Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

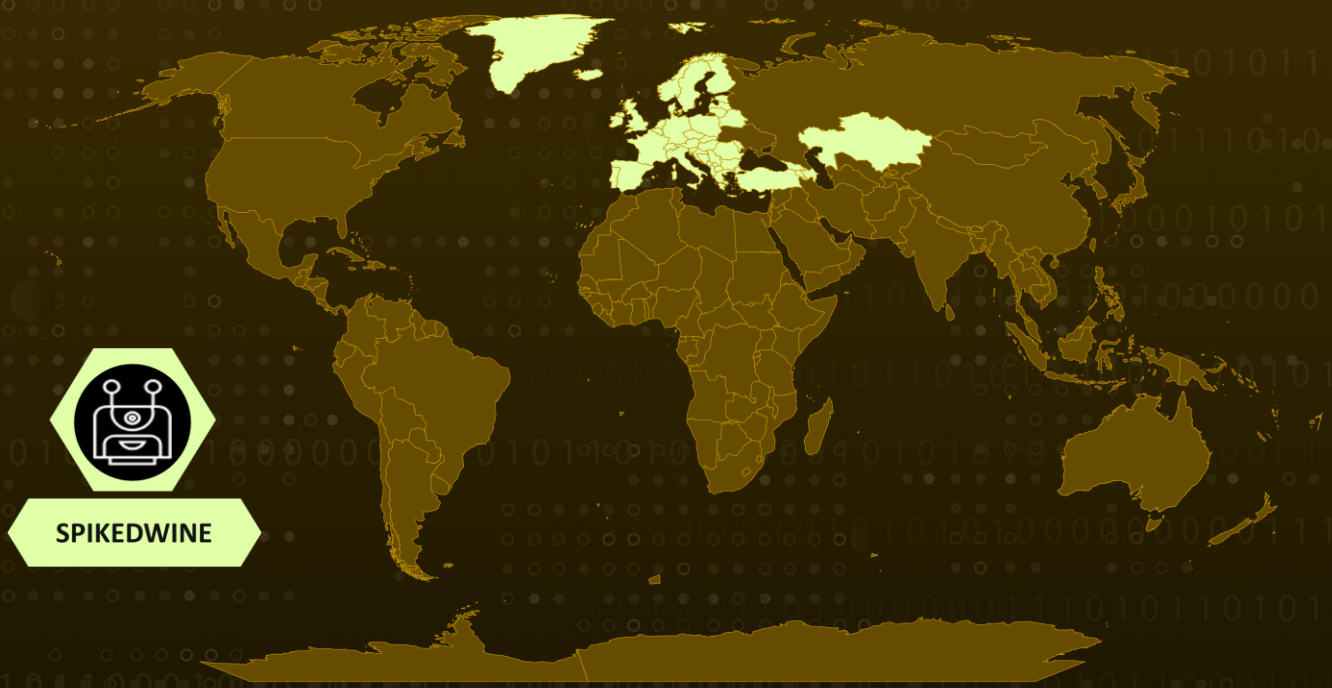
SPIKEDWINE Ploy to Infiltrate EU Diplomatic Circles

Date of Publication	Admiralty Code	TA Number
February 29, 2024	A1	TA2024081

Summary

Attack Commenced: January 2024
Malware: WINELOADER
Threat Actor: SPIKEDWINE
Attack Region: Europe
Targeted Industry: Diplomats
Attack: The SPIKEDWINE threat actor has been identified orchestrating a sophisticated cyber operation targeting European Union diplomats with a deceptive wine-tasting event. Its primary goal is to disrupt geopolitical relations between India and Europe through the deployment of a modular backdoor named WINELOADER.

Attack Regions



Attack Details

#1 An undisclosed threat actor, identified as SPIKEDWINE, has been observed orchestrating a sophisticated cyber operation to deploy a modular backdoor named WINELOADER. This effort involves enticing European Union (EU) diplomats through a deceptive wine-tasting event, with the primary aim of disrupting geopolitical relations between India and Europe.

#2 The employed method entails the distribution of a PDF file disguised as an invitation letter from the Ambassador of India, ostensibly inviting diplomats to a wine-tasting event scheduled for February 2024. Within this PDF, a link leads recipients to a forged questionnaire, redirecting them to a malicious ZIP archive hosted on a compromised website, thus initiating the infection sequence.

#3 This ZIP archive contains an HTA file housing obfuscated JavaScript code, facilitating the retrieval of an encoded ZIP archive containing WINELOADER from the same domain. WINELOADER is equipped with a core module designed to execute commands from the Command and Control (C2) server, inject itself into a dynamic-link library (DLL), and adjust the sleep interval between beacon requests.

#4 To enhance its covert operations, the SPIKEDWINE threat actor encrypts the core module, subsequent modules downloaded from the C2 server, and all related strings and data exchanges with a fixed 256-byte RC4 key.

#5 SPIKEDWINE has taken additional measures to avoid detection, employing advanced backdoor techniques such as re-encryption and memory buffer zeroing to safeguard sensitive data within the system's memory and thwart memory forensics solutions. Noteworthy is SPIKEDWINE's use of compromised network infrastructure at every stage of the attack chain.

Recommendations

Email Security and Document Verification: Employ advanced email security measures to detect and filter malicious attachments, especially those masquerading as invitation letters. Implement document verification processes to ensure the authenticity of official communications.

Network Traffic Monitoring and Anomaly Detection: Implement robust network traffic monitoring systems with anomaly detection capabilities to identify and respond promptly to any unusual activities, especially those related to compromised network infrastructure used by threat actors.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration
T1204.002 Malicious File	T1656 Impersonation	T1204.001 Malicious Link	T1574.002 DLL Side-Loading
T1055.001 Dynamic-link Library Injection	T1573.001 Symmetric Cryptography	T1041 Exfiltration Over C2 Channel	T1584 Compromise Infrastructure
T1053.005 Scheduled Task	T1547.001 Registry Run Keys / Startup Folder	T1140 Deobfuscate/Decode Files or Information	T1036.001 Invalid Code Signature
T1036.004 Masquerade Task or Service	T1027.007 Dynamic API Resolution	T1027.009 Embedded Payloads	T1218.005 Mshta
T1033 System Owner/User Discovery	T1071.001 Web Protocols	T1001.001 Junk Data	T1598.002 Spearphishing Attachment

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	72b92683052e0c813890caf7b4f8bfd331a8b2afc324dd545d46138f677178c4, ad43bbb21e2524a71bad5312a7b74af223090a8375f586d65ff239410bbd81a7, 3739b2eae11c8367b576869b68d502b97676fb68d18cc0045f661fbe354afcb9, 1c7593078f69f642b3442dc558cddff4347334ed7c96cd096367afd08dca67bc, e477f52a5f67830d81cf417434991fe088bfec21984514a5ee22c1bcffe1f2bc, f61cee951b7024fca048175ca0606bfd550437f5ba2824c50d10bef8fb54ca45, c1223aa67a72e6c4a9a61bf3733b68bfbe08add41b73ad133a7c640ba265a19e, b014cdff3ac877bdd329ca0c02bdd604817e7af36ad82f912132c50355af0920, 7600d4bb4e159b38408cb4f3a4fa19a5526eec0051c8c508ef1045f75b0f6083
URLs	hxxps://castechtools[.]com/api.php, hxxps://seeceafcleaners[.]co[.]uk/cert.php, hxxps://seeceafcleaners[.]co[.]uk/wine.php, hxxps://passatempobasico[.]com[.]br/wine.php

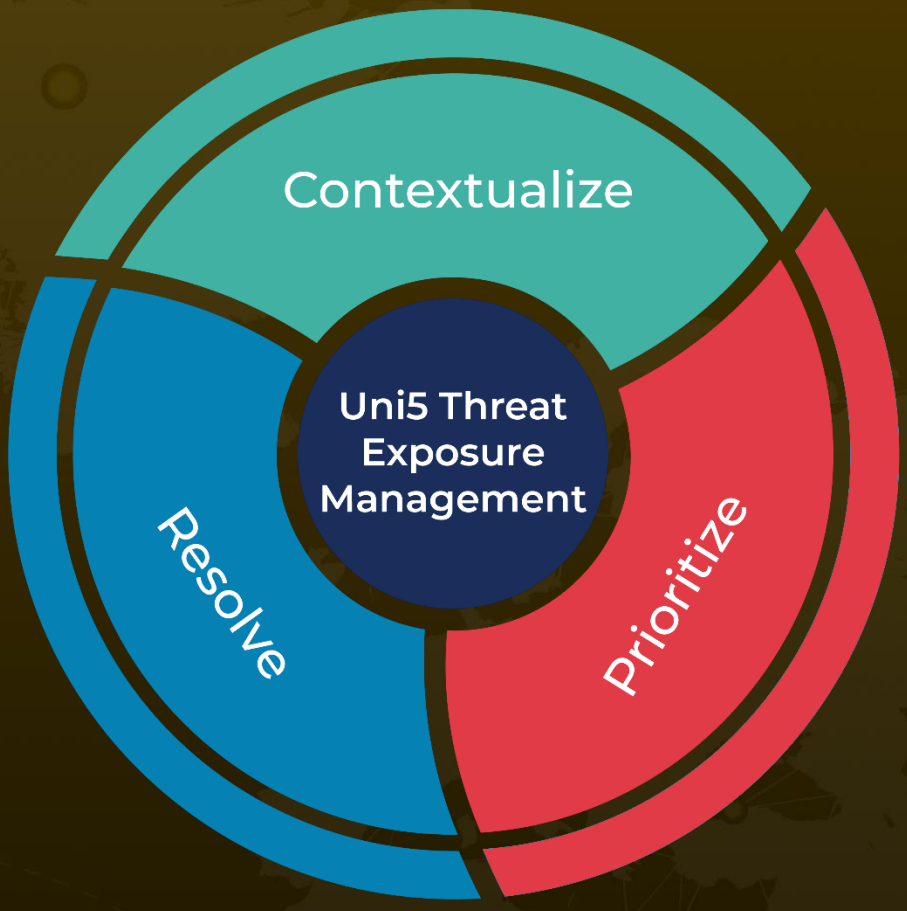
References

https://www.zscaler.com/blogs/security-research/european-diplomats-targeted-spikedwine-wineloader

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

February 29, 2024 • 3:00 AM

More at www.hivepro.com