Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

RedEyes Exploiting Ably Platform Using FadeStealer and Wiretapping Capabilities

Date of Publication	Admiralty Code	TA Number
June 23, 2023	A1	TA2023277

Summary

First appeared: May 2023
Actor Name: Red Eyes (APT 37, Reaper, Ricochet Chollima, ScarCruft, Thallium, Group 123, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)
Target: Individuals of North Korean defectors, human rights activists, journalists, and policymakers, university professors for surveillance purposes.
Malware: FadeStealer, CHM malware, AblyGo backdoor
Affected Platform: Ably
Attack: RedEyes, a state-sponsored APT group, is targeting individuals through spear phishing emails and employing an Infostealer with wiretapping capabilities, utilizing the Ably platform for command and control.

Attack Regions

Attack Details

#1

RedEyes, a state-sponsored APT group, has recently been conducting targeted attacks against individuals such as North Korean defectors, human rights activists, and university professors. Their attacks involve sophisticated techniques and tools.

#2

RedEyes was observed using an Infostealer named FadeStealer with wiretapping capabilities and a backdoor developed using GoLang, which exploited the Ably platform for command and control. FadeStealer exhibits advanced capabilities such as organizing exfiltrated data into separate folders and employing RAR compression with split volumes to restrict the size of compressed files.

#3

The initial breach occurred through spear phishing emails containing a disguised CHM file that appeared as a password-protected document. When executed, the CHM file executed a malicious script, establishing persistence on the compromised system and acting as a backdoor.

#4

RedEyes utilized the Ably platform and GoLang backdoor to send commands and control the compromised systems. The API key required for communication was stored in a GitHub repository, allowing anyone with the key to access the threat actor's channel and receive commands.

#5

After gaining control, the threat actor employed privilege escalation techniques and executed additional malware. They utilized the “AblyGo backdoor” and PowerShell to conduct exfiltration activities, including wiretapping, keylogging, and the theft of data from removable media devices and smartphones.

Recommendations

Robust Email Filtering and Anti-Phishing Measures: Implement advanced email filtering solutions and anti-phishing technologies to detect and block malicious emails containing suspicious attachments or links. This will significantly reduce the risk of employees interacting with RedEyes phishing attempts.

Endpoint Protection and Regular Updates: Maintain up-to-date endpoint protection solutions, including anti-malware and anti-virus software, on all devices. Regularly update operating systems, software applications, and security solutions to patch known vulnerabilities that could be exploited by RedEyes attackers. By keeping systems protected and current, organizations can significantly mitigate the risk of successful RedEyes attacks.

File Extension Awareness: Enable the display of file extensions on operating systems to help users identify potentially malicious file types, such as CHM or LNK files. Instruct users to exercise caution when opening files with uncommon or suspicious extensions.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0011 Command and Control	TA0005 Defense Evasion	TA0002 Execution
TA0007 Discovery	TA0001 Initial Access	TA0009 Collection	TA0008 Lateral Movement
T1068 Exploitation for Privilege Escalation	TA0004 Privilege Escalation	T1204 User Execution	T1140 Deobfuscate/Decode Files or Information
T1059 Command and Scripting Interpreter	T1056 Input Capture	T1560 Archive Collected Data	T1176 Browser Extensions
T1059.001 PowerShell	T1218 System Binary Proxy Execution	T1547 Boot or Logon Autostart Execution	T1106 Native API

T1566.001 Spearphishing Attachment	T1566 Phishing	T1036 Masquerading	T1218.005 Mshta
T1547.001 Registry Run Keys / Startup Folder	T1546.015 Component Object Model Hijacking	T1546 Event Triggered Execution	T1574.002 DLL Side-Loading
T1574 Hijack Execution Flow	T1056.001 Keylogging	T1025 Data from Removable Media	T1027 Obfuscated Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	172[.]93[.]181[.]249
URLs	http://172[.]93[.]181[.]249/file/ http://172[.]93[.]181[.]249/control/html/1[.]xn--html-y96a http://172[.]93[.]181[.]249/control/html/1[.]html http://172[.]93[.]181[.]249/control/data/
MD5	f44bf949abead4af0966436168610bcc 59804449f5670b4b9b3b13efdb296abb 3c475d80f5f6272234da821cc418a6f7 3277e0232ed6715f2bae526686232e06 1c1136c12d0535f4b90e32aa36070682 1352abf9de97a0faf8645547211c3be7

References

https://asec.ahnlab.com/en/54349/

https://www.infosecurity-magazine.com/news/redeyes-group-targets-individuals/

https://www.hivepro.com/reaper-north-korean-hacking-group-targets-defectors/

https://www.hivepro.com/how-scarcruft-apt-group-enhances-its-toolkit-with-a-powerful-dolphin-backdoor/

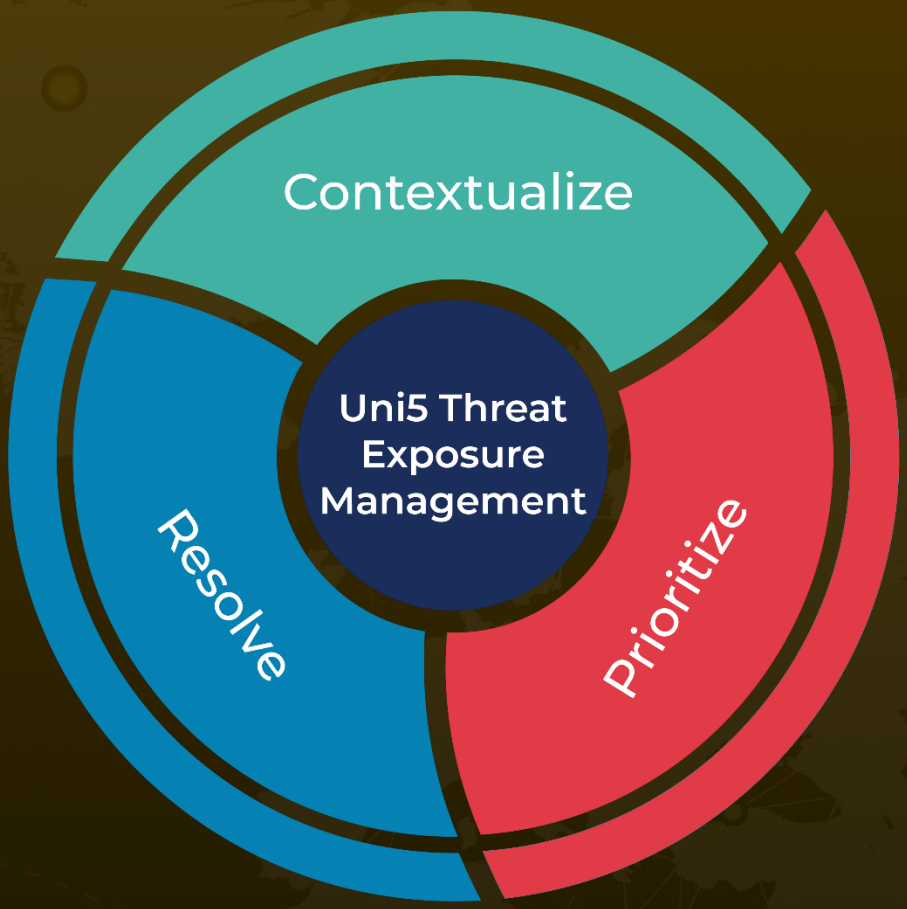
https://www.hivepro.com/internet-explorer-zero-day-vulnerability-exploited-by-apt-37/

https://www.hivepro.com/apt37-employs-konni-malware-to-target-high-level-organizations/

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

June 23, 2023 • 7:30 AM

More at www.hivepro.com