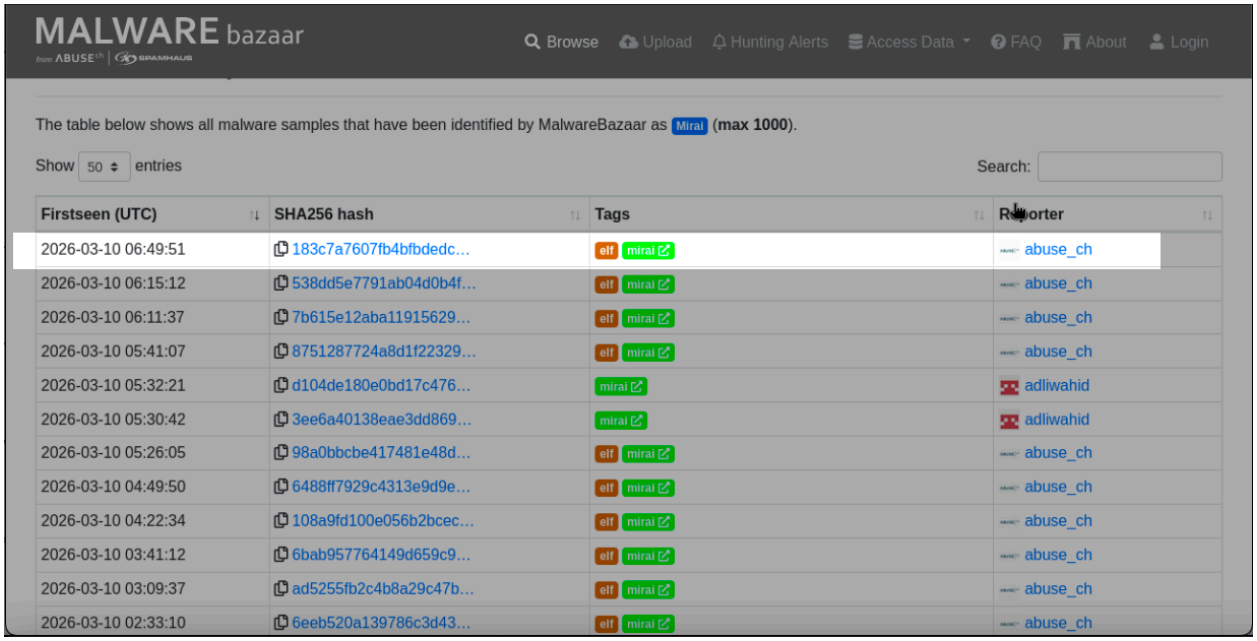
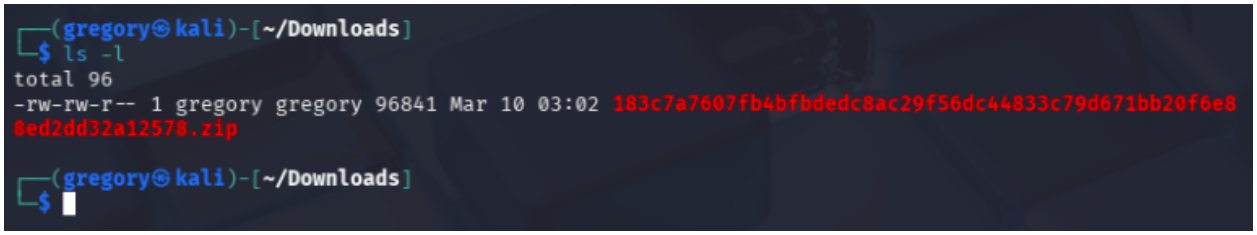
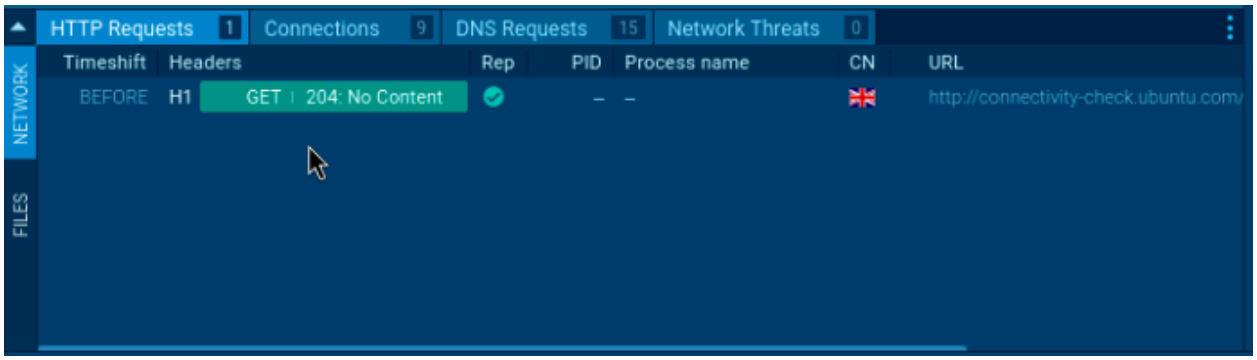
The following sample with the “Mirai” tag was selected.



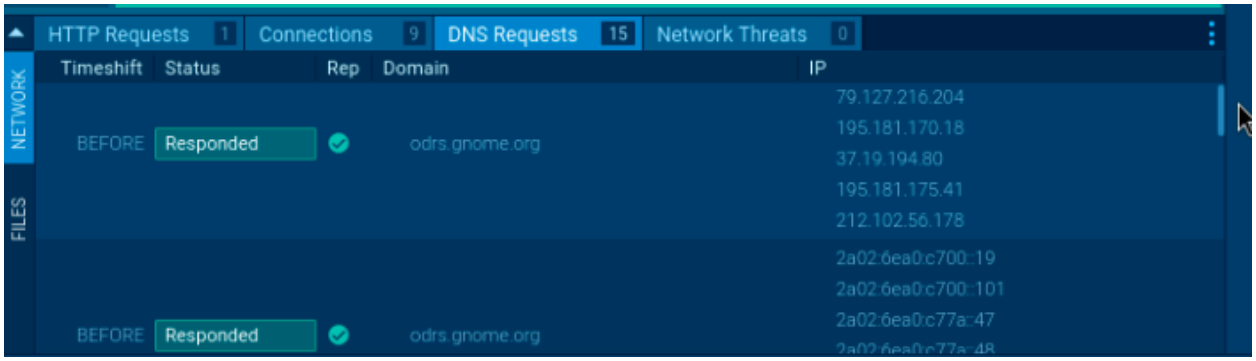
The sample is present in the VM’s downloads folder.

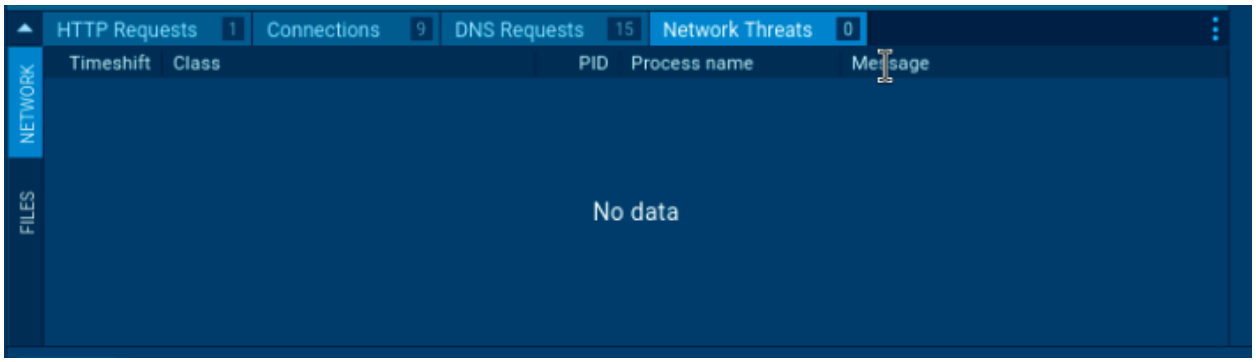


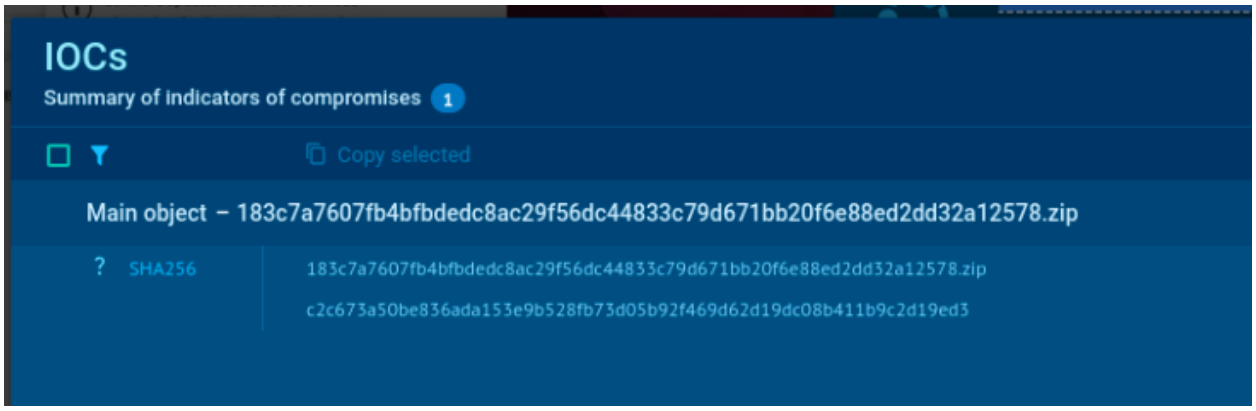
The only indicator of compromise was the sample’s hash value.

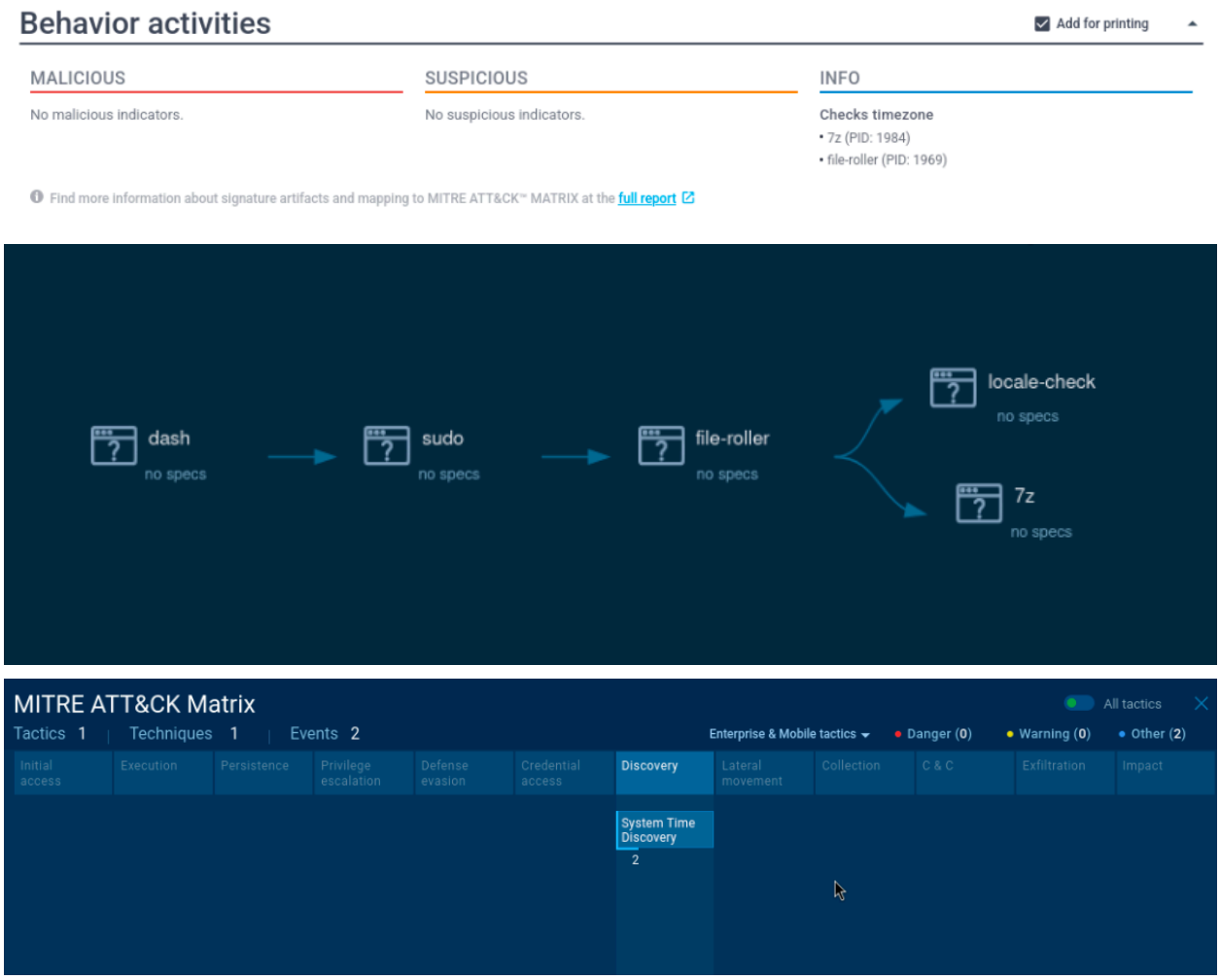



HTTP Requests 1
Connections 9
DNS Requests 15
Network Threats 0
NETWORK
FILES
Timeshift Protocol Rep PID Process name CN IP Port Domain ASN
BEFORE TCP – – 91.189.91.98 80 connectivity- CANONICA
BEFORE UDP 456 avahi-daemon ? 224.0.0.251 5353 – –
BEFORE TCP – – 91.189.91.49 80 connectivity- CANONICA
BEFORE TCP – – 79.127.211.89 443 odrs.gnome CDN77 _
BEFORE TCP – – 185.125.188.54 443 api.snapcraft CANONICA
BEFORE TCP – – 91.189.91.49 80 connectivity- CANONICA
8690 ms TCP 473 snapd 185.125.188.57 443 api.snapcraft CANONICAL


HTTP Requests 1
Connections 9
DNS Requests 15
Network Threats 0
NETWORK
FILES
Timeshift Status Rep Domain IP
BEFORE Responded odrs.gnome.org
79.127.216.204
195.181.170.18
37.19.194.80
195.181.175.41
212.102.56.178
BEFORE Responded odrs.gnome.org
2a02:6ea0:c700::19
2a02:6ea0:c700::101
2a02:6ea0:c77a::47

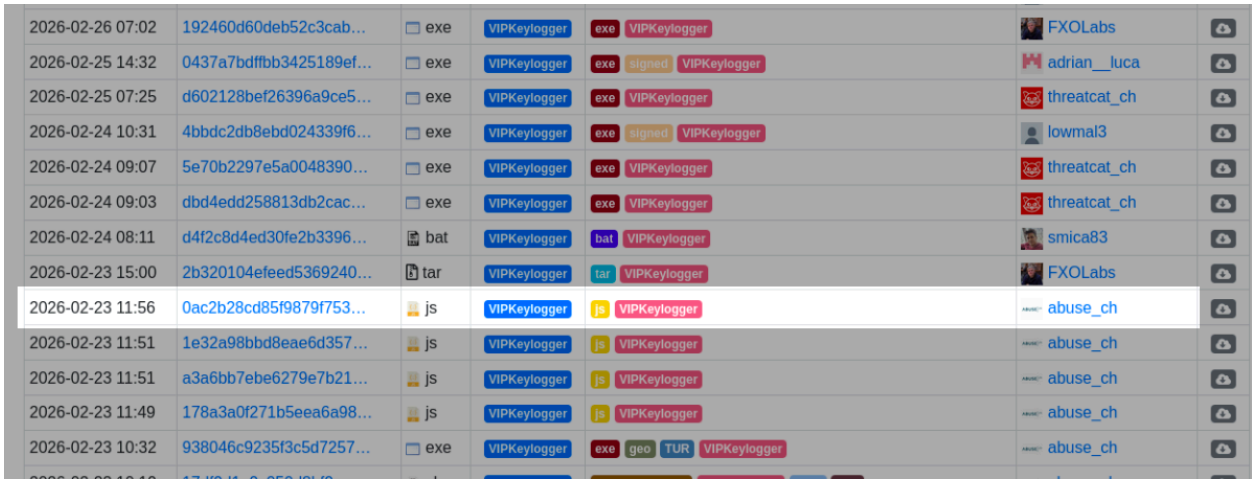

HTTP Requests 1
Connections 9
DNS Requests 15
Network Threats 0
NETWORK
FILES
Timeshift Class PID Process name Message
No data


IOCs
Summary of indicators of compromises 1
Copy selected
Main object – 183c7a7607fb4bfbdedc8ac29f56dc44833c79d671bb20f6e88ed2dd32a12578.zip
? SHA256
183c7a7607fb4bfbdedc8ac29f56dc44833c79d671bb20f6e88ed2dd32a12578.zip
c2c673a50be836ada153e9b528fb73d05b92f469d62d19dc08b411b9c2d19ed3



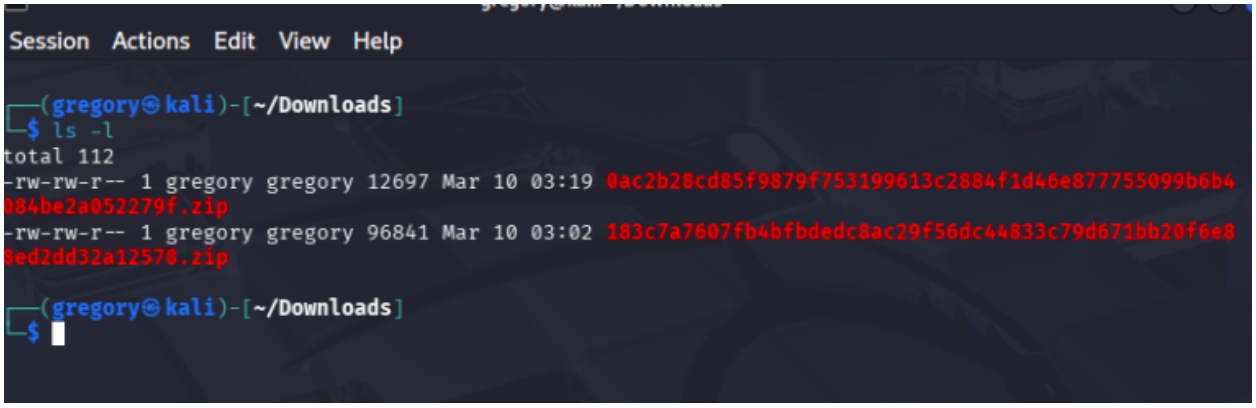
From the analysis, little malicious activity was found. The program appears to simply find basic information about the system's time and location. Perhaps a longer or more in-depth analysis would reveal an attempt to connect to a larger botnet, but this seemingly did not occur during the current analysis. Though little is immediately apparent about this malware sample, Mirai, as a whole, has several notable characteristics. The malware aims to infect devices to add them to a botnet, which could subsequently be used to engage in distributed denial of service attacks, among others. The malware typically targets IoT devices which run on some distribution of Linux. As the infected device must communicate with the command and control server for instructions, the kinds of connections an infected device makes can be used to identify the presence of the malware. Frequent communications with unknown devices could indicate that the device is receiving instruction or, alternatively, being used to perform a DDoS attack.

The second malware sample is chosen with the “VIPKeylogger” tag.



2026-02-26 07:02	192460d60deb52c3cab...	exe	VIPKeylogger	exe VIPKeylogger	FXOLabs
2026-02-25 14:32	0437a7bdffbb3425189ef...	exe	VIPKeylogger	exe signed VIPKeylogger	adrian__luca
2026-02-25 07:25	d602128bef26396a9ce5...	exe	VIPKeylogger	exe VIPKeylogger	threatcat_ch
2026-02-24 10:31	4bbdc2db8ebd024339f6...	exe	VIPKeylogger	exe signed VIPKeylogger	lowmal3
2026-02-24 09:07	5e70b2297e5a0048390...	exe	VIPKeylogger	exe VIPKeylogger	threatcat_ch
2026-02-24 09:03	dbd4edd258813db2cac...	exe	VIPKeylogger	exe VIPKeylogger	threatcat_ch
2026-02-24 08:11	d4f2c8d4ed30fe2b3396...	bat	VIPKeylogger	bat VIPKeylogger	smica83
2026-02-23 15:00	2b320104efeed5369240...	tar	VIPKeylogger	tar VIPKeylogger	FXOLabs
2026-02-23 11:56	0ac2b28cd85f9879f753...	js	VIPKeylogger	js VIPKeylogger	abuse_ch
2026-02-23 11:51	1e32a98bbd8eae6d357...	js	VIPKeylogger	js VIPKeylogger	abuse_ch
2026-02-23 11:51	a3a6bb7ebe6279e7b21...	js	VIPKeylogger	js VIPKeylogger	abuse_ch
2026-02-23 11:49	178a3a0f271b5eea6a98...	js	VIPKeylogger	js VIPKeylogger	abuse_ch
2026-02-23 10:32	938046c9235f3c5d7257...	exe	VIPKeylogger	exe geo TUR VIPKeylogger	abuse_ch

Again, the sample can be found in the downloads folder.

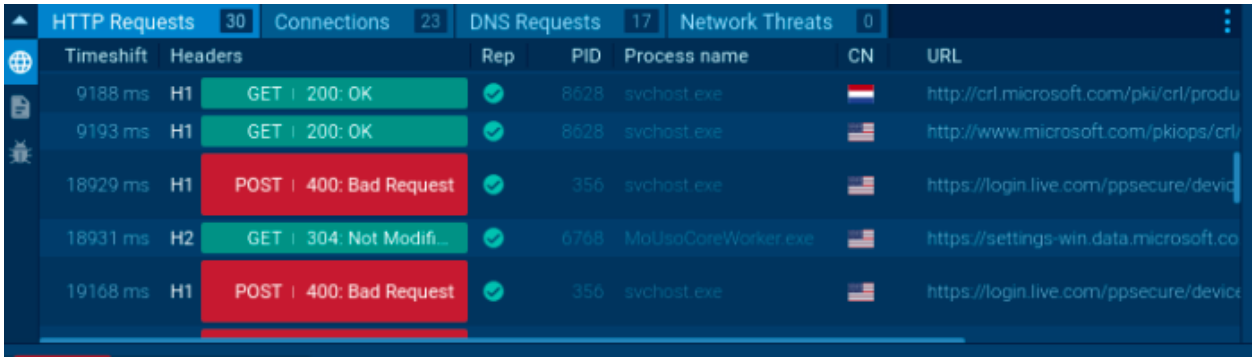


```
Session  Actions  Edit  View  Help

┌──(gregory㉿kali)-[~/Downloads]
└─$ ls -l
total 112
-rw-rw-r-- 1 gregory gregory 12697 Mar 10 03:19 0ac2b28cd85f9879f753199613c2884f1d46e877755099b6b4
084be2a052279f.zip
-rw-rw-r-- 1 gregory gregory 96841 Mar 10 03:02 183c7a7607fb4bfbdedc8ac29f56dc44833c79d671bb20f6e8
8ed2dd32a12578.zip

┌──(gregory㉿kali)-[~/Downloads]
└─$
```

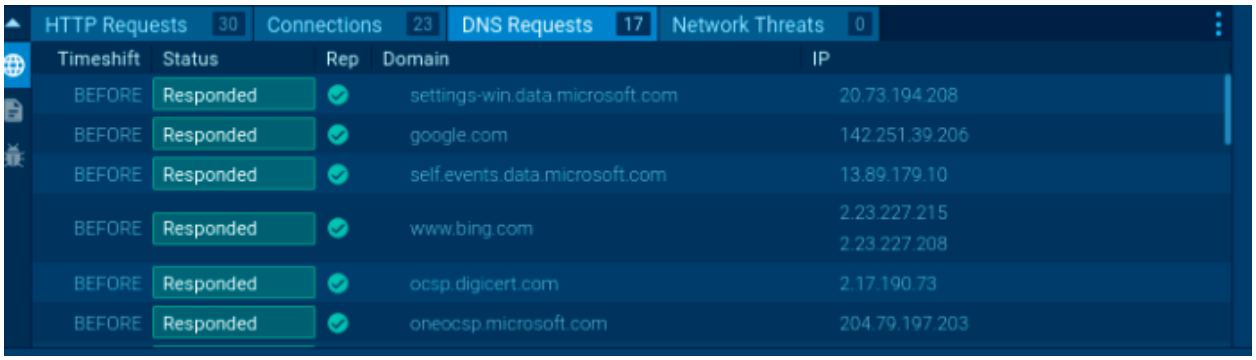
This time, the malware has a much higher level of activity.

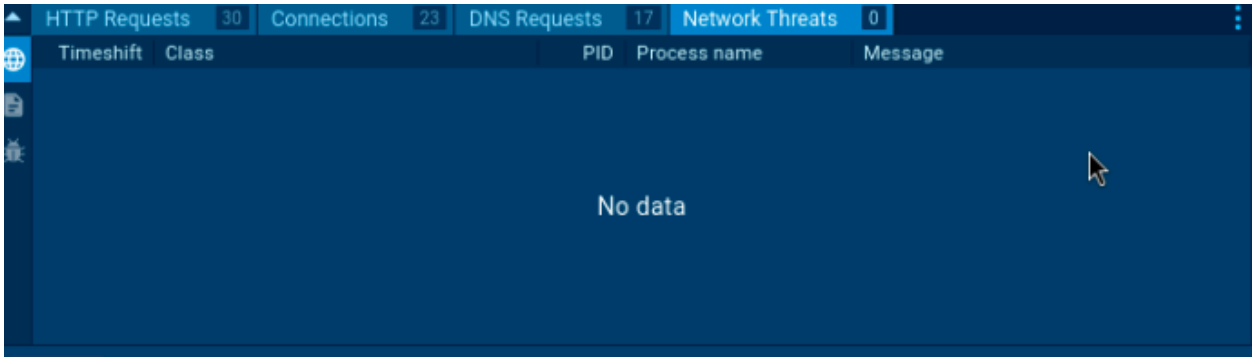


HTTP Requests 30 | Connections 23 | DNS Requests 17 | Network Threats 0

Timeshift	Headers		Rep	PID	Process name	CN	URL
9188 ms	H1	GET ı 200: OK	✓	8628	svchost.exe		http://crl.microsoft.com/pki/crl/produ
9193 ms	H1	GET ı 200: OK	✓	8628	svchost.exe		http://www.microsoft.com/pkiops/crl/
18929 ms	H1	POST ı 400: Bad Request	✓	356	svchost.exe		https://login.live.com/ppsecure/devic
18931 ms	H2	GET ı 304: Not Modifi...	✓	6768	MoUsoCoreWorker.exe		https://settings-win.data.microsoft.co
19168 ms	H1	POST ı 400: Bad Request	✓	356	svchost.exe		https://login.live.com/ppsecure/devic


HTTP Requests 30
Connections 23
DNS Requests 17
Network Threats 0
Timeshift Protocol Rep PID Process name CN IP Port Domain ASN
BEFORE UDP 4 System 192.168.100.255 137 – Not routed
BEFORE TCP 7736 RUXIMICS.exe 20.73.194.208 443 settings-win... MICROSOF
BEFORE TCP 6768 MoUsoCoreWorker.exe 20.73.194.208 443 settings-win... MICROSOF
BEFORE TCP 8628 svchost.exe 20.73.194.208 443 settings-win... MICROSOFT
BEFORE TCP – – 2.23.227.215 443 www.bing.com AKAMAI-AS
BEFORE TCP – – 2.17.190.73 80 ocsp.digicert... AKAMAI-AS
BEFORE TCP – – 204.79.197.203 80 oneocsp.mic... MICROSOFT


HTTP Requests 30
Connections 23
DNS Requests 17
Network Threats 0
Timeshift Status Rep Domain IP
BEFORE Responded settings-win.data.microsoft.com 20.73.194.208
BEFORE Responded google.com 142.251.39.206
BEFORE Responded self.events.data.microsoft.com 13.89.179.10
BEFORE Responded www.bing.com 2.23.227.215 2.23.227.208
BEFORE Responded ocsp.digicert.com 2.17.190.73
BEFORE Responded oneocsp.microsoft.com 204.79.197.203


HTTP Requests 30
Connections 23
DNS Requests 17
Network Threats 0
Timeshift Class PID Process name Message
No data

IOCs

Summary of indicators of compromises 12

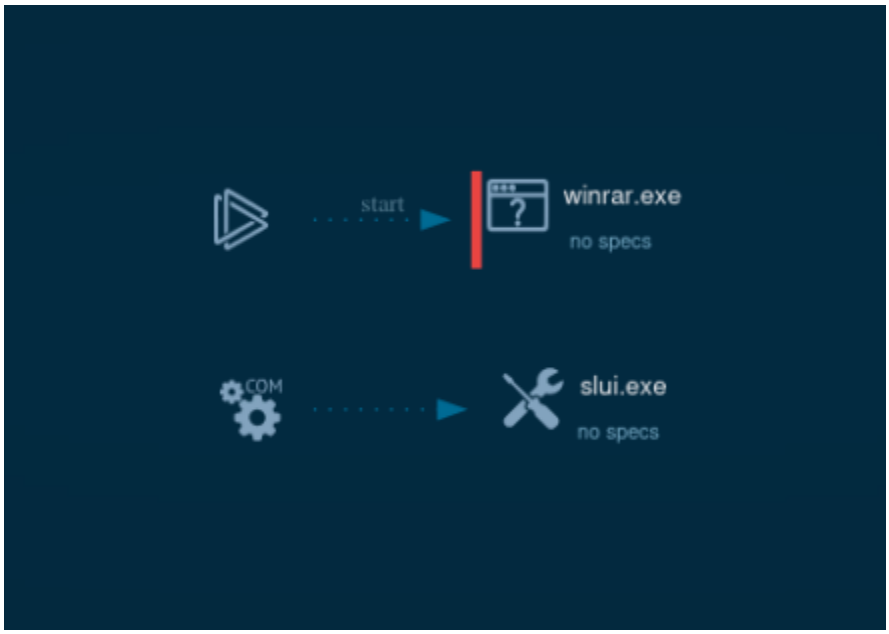
Copy selected

Main object – 0ac2b28cd85f9879f753199613c2884f1d46e877755099b6b4084be2a052279f.zip

SHA256	0ac2b28cd85f9879f753199613c2884f1d46e877755099b6b4084be2a052279f.zip
	d1d4b896afcc34ffa9ea281c109f06dbb90980044b7f62c5a9b1be252406612a

HTTP/HTTPS requests (11)

URL	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAjTxtAB8my1oj8MfWpz%2F7Y%3D
URL	http://oneocsp.microsoft.com/ocsp/MFQwUjBQME4wTDAJBgUrDgMCGgUABBQ3L3%2F%2Fa6ADK8NraY2GXzVaYrHG4AQUb6t%2B2v%2BXQ3LsO2d33oJhNYhHQoUCEzMAAAAGb6JMMcOVb6sAAAAAAAY%3D
URL	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAz1vQYrVgL0erhQLCPM8GY%3D
URL	https://login.live.com/ppsecure/deviceaddcredential.srf
URL	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl
URL	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl
URL	https://login.live.com/RST2.srf
URL	https://settings-win.data.microsoft.com/settings/v3.0/WSD/WaaSAssessment?os=Windows&osVer=10.0.19041.1.amd64fre.vb_release.191206-



General Info

Add for printing

File name: 0ac2b28cd85f9879f753199613c2884f1d46e877755099b6b4084be2a052279f.zip

Full analysis: https://app.any.run/tasks/3beb5e61-ddf7-4977-bd80-447cae5f709d

Verdict: Malicious activity

Threats: **Keylogger**

A keylogger is a type of spyware that infects a system and has the ability to record every keystroke made on the device. This lets attackers collect personal information of victims, which may include their online banking credentials, as well as personal conversations. The most widespread vector of attack leading to a keylogger infection begins with a phishing email or link. Keylogging is also often present in remote access trojans as part of an extended set of malicious tools.

Malware Trends Tracker >>>

Analysis date: March 10, 2026 at 03:21:52

OS: Windows 10 Professional (build: 19044, 64 bit)

Tags: auto | vipkeylogger | keylogger | arch-scr

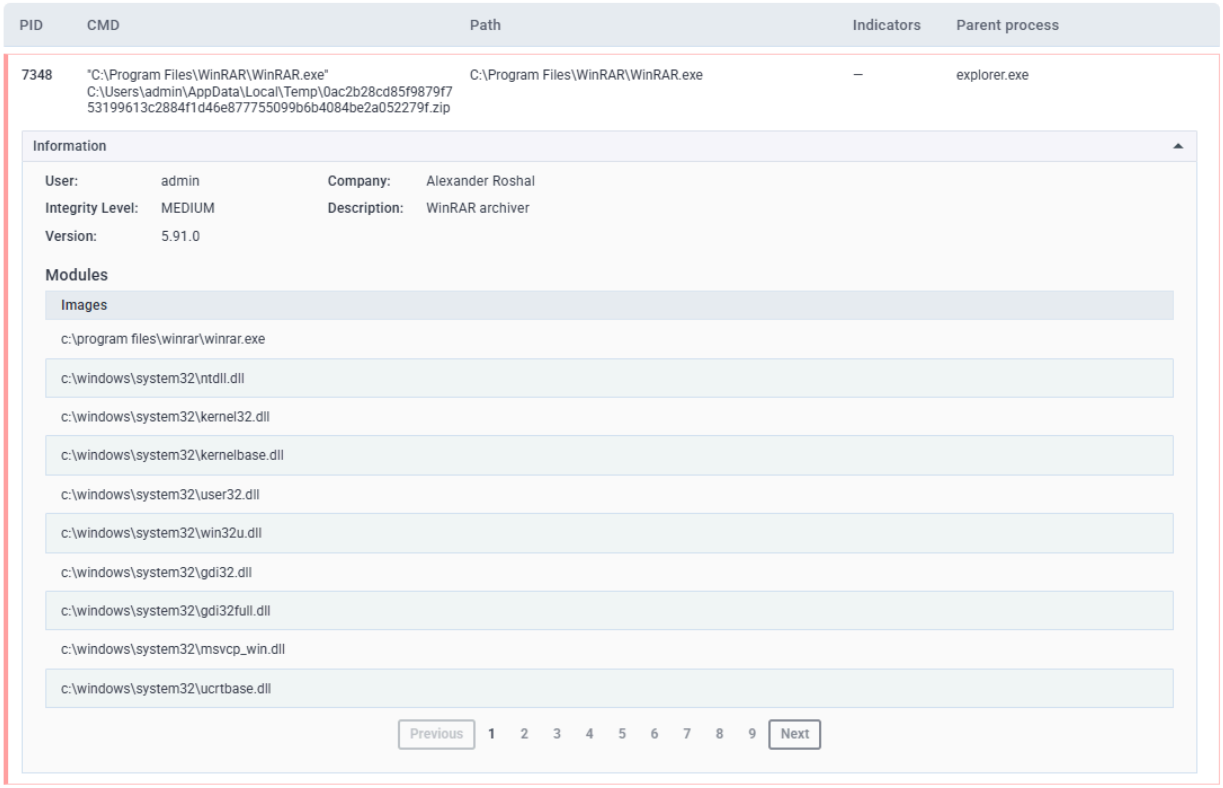
Indicators:

Registry activity

Add for printing

Total events	Read events	Write events	Delete events
5 116	5 106	10	0

Modification events



As its name would imply, VIPKeylogger is a keylogger, which attempts to obtain sensitive information from infected systems. Multiple executable files are run by the spyware, which appear to be made to capture keyboard and similar inputs from the target system. It seems as though several of the attempted connections aim to access Microsoft services, among other domains. Though it is difficult to determine with a cursory examination, this may be done to compromise one's use of these services, or as a way to forward obtained information back to the attacker.

Mirai and VIPKeylogger have several crucial differences in how they operate. VIPKeylogger is primarily focused on obtaining information from the target system, and does not truly seek to "take over" the device to use it for malicious purposes. Doing so, in fact, might impede its goal of information collection. Given that VIPKeylogger aims to collect passwords and other sensitive information typed by victims, evading detection is important for this malware. More intrusive actions, which could lead to detection, are thus avoided. Mirai, on the other hand, simply seeks to utilize devices in a wider botnet for further malicious activities. Due to their weaker nature and pervasiveness, IoT devices are thus appealing targets. Given that these are the primary devices targeted by Mirari, though, a keylogger function would likely have little practical benefit for these attackers. A victim would not be likely to access a banking application from their smart TV, for example. While both Mirai and VIPKeylogger are, of course, both prominent kinds of malicious programs, they do not possess many additional similarities beyond this.