Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

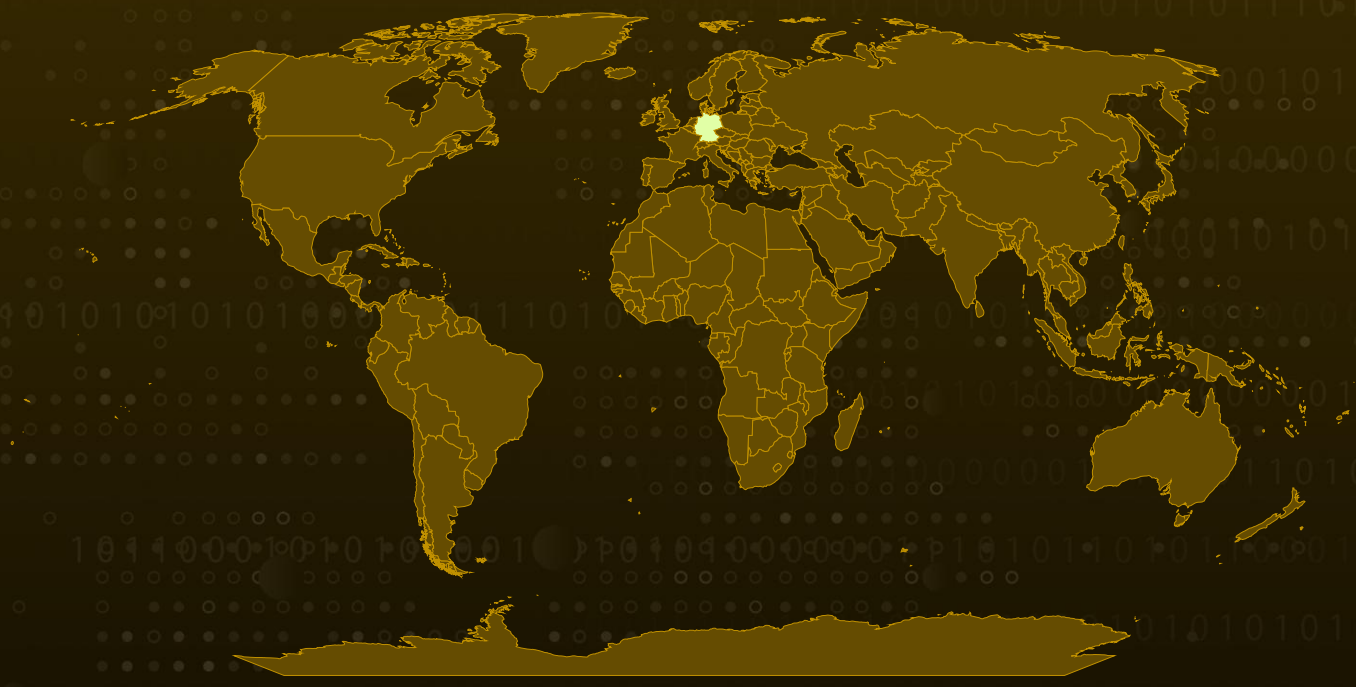
German Entities Under Attack: Sliver Implant Delivered via Malicious LNK Files

Date of Publication	Admiralty Code	TA Number
January 22, 2025	A1	TA2025015

Summary

Attack Discovered: January 2025
Targeted Countries: Germany
Affected Platform: Windows
Malware: Silver
Attack: A new cyberattack targeting German organizations has been discovered. The attackers are using advanced methods to break into systems and avoid being detected. The attack starts with an archive file that contains a fake LNK file, which is likely spread through spear-phishing emails, although the exact way it starts is unclear. Once opened, the attack uses techniques like DLL Sideloading, DLL Proxying, and deploying a tool called Sliver to gain access and stay hidden in the victim's network.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 A sophisticated cyber campaign targeting German organizations has been uncovered, employing advanced techniques to infiltrate systems while maintaining a façade of legitimacy. The attack begins with a spear-phishing email delivering an archive file. This archive contains a deceptive LNK file disguised as a PDF, alongside legitimate executables, a malicious DLL, an encrypted DAT file, and a decoy document.

#2 When the victim extracts the archive, only the LNK file is visible, while the other components stay hidden. Executing the LNK file opens a decoy document that looks like a legitimate Home Office Agreement. At the same time, it runs commands using cmd.exe to copy files to specific directories. A new directory named "Intel" is created in the user's local app data folder, where a legitimate Windows executable, wksprt.exe, is stored. Hidden files are also placed here. To ensure persistence, the LNK file creates a shortcut in the Startup folder, triggering wksprt.exe to run when the system starts up.

#3 The attack exploits DLL sideloading and proxying techniques to carry out malicious actions. The legitimate wksprt.exe sideloads the malicious IPHLPAPI.dll, which pretends to be a system file. This malicious DLL then proxies function calls to a modified legitimate DLL, IPHLPLAPI.dll, while executing its own code. It decrypts ccache.dat, extracting shellcode that further decrypts and runs the final payload a Sliver implant.

#4 Sliver implant is an open-source tool, commonly used for red-teaming, is repurposed by the attackers for their malicious activities. Once deployed, the implant connects to external endpoints, allowing the attackers to perform further operations within the compromised network.

#5 The campaign is attributed to **APT29**, a well-known Russian state-sponsored threat group, as several indicators suggests it can be their work. The attack reflects APT29's typical tactics, such as stager DLL usage, shellcode injection, and the deployment of the Sliver framework. However, the introduction of DLL proxying marks a notable evolution in their methods. By combining these sophisticated evasion techniques and persistence mechanisms, the attackers aim to secure prolonged access to high-value targets.

Recommendations

Enhanced Email Security: Enhance email security by Implementing advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts.

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Monitoring for Sliver Framework Activities: Monitoring network traffic for unusual behavior, such as unexpected outbound connections, is crucial for detecting activities linked to the Sliver framework. By proactively analyzing network traffic and cross-referencing anomalies with known threat indicators, organizations can enhance their ability to identify and mitigate this threat effectively.

Implement Application Whitelisting: Establish application whitelisting policies to restrict the execution of LNK files and other potentially harmful components. Ensure that only trusted and verified applications can run on the system to mitigate unauthorized execution of malicious payloads.

Use EDR Solutions for Enhanced Protection: Implement Endpoint Detection and Response (EDR) solutions to spot and block harmful actions like DLL sideloading and shellcode injection. EDR tools can keep an eye on endpoint activities, helping to quickly identify and stop threats before they cause damage.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment
T1059 Command and Scripting Interpreter	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1574 Hijack Execution Flow
T1574.002 DLL Side-Loading	T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1071 Application Layer Protocol

T1071.001 Web Protocols	T1036 Masquerading	T1204 User Execution	T1204.002 Malicious File
T1140 Deobfuscate/Decode Files or Information	T1656 Impersonation		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	83a70162ec391fde57a9943b5270c217d63d050aae94ae3efb75de45df5298be, f778825b254682ab5746d7b547df848406bb6357a74e2966b39a5fa5eae006c2, 9b613f6942c378a447c7b75874a8fff0ef7d7fd37785fdb81b45d4e4e2d9e63d, 86f8a979bd887955f0491a0ed5e00de2f3fe53e6eb5856fb823115ce43b7c0ca
File Name	Homeoffice-Vereinbarung-2025.7z
URLs	hxxp[:]//www[.]technikzwerg[.]de/auth/auth/authenticate/samples[.]html hxxp[:]//www[.]technikzwerg[.]de/auth/auth/authenticate/samples[.]php

References

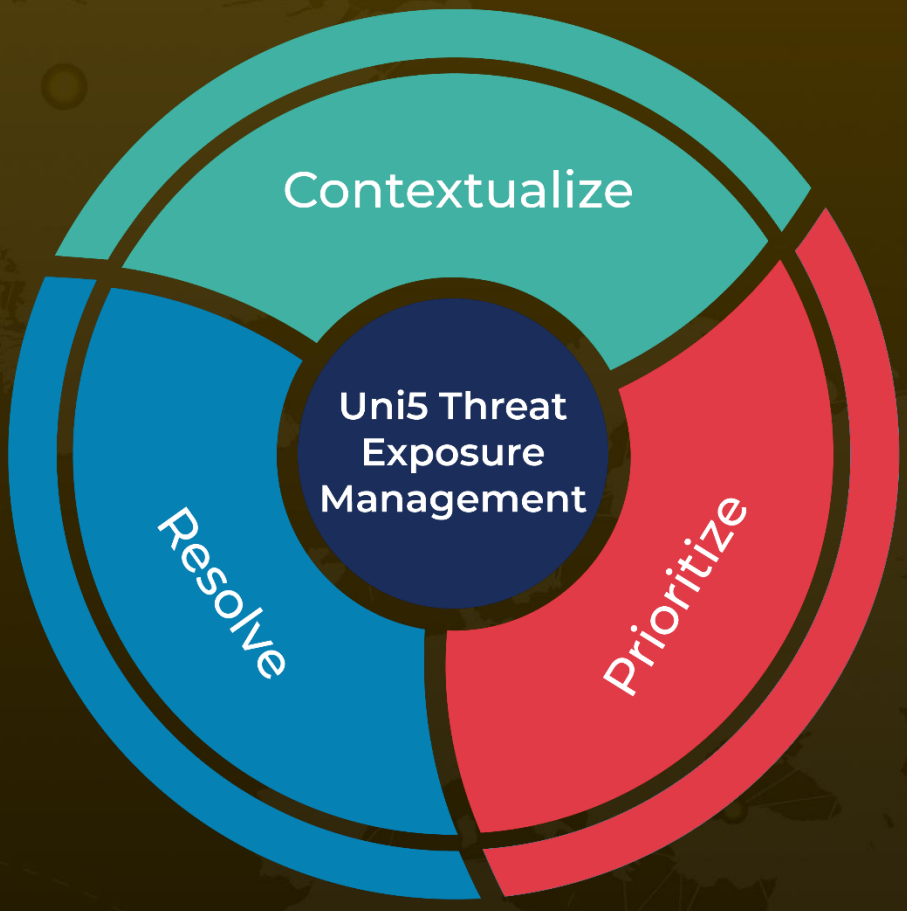
https://cyble.com/blog/sliver-implant-targets-german-entities-with-dll-sideloading-and-proxying-techniques/

https://www.hivepro.com/threat-advisory/apt29-a-deep-dive-into-russias-cyber-espionage/

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

January 22, 2025 • 5:40 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com