ZLAB

Malware Analysis Report

A new variant of Ursnif Banking Trojan served by the Necurs botnet hits Italy

21/06/2018

CSE CyberSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Table of Contents

Introduction

Starting from 6th June, a new version of the infamous banking trojan Ursnif hit Italian companies. This malware is well known to the cyber-security community, the Ursnif banking Trojan was the most active malware code in the financial sector in 2016 and the trend continued through 2017 to date.

In previous campaigns, the Ursnif banking Trojan targeted users in Japan, North America, Europe and Australia, later the authors improved their evasion technique to target users worldwide, especially in Japan.

The malware is able to steal users' credentials, credentials for local webmail, cloud storage, cryptocurrency exchange platforms and e-commerce sites.

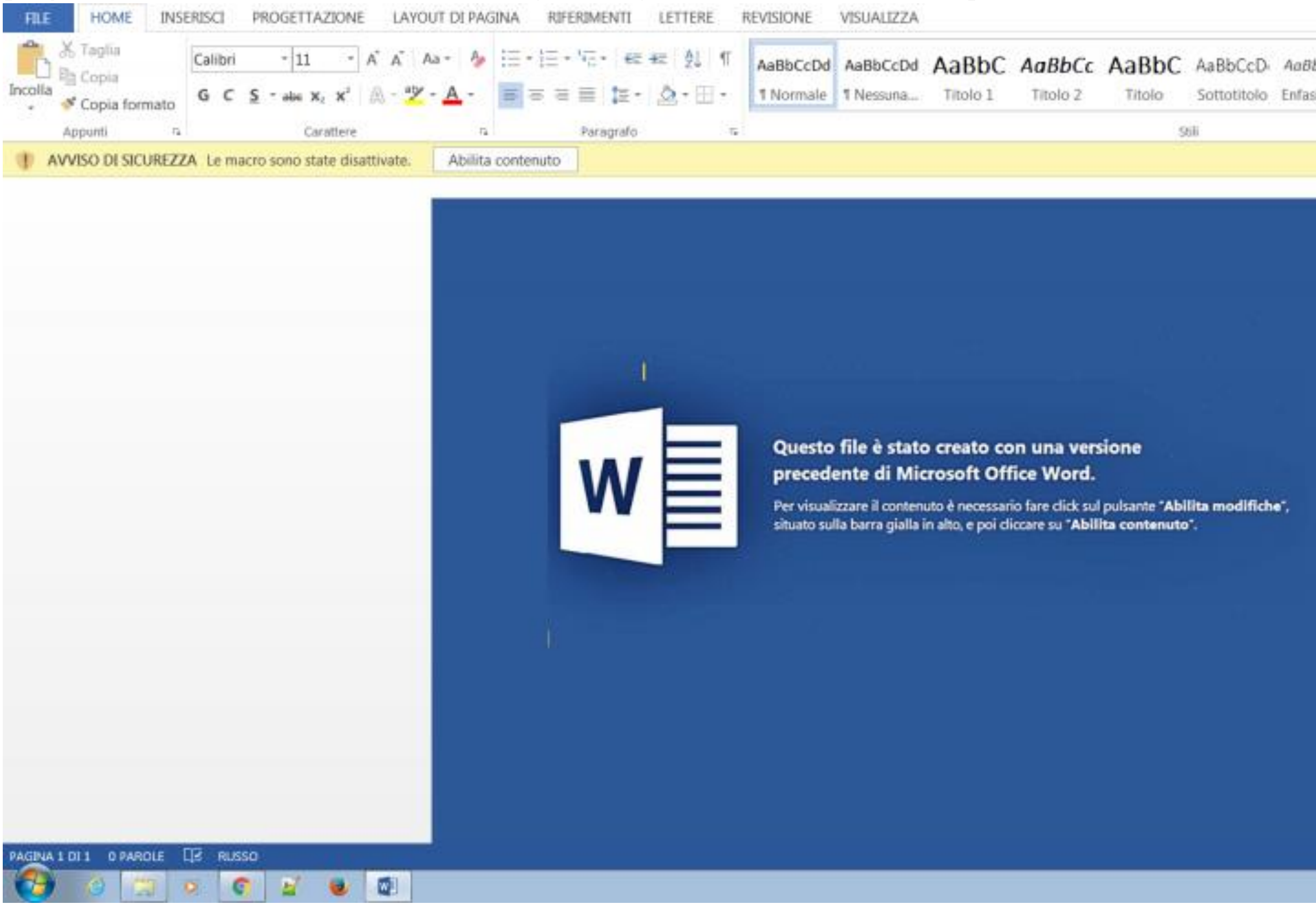
The malware has been active since at least 2009, as reported by Microsoft.

The technical information reported by Microsoft refers to an older version of the malware, but the version that is spreading in Italy presents many improvements.

CSE Cybsec ZLab researchers are conducting analysis on the latest version of the malware. The experts started the investigation after the discovery of a suspicious file that was used in a targeted attack against one of its customers.

The attachment used in the campaign that hit Italian companies is a weaponized Microsoft Word document, it uses a social engineering technique to trick users into enabling macros in order to allow the correct view of its content.

[caption id="attachment_73869" align="alignnone" width="1024"]



AVVISO DI SICUREZZA Le macro sono state disattivate.

Questo file è stato creato con una versione precedente di Microsoft Office Word.

Per visualizzare il contenuto è necessario fare click sul pulsante "Abilita modifiche", situato sulla barra gialla in alto, e poi cliccare su "Abilita contenuto".

Ursnif phishing Word document screen

Moreover, Ursnif once infected a new machine will attempt to spread to any other users in the address book of the compromised email accounts.

In order to trick the victim into opening the malicious email, the message is presented as the reply to an existing conversation conducted by the victim in the past.

Two following features of the email messages suggest they are counterfeit:

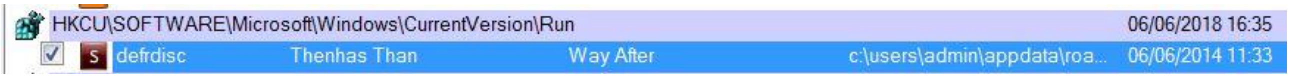
- The email body is written in incorrect Italian language.
- The attachment is a Word document which pretends to have been created with an older version of Microsoft Office and, as usual, invites the user to enable the macros (as shown in Figure 1). The name of this file is exceedingly tricky because the malware keeps track of the victim company name: it concatenates the name of the company with the

keyword “Richiesta” (in Italian means request), the resulting complete name of the weaponized file used to target Italian companies is “[VICTIM_COMPANY_NAME]_Richiesta.doc”.

The second step of the infection process begins only after enabling macros: the macros launched a malicious script that downloads and execute a payload from a server controlled by the attackers. It first downloads a malicious binary in the path *“%APPDATA%\Local\Temp\[temporary-name].exe*”, then it downloads another executable in the path *“%APPDATA%\Roaming\Microsoft\BthsSSDP\cmiftall.exe*”.

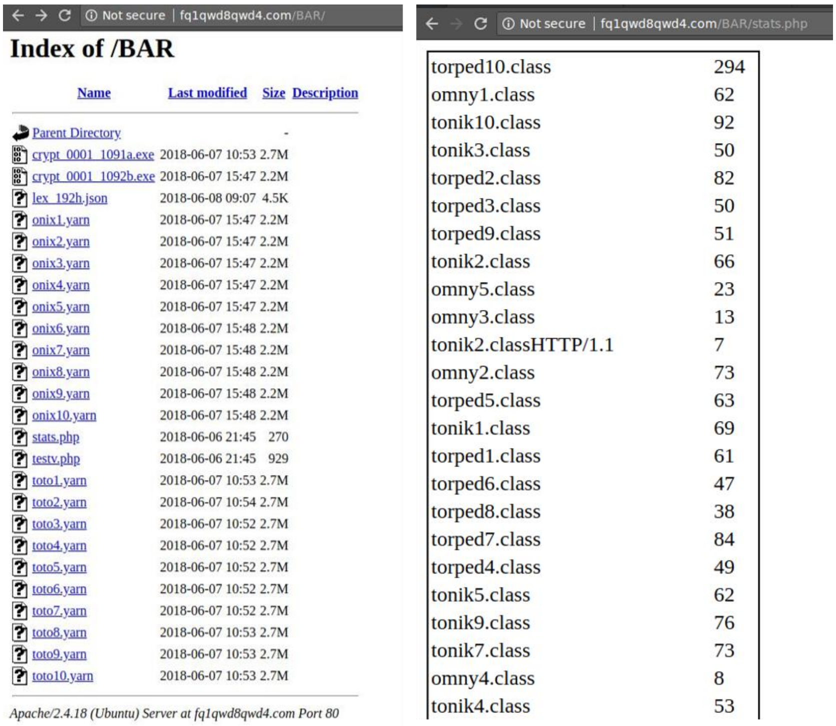
The latest Ursnif variant used the same name for any sample analyzed by the researchers.

This *cmiftall.exe* file is used to survive and implement the persistence mechanism even after the reboot, the malicious code set up the registry key “*HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*”.



HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				06/06/2018 16:35
☑ defrdisc	Thenhas Than	Way After	c:\users\admin\appdata\roa...	06/06/2014 11:33

Figure 1 - Persistence Key set.



Index of /BAR

Name	Last modified	Size	Description
Parent Directory		-	
crypt_0001_1091a.exe	2018-06-07 10:53	2.7M	
crypt_0001_1092b.exe	2018-06-07 15:47	2.2M	
lex_192h.json	2018-06-08 09:07	4.5K	
onix1.yarn	2018-06-07 15:47	2.2M	
onix2.yarn	2018-06-07 15:47	2.2M	
onix3.yarn	2018-06-07 15:47	2.2M	
onix4.yarn	2018-06-07 15:47	2.2M	
onix5.yarn	2018-06-07 15:47	2.2M	
onix6.yarn	2018-06-07 15:48	2.2M	
onix7.yarn	2018-06-07 15:48	2.2M	
onix8.yarn	2018-06-07 15:48	2.2M	
onix9.yarn	2018-06-07 15:48	2.2M	
onix10.yarn	2018-06-07 15:48	2.2M	
stats.php	2018-06-06 21:45	270	
testv.php	2018-06-06 21:45	929	
toto1.yarn	2018-06-07 10:53	2.7M	
toto2.yarn	2018-06-07 10:54	2.7M	
toto3.yarn	2018-06-07 10:52	2.7M	
toto4.yarn	2018-06-07 10:52	2.7M	
toto5.yarn	2018-06-07 10:52	2.7M	
toto6.yarn	2018-06-07 10:52	2.7M	
toto7.yarn	2018-06-07 10:52	2.7M	
toto8.yarn	2018-06-07 10:53	2.7M	
toto9.yarn	2018-06-07 10:53	2.7M	
toto10.yarn	2018-06-07 10:53	2.7M	

Apache/2.4.18 (Ubuntu) Server at fq1qwd8qwd4.com Port 80

torped10.class	294
omny1.class	62
tonik10.class	92
tonik3.class	50
torped2.class	82
torped3.class	50
torped9.class	51
tonik2.class	66
omny5.class	23
omny3.class	13
tonik2.classHTTP/1.1	7
omny2.class	73
torped5.class	63
tonik1.class	69
torped1.class	61
torped6.class	47
torped8.class	38
torped7.class	84
torped4.class	49
tonik5.class	62
tonik9.class	76
tonik7.class	73
omny4.class	8
tonik4.class	53

Figure 2 – Open directory on one of the server

The Ursnif banking Trojan can operates without being noticed by both the user and the Operating System because it is capable to inject its malicious code into the “explorer.exe” process, which is one the most important processes in the Microsoft’s OS.

We already studied and reported this advanced technique in January, in which, was analyzed a previous variant of the Ursnif malware. The report is available at the following URL:

https://securityaffairs.co/wordpress/67636/malware/process-hollowing-ursnif-malware.html

Furthermore, we discovered several websites used as a sort of repository for the malware. The repository were containing many other samples of the Ursnif malware, in one case the website also included another directory containing statistics of the malware, including the number of the downloads.

This latter particular suggests the repository was part of a malware-as-a-service platform that was offering the malicious code for rent.

The Italian campaign

Through surfing in the principal threat intelligence and information sharing platforms, we discovered other malicious documents using the same name pattern and showing the same screen of Figure 1.

Below the key findings of the analysis we have conducted:

- The weaponized files were contacting different domains.
- Each bait file was using a different macro, we identified at least three different code styles to implement the same behavior.
- Going on with the days, the contacted domains started to go offline. We hypothesize that the threat actor halted the attacks after it was discovered.

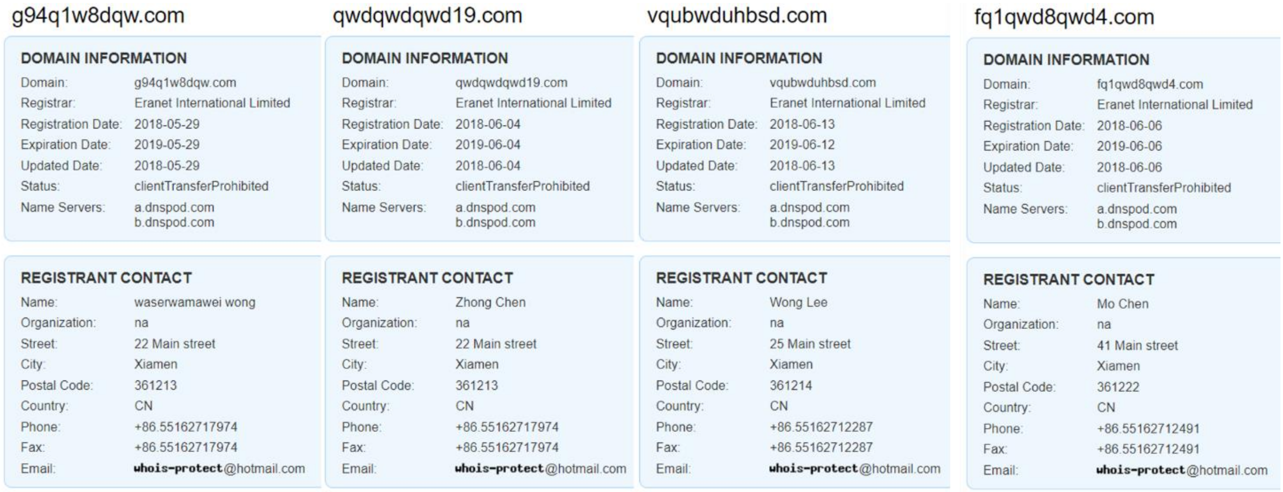
Below the list of samples we analyzed and the associated domains:

Document’s name	Domain	IP	Hash (MD5)
AdelaideConsulting_Richiesta.doc	qwdqwdqwd19.com	151.80.162.223	c97e623145f7b44497b31ef31a39efed
AMLM_Richiesta.doc	g94q1w8dqw.com	45.41.80.86	b48f658dbd0ef764778f953e788d38c9
Comune_di_Lequio_Tanaro_Richiesta.doc	vqubwduhbsd.com	23.227.201.166	6f571b39fcde69100eb7aec3c0db0a98

ComunediVALDELLATORRE_Richiesta.doc	fq1qwd8qwd4.com	172.106.170.85	29ca7312b356531f9a7a4c1c8d164bdd
IV_Richiesta.doc	wdq9d5q18wd.com	-	535a4ebb8aef4c3f18d9b68331f4b964
OrdineDeiGiornalisti_Richiesta.doc	fq1qwd8qwd4.com	172.106.170.85	347ce248b44f2b26adc600356b6e9034
WSGgroup_Richiesta.doc	vqubwduhbsd.com	23.227.201.166	3c301ff033cb3f1af0652579ad5bc859
CB_Richiesta.doc	fq1qwd8qwd4.com	172.106.170.85	1e8d75b5c93913f0f0e119a9beb533cb

Table 1 - Synthetizing table of document samples.

Due to the impossibility of analyzing each payload because attackers have shut down the associated server we conducted a domain analysis through WHOIS queries for each domain.



g94q1w8dqw.com

DOMAIN INFORMATION
Domain: g94q1w8dqw.com
Registrar: Eranet International Limited
Registration Date: 2018-05-29
Expiration Date: 2019-05-29
Updated Date: 2018-05-29
Status: clientTransferProhibited
Name Servers: a.dnspod.com
b.dnspod.com

REGISTRANT CONTACT
Name: waserwamawei wong
Organization: na
Street: 22 Main street
City: Xiamen
Postal Code: 361213
Country: CN
Phone: +86.55162717974
Fax: +86.55162717974
Email: whois-protect@hotmail.com

qwdqwdqwd19.com

DOMAIN INFORMATION
Domain: qwdqwdqwd19.com
Registrar: Eranet International Limited
Registration Date: 2018-06-04
Expiration Date: 2019-06-04
Updated Date: 2018-06-04
Status: clientTransferProhibited
Name Servers: a.dnspod.com
b.dnspod.com

REGISTRANT CONTACT
Name: Zhong Chen
Organization: na
Street: 22 Main street
City: Xiamen
Postal Code: 361213
Country: CN
Phone: +86.55162717974
Fax: +86.55162717974
Email: whois-protect@hotmail.com

vqubwduhbsd.com

DOMAIN INFORMATION
Domain: vqubwduhbsd.com
Registrar: Eranet International Limited
Registration Date: 2018-06-13
Expiration Date: 2019-06-12
Updated Date: 2018-06-13
Status: clientTransferProhibited
Name Servers: a.dnspod.com
b.dnspod.com

REGISTRANT CONTACT
Name: Wong Lee
Organization: na
Street: 25 Main street
City: Xiamen
Postal Code: 361214
Country: CN
Phone: +86.55162712287
Fax: +86.55162712287
Email: whois-protect@hotmail.com

fq1qwd8qwd4.com

DOMAIN INFORMATION
Domain: fq1qwd8qwd4.com
Registrar: Eranet International Limited
Registration Date: 2018-06-06
Expiration Date: 2019-06-06
Updated Date: 2018-06-06
Status: clientTransferProhibited
Name Servers: a.dnspod.com
b.dnspod.com

REGISTRANT CONTACT
Name: Mo Chen
Organization: na
Street: 41 Main street
City: Xiamen
Postal Code: 361222
Country: CN
Phone: +86.55162712491
Fax: +86.55162712491
Email: whois-protect@hotmail.com

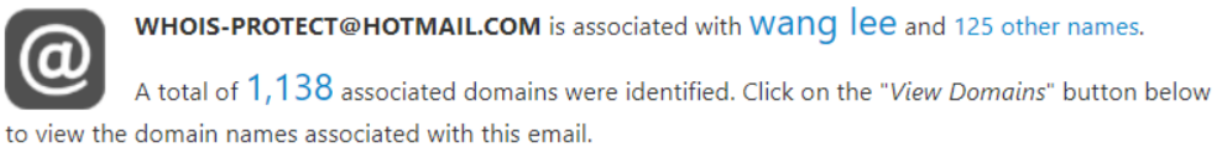
Figure 3 - WHOIS information about domains related to Ursnif

The discovery

The domain analysis revealed that all the domains were registered by the same email address, “*whois-protect[@]hotmail[.]com*”.

This email address suggests a reference to a particular service for the privacy protection provided by the WHOIS service, but, in reality, it is a simple registered email account on the Hotmail platform. This means that the attackers used it to register the domains.

Investigating on the email address, we discovered that it was used to register about 1000 different domains:



WHOIS-PROTECT@HOTMAIL.COM is associated with wang lee and 125 other names.

A total of 1,138 associated domains were identified. Click on the "*View Domains*" button below to view the domain names associated with this email.

Figure 4 - Number of domains registered by whois-protect email

Moreover, this email address has a very bad reputation in the security community, because it was associated to the infamous botnet Necurs.

We found a reference to the address in one of the reports published by Cisco Talos:

https://blog.talosintelligence.com/2018/01/the-many-tentacles-of-necurs-botnet.html

It is well known that Necurs is the responsible of the 97% of the worldwide malicious spam campaigns that spread other malwares such as TrickBot, Dridex, Loki, Emotet, Scarab, etc.

This is the first time we found a link between the Ursnif campaign and the infamous botnet, this means that threat actors started spreading the Ursnif banking trojan leveraging Necurs malicious infrastructure.

Yara rules

```
rule Ursnif_Dropper {
    meta:
        description = "Yara Rule for Ursnif documents dropper"
        author = "CSE CybSec Enterprise - Z-Lab"
        last_updated = "2018-06-21"
        tlp = "white"
        category = "informational"
    strings:
        $a = { 56 42 5F 4E 61 6D 00 65 }

         $ab = { 71 5A 6C 55 45 74 77 55 00 41 6E 7A 22 }
         $ac = { 6D 49 44 00 7A 5A 6F 66 70 59 }
         $ad = { 61 66 00 A2 00 67 65 53 6F 50 69 }
        $ae = { 04 07 65 44 63 C0 4A 59 57 0D 0A 58 }
        $af = { 6A 62 77 00 53 59 51 49 75 4E 66 4B 10 6D }
        $ag = { 73 69 7A 00 48 4A 6A 49 44 22 }
        $ah = { 6A 62 77 00 53 59 51 49 75 4E 66 4B 10 6D }
    condition:
        $a and 1 of ($a*)
}

rule Ursnif_Executable {
    meta:
        description = "Yara Rule for Ursnif executable"
        author = "CSE CybSec Enterprise - Z-Lab"
        last_updated = "2018-06-21"
        tlp = "white"
        category = "informational"
    strings:
        $a = "uegnppk_umtrcrrusf"

        $b = { 59 7C 44 FA C0 B8 FF }
        $c = { 41 DD 40 20 D8 C9 DD 58 }
    condition:
        all of them
}
```

IOCs

DOMAINS

qwdqwdqwd19.com
g94q1w8dqw.com
vqubwduhbsd.com
fq1qwd8qwd4.com
wdq9d5q18wd.com
qwd1q6w1dq6wd1.com
qw8e78qw7e.com
qwdohqwnduasndwjd212.com

IPs

23.227.201.166
172.106.170.85
89.37.226.117
86.105.1.131
62.113.238.147
89.37.226.156
198.55.107.164

EMAILs

whois-protect@hotmail.com
zhejiangshangbang@qq.com

HASHES

C97E623145F7B44497B31EF31A39EFED
B48F658DBD0EF764778F953E788D38C9
6F571B39FCDE69100EB7AEC3C0DB0A98
29CA7312B356531F9A7A4C1C8D164BDD
535A4EBB8AEF4C3F18D9B68331F4B964
347CE248B44F2B26ADC600356B6E9034
3C301FF033CB3F1AF0652579AD5BC859

716D8D952102F313F65436DCB89E90AE
FD26B4B73E73153F934E3535A42B7A16