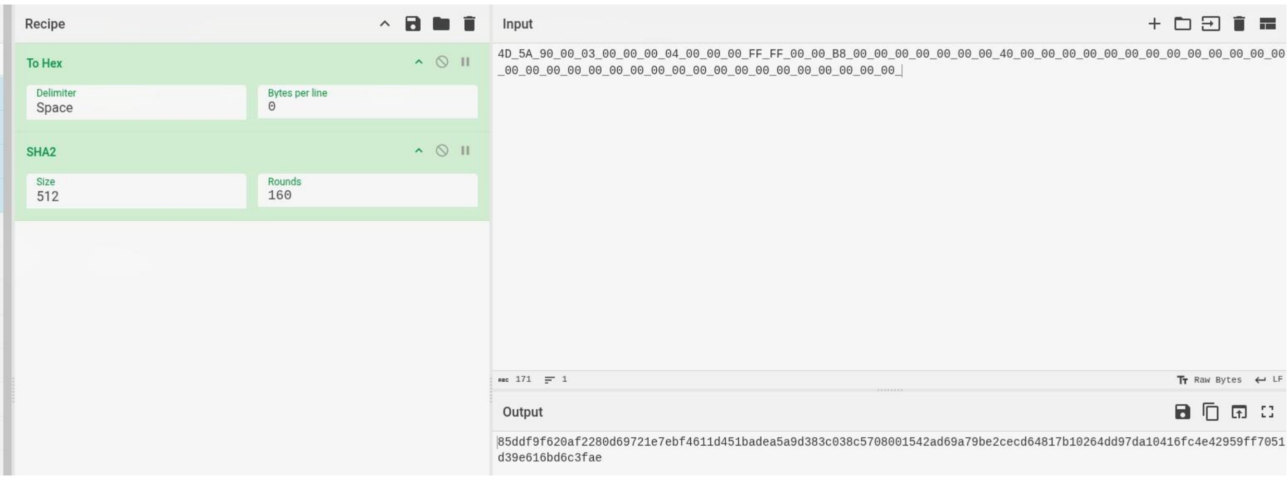
Using WHOIS, we enter the IP address 45.126.204.4. We see the URL: https://www.reliablesite.net

```
ruslan@pop-os:~$ whois 45.126.209.4
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '45.126.208.0 - 45.126.211.255'

% Abuse contact for '45.126.208.0 - 45.126.211.255' is 'abuse@reliablesite.net'

inetnum:        45.126.208.0 - 45.126.211.255
netname:        RELIABLESITE-AP
descr:          ReliableSite.Net LLC
country:        SG
geoloc:         25.7975441 -80.2322913
org:            ORG-RL9-AP
admin-c:        RLA10-AP
tech-c:         RLA10-AP
abuse-c:        AR1015-AP
status:         ALLOCATED PORTABLE
remarks:        -+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
remarks:        To report network abuse, please contact the IRT
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        For assistance, please contact the APNIC Helpdesk
remarks:        -+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
remarks:        Geofeed https://www.reliablesite.net/geofeed.csv
remarks:        geofeed: https://www.reliablesite.net/geofeed.csv
mnt-by:         APNIC-HM
mnt-lower:      MAINT-RELIABLESITE-AP
mnt-routes:     MAINT-RELIABLESITE-AP
mnt-irt:        IRT-RELIABLESITE-AP
last-modified:  2023-08-15T16:40:57Z
source:         APNIC
```

Answer: reliablesite.net

3. By analyzing the malicious scripts, two payloads were identified: a loader and a secondary executable. What is the SHA256 of the malware executable?

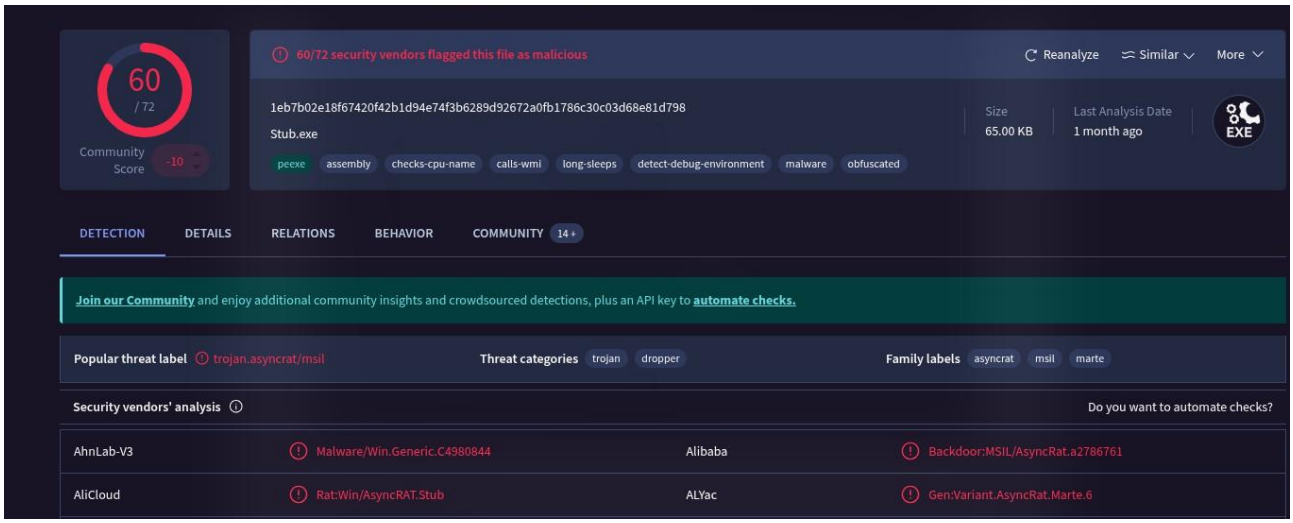
Using CyberChef, we calculate Hex → SHA2



Answer: 1eb7b02e18f67420f42b1d94e74f3b6289d92672a0fb1786c30c03d68e81d798

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

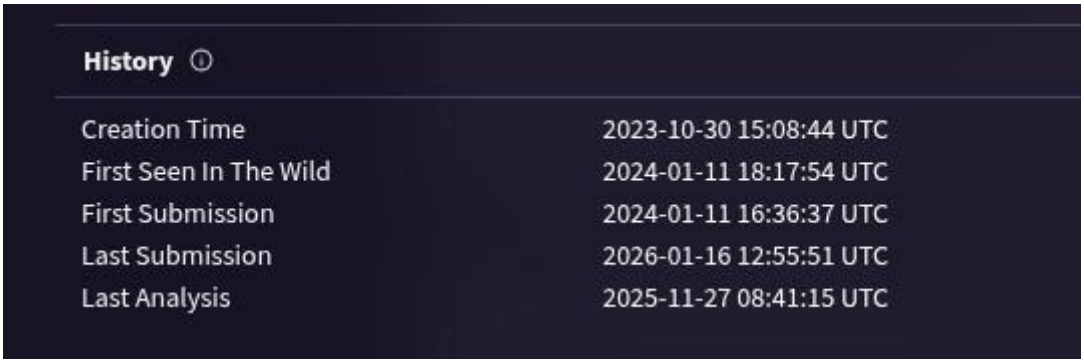
Paste the hash into VirusTotal



Answer: asyncrat

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

In details we can find History



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

osoft.NET\Framework\v4.0.30319\RegSvcs.exe

Склеиваем с $NA:

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

Answer: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.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