Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

The Bitter Group Targets Chinese Agencies with CHM Malware via Email Attachments

Date of Publication	Admiralty Code	TA Number
April 13, 2023	A1	TA2023183

Summary

First appeared: March 2023
Attack Region: China
Actor name: Bitter APT (T-APT-17, APT-C-08, Orange Yali)
Malware: CHM Malware
Attack: The Bitter group targets South Asian government agencies with Office documents and has recently distributed CHM malware to specific Chinese organizations via email attachments.

Attack Regions

Attack Details

#1 The Bitter group is an attack group that targets government agencies in South Asia and has been using Office documents to distribute malicious codes. Recently, they have been distributing CHM malware to specific organizations in China through email attachments with compressed CHM files.

#2 The CHM files create empty help windows or contain information related to “China Central United Front Department” and “China-Russia Peace and Development Committee”. The files execute malicious scripts that create tasks to execute malicious commands and access and download additional malicious files.

#3 The loaded malicious DLL collects user information and creates a task for persistence. The malicious scripts within the CHM files are difficult for users to recognize, as the Click method that executes the shortcut object is obfuscated. The malware also tries to connect to C2 for various malicious actions.

Recommendations

Be cautious when opening email attachments, especially from unknown senders. Verify the sender's identity and scan attachments for malware before opening them.

Keep your systems and software up to date, and regularly update your operating system and software with the latest security patches and updates to ensure that you have the latest security protections. Use reputable antivirus and antimalware software to help protect your systems against malware attacks.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0001 Initial Access
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1007 System Service Discovery
T1204 User Execution	T1566 Phishing	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter
T1218 System Binary Proxy Execution	T1218.007 Msiexec	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading
T1053 Scheduled Task/Job	T1083 File and Directory Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
Hostname	msdata[.]ddns[.]net bluelotus[.]mail-gdrive[.]com
	https://coauthcn[.]com/hbz[.]php?id=%computername% https://bluelotus[.]mail-gdrive[.]com/Services[.]msi http://msdata[.]ddns[.]net:443
SHA256	cd3effd25629ab9c440ed8bedb9bfb312c73a022cad5078684784ea07eff2c68 43c8ada7cb7c046893dd96aef195856ec94f62823ca1a2987adf31899788c92d
SHA1	365203360046573682932 69d72dfc535f30fd8a619875ccc639e103e9045bbc71f4a5ce44433d1c0
MD5	a7e8d75eae4f1cb343745d9dd394a154

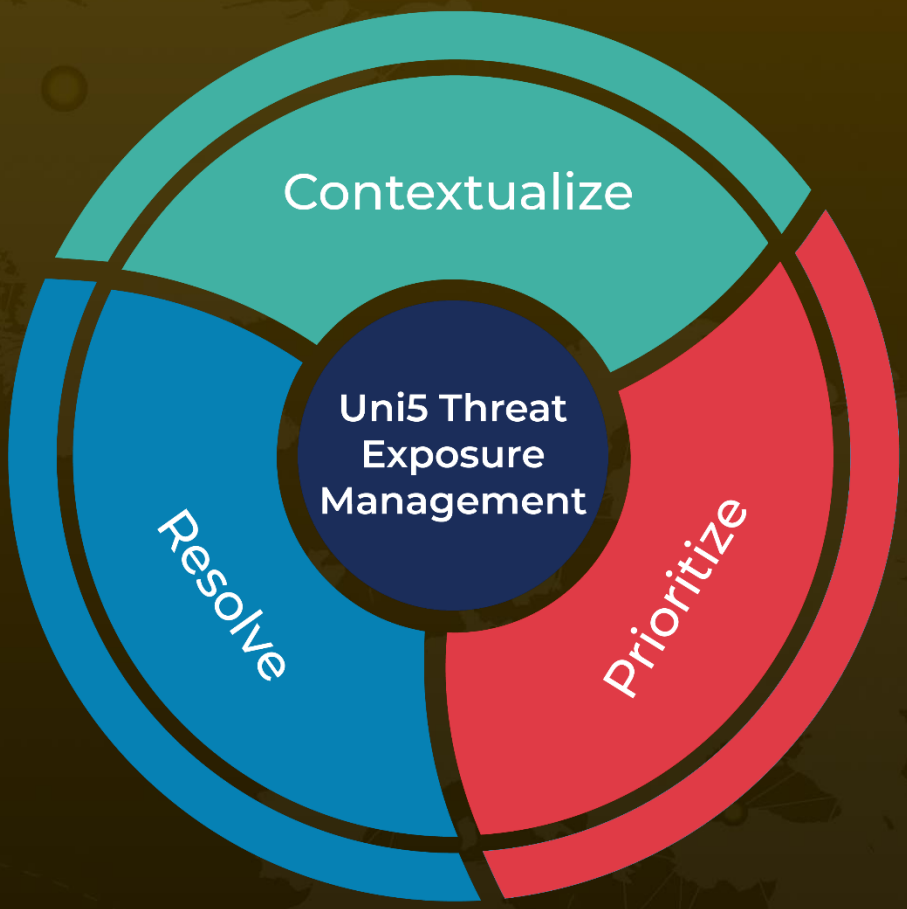
References

https://asec.ahnlab.com/ko/50851/
https://www.hivepro.com/bitter-apt-group-targets-chinese-energy-sector-with-new-phishing-campaign/

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

April 13, 2023 • 4:30 AM

More at www.hivepro.com