Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Art of Impersonation Poses a Threat to Korean IT Powerhouses

Date of Publication	Admiralty Code	TA Number
January 25, 2024	A1	TA2024033

Summary

Attack Commenced: January 2024
Malware: AsyncRAT, VenomRAT
Targeted Industries: IT
Attack Region: Korea
Attack: Malicious entities have adeptly employed advanced strategies, masquerading as reputable Korean IT companies. Their methodology involves orchestrating phishing campaigns and distributing emails harboring a camouflaged LNK file concealed within a compressed archive. The overarching objective is to establish persistence, achieved through the deployment of Remote Access Tools (RATs) such as AsyncRAT and VenomRAT.

Attack Regions

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

Attack Details

#1 In recent campaigns, malicious actors have adopted the tactic of impersonating Korean IT companies. They deploy sophisticated phishing emails that carry an attached LNK file, cleverly masked as a legitimate Word document within a compressed file.

#2 This compressed file also conceals a genuine text file, masquerading as a survey. The ultimate malicious payload consists of two distinct threats: AsyncRAT and VenomRAT. VenomRAT, identified as a remote access tool in 2020, serves as a means for threat actors to manipulate infected systems from a distance.

#3 It is noteworthy that VenomRAT is essentially a clone of QuasarRAT. AsyncRAT, on the other hand, is an open-source tool accessible through the NYANxCAT Github repository. The blues.exe file, downloaded alongside the Word document, operates as a downloader-type malware disguised as a certification from a reputable Korean IT company.

#4 Upon execution, this file initiates the download of additional scripts via PowerShell. The ensuing shellcode execution encompasses keylogging activities and the unauthorized extraction of the victim's system information.

Recommendations

Enhance Email Security Protocols: Strengthen email security measures to filter out phishing emails. Educate employees on recognizing and reporting suspicious emails, especially those with disguised LNK files or compressed attachments.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect any suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Heighten Employee Awareness: Educate employees on cybersecurity best practices, emphasizing the importance of vigilance against phishing attempts. Encourage reporting of any suspicious emails or activities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration	T1041 Exfiltration Over C2 Channel
T1056.001 Keylogging	T1566 Phishing	T1598.002 Spearphishing Attachment	T1204.002 Malicious File
T1105 Ingress Tool Transfer	T1005 Data from Local System	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1204 User Execution	T1562 Impair Defenses	T1083 File and Directory Discovery	T1056 Input Capture
T1036 Masquerading			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2dfaa1dbd05492eb4e9d0561bd29813b, f57918785e7cd4f430555e6efb00ff0f, e494fc161f1189138d1ab2a706b39303, 2d09f6e032bf7f5a5d1203c7f8d508e4, 335b8d0ffa6dffa06bce23b5ad0cf9d6
URLs	hxxp://194.33.191[.]248:7287/docx1.hta, hxxp://194.33.191[.]248:7287/qfqe.docx, hxxp://194.33.191[.]248:7287/blues.exe, hxxp://194.33.191[.]248:7287/sys.ps1, hxxp://194.33.191[.]248:7287/adb.dll
IPv4:Port	194.33.191[.]248:4449

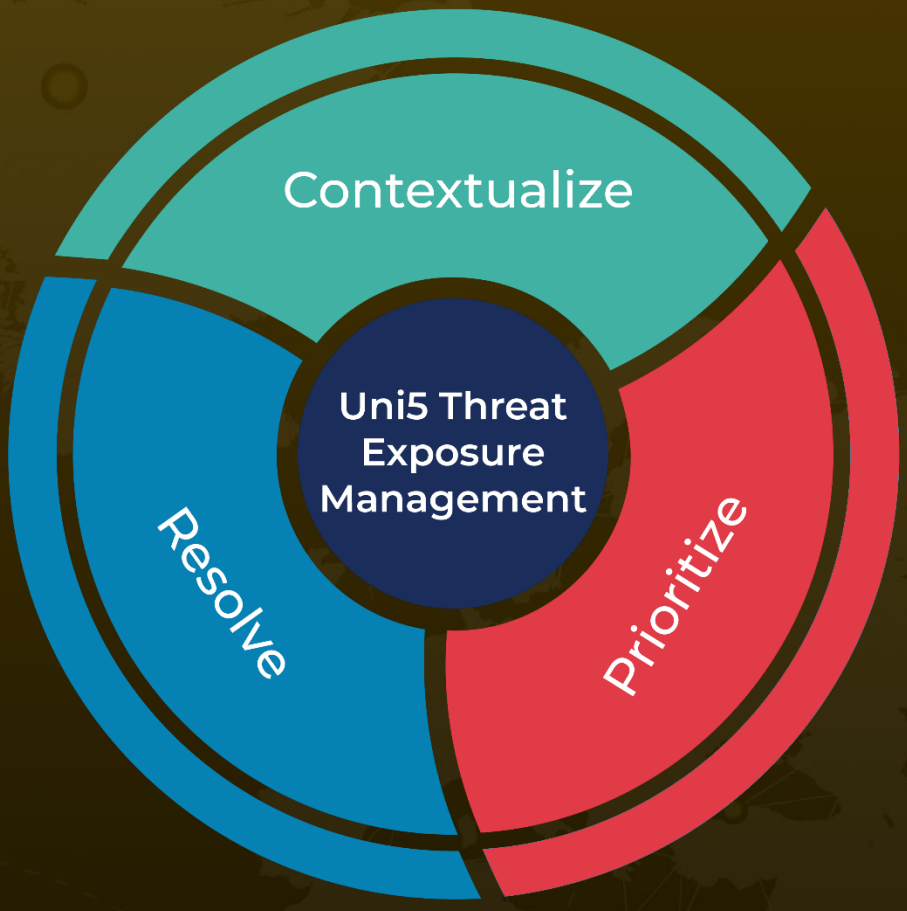
References

https://asec.ahnlab.com/en/60805/

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 25, 2024 • 3:40 AM

© 2024 All Rights are Reserved by Hive Pro®

More at www.hivepro.com