



# Ursnif: Long Live the Steganography!

02/07/2019

## Introduction

Another wave of Ursnif attacks hits Italy.

Ursnif is one of the most active banking trojan. It is also known as GOZI, in fact it is a fork of the original Gozi-ISFB banking Trojan that got its source code leaked in 2014 updating and evolving Gozi features over the years. Also in this variant, Ursnif use weaponized office document with a VBA macro embedded that act as a dropper and multi-stage highly obfuscated powershell scripts in order to hide the real payload. In addition, this Ursnif use also steganography to hide the malicious code and avoid AV detection.

Moreover, this variant uses the *QueueUserAPC* process injection technique to inject into explorer.exe in a more stealthier way, because no remote threads are created in the target process.

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. Clicca [qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti

Figure 1.  
Ursnif  
macro-  
weaponized  
document.

Extracting the macro code, shows the malware, in the first instance, checks the victim country using the *Application.International* MS Office property. If the result corresponds to Italy (code 39), the macro executes the next command using *Shell* function.

Figure  
2.  
Part  
of  
Visual  
Basic  
macro  
code.

The remaining functions of the macro are used to prepare the shell command to launch, concatenating several strings encoded in different ways (mainly in decimal and binary). The resulting command contains a huge binary string, which will be converted into a new Powershell command using the function:

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. Clicca [qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti

- [https://images2.imgbox\[.\]com/55/c4/rBzwpAzi\\_o.png](https://images2.imgbox[.]com/55/c4/rBzwpAzi_o.png)
- [https://i.postimg\[.\]cc/PH6QvFvF/mario.png?dl=1](https://i.postimg[.]cc/PH6QvFvF/mario.png?dl=1)

The apparently legit image actually contains a new Powershell command. The weaponized image is crafted using the Invoke-PSImage script, which allows to embeds the bytes of a script into the pixels of a PNG file.

Figure 4.  
Powershell  
script  
hidden  
into  
“Fancy  
Mario”’s  
image.

Et voilà, another obfuscated Powershell stage. The payload is encoded in Base64, so it is easy to move on and reveal the next code.

Figure 5.  
Another stage  
of  
deobfuscation

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. [Clicca qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti

Figure 6.  
Powershell  
script  
downloading  
the Ursnif  
loader.

It executes another check against victim's country, ensuring it is Italy. The information derives from the command:

**Get-Culture | Format-List -Property \***

If the check is positive, the script will download an EXE payload from *http://fillialopago[.]info/~DF2F63*, store it in *%TEMP%\Twain001.exe* and then execute it.

At the analysis time, the file is not detected by most antiviruses:

Figure 7.  
Ursnif  
loader  
detection  
rate

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. Clicca [qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti

Figure 8.  
IWebBrowser.Navigate  
function invocation.

The server responds to this request sending encrypted data, as show in the following figure

Figure 9.  
Part of  
network  
traffic  
containing  
some  
encrypted  
data.

After a decryption routine, all useful data is stored into registry keys at  
*HKCU\Software\AppDataLow\Software\Microsoft\{GUID}*.

Figure  
10.  
Registry  
keys set

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. Clicca [qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti

Figure 11.  
Command  
executed  
at  
machine's  
startup.

The command's only goal is to execute the data contained into *"cmiftall"* regvalue through Powershell engine.

```
C:\Windows\system32\wbem\wmic.exe /output:clipboard process call create "powershell -w hidden iex([System.Text.Encoding]::ASCII.GetString((get-itemproperty 'HKCU:\Software\AppDataLow\Software\Microsoft\94502524-E302-E68A-0D08-C77A91BCEB4E').cmiftall))"
```

The *"cmiftall"*'s data is simply a Powershell script encoded in Hexadecimal way, so it is possible to reconstruct its behavior.

Figure 12.  
Powershell  
script  
used to  
inject the

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. [Clicca qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti

So, using the Powershell script stored into regkey (shown above), Ursnif is able to allocate space enough for its malicious byte array, containing the final payload, and to start it as legit process' thread through *QueueUserAPC* and *SleepEx* calls.

The Ursnif's complete workflow is shown in figure:

Figure 13.  
Ursnif's  
workflow.

Finally, from data contained into last script's byte array, it is possible to extract a DLL which corresponds to what Ursnif inject into *explorer.exe* process.

This DLL seems to be corrupted, as stated by some static analysis tools:

Figure 14.  
Info about  
the  
malformed  
DLL.

However, when it is loaded in memory using APC injection technique, it works with no problems.

Submitting the file to VirusTotal the result is devastating: 0/56 anti-malware detects it

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. Clicca [qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti

# Conclusions

As stated first by us in the previous Ursnif analysis in December 2018 and after by Cisco Talos Intelligence in January 2019, also this new Ursnif sample uses the same APC injection technique to instill its final binary into *explorer.exe* process, along with obfuscation and steganography in order to hide its malicious behaviour. Ursnif is more active and widespread than yesterday, the contacted C2 is not reachable but the malware implant is still alive due to the fact that the crooks are constantly changing their C2 to diverting tracking and analysis.

Yoroi ZLab - Cybaze researchers are continuing the analysis of this undetected DLL in order to extract information and evidences to share with the research community.

# Indicators of Compromise

## Hashes

- 630b6f15c770716268c539c5558152168004657beee740e73ee9966d6de1753f (old sample)
- f30454bcc7f1bc1f328b9b546f5906887fd0278c40d90ab75b8631ef18ed3b7f (new sample)
- 93dd4d7baf1e89d024c59dbffce1c4cbc85774a1b7bcc8914452dc8aa8a79a78 (final binary)

## Dropurls

- [https://images2.imgbox\[.\]com/55/c4/rBzwpAzi\\_o.png](https://images2.imgbox[.]com/55/c4/rBzwpAzi_o.png)

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. Clicca [qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti



- roiboutique[.]ru
- uusisnfbfaa[.]xyz
- nolavalt[.]icu
- sendertips[.]ru

## IPs

- 185.158.248.142
- 185.158.248.143

## Artifacts

- HKCU:\Software\AppDataLow\Software\Microsoft\94502524-E302-E68A-0D08-C77A91BCEB4E

# Yara rules

```
import "pe"

rule Ursnif_201902 {
  meta:
    description = "Yara rule for Ursnif loader - January version"
    author = "Yoroi - ZLab"
    last_updated = "2019-02-06"
    tlp = "white"
    category = "informational"
```

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. [Clicca qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti

Yoroi S.r.l.

Piazza Sallustio, 9  
00187 Roma (RM)

## Contact

info@yoroi.company

+39 051 0301005

## Legal

Terms & Conditions

MOG D.Lgs 231/01

Privacy Policy

Cookie Policy

Code of Ethics and  
Conduct

## Warning system

Subscribe to our early warning system

Downloads

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. Clicca [qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti



P.IVA.  
03407741200  
- R.E.A. RM  
1559639 -  
Codice  
Fiscale  
03407741200  
- Capitale  
Sociale:  
Euro  
100.000 IV  
Yoroi S.r.l.  
società  
soggetta ad  
attività di  
direzione e  
coordinamento  
esercitata  
dalla Tinexta  
S.p.A.

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. [Clicca qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti



credits: **SimpleNetworks**

Questo sito, come la maggior parte dei siti web, utilizza cookie, anche di terze parti, per migliorare la tua esperienza di navigazione e raccogliere informazioni sull'utilizzo del sito stesso. Cliccando su "Accetta tutti" ti dichiari d'accordo all'utilizzo di cookie analitici (che ci aiutano a capire in che modo gli utenti usano il sito e come migliorarlo, insieme ai nostri servizi) e di tracciamento (inclusi quelli di nostri partner di fiducia) che ci aiutano a decidere quali prodotti mostrarti, a misurare il volume di visite sul nostro sito e a darti la possibilità di mettere "mi piace" e di condividere contenuti direttamente sui social media. [Clicca qui](#) per vedere a cosa hai dato il tuo consenso e trovare più informazioni sui cookie che utilizziamo.

[Read More](#)

Gestisci Impostazioni

Rifiuta Tutti

Accetta tutti