Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

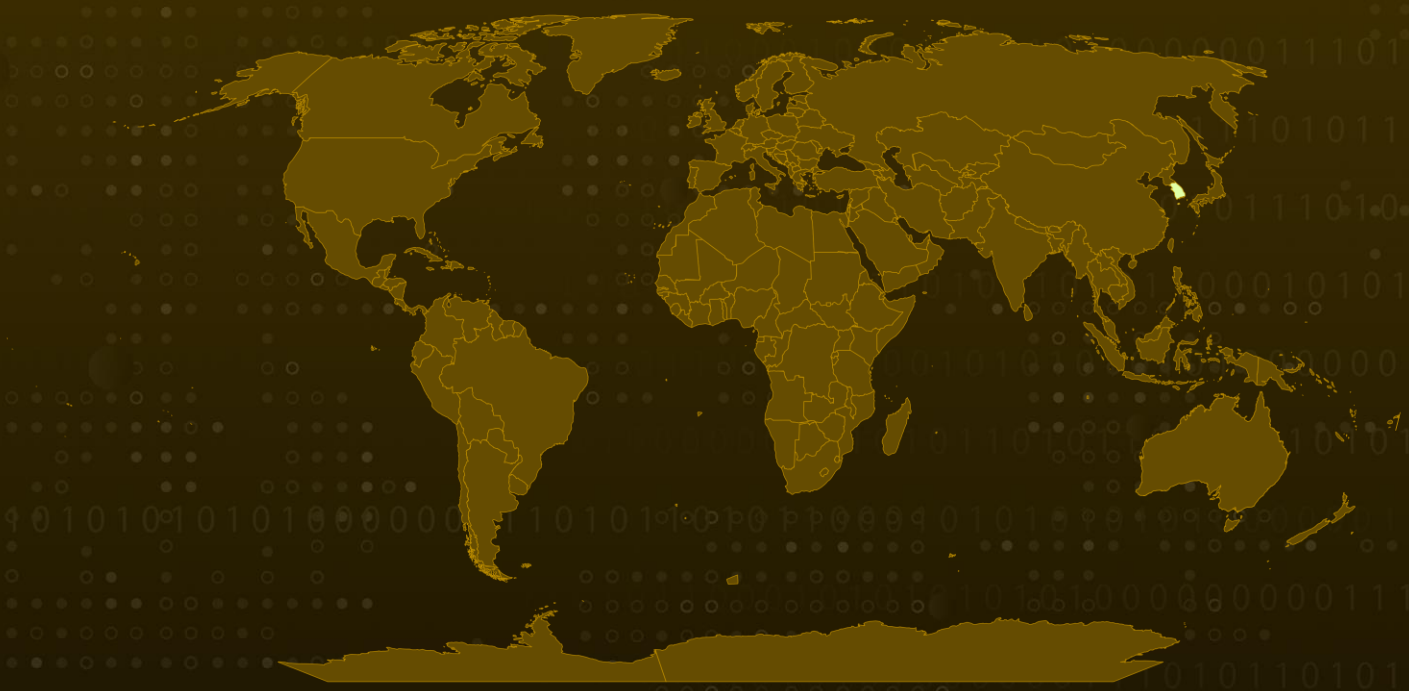
The RokRAT Epidemic in South Korea

Date of Publication	Admiralty Code	TA Number
May 10, 2024	A1	TA2024182

Summary

First Seen: 2016
Malware: RokRAT
Attack Region: South Korea
Attack: The RokRAT malware specifically aims at South Korean users, utilizing LNK files camouflaged within seemingly authentic documents.

Attack Regions



Attack Details

#1 The RokRAT malware propagates through LNK files, specifically targeting South Korean users. Concealed within seemingly authentic documents, this malicious software springs into action upon activation, initiating PowerShell commands.

#2 These commands, in turn, trigger the execution of supplementary files, facilitating the extraction of user data, which is then relayed to the perpetrators' command and control (C2) servers. Typically disseminated as an encoded binary file, RokRAT is retrieved and decrypted by shellcode subsequent to the exploitation of weaponized documents.

#3 Upon execution of the LNK file, PowerShell commands are invoked to establish and execute a seemingly legitimate document file. Subsequently, the malware generates three additional files within the %public% directory

#4 Eventually, RokRAT unleashes its full capabilities, including capturing screenshots, recording keystrokes, and circumventing analysis through anti-virtual machine mechanisms while also leveraging cloud storage APIs. The harvested data finds temporary refuge in the %TEMP% folder before being transmitted to the malevolent actor's cloud server.

Recommendations

- **User Education and Awareness:** Educate users about the dangers of opening suspicious documents or files received via email or other channels. Encourage them to be cautious and vigilant when interacting with unknown or unexpected content.
- **Implement Application Whitelisting:** Use application whitelisting to control the execution of unauthorized applications, thereby preventing the deployment of malicious payloads.
- **Behavioral Analysis and Anomaly Detection:** Utilize advanced security solutions capable of analyzing the behavior of files and processes in real-time. This can help detect anomalous behavior indicative of RokRAT malware activity.
- **Network Traffic Monitoring:** Employ network traffic monitoring tools to detect any unusual or suspicious activity, especially related to the transmission of data to external servers, which could indicate a RokRAT infection.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1010 Application Window Discovery
T1115 Clipboard Data	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic	T1059 Command and Scripting Interpreter
T1555.003 Credentials from Web Browsers	T1555.004 Windows Credential Manager	T1005 Data from Local System	T1622 Debugger Evasion
T1140 Deobfuscate/Decode Files or Information	T1041 Exfiltration Over C2 Channel	T1567.002 Exfiltration to Cloud Storage	T1083 File and Directory Discovery
T1070.004 File Deletion	T1105 Ingress Tool Transfer	T1056.001 Keylogging	T1056 Input Capture
T1112 Modify Registry	T1027 Obfuscated Files or Information	T1057 Process Discovery	T1204.002 Malicious File
T1033 System Owner/User Discovery	T1082 System Information Discovery	T1113 Screen Capture	T1012 Query Registry
T1055 Process Injection	T1059.001 PowerShell	T1059.009 Cloud API	

Indicators of Compromise (IOCs)

TYPE	VALUE
Email	tanessha[.]samuel[@]gmail[.]com, tianling0315[@]gmail[.]com, w[.]sarah0808[@]gmail[.]com, softpower21cs[@]gmail[.]com
MD5	b85a6b1eb7418aa5da108bc0df824fc0, 358122718ba11b3e8bb56340dbe94f51, 35441efd293d9c9fb4788a3f0b4f2e6b, 68386fa9933b2dc5711dffcee0748115, bd07b927bb765ccfc94fadbc912b0226, 6e5e5ec38454ecf94e723897a42450ea, 3114a3d092e269128f72cfd34812ddc8, bd98fe95107ed54df3c809d7925f2d2c

References

https://asec.ahnlab.com/en/65076/

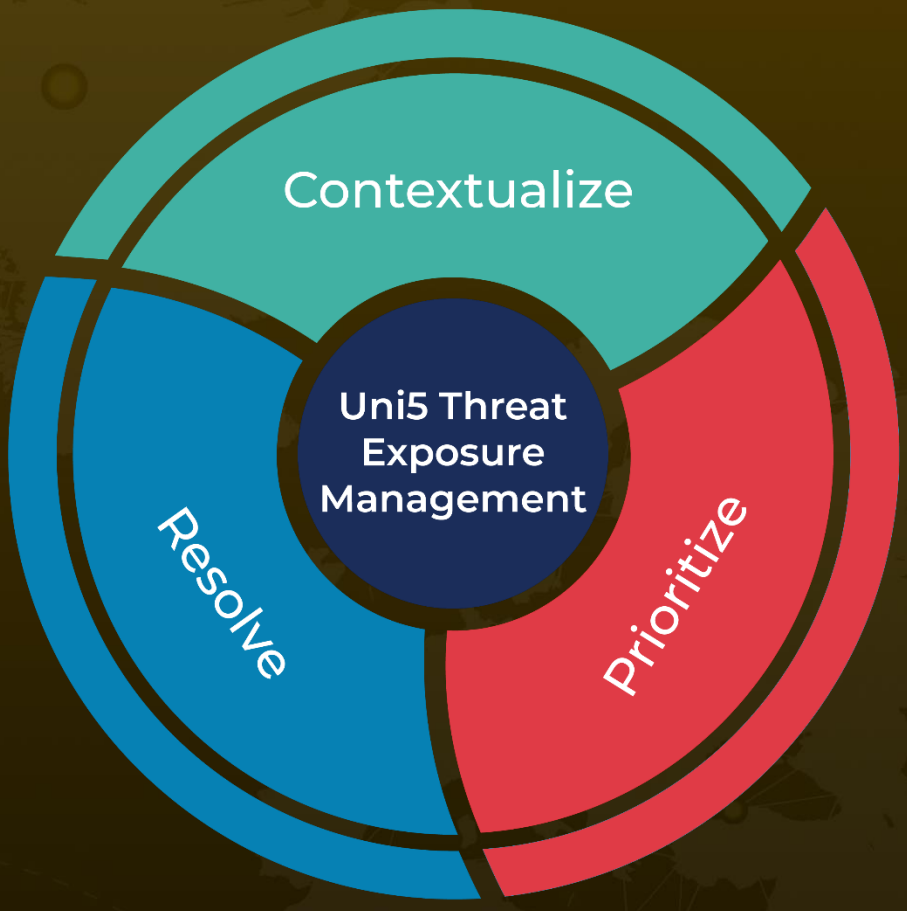
https://attack.mitre.org/software/S0240/

https://www.hivepro.com/threat-advisory/scarcruft-unleashes-tailored-attacks-on-cybersecurity-frontlines/

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

May 10, 2024 • 5:30 AM

More at www.hivepro.com