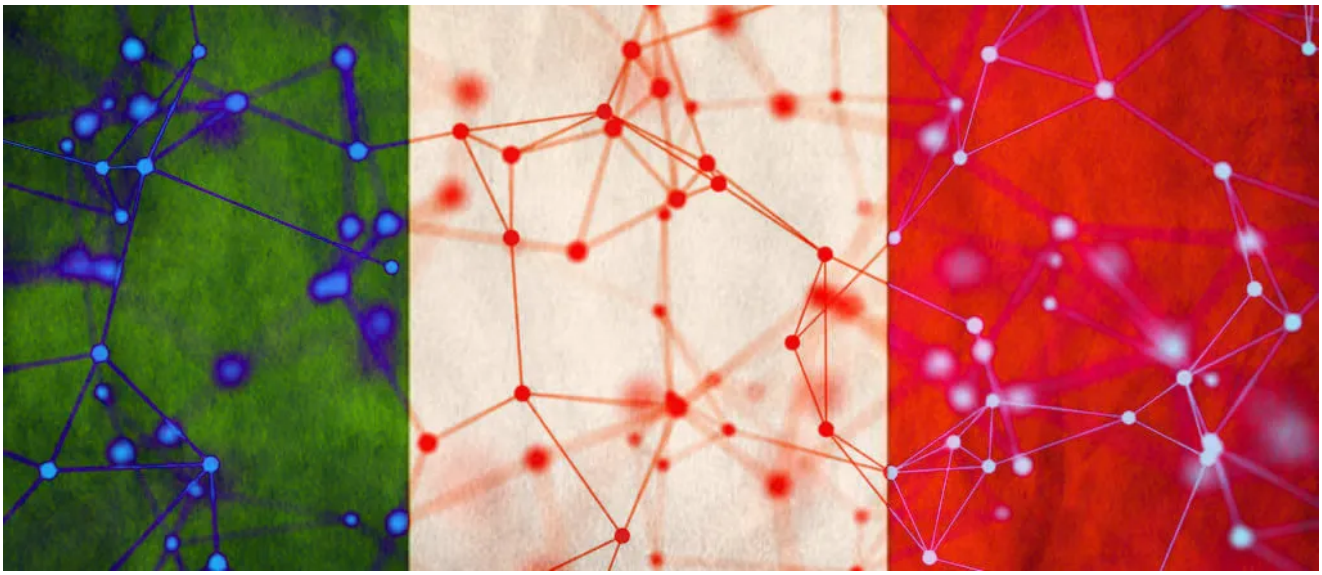
Connecting the dots inside the Italian APT Landscape

yoroi.company/research/connecting-the-dots-inside-the-italian-apt-landscape/

February 4, 2021



02/04/2021

Introduction

The news of the hack of one of the major strategic Italian companies circulated in the first half of December 2020 shocked a huge part of the national security community: Leonardo SpA (formerly Finmeccanica) runs critical services and projects directly related to the Italian defense industry and military corps.

On 5th December 2020, the Italian police (CNAIPIC) published a press statement revealing the Aerostructures and Aircraft division has been hacked for a long time. The malicious APT presence was dated back to 2015 and lasted for about two years inside the Leonardo division.

Only few details have been disclosed by the Italian police, but enough to enable the security community to expand this case and unveil technical details about the tools used by the silent intruders. For instance, recently Reaqta hunted for malware samples related to the intrusion and identified a couple of samples closely matching the CNAIPIC press statement.

We have been looking at this case since December 2020 and tracked this new actor as TH-261. But in the initial weeks of 2021 we noticed something unattended: a set of similarities on recent ongoing attacks made us really suspicious about the nature and evolution of this threat.

Technical Analysis

The starting point of our research was Italian police press statement. Here the only technical detail provided by the policy was a singular network indicator: “www.fujinama.altervista[.org”.

Third party analysis published on 8th of January 2021 pointed out a couple of samples related to the case, but no hash was provided. So we methodologically started to hunt for the samples they were describing in the article, especially for the named “cftmon.exe”, that one specifically dated back on 2015, the initial date of the intrusion reconstructed by the local law enforcement agency.

The “Fujinama” Samples Hunt

Through our threat intelligence investigations, we were able find a sample candidate using the Yara Rule and available technical indicators. We ended up to this candidate: “3c4444c8339f2b4c04931a379daf9d041854b168e45f949515f90b124821d626”.

Figure 1: VirusTotal statistics of the suspect sample

The sample of the above screen was named “cftmon”, the same name reported on both CNAIPIC and Reaqta articles. At this point, we investigate other static attributes to find out as many elements as possible to confirm we were looking at the specific sample related to the Leonardo’s intrusion.

Figure 2: Static information about the sample

The malware has been compiled the day 2015-07-14, the same timestamp reported in the Reaqta report, so this thing could indicate two things:

- the sample is actually compiled in that date, so the threat actor prepared the attack with high precision and detail
- the sample has a fake compilation stamp and it has been compiled just before the intrusion

As reported in other technical reports, the malware code is quite particular and does not have any type of code-protection systems. Also the network traffic to the C2 has no sophisticate encryption or random looking encoding.

Figure 3: Tracing of some critical API Windows calls

As reported in the official bulletins, the malware massively uses the Windows API calls “InternetConnectA” and “HttpOpenRequestW” and there is the correspondence of the C2 emerged: “fujinama.altervista[.org”, as reported by Italian Police.

Moreover, we individuated the three basic functionalities: take screenshots, capture keystrokes, execute commands coming from the C2.

Anyway, considering the absence of any stomping and the whole technical, we are quite confident we are looking at the malicious code written by this mysterious APT.

The Second Sample from the Past: “Igfxtray”

During the monitoring of this threat, we focused also onto the research of related samples, in order to have the widest view of the topic.

In particular, we found another related sample of the “Fujinama” one. It has been reported also inside the report of Reaqta, where they carry out the decision that the sample is allegedly the same, but it belongs to another campaign.

Figure 4: Static information about the sample

In this case, the code is perfectly compatible with the Fujinama sample. We have exactly the same pieces of code evidence for the keylogging routine:

Figure 5: Evidence of the similarity between Fujinama sample (on the left) and igfxtray sample (on the right)

However there are also some differences between the two samples:

- The strings of the Igfxtray malware are English-speaking and other ones are base64 encoded
- The C2 is hosted on “webhostapp” ISP instead of “Altervista”

However, we have also a set of similarities to be analyzed:

Figure 6: Comparison of the strings between Fujinama sample (on the left) and igfxtray (on the right)

On the left there is a piece of the extracted strings of the “Fujinama” and on the right “igfxtray”. We separated the relevant strings into two colors: the red indicates the correspondence between the italian configuration strings of “Fujinama” sample and the English-Base64 encoded of “igfxtray” one; The blue color indicates the difference of the provider of the C2.

Ultimately, the compatibility of the sample is no doubt confirmed.

Cashback 2021

A big surprise happened when we analyzed a malware reported by CERT-AGID, the CERT of the Italian Agency for Digitisation. This time, the malware was spread as malspam mail with a current theme in Italy: “Cashback di Stato”, a recent governmental initiative to incentive digital payments leveraging cashback mechanisms.

Figure 7: View of the malicious mail (CREDITS CERT AGID)

The downloaded file is not a PDF file, but it is actually an executable compiled in VB6.

Figure 5: Static Information about the sample

The sample compilation stamp is 2021-01-05, just when the malware has spread in the wild and its main communication is FTP, all communication with the C2 in fact rely on this protocol.

The “Cashback di Stato” sample adopts a multistage infection chain. As reported by the Italian CERT, the keylogger component is downloaded in a second moment from the FTP server.

Figure 8: Keylogging routine of the component of “Cashback di Stato” Sample

The “Cashback di Stato” version uses the “SetWindowsHookEx” API call to perform keylogging, a technique a bit more evolved than the Fijinama’s “GetAsyncKeyState”.

Figure 9: Keylogging routine of the component of “Cashback di Stato” Sample

Besides these differences, we noticed some potential inner connections deeper with Leonardo's samples which made room for profound questions we will deepen in the following sections.

A Common Matrix?

The first aspect we notice wes in the code itself. The absence of any self-protection mechanism is very very uncommon nowadays: the usage of packers, protectors and encryptors are recurrent practice in almost all cyber criminal environments. Noticing no protection layers is something characteristic of custom code samples, many times developed by groups or actors with software developing skill sets in the house, able to craft their weapons from scratch rather than leveraging off-the shelf tools.

The “Fujinama” samples show no trace of complex frameworks, all the code is straightforward and seems hand made directly in VB6. The structure itself is really basic: the malware application logic is coded and triggered within a hidden form and a few timers.

The same structure and the same consideration could be formulated even for the 2021’s Cashback samples.

Figure 10: Left. “Fujinama” sample 2015 - Right. “Cashback” sample 2021

We had a similar impression like the one we had dissecting these samples when looking at the command and control infrastructure: the Italian web blogging platform services “Altervista” was also used in the 2015 sample and the 2021 one. Even in this case, the use

of this platform is not so common in mainstream attack campaigns.

Another impression we had reviewing these samples regards the rate of changes of such samples. In fact, despite some changes in the code and in the modularity suggest we are looking at an evolving piece of code, but this evolution maintains some constants, for instance in the building environment, in the naming schema and malware application dynamics itself.

The following table synthesize all the TTPs emerged and the similarities between all of the three samples, trying to clarify the potential connection among them:

TTPs	**Sample "Fujinama" 2015**	**Sample"Cashback" 2021**	**Sample"lgfxtray" 2017**
VB6 Compiler [T1059.005]	YES (MS Visual Basic 5.0-6.0 EXE)	YES (MS Visual Basic 5.0-6.0 EXE)	YES (MS Visual Basic 5.0-6.0 EXE)
File name Masquerading [T1036]	cftmon.exe	sysC32cmd.exe	lgfxtray.exe
Lack of Obfuscation [T1001]	YES	YES	YES
PE Information [T1036.003]	Italian	Italian	Italian
Persistence [T1547.001]	NO	YES	NO
C2	Altervista	Altervista	webhostapp
Modular Infection	NO	YES	NO
C2 Communication Protocol [T1071]	HTTP [T1071.001]	FTP [T1071.002]	HTTP [T1071.001]
Keylogger [T1056.001]	YES(GetAsyncKeyState)	YES (SetWindowsHookEx)	YES (GetAsyncKeyState)
Take screenshot [T1113]	YES	YES	YES

Download File [T1105]	NO	YES	NO
Execute Command [T1059.003]	YES	YES	YES
Upload File [TA0010]	YES	YES	YES

Table 1: Synthetic table of the TTPs among the three samples

Conclusion

Considering we might look at an evolving codebase among 6 years, we think the TTPs of the actor behind it are somehow compatible with a moderate confidence.

But we need to make a distinction, at the moment we don't have any clues about the reason for these similarities and the hypothesis may be several and really different from each one: for instance we may be looking to an evolving code base of a single actor, or to two different independent codebases of people with - or without - any kind of connection, or also a code base inherited and evolved by an additional actor.

Current contextual elements are not enough to formulate a definitive statement, but as malware analysts we are noticing a potential connection crossing the years from the technical and methodological point of view.

Indicators of Compromise

- Dropurl:
  - https://bit].ly/3naIYxK
  - http://www].studiocpv].it/dealerfree/ModuloCitrixTelecomDaCompilare%5D.pdf.zip
- C2:
  - fujinama[.altervista[.org
  - failaspesa[.altervista[.org
  - ffaadd332211.altervista[.org
  - xhdyeggeeefeew[.000webhostapp[.com
- Data Exfiltration:
  - keylogging
  - screenshots
- Persistence:
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- Hash:
  - 3c4444c8339f2b4c04931a379daf9d041854b168e45f949515f90b124821d626
  - 00092c4212f31387983e7e4b03d4f8362e58a43861d8073e71d20e95addeb8a2
  - 646dbe5de074ba301f2e2eccd9ccbb9b58c86dafc69cbf00ecd7fe9365f8f1f2
  - 500631db833b2729f784e233225621ddff411d7da49bd82cfd51a49b9600438f

This blog post was authored by Luigi Martire and Luca Mella