Dancing through a multi-language phishing campaign in Europe)

Published: 2025-06-16 · Archived: 2026-04-06 00:26:28 UTC

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.

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.

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.

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.

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.
