Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

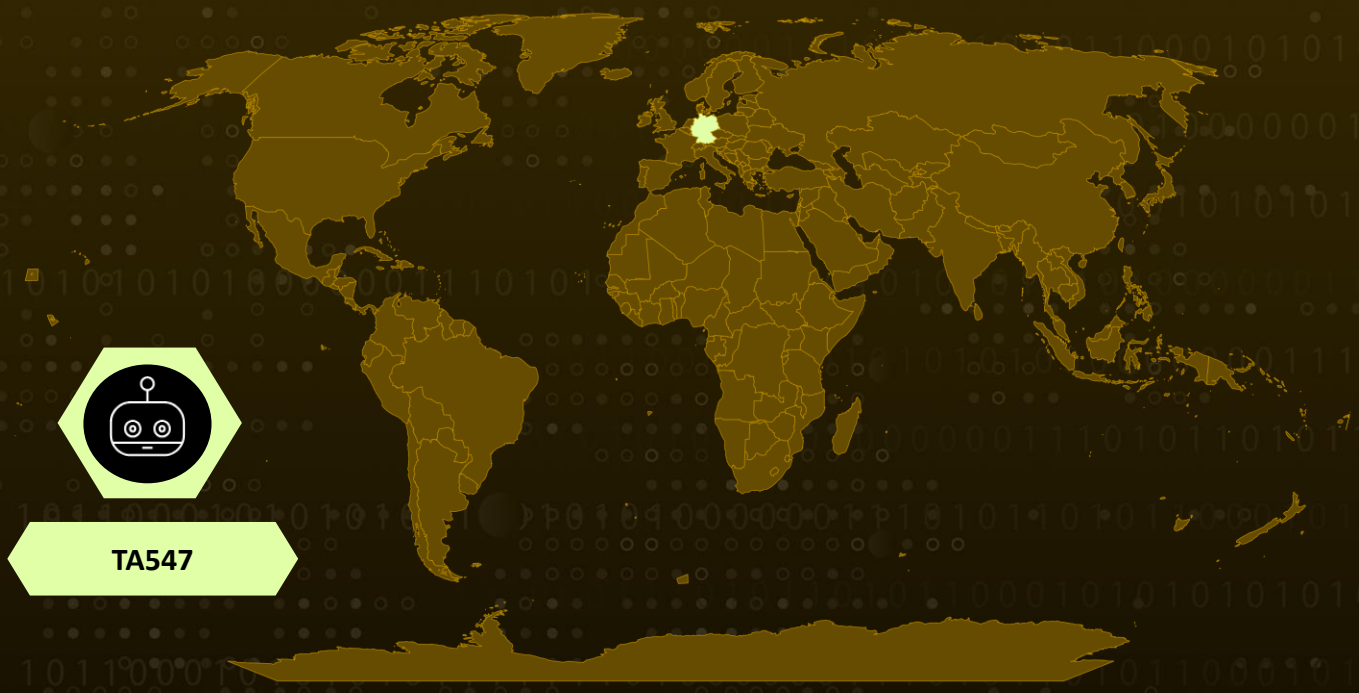
TA547 Malware Campaign Hits German Businesses

Date of Publication	Admiralty Code	TA Number
April 12, 2024	A1	TA2024143

Summary

Attack Began: March, 2024
Targeted Countries: Germany
Malware: Rhadamanthys
Threat Actor: TA547 (aka Scully Spider)
Affected Platform: Windows
Attack: TA547, a financially motivated cybercriminal group, targeted German organizations with invoice-themed phishing emails. These emails contained malicious LNKs that downloaded Rhadamanthys malware, an information stealer. Researchers suspect the PowerShell script used in the attack might be generated by a large language model, highlighting a concerning evolution in cybercrime tactics

Attack Regions



Attack Details

#1 TA547, a financially motivated cybercriminal group with a history of targeting various regions, has set its sights on German organizations. This recent attack campaign employed a new weapon in their arsenal, the Rhadamanthys information stealer. This marks the first time TA547 has employed Rhadamanthys, a data-stealing malware used by multiple other cybercriminals.

#2 Previously, TA547 relied on compressed JavaScript attachments to gain initial access to victim systems. However, in this campaign, they shifted to compressed LNK files, most likely shortcuts disguised as legitimate documents.

#3 The attack unfolded through phishing emails that appeared to originate from Metro, a well-known German retail giant. These emails mimicked invoice-related communications, a common tactic used to lure unsuspecting victims into clicking malicious attachments. The emails contained password-protected ZIP files. Once a recipient opened the ZIP and entered the provided password, an LNK file would be triggered. This LNK file, in turn, would initiate a remote PowerShell script.

#4 Security researchers suspect that this PowerShell script might have been generated by a large language model (LLM), a powerful AI tool capable of producing human-quality text. The script's characteristics, such as grammatically correct and highly specific comments preceding each component, hinted at this possibility. This would mark a worrying trend, suggesting that cybercriminals are exploring ways to leverage AI for more sophisticated attacks.

#5 The PowerShell script then played a crucial role in the infection process. It downloaded the actual payload, the Rhadamanthys malware directly into the system's memory. This technique, known as a fileless attack, bypasses traditional disk-based detection methods, making it more challenging to identify and prevent.

#6 This TA547 campaign highlights the evolving landscape of cyber threats. The group's shift in tactics, the potential use of AI-generated scripts, and the deployment of a new information-stealing malware demonstrate the constant need for heightened vigilance and robust cybersecurity measures.

Recommendations

Update Security Measures: Ensure that all security measures, including antivirus, firewalls, and intrusion detection systems, are up to date. Regularly update security patches and definitions to detect and block known threats, including Rhadamanthys.

Email Filtering and Security Software: Deploy advanced email filtering solutions capable of detecting and blocking malicious emails before they reach users' inboxes. Implement security software that can identify and quarantine suspicious attachments or links.

Disable PowerShell for Non-Administrative Users: Restrict the use of PowerShell to only authorized personnel, particularly non-administrative users who do not require its functionalities for daily tasks. This can help prevent unauthorized execution of malicious PowerShell scripts.

Monitoring and Detection: Deploy advanced threat detection and monitoring tools capable of identifying and mitigating malware attacks in real-time. This includes behavior-based analytics, intrusion detection systems, and endpoint protection solutions.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	T1566.001 Spearphishing Attachment
T1566 Phishing	T1204 User Execution	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information
T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1036 Masquerading	T1204.002 Malicious File

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxps://bolibachan[.]com/g[.]txt
Domain	indscpm[.]xyz
IPv4:Port	94[.]131[.]104[.]223[:]443

References

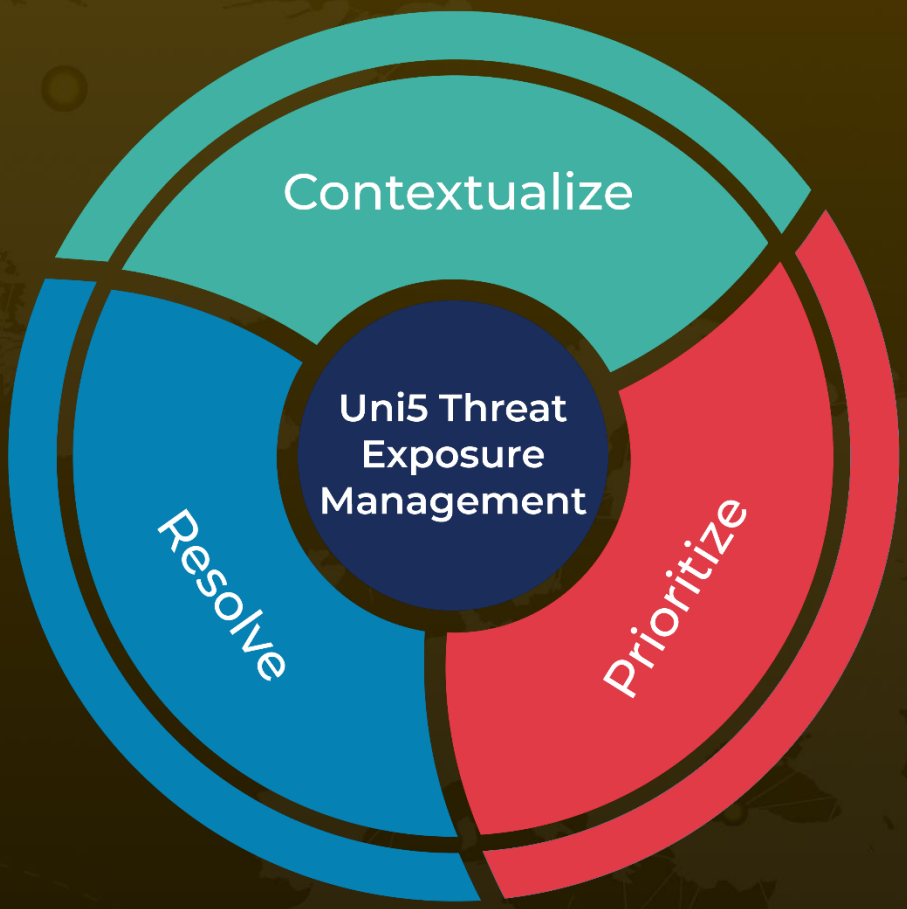
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer

https://www.hivepro.com/threat-advisory/rhadamanthys-stealer-version-0-5-0-upgrade-overview/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 12, 2024 • 3:30 AM

More at www.hivepro.com