TA547 Targets German Organizations: Rhadamanthys Stealer | Proofpoint US

By Tommy Madjar, Selena Larson and the Proofpoint Threat Research Team

Published: 2024-04-03 · Archived: 2026-04-05 13:14:52 UTC

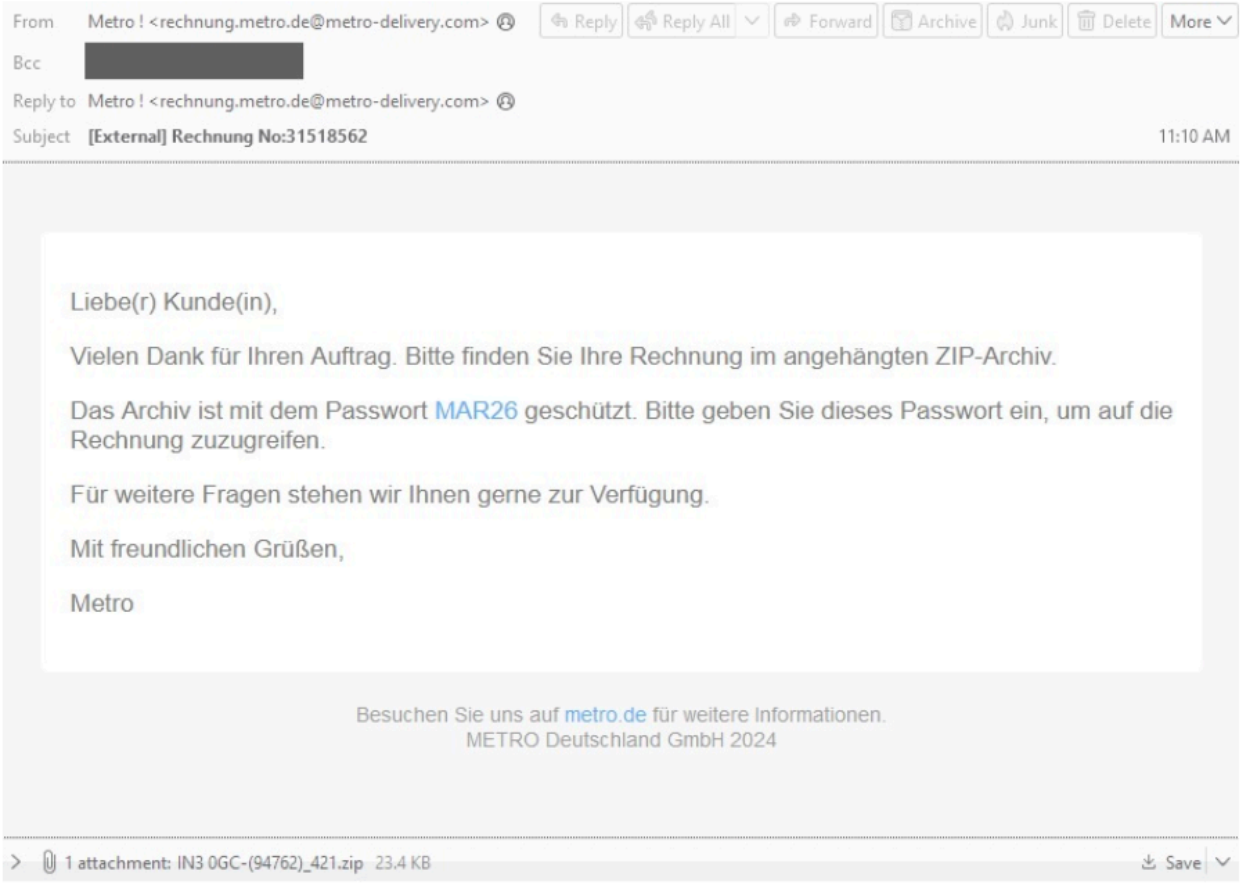
April 10, 2024

What happened

Proofpoint identified TA547 targeting German organizations with an email campaign delivering Rhadamanthys malware. This is the first time researchers observed TA547 use Rhadamanthys, an information stealer that is used by multiple cybercriminal threat actors. Additionally, the actor appeared to use a PowerShell script that researchers suspect was generated by large language model (LLM) such as ChatGPT, Gemini, CoPilot, etc.

Emails sent from the threat actor impersonated the German retail company Metro purporting to relate to invoices.

From: Metro ! <rechnung.metro.de@metro-delivery[.]com>
Subject: Rechnung No:31518562
Attachment: in3 0gc-(94762)_6563.zip



Example TA547 email impersonating the German retail company Metro.

The emails targeted dozens of organizations across various industries in Germany. Messages contained a password-protected ZIP file (password: MAR26) containing an LNK file. When the LNK file was executed, it triggered PowerShell to run a remote PowerShell script. This PowerShell script decoded the Base64-encoded Rhadamanthys executable file stored in a variable and loaded it as an assembly into memory and then executed the entry point of the assembly. This essentially executed the malicious code in memory without writing it to disk.

Notably, when deobfuscated, the second PowerShell script that was used to load Rhadamanthys contained interesting characteristics not commonly observed in code used by threat actors (or legitimate programmers). Specifically, the PowerShell script included a pound sign followed by grammatically correct and hyper specific comments above each component of the script. This is a typical output of LLM-generated coding content, and suggests TA547 used some type of LLM-enabled tool to write (or rewrite) the PowerShell, or copied the script from another source that had used it.

```
# Assuming the Base64 string is directly encoded without UTF-16LE
$base64EncodedExe = "[base64]" # Replace with your actual Base64 string

# Directly convert from Base64 to bytes
$decodedBytes = [System.Convert]::FromBase64String($base64EncodedExe)

# Use the correct overload of Assembly.Load that accepts a byte array
$assembly = [System.Reflection.Assembly]::Load($decodedBytes)

# Invoke the assembly's entry point. This assumes no arguments are needed for the entry method.
if ($assembly.EntryPoint -ne $null -and $assembly.EntryPoint.GetParameters().Count -eq 0) {
    $assembly.EntryPoint.Invoke($null, $null)
} elseif ($assembly.EntryPoint -ne $null) {
    $assembly.EntryPoint.Invoke($null, [object[]] @([string[]] @()))
} else {
    Write-Host "Assembly entry point not found or cannot be invoked directly."
}
```

Example of PowerShell suspected to be written by an LLM and used in a TA547 attack chain.

While it is difficult to confirm whether malicious content is created via LLMs – from malware scripts to social engineering lures – there are characteristics of such content that points to machine-generated rather than human-generated information. Regardless of whether it is human or machine-generated, the defense against such threats remains the same.

Attribution

TA547 is a financially motivated cybercriminal threat considered to be an initial access broker (IAB) that targets various geographic regions. Since 2023, TA547 typically delivers NetSupport RAT but has occasionally delivered other payloads including StealC and Lumma Stealer (information stealers with similar functionality to Rhadamanthys). They appeared to favor zipped JavaScript attachments as initial delivery payloads in 2023, but the actor switched to compressed LNKs in early March 2024. In addition to campaigns in Germany, other recent geographic targeting includes organizations in Spain, Switzerland, Austria, and the U.S.

Why it matters

This campaign represents an example of some technique shifts from TA547 including the use of compressed LNKs and previously unobserved Rhadamanthys stealer. It also provides insight into how threat actors are leveraging likely LLM-generated content in malware campaigns.

LLMs can assist threat actors in understanding more sophisticated attack chains used by other threat actors, enabling them to repurpose these techniques once they understand the functionality. Like LLM-generated social engineering lures, threat actors may incorporate these resources into an overall campaign. It is important to note, however, that while TA547 incorporated suspected LLM-generated content into the overall attack chain, it did not change the functionality or the efficacy of the malware or change the way security tools defended against it. In this case, the potentially LLM-generated code was a script which assisted in delivering a malware payload but was not observed to alter the payload itself. Because many of Proofpoint's detection mechanisms are behavior-based, the origin of any given malicious software will not impact our ability to detect malicious actions taken on a host. In the same way LLM-generated phishing emails to conduct business email compromise (BEC) use the same characteristics of human-generated content and are caught by automated detections, malware or scripts that incorporate machine-generated code will still run the same way in a sandbox (or on a host), triggering the same automated defenses.

Example Emerging Threats signatures

2854802 ETPRO MALWARE Suspected Rhadamanthys Related SSL Cert

2853002 ETPRO MALWARE Rhadamanthys Stealer - Data Exfil

2853001 ETPRO MALWARE Rhadamanthys Stealer - Payload Response

2043202 ET MALWARE Rhadamanthys Stealer - Payload Download Request

Indicators of compromise

Indicator	Description	First Seen
hxxps://bolibachan[.]com/g[.]txt	PowerShell Payload	26 March 2024
indscpm[.]xyz	Rhadamanthys C2	26 March 2024
94[.]131[.]104[.]223:443	Rhadamanthys C2	26 March 2024

Subscribe to the Proofpoint Blog
