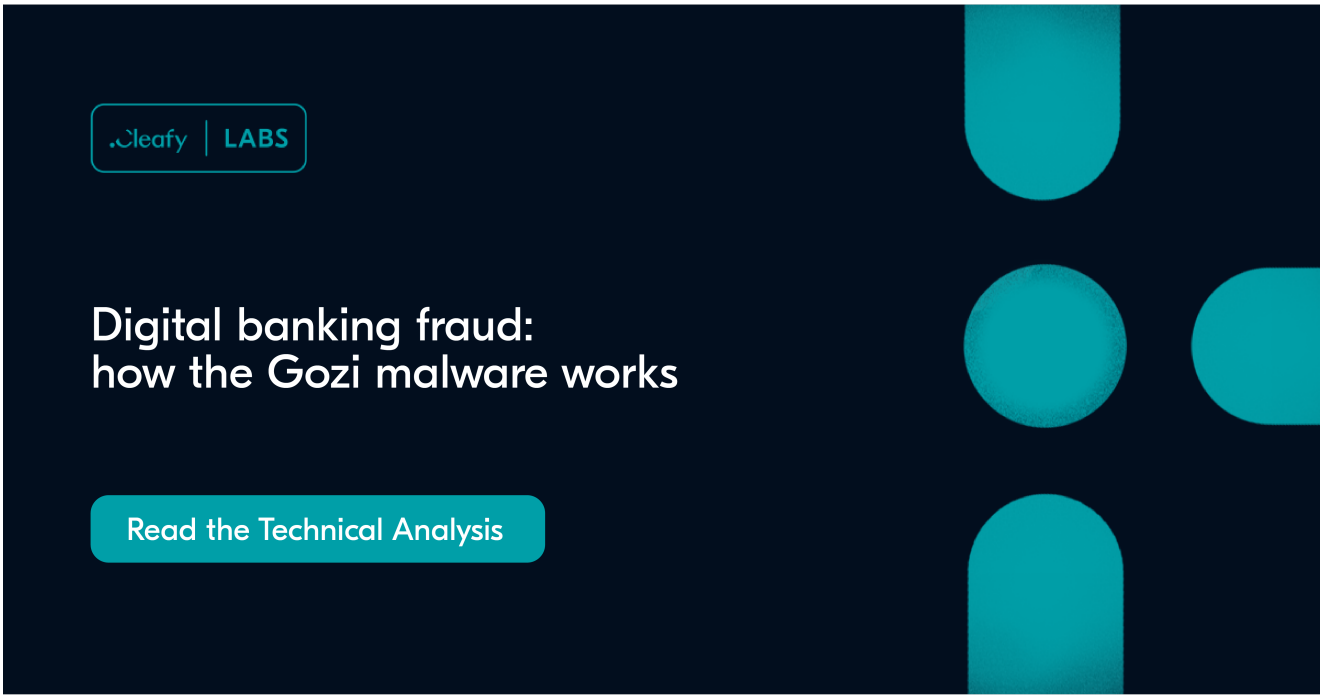
Digital banking fraud: how the Gozi malware works

cleafy.com/cleafy-labs/digital-banking-fraud-how-the-gozi-malware-work

Federico Valentini, Francesco Iubatti



Download your PDF guide to TeaBot

Get your free copy to your inbox now

Download PDF Version

Introduction

Also known as RM3, ISFB, Ursnif, Dreambot, CRM, and Snifula, Gozi can be considered as a group of malware families which are based on the same malicious codebase. Historically, it has been known as one of the most widely spread and longest-standing Banking Trojans with more than 14 years of activity. Its unique modular architecture facilitates multiple **Threat Actors** (TAs) in carrying on with their own malicious purposes, which in most cases are included in the following categories:

- Banking fraud
- eCommerce fraud
- POS devices compromise
- Ransomware

Since its source-code was leaked in 2015, tracking all the different variants appears to be knotty and time consuming due to its fragmentation and the several distinct names used by security firms and researchers. The main functionalities of Gozi families, and derivatives, include:

- Acting as info-stealer by collecting system activities and data (including network and browser data)
- Recording keystrokes (keylogging)
- Recording videos or making screenshots
- Performing MitB attacks on the targeted websites (e.g., Formgrabbing, Web-injects)
- Redirect browser navigation to malicious websites
- Enabling hVNC (hidden-VNC) and SOCKS proxy

Focusing on the **Banking fraud** category, during the last 2 years we were able to analyze in-depth a specific TA (or a group of affiliates) which distributes Gozi infections on EU territory to corporate banks and their customers.

During our analysis, we were able to extract multiple TTPs on how this specific TA leverages Gozi to execute unauthorized transactions to a well-organized network of bank mule accounts controlled by the same group.

OUR FINDINGS

More than 50 different banks and financial institutions appear to be targeted by this group, which includes both retail and corporate environments in Europe.

Through Gozi, the TA delivers a specific Web-inject family, which we dubbed as RATBANK (also known as ‘delsrc’), which is used to discriminate interesting bots and to perform **Account Takeover (ATO) fraud** only on valid ones.

The TA behind this pattern has a deep knowledge of how those targeted corporate banking environments work, which steps are needed to authorize a bank transfer, and how different 2FA (two factor authentication) mechanisms can be bypassed, by identifying specific weaknesses in their implementation.

During Q4 2020, the same group started distributing another Android malware (Alien) to expand their attack surface also on mobile devices.

The TA has access to native-speaking operators who perform vishing attacks in the attempt to elicit victims during the execution of an ATO scenario and to try to isolate all the communication between victims and their banks with Social Engineering tricks.

The TA has access to a significant and well-structured set of money mule accounts, in multiple SEPA (Single Euro Payment Area) and NON-SEPA countries, which are typically discriminated against by the amount of the unauthorized transaction.

In the last 2 years, we identified **more than 100 bank accounts** controlled by this group, with the largest amount being **1,5M Euro, handled in a single bank transfer** during a targeted Account Takeover fraud.

Gozi malspam distribution: a recent example

Gozi has a very stable malspam distribution routine as many different campaigns have been used to spread this malware. In recent malspam campaigns, the well-known actor TA551 has been caught multiple times pushing Gozi infection to European citizen as follows:

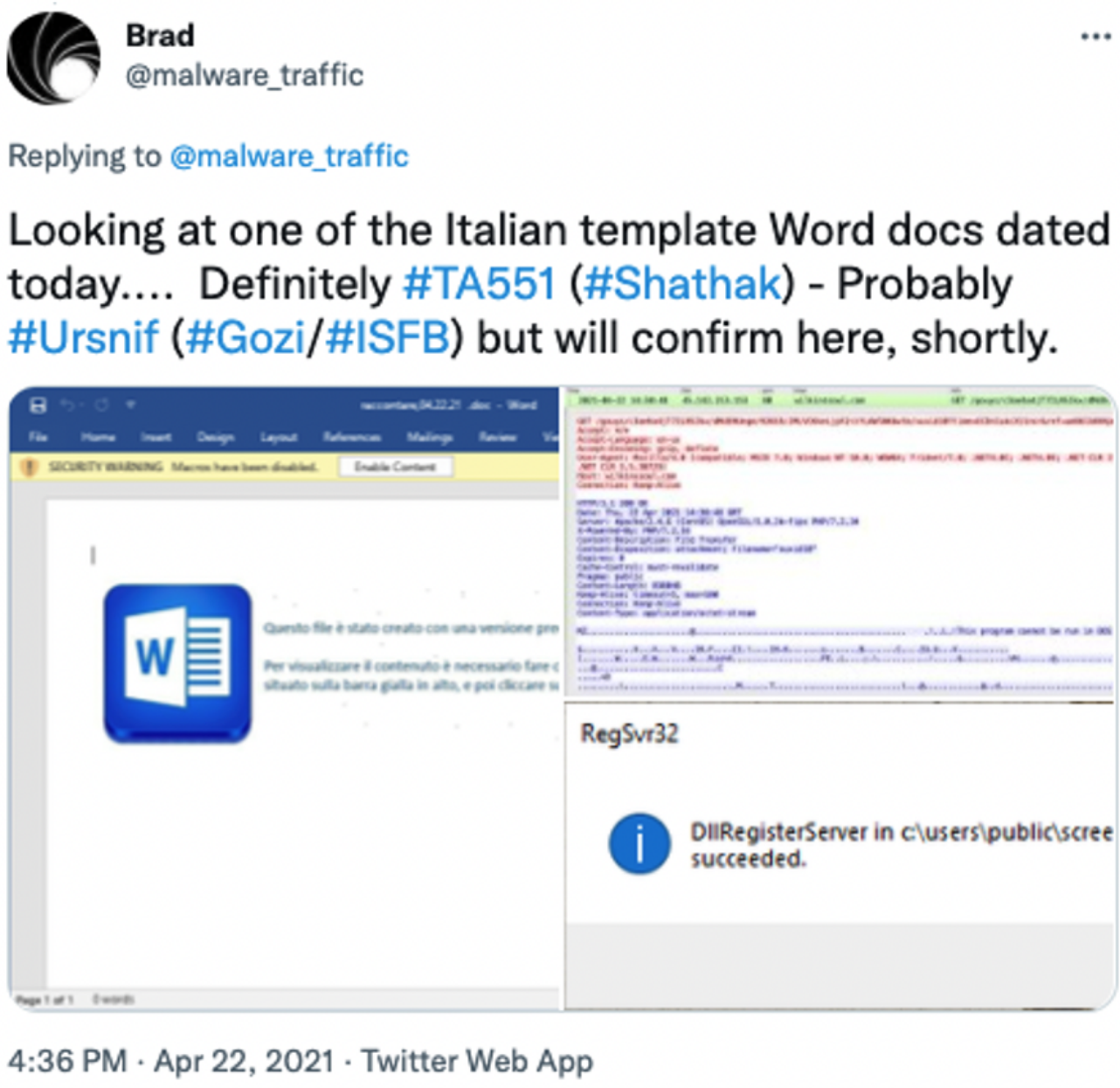


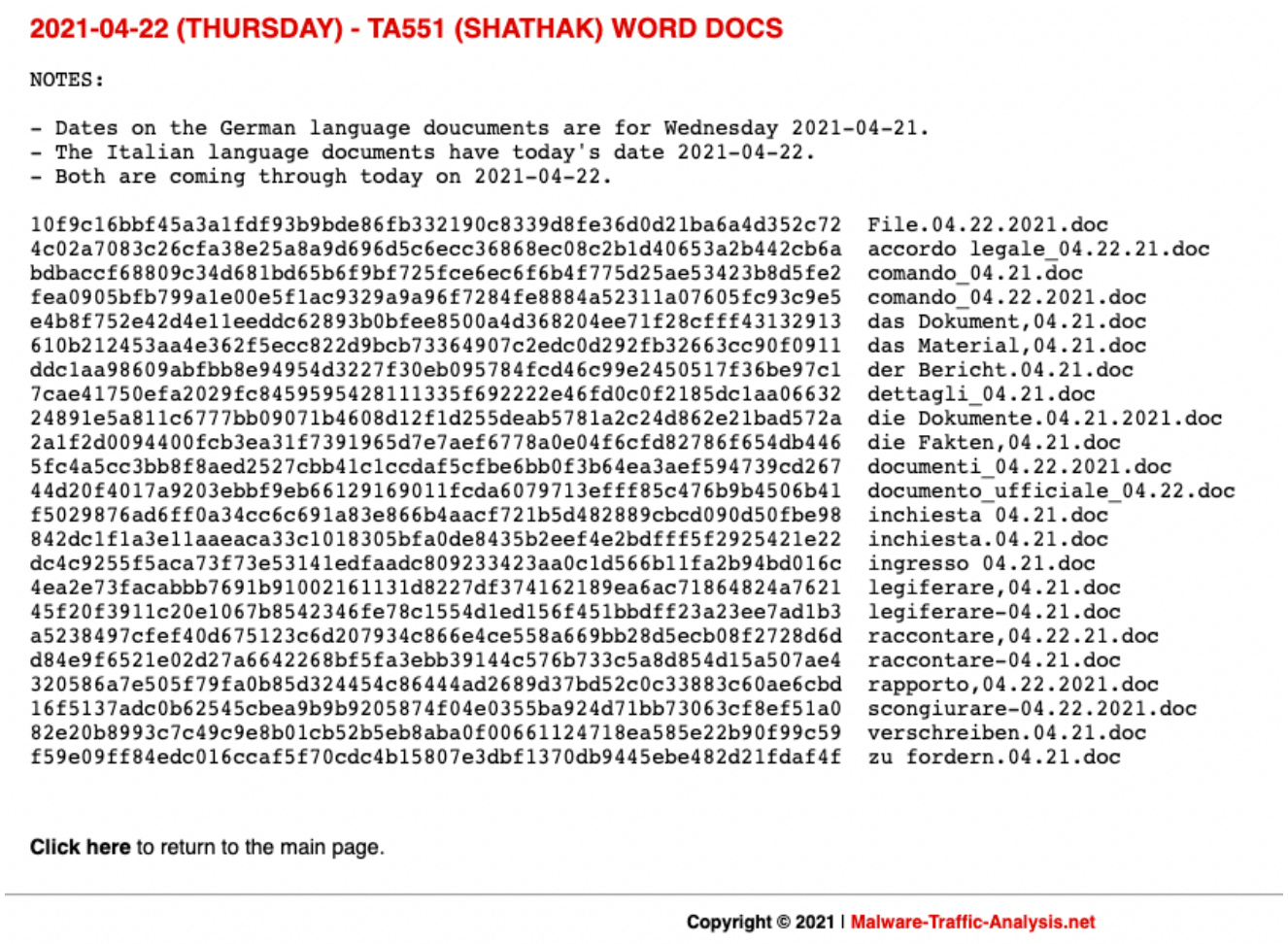
Figure 1 – TA551/Shathak [1] pushing Gozi in Europe (April 2020)

TA551 (also known as Shathak) is a sophisticated threat actor behind an email-based malware distribution campaign that often targets end-users on a global scale.Historically, TA551 has pushed different payloads belonging to multiple malware families such as

Gozi/Ursnif, IcedID, and Trickbot.

Even though TA551 often targets English-speaking victims, it has been caught targeting German, Italian and Japanese users as well by using geofencing techniques that make payloads not accessible to users in all regions and better protected against malware analysts and researchers.

The following list shows multiple maldocs that, last April, spread Gozi infection from a specific **TA551/Shathak** campaign focused on both German and Italian lures:



2021-04-22 (THURSDAY) - TA551 (SHATHAK) WORD DOCS

NOTES:

- Dates on the German language doucuments are for Wednesday 2021-04-21.
- The Italian language documents have today's date 2021-04-22.
- Both are coming through today on 2021-04-22.

10f9c16bbf45a3a1fdf93b9bde86fb332190c8339d8fe36d0d21ba6a4d352c72	File.04.22.2021.doc
4c02a7083c26cfa38e25a8a9d696d5c6ecc36868ec08c2b1d40653a2b442cb6a	accordo legale_04.22.21.doc
bdbaccf68809c34d681bd65b6f9bf725fce6ec6f6b4f775d25ae53423b8d5fe2	comando_04.21.doc
fea0905bfb799a1e00e5f1ac9329a9a96f7284fe8884a52311a07605fc93c9e5	comando_04.22.2021.doc
e4b8f752e42d4e11eeddc62893b0bfee8500a4d368204ee71f28cfff43132913	das Dokument,04.21.doc
610b212453aa4e362f5ecc822d9bcb73364907c2edc0d292fb32663cc90f0911	das Material,04.21.doc
ddc1aa98609abfbb8e94954d3227f30eb095784fcd46c99e2450517f36be97c1	der Bericht.04.21.doc
7cae41750efa2029fc84595954281111335f692222e46fd0c0f2185dc1aa06632	dettagli_04.21.doc
24891e5a811c6777bb09071b4608d12f1d255deab5781a2c24d862e21bad572a	die Dokumente.04.21.2021.doc
2a1f2d0094400fcb3ea31f7391965d7e7aef6778a0e04f6cfd82786f654db446	die Fakten,04.21.doc
5fc4a5cc3bb8f8aed2527cbb41c1ccdaf5cfbe6bb0f3b64ea3aef594739cd267	documenti_04.22.2021.doc
44d20f4017a9203ebbf9eb66129169011fcda6079713efff85c476b9b4506b41	documento_ufficiale_04.22.doc
f5029876ad6ff0a34cc6c691a83e866b4aacf721b5d482889cbcd090d50fbe98	inchiesta 04.21.doc
842dc1f1a3e11aaeaca33c1018305bfa0de8435b2eef4e2bdfff5f2925421e22	inchiesta.04.21.doc
dc4c9255f5aca73f73e53141edfaadc809233423aa0c1d566b11fa2b94bd016c	ingresso 04.21.doc
4ea2e73facabbb7691b91002161131d8227df374162189ea6ac71864824a7621	legiferare,04.21.doc
45f20f3911c20e1067b8542346fe78c1554d1ed156f451bbdff23a23ee7ad1b3	legiferare-04.21.doc
a5238497cfef40d675123c6d207934c866e4ce558a669bb28d5ecb08f2728d6d	raccontare,04.22.21.doc
d84e9f6521e02d27a6642268bf5fa3ebb39144c576b733c5a8d854d15a507ae4	raccontare-04.21.doc
320586a7e505f79fa0b85d324454c86444ad2689d37bd52c0c33883c60ae6cbd	rapporto,04.22.2021.doc
16f5137adc0b62545cbea9b9b9205874f04e0355ba924d71bb73063cf8ef51a0	scongiurare-04.22.2021.doc
82e20b8993c7c49c9e8b01cb52b5eb8aba0f00661124718ea585e22b90f99c59	verschreiben.04.21.doc
f59e09ff84edc016ccaf5f70cdc4b15807e3dbf1370db9445ebe482d21fdaf4f	zu fordern.04.21.doc

Click here to return to the main page.

Figure 2 - Gozi maldocs pushed[2] by TA551/Shathak

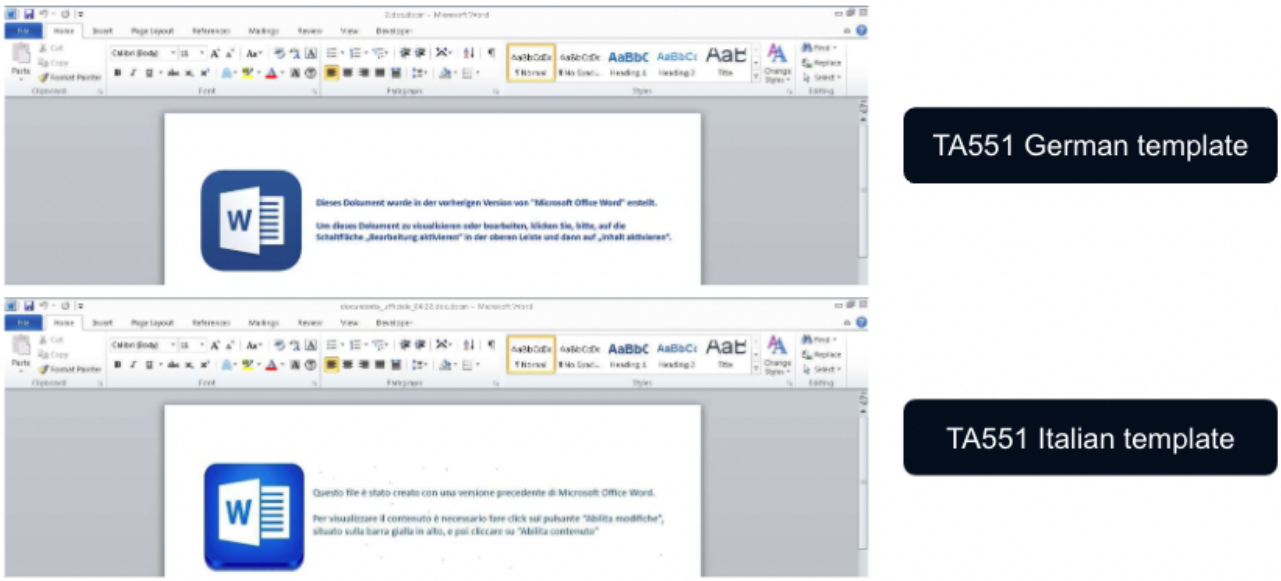


Figure 3 - TA551/Shathak German and Italian maldoc template

From a high-level perspective, atypical Gozi infection is characterized by the following steps:

1. The user opens the Word document attached to the received email and enables a malicious macro which triggers the download of a dynamic link library (*.dll*) from a remote server.
2. The downloaded *.dll* will be executed via *RegSvr32.exe* and unpack the core Gozi loader into memory, which is designed to manage all the interactions with the infected machine (e.g download/launch additional modules, update configuration, etc.).
3. Gozi uses Internet Explorer (IE) COM objects to communicate with its C2server; it creates a running instance through the *CoCreateInstance()* API.

The previous steps can be better visualized with the following “process graph view” which has been extracted from a recent Gozi malspam campaign:

Figure 4 - Gozi process tree view[3]
[1] Source: https://twitter.com/malware_traffic/status/1385241028924518410

[2] Source: https://www.malware-traffic-analysis.net/2021/04/22/index.html

[3] Source: https://app.any.run/tasks/5c628008-9f2c-49d1-8a94-aa878e46076f/

Exploring the “Gozi fraud core toolkit”

After a new victim has been successfully infected, the TA will deliver a specific configuration through the core Gozi loader, to instruct the bot on where to retrieve additional modules (also referred to as “second stages”), which typically includes:

- Web-inject kit(s) for the targeted applications
- hVNC module
- SOCKS module

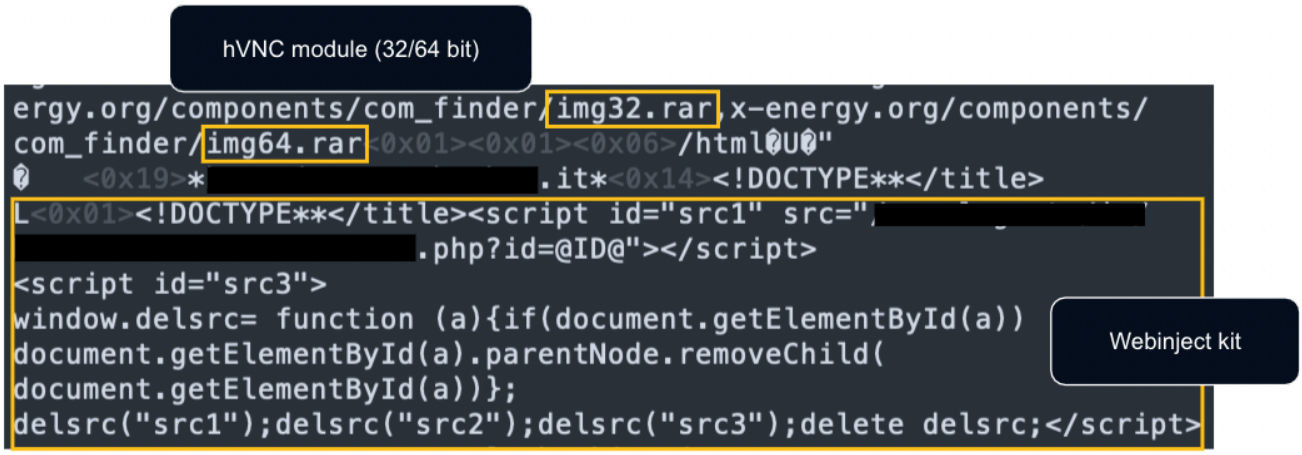


Figure 5 - Fraud-related additional modules (hVNC, Web-injects) from Gozi configuration

Web-injects are typically part of a MitB attack with the goal of modifying the content of a legitimate web page in real-time by performing API hooking. They are considered as an extension of the formgrabbing technique since they can intercept and manage web responses, altering the content before it is displayed on the browser (bypassing TLS protocol).

hVNC stands for **Hidden VNC** and means that the malware controls a machine without the victim's knowledge. Instead of controlling a victim's desktop, an attacker can open a hidden instance in the shape of a virtual desktop and control it invisibly behind the scenes, even as the unwitting victim continues using his or her computer.

SOCKS module enables TA to remotely connect to the infected bot, routing all the internet data through the same IP address as the victim, bypassing anti-fraud countermeasures such as network heuristics, etc.

We refer to those three modules as the **"Gozi fraud core toolkit"** since those are the modules used by high-skilled fraud operators for conducting banking fraud nowadays which typically happens only on the most valuable bots. This is an interesting pattern that we observed especially over the last year: from the initial malspam campaign to the actual banking fraud attempt, it can take weeks or even months, and *during this period operators enrich their botnet automatically via RATBANK*, exfiltrating in the background useful information, such as:

- Valid credentials
- Personal information and phone numbers(for further vishing attacks, if required)
- Account balances
- Recent bank transfers
- 2FA mechanism in use (e.g., SMS based, token based, QR codes)

RATBANK appears to be the main Web-inject kit used by this TA, which works as aRitB (**RAT in the Browser**), injecting a malware code into the browser memory by using MitB (Man in the Browser) techniques. In this way the victim's browser becomes a middle man

component for all monitored web sessions. These specific attacks are very hard to detect since the compromised user continues to act undisturbed in a normal-looking web session on his own device and with his own IP address, known to (and therefore not suspected by) the targeted bank.

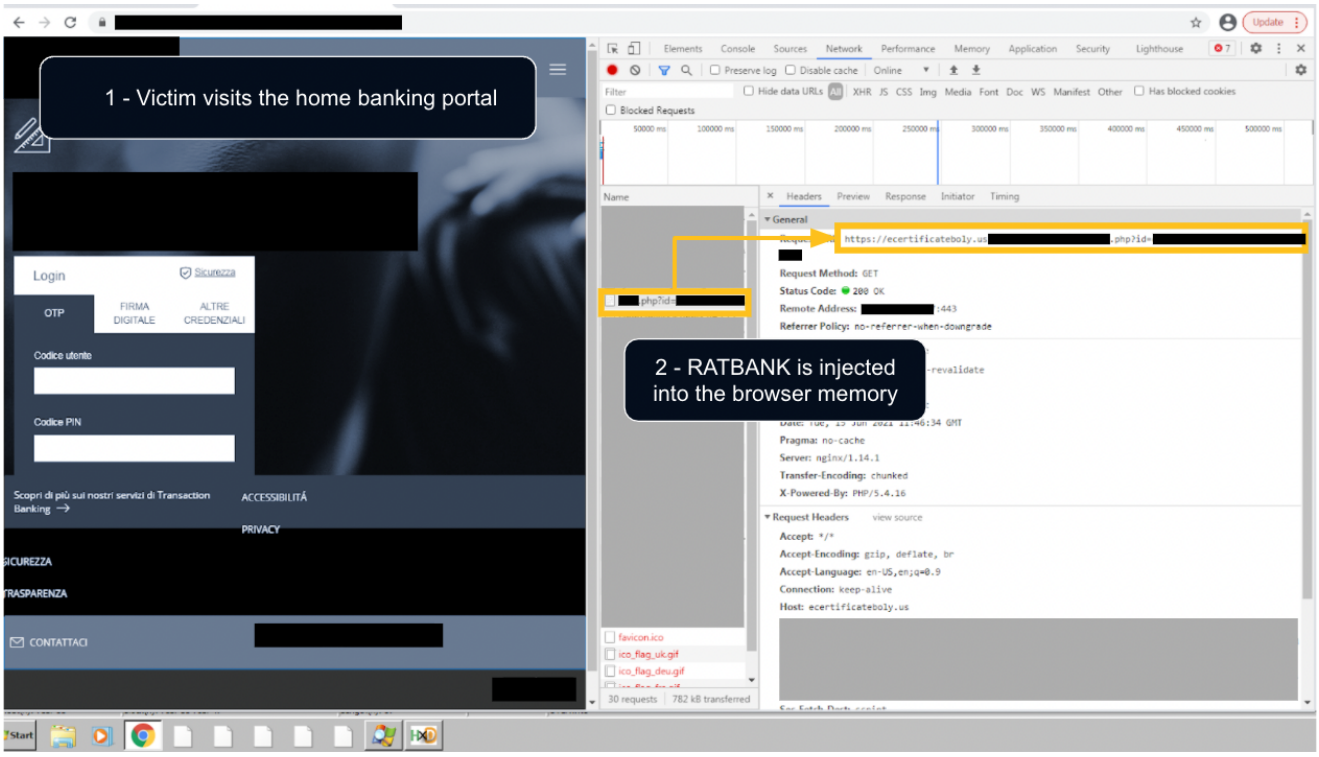


Figure 6 - RATBANK injected during the login process into a targeted website

During our analysis, we were also able to intercept “less-common” configurations where we noticed the usage of another Web-inject kit in addition to RATBANK, also known as **tables**, and well described in the following research published by FireEye in 2018.

Figure7 - Two different Web-inject kits found on recent Gozi campaigns

An example of a related sample that has been caught delivering this specific configuration has been provided in **Appendix 1: IOCs**.

Once extracted, we identified more than 50 different financial institutions targeted by this specific configuration, including both retail and corporate banking environments, as shown in the following table:

Country	Number of targets	Webinjects kit (family)	Additional modules
Italy	39	RATBANK (delsrc)	SOCKS-5, hVNC
Germany	12	tables	NA

Appendix1: IOCs

2ef16b02901c1bdd819ddf1aa96f3994 (Gozi maldoc)

0b26191e482cf7c321efeb8d2569caac (Gozi loader)

x-energy[.org/components/com_finder/img32.rar(hVNC 32 bit)

x-energy[.org/components/com_finder/img64.rar(hVNC 64 bit)

ecertificateboly[.us (RATBANK C2)