Multilayered Email Attack: How a PDF Invoice and Geo-Fencing Led to RAT Malware

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

May 8, 2025

Article Contents

By Ran Mizrahi | May 08, 2025
Affected platforms: Windows (primarily), Linux & macOS (if Java is installed)
Impacted parties: Users on systems with Java Runtime Environment (JRE) installed
Impact: Grants remote access to attackers, enabling them to execute commands, log keystrokes, access files, activate webcam/microphone, and fully control the infected system
Severity level: High

The FortiMail IR team recently uncovered a new email campaign distributing a Remote Access Trojan (RAT) using multiple evasion techniques to target organizations in Spain, Italy, and Portugal. The campaign leverages the **serviciodecorreo** email service provider, which is configured as an authorized sender for various domains and successfully passes SPF validation.

[2025 Global Threat Landscape Report]

[Use this report to understand the latest attacker tactics, assess your exposure, and prioritize action before the next exploit hits your environment.]

Additionally, it employs advanced evasion strategies, including the abuse of two file-sharing platforms, geolocation filtering, and Ngrok to create secure, obfuscated tunnels. These tactics further complicate detection and effectively mask the attack's true origin, ultimately facilitating the distribution of RATty malware.

This campaign highlights the increasing sophistication of malware attack methodologies, leveraging the legitimate functionalities of remote administration tools for malicious purposes.

The Infection Chain—The PDF and HTML files vary in each email from this campaign, but the malware campaign pattern remains the same.

Overview

The Email

The attacker exploits serviciodecorreo.es, a legitimate Spanish email service authorized to send emails on behalf of various domains. Since the SPF record for these domains designates serviciodecorreo.es as a valid sender, the malicious emails successfully pass SPF checks, creating the illusion of legitimacy.

Consequently, these emails are more likely to bypass security filters, making it easier for them to be accepted by the recipient's mail server. This increases the likelihood of a successful attack, as the deceptive nature of the emails goes unnoticed.

The sender attaches a PDF file asking the recipient to review two new invoices. This makes the recipient believe this email is important, which may influence them to check the attached files and details. This is basic social engineering to tempt the recipient into acting with less caution and under pressure.

The PDF File Attachment

The attached PDF file displays a message indicating that the file is not being shown correctly and instructs the recipient to click a button to download the file locally. The button contains a Dropbox (file-sharing platform) link to download an HTML file named "Fattura" (Translation: “Invoice”). The choice of this file name plays into the social engineering tactic, aiming to persuade the recipient to click and view the information, ultimately leading to the delivery of a malicious payload.

The HTML File

The HTML file contains a basic validation step with an "I am not a robot" prompt.

After completing the verification, a simple HTML page is displayed with instructions to click a button to view the document. The button redirects the user to a link generated by Ngrok, a tunneling tool that allows users to expose local servers to the internet through secure, temporary URLs.

Translation: To view this document, click on the download button below

The Response URL

The following URL abuses the MediaFire file-sharing platform by automatically downloading the JAR file (FA-43-03-2025.jar) when accessed.

hxxps://download1528[.]mediafire[.]com/35ougpab4uhgHgb3Pmqh8niQ0hzS9b-TtTro5oPV5iUIULfNckqgXvjXQ6aTp-NF-k8EflSnFWC--Ffh4aX1NlYrzaPzgFlyxHVe0fKkLE1p3u5cntfU25orm92QdoQmXE9-gyl4hRgSYpaNcd3o12kJnPRbJhD3aqbl1Qx3vqbUtk8/ayp0ikmndrdseht/FA-43-03-2025.jar

Using a legitimate file-sharing service helps attackers further evade detection, as security filters are less likely to flag downloads from trusted platforms. This tactic makes detection and blocking more difficult for security companies since automated analysis systems, sandbox environments, and security researchers often inspect URLs from locations outside the targeted region. By selectively delivering the malware only to specific geolocations, attackers reduce the risk of early detection and increase the likelihood of a successful attack.

Below, we can see how this evasion leads to a Google Drive link containing a legitimate file:

Bypassing Email Security Filters with Ngrok

Ngrok is primarily used to test webhooks, develop locally hosted applications, and bypass NAT/firewall restrictions. However, as in this case, threat actors can misuse Ngrok to create dynamic, hard-to-detect phishing links that evade traditional security filters.

Attackers use Ngrok to dynamically generate URLs that help them evade email security filtering mechanisms. One key technique they employ is geo-based cloaking, which serves different content depending on the user's location.

In this case, when users access the Ngrok-generated URL from any country except Italy, they are redirected to a seemingly legitimate Google Drive document, making it harder for email security solutions to classify the URL as malicious.

The attached fake invoice is identical for all targeted organizations. It is a purported invoice from the global health organization Medinova Health Group, and it has been designed to bypass most email security mechanisms.

The seemingly legitimate invoice, shared via Google Drive, is unlikely to raise suspicion during email scanning and is intended to slip past email security engines without triggering any suspicion of malicious intent.

However, when the request originates from Italy, the URL changes entirely, leading to downloading a malicious JAR file.

Most email security systems perform email analysis from generic or cloud-based environments, not tied to a specific geographic location. As a result, when these systems access the embedded URL, they are redirected to a harmless decoy page rather than the

malicious file. This geofencing technique ensures that only users in the targeted regions -in this case, Italy - can reach the actual malicious content.

The JAR File

The .jar file contains a type of Ratty malware. The file name, "FA-43-03-2025.jar," resembles a neutral reference number. While such naming conventions are not unusual, this name was probably specifically chosen to prompt the end user to click and execute the file, assuming it is related to a payment document, thus encouraging hasty and careless action.

Ratty RAT: A Java-Based Remote Access Trojan

Ratty RAT is a Java-based Remote Access Trojan (RAT) typically distributed as a .jar file. Since Java is a cross-platform language, Ratty RAT can run on various operating systems as long as the Java Runtime Environment (JRE) is installed.

Threat actors use Ratty RAT to execute remote commands, log keystrokes, capture screenshots, and steal sensitive data, often as part of email-based social engineering campaigns with malicious attachments.

While it is commonly delivered as a .jar file, attackers may also package it as an MSI (Microsoft Installer) file to increase its legitimacy and evade detection. By bundling the RAT inside an MSI, they can disguise it as legitimate software or an update, making it easier to trick users into executing the malware.

What Makes This Email Campaign Particularly Sophisticated

What makes this email campaign particularly sophisticated is its combination of multiple tactics designed to evade detection and exploit trusted platforms. Its multi-layered strategy uses social engineering techniques to manipulate recipients into clicking on malicious links.

The initial email, disguised as an invoice and sent from a sender who appears legitimate, serves as the entry point. The attacker clearly conducted prior research, identifying which domains allow the use of the specific email service for sending emails, thereby bypassing some critical security measures.

The attackers also abuse file-sharing platforms like Dropbox and MediaFire to deliver their malicious payload while leveraging geolocation techniques to tailor the attack based on the recipient's location. Additionally, the use of Ngrok complicates detection by creating secure, obfuscated tunnels that mask the true origin of the attack.

Together, these elements create a highly advanced and effective method of distributing malware, including RATty (Remote Access Trojan), which is challenging for traditional security systems to detect and block.

Fortinet Protections

Fortinet provides multiple layers of protection against this threat. FortiGate and FortiClient detect and block the malicious JAR file using the latest antivirus (AV) signatures. Customers are advised to ensure their systems are regularly updated with the most recent AV database.

Fortinet customers are also already protected from this campaign with FortiGuard's AntiSPAM, Web Filtering, IPS, and AntiVirus services. FortiMail recognizes the phishing email as "virus detected," and the FortiMail Content Disarm and Reconstruction (CDR) function automatically detects and mitigates this threat.

In addition, FortiSandbox, embedded in Fortinet's FortiMail, web filtering, and antivirus solutions, provides real-time anti-phishing protection against known and unknown phishing attempts.

Perception Point Email Security, now part of Fortinet FortiMail, also proactively detects and blocks emails containing malicious geo-fenced URLs used to deliver malware and phishing content and the RATty JAR file itself. This is achieved through advanced dynamic scanning and static analysis techniques.

Combined, these detection capabilities ensure threats are mitigated during delivery, through malicious emails and links, and upon download, delivering end-to-end protection across the entire attack chain.

In addition to technical defenses, organizations should adopt Security Awareness Training (SATs) programs and conduct regular phishing simulations. Fortinet's free NSE training: NSE 1 – Information Security Awareness module on Internet threats is designed to help end users learn how to identify and protect themselves from phishing attacks.

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks. By empowering users to recognize and respond to suspicious content, these initiatives significantly lower the risk of successful phishing or malware attacks.

If you believe this or any other cybersecurity threat has impacted your organization, please contact our Global FortiGuard Incident Response Team.

You can also sign up to receive future alerts to stay informed of new and emerging threats.

IOCs

IPs

143.47.53.106
130.51.20.126
199.232.214.172
199.232.210.172

Domains:

jw8ndw9ev[.]localto[.]net
l5ugb6qxh[.]localto[.]net

Hash (sha256):

a1c2861a68b2a4d62b6fbfc7534f498cefe5f92f720466d24ae1b66ebc9f5731
d20d14792c91107f53318ff7df83b9cd98acd3c394959a74e72278682822b600
9184ff2cdd05fcaf111db23123479c845b2ece2fedccc2524b2de592f9980876
5f897fec78e2fd812eb3bc451222e64480a9d5bc97b746cc0468698a63470880
6153c80b17cb990caad1d80cac72c867d4ecfa1a84b7ab286b7373cd4168794e
469b8911fd1ae2ded8532a50e9e66b8d54820c18ccdba49d7a38850d6af54475
af8b6ac45918bc87d2a164fae888dab6e623327cba7c2409e4d0ef1dde8d1793