Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

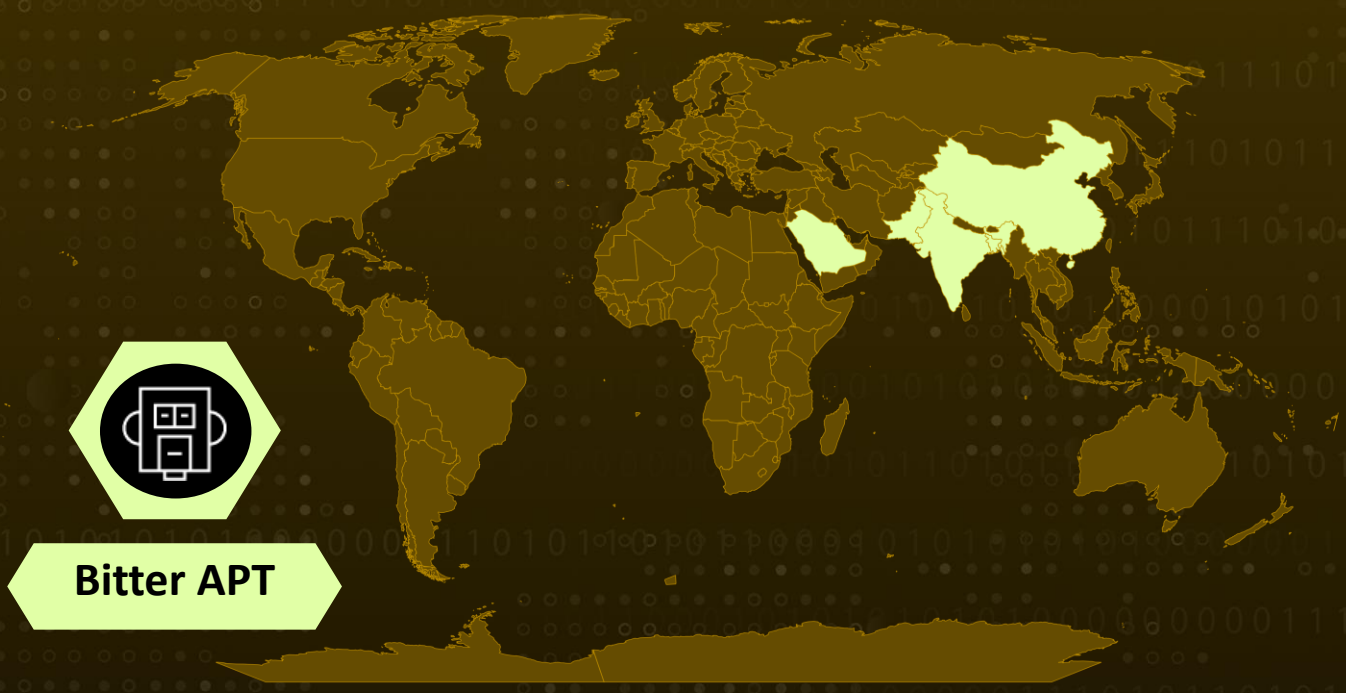
Bitter APT Group Targets Chinese Energy Sector with New phishing Campaign

Date of Publication	Admiralty Code	TA Number
March 28, 2023	A1	TA2023162

Summary

First Appearance: 2013
Actor Name: Bitter APT
Target Region: Bangladesh, China, India, Pakistan, and Saudi Arabia
Target Sector: Energy, Engineering, Government

Actor Map



Actor Details

#1 A new cyber espionage campaign targeting the energy sector in China by the South Asian threat group Bitter APT. The campaign involves the use of social engineering tactics through phishing emails that contain malicious payloads in the form of Microsoft Compiled HTML Help (CHM) files and Excel files with Equation Editor exploits.

#2 The payloads are compressed inside RAR files to avoid static analysis, and they create scheduled tasks for persistence and downloading of further malware payloads. The report also notes updates to the first-stage payloads used, with new layers of obfuscation and additional decoys used for social engineering.

#3 The phishing emails are designed to look like they are coming from the Embassy of Kyrgyzstan, using a free email provider and the name and details of an actual attaché of the Kyrgyz embassy in China to add to the supposed legitimacy of the email.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Bitter APT	South Asia **MOTIVE** Information theft and espionage	Bangladesh, China, India, Pakistan, and Saudi Arabia.	Energy, Engineering, Government.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0003 Persistence	TA0011 Command and Control
TA0043 Reconnaissance	TA0001 Initial Access	TA0007 Discovery	TA0004 Privilege Escalation
T1589.002 Email Addresses	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1203 Exploitation for Client Execution	T1036 Masquerading	T1053.005 Scheduled Task	T1218.007 Msiexec
T1218.001 Compiled HTML File	T1082 System Information Discovery	T1071.001 Web Protocols	T1041 Exfiltration Over C2 Channel
T1566 Phishing	T1218 System Binary Proxy Execution	T1071 Application Layer Protocol	T1053 Scheduled Task/Job

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	5f663f15701f429f17cc309d10ca03ee00fd20f733220cc9d2502eff5d0cd1a1 eb7aebded5549f8b006e19052e0d03dc9095c75a800897ff14ef872f18c8650e cac239cf09a6a5bc1f9a3b29141336773c957d570212b97f73e13122fe032179 8d2f6b0d7a6a06708593cc64d9187878ea9d2cc3ae9a657926aa2a8522b93f74 33905e2db3775d2e8e75c61e678d193ac2bab5b5a89d798effbceb9ab202d799 5c85194ade91736a12b1eeeb13baa0b0da88c5085ca0530c4f1d86342170b3bc Ef4fb1dc3d1ca5ea8a88cd94596722b93524f928d87dff0d451d44da4e9181f1 b2566755235c1df3371a7650d94339e839efaa85279656aa9ab4dc4f2d94bbfa 33a20950e7f4b2191706ddf9089f1e91be1e5384cca00a57cf6b58056f70c96b 7e7e90b076ef3ea4ef8ed4ef14fb599a2acb15d9ce00c78e5949186da1e355cf 07504fcef717e6b74ed381e94eab5a9140171572b5572cda87b275e3873c8a88 06b4c1f46845cee123b2200324a3ebb7fdbea8e2c6ef4135e3f943bd546a2431 ded0635c5ef9c3d63543abc36a69b1176875dba84ca005999986bd655da3a446
Domains	qwavemediaservice[.]net mirzadihatti[.]com coauthcn[.]com

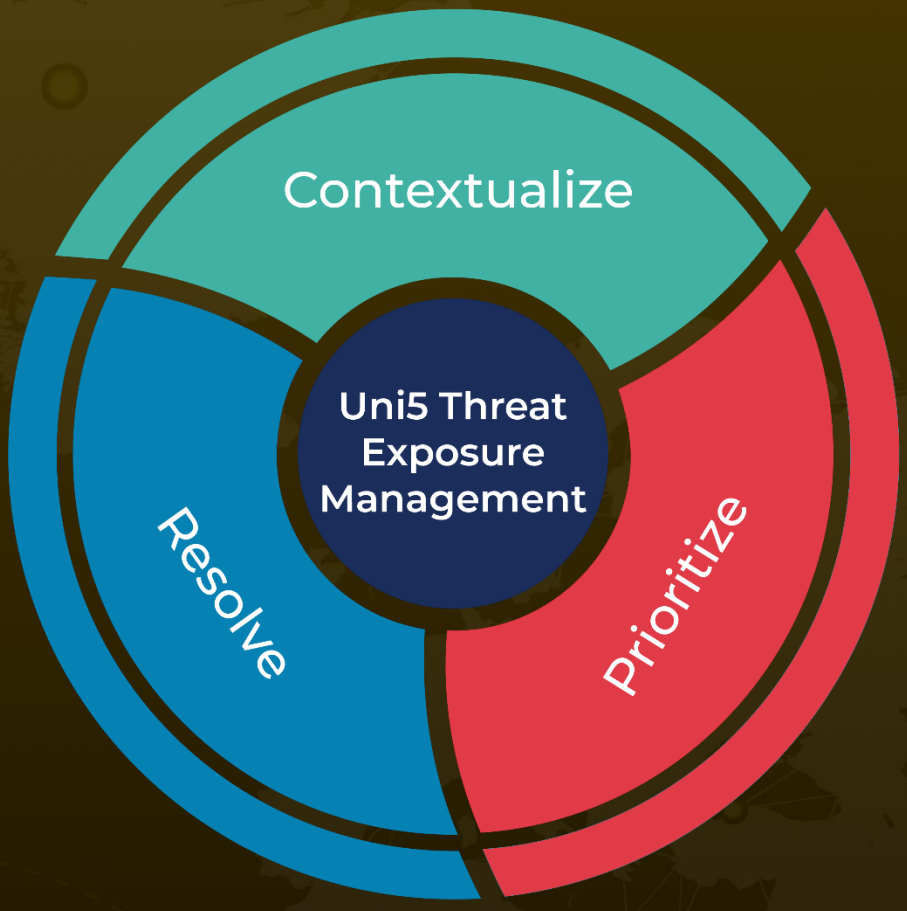
References

https://www.intezer.com/blog/research/phishing-campaign-targets-nuclear-energy-industry/

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 28, 2023 • 02:00 AM

More at www.hivepro.com