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.

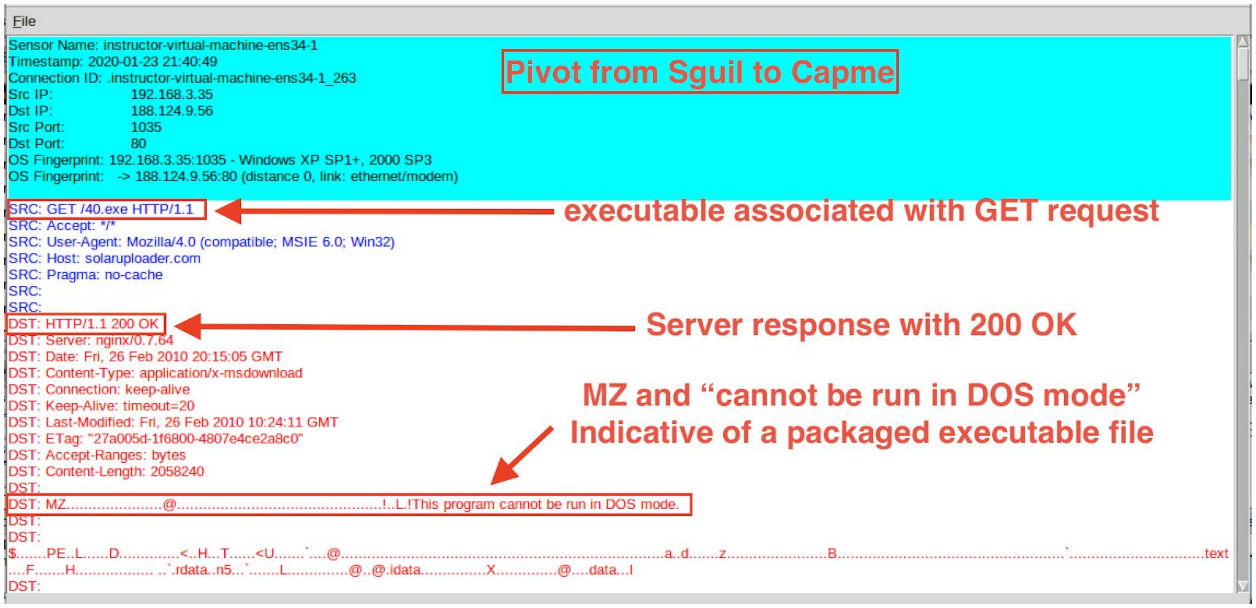
Reconnaissance	Email addresses possibly exposed through vendor and/or customer mailing lists.
Weaponization	JavaScript downloader called JS/Nemucod, which is attached directly to the emails inside os a ZIP file.
Delivery	Unsolicited SPAM email.
Exploitation	Nemucod will use three different ActiveX controls: 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	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. 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.
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.

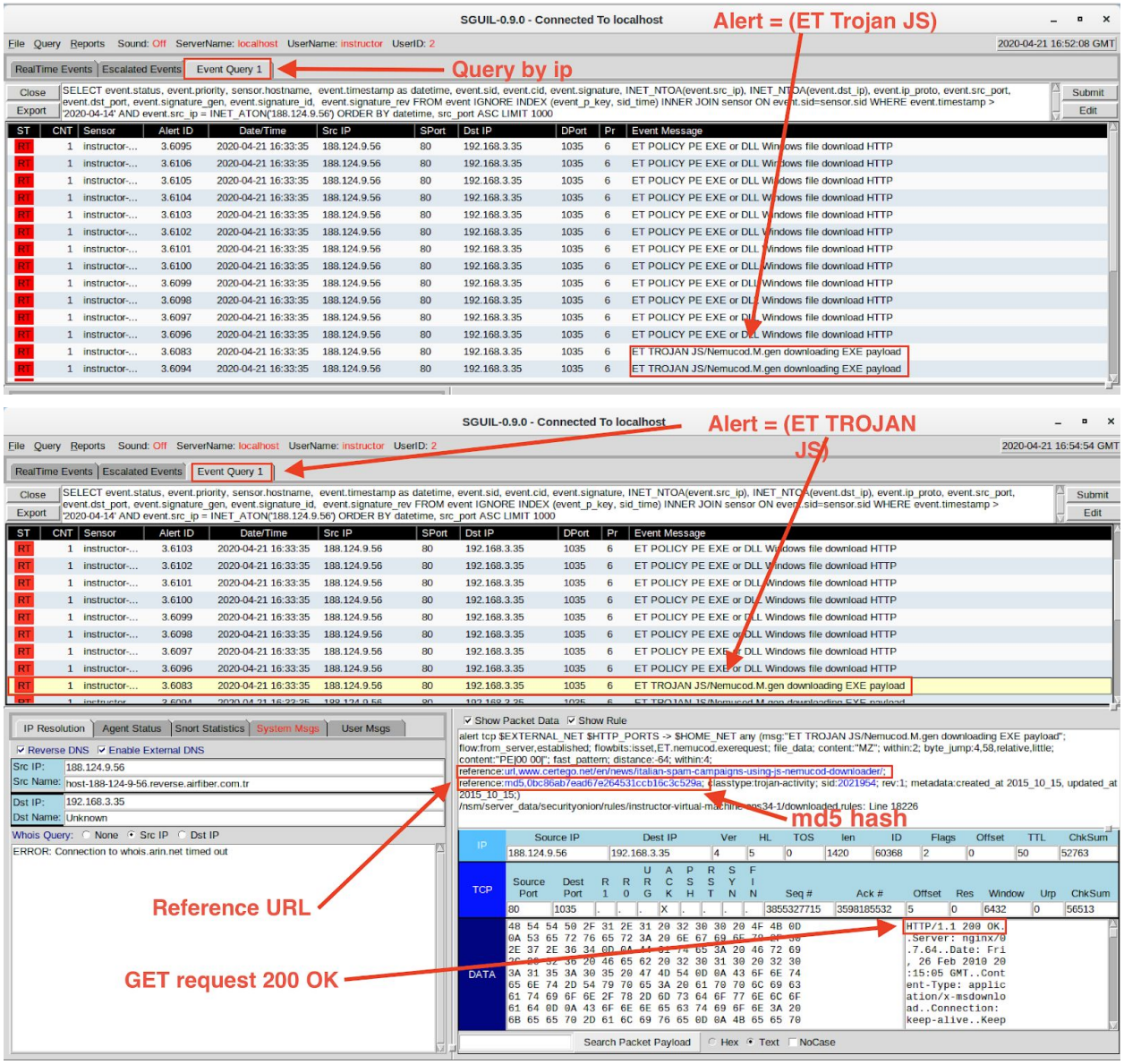
4. What are your recommended mitigation strategies?

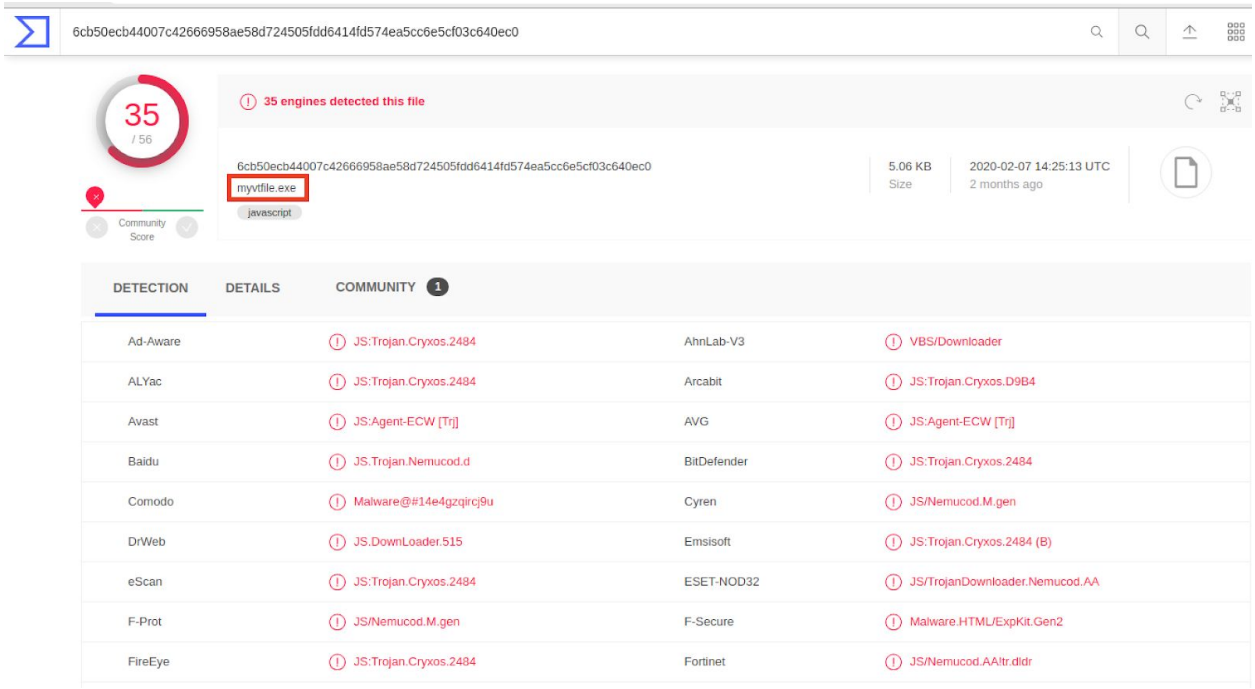
Enforce security awareness programs with regularity.

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/gozipdf




SGUIL-0.9.0 - Connected To localhost
Alert = (ET Trojan JS)
Query by ip
Alert = (ET TROJAN JS)
Reference URL
GET request 200 OK
md5 hash


6cb50ecb44007c42666958ae58d724505fdd6414fd574ea5cc6e5cf03c640ec0
35
/ 56
Community Score
35 engines detected this file
6cb50ecb44007c42666958ae58d724505fdd6414fd574ea5cc6e5cf03c640ec0
myvtfile.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

Italian spam campaigns using JS/Nemucod downloader | C

Italian spam campaigns us × | VirusTotal × | +

certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader/

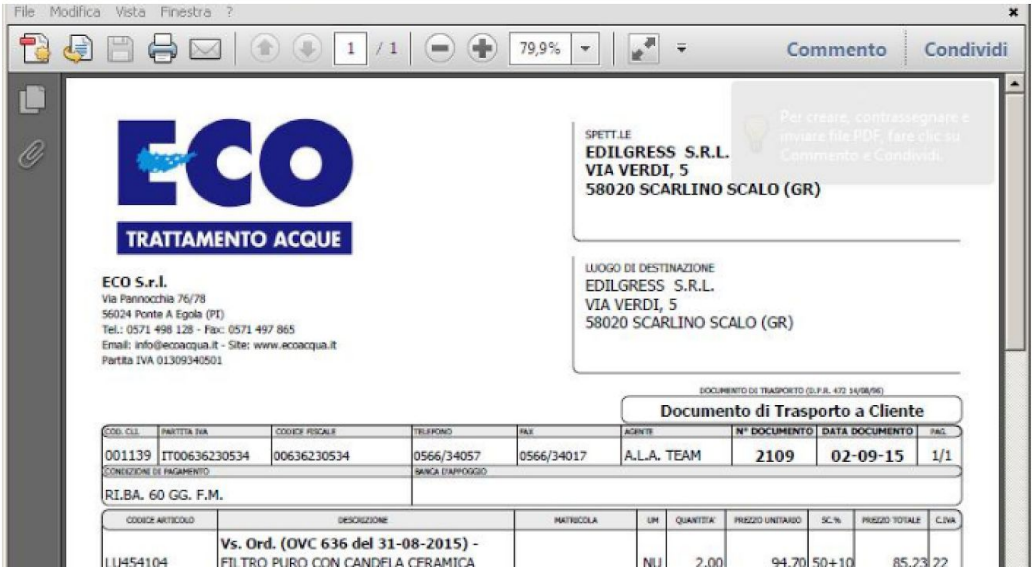
certego

Company

You are here: Home > News > Italian spam campaigns using JS/Nemucod downloader

Italian spam campaigns using JS/Nemucod downloader

15 October 2015



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:

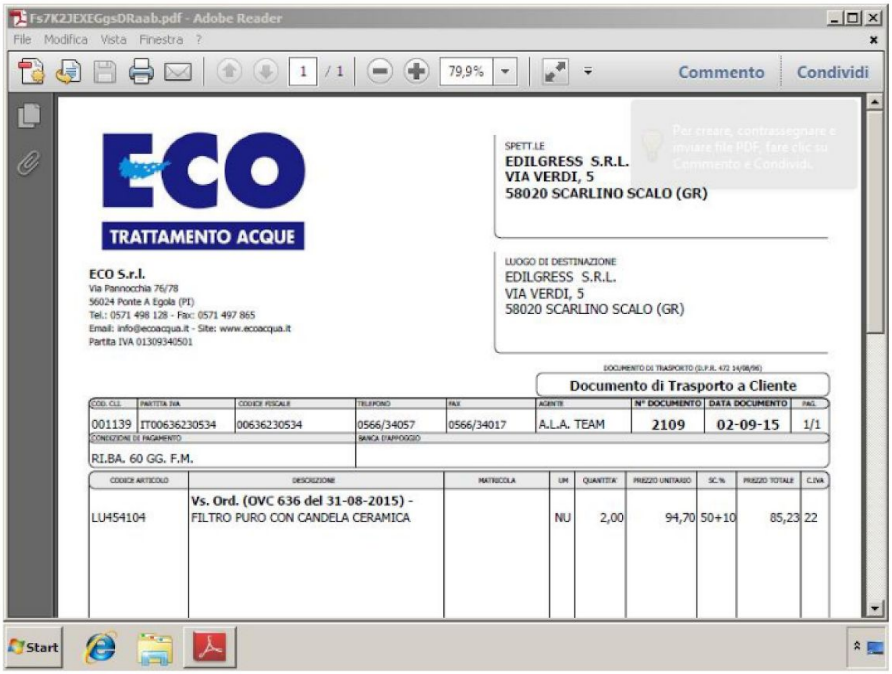
```
fattura_28234_del_07_10_2015.zip
```

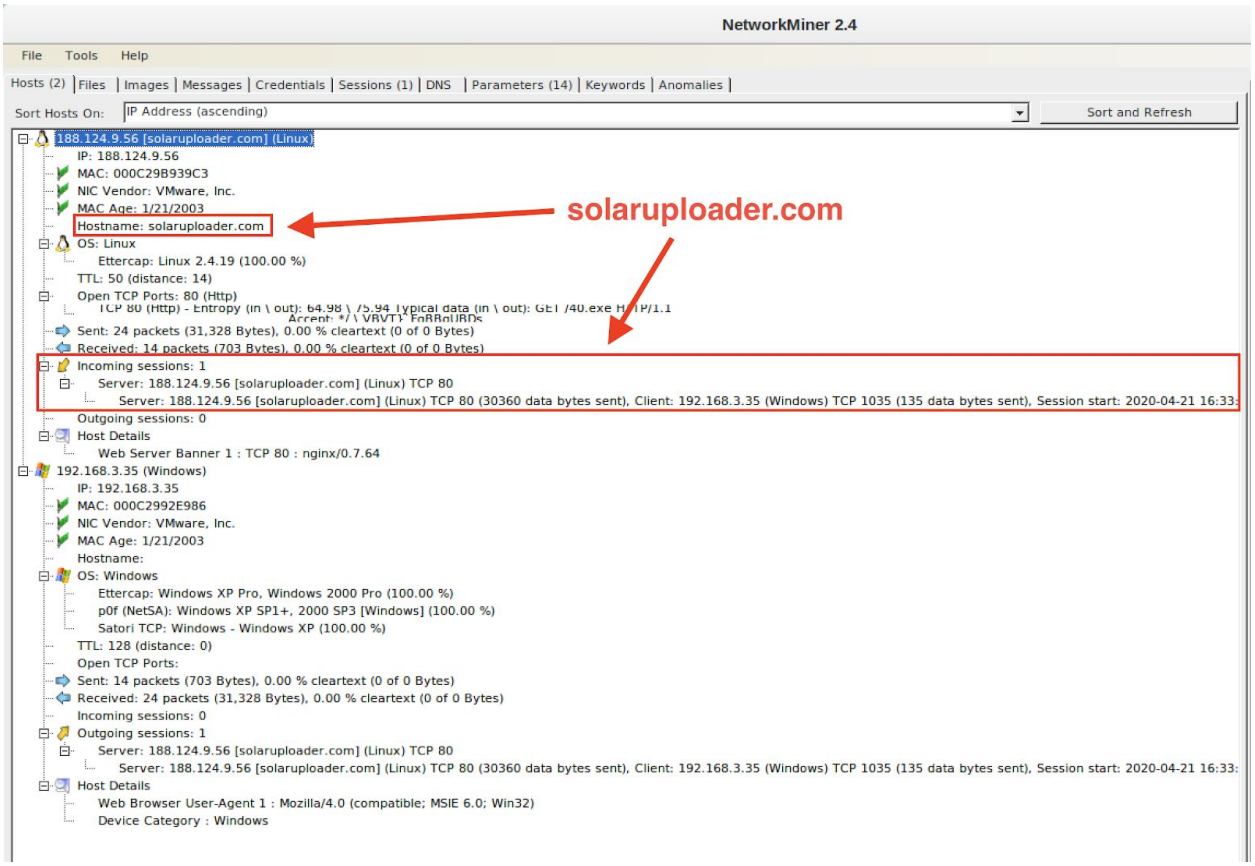
Some examples of the JavaScript files inside the zip are:

```
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 uses 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)
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
solaruploader.com

certego

Company Services N

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 infostealer. 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 server 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.