Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

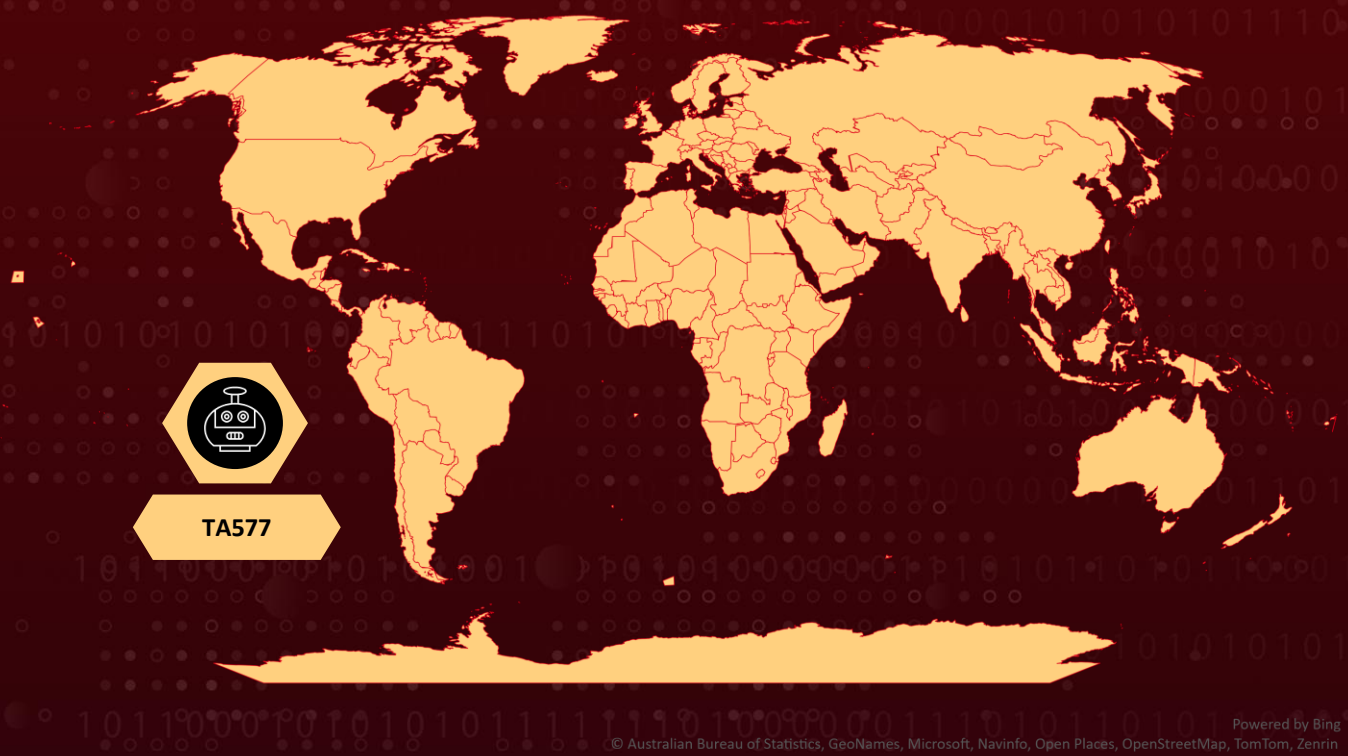
TA577 Targeting Windows NTLM Hashes in Global Campaigns

Date of Publication	Admiralty Code	TA Number
March 5, 2024	A1	TA2024086

Summary

Attack Began: February 26, 2024
Targeted Countries: Worldwide
Threat Actor: TA577
Malware: Pikabot
Affected Platform: Windows
Attack: TA577, a significant cyber threat group, has shifted tactics to steal NTLM authentication data, utilizing thread hijacking and customized HTML attachments. Organizations should block outbound SMB to thwart exploitation and remain vigilant against evolving attack methods.

Attack Regions



Attack Details

#1 TA577, a significant cybercriminal threat actor, has been observed employing a new attack chain aimed at stealing NT LAN Manager (NTLM) authentication information. This uncommon objective was detected by security researchers during campaigns on February 26th and 27th, 2024. These campaigns targeted hundreds of organizations globally, utilizing tens of thousands of messages. The attacks involved thread hijacking, wherein messages appeared as replies to previous emails, and contained zipped HTML attachments.

#2 Each attachment had a unique file hash, and the HTML files within were customized for each recipient. When opened, these files triggered a connection attempt to a Server Message Block (SMB) server, owned by the threat actor, to capture NTLM hashes. Security researchers noted the absence of malware delivery, suggesting the aim was to collect NTLMv2 Challenge/Response pairs. These hashes could be exploited for password cracking or "Pass-The-Hash" attacks within the targeted organization's environment.

#3 Evidence indicates the use of the open-source toolkit Impacket on the SMB servers, identifiable by default characteristics in the traffic. Connections to these servers could potentially compromise NTLM hashes and reveal sensitive information such as usernames and computer names.

#4 Notably, the attacker's method of delivering the malicious HTML in a zip archive allows the attack to evade security measures on Outlook mail clients patched since July 2023. Disabling guest access to SMB does not mitigate the attack, as authentication attempts are still made to the external SMB server.

#5 TA577's shift towards stealing NTLM credentials marks a departure from their typical malware delivery tactics. They have recently been observed delivering Pikabot using various attack chains. Their ability to quickly adopt and distribute new tactics suggests a deep understanding of the threat landscape and a commitment to bypassing detection methods. Organizations are advised to block outbound SMB to prevent exploitation, as multiple threat actors have been observed abusing file scheme URIs for malware delivery.

Recommendations

Implement Email Security Measures: Enhance email security by deploying advanced threat protection solutions capable of detecting and blocking malicious attachments and URLs. Employ email filtering and scanning techniques to identify and quarantine suspicious emails, especially those containing zipped HTML attachments.

SMB Traffic Monitoring and Filtering: Monitor and filter SMB traffic at the network perimeter to prevent unauthorized connections to external SMB servers. Implement firewall rules and intrusion detection/prevention systems to detect and block suspicious SMB traffic.

Endpoint Protection: Deploy advanced endpoint protection solutions that include anti-malware, anti-phishing, and behavior-based detection capabilities. Ensure that endpoint security software is configured to detect and block malicious activities, including attempts to exploit vulnerabilities.

Network Segmentation: Implement network segmentation to restrict the lateral movement of attackers within the network. Segment critical systems and sensitive data from less secure areas of the network to minimize the impact of a successful breach.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0008 Lateral Movement	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	T1021.002 SMB/Windows Admin Shares	T1021 Remote Services
T1566.001 Spearphishing Attachment	T1566 Phishing	T1204.002 Malicious File	T1204 User Execution
T1021.002 SMB/Windows Admin Shares	T1574 Hijack Execution Flow	T1021 Remote Services	T1555.004 Windows Credential Manager
T1555 Credentials from Password Stores			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://89[.]117[.]1[.]161/mtdi/ZQCw[.]txt, hxxp://89[.]117[.]2[.]33/hvwsuw/udrh[.]txt, hxxp://146[.]19[.]213[.]36/vei/yEZZ[.]txt, hxxp://176[.]123[.]2[.]146/vbcsn/UOx[.]txt, hxxp://89[.]117[.]1[.]160/4bvt1yw/iC[.]txt, hxxp://89[.]117[.]2[.]34/4qp/8Y[.]txt, hxxp://104[.]129[.]20[.]167/xhsmd/bOWEU[.]txt, hxxp://146[.]19[.]213[.]36/dbna/H[.]txt, hxxp://89[.]117[.]2[.]33/7ipw/7ohq[.]txt, hxxp://89[.]117[.]2[.]34/3m3sxh6/IuM[.]txt, hxxp://103[.]124[.]104[.]22/zjxb/bO[.]txt, hxxp://89[.]117[.]1[.]161/epxq/A[.]txt, hxxp://176[.]123[.]2[.]146/5aohv/9mn[.]txt, hxxp://66[.]63[.]188[.]19/bmkmsw/2[.]txt, hxxp://89[.]117[.]1[.]160/zkf2r4j/VmD[.]txt, hxxp://103[.]124[.]104[.]76/wsr6oh/Y[.]txt, hxxp://103[.]124[.]105[.]208/wha5uxh/D[.]txt, hxxp://103[.]124[.]105[.]233/yusx/dMA[.]txt, hxxp://103[.]124[.]106[.]224/uuny19/bb1nG[.]txt, hxxp://85[.]239[.]33[.]149/naams/p3aV[.]txt, hxxp://155[.]94[.]208[.]137/tgnd/zH9[.]txt

References

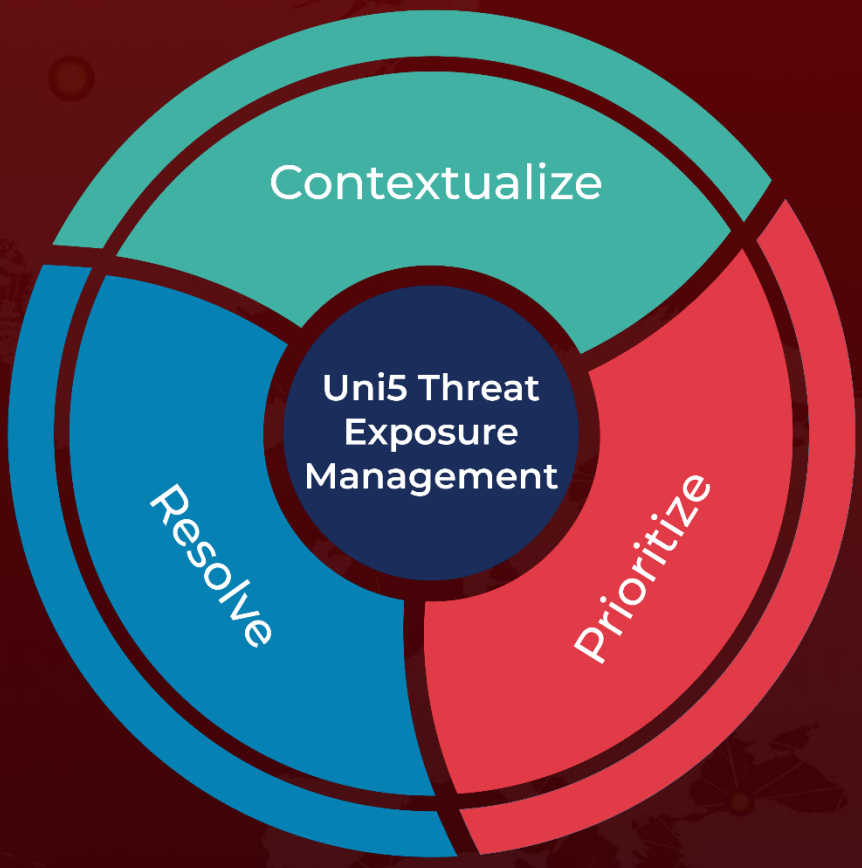
https://www.proofpoint.com/us/blog/threat-insight/ta577s-unusual-attack-chain-leads-ntlm-data-theft

https://www.hivepro.com/threat-advisory/pikabot-malware-unleashes-threat-via-malvertising/

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

March 5, 2024 • 6:30 AM

More at www.hivepro.com