Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

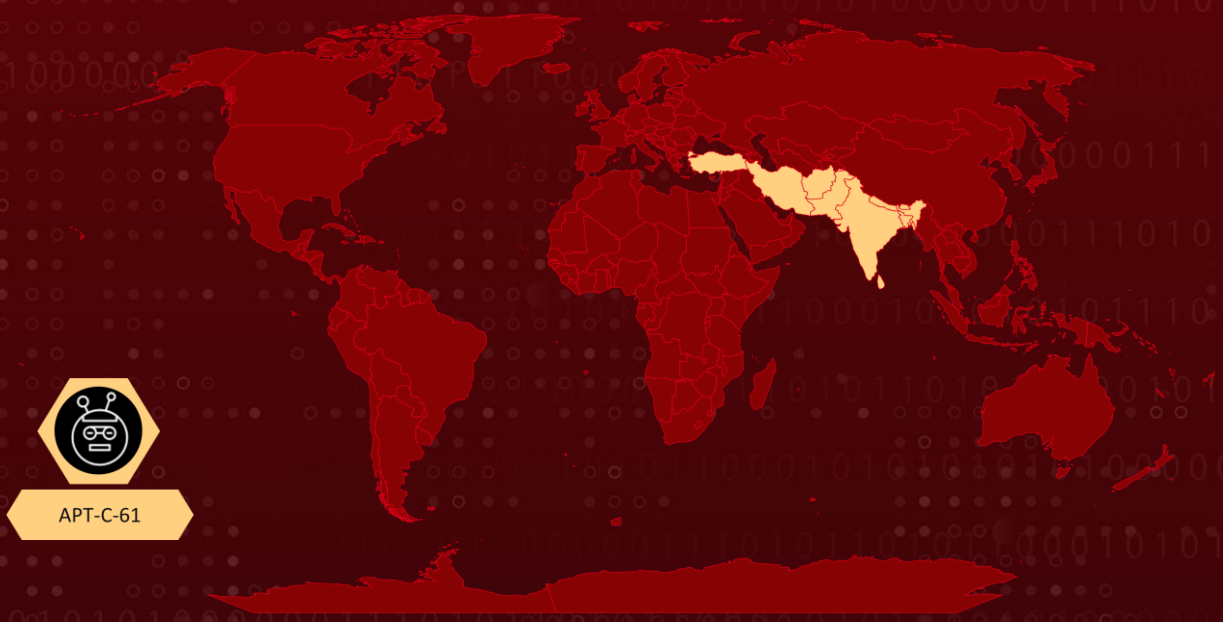
A New APT named APT-C-61 Targets South Asia

Date of Publication	Admiralty code	TA Number
March 2, 2023	A1	TA2023113

Summary

First Appearance: January 2020
Actor Name: APT-C-61
Target Region: South Asia, Iran, Turkey
Target Sectors: National Institutions, Military, Government, Chemical, Diplomats, and Scientific Research

Actor Map



Actor Details

#1 APT-C-61, which is also known as Tengyun Snake, is an APT group that has been operational since January 2020 in South Asia. This group primarily targets significant sectors, including national institutions, military industry, scientific research, and national defense in Pakistan and Bangladesh, among other countries. The APT employs social engineering tactics and spear-phishing emails to spread malware onto target devices. Additionally, they rely on cloud services for their C2 infrastructure, load delivery, and stolen data storage. The Trojan utilized by this group is coded in Python.

#2 This organization is a new attack group and has no association with other APT groups like Mansling Flower and Rattlesnake in South Asia. The Tengyun Snake group has a considerably high level of activity and has expanded its operations to Iran and Turkey.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
APT-C-61 (Tengyun Snake)	Unknown **MOTIVE** Information Theft and espionage	South Asia, Iran, Turkey	National Institutions, Military, Government, Chimical, Diplomats and Scientific Research

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 actor 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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1566 Phishing	T1566.001 Spearphishing Attachment	T1027 Obfuscated Files or Information
T1041 Exfiltration Over C2 Channel	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1083 File and Directory Discovery
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.006 Python	T1071 Application Layer Protocol
T1132 Data Encoding	T1560 Archive Collected Data	T1119 Automated Collection	T1537 Transfer Data to Cloud Account
T1559 Inter-Process Communication	T1559.002 Dynamic Data Exchange	T1218 System Binary Proxy Execution	T1218.005 Mshta
T1204 User Execution	T1204.001 Malicious Link	T1204.002 Malicious File	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2a791878c7840a3b59ed9ff605f857954efaf99491544221b06326edf6ae640e 55f7635da08586b775db3f38df2bf261754a2daf31cb728b21647ed1e47ebcd1 c9bf3622b71686e1a16aae4e8edfd60e2bd0bb4ca46c3472b882ffff8398c886
URLs	hxxps[:]//1drv[.]ms/u/s!AsnveMg8eWB2gRTZAmgFMB1LxkyY?e=Z7s0MP

TYPE	VALUE
Domains	en-office365updateescente[.]herokuapp[.]com en-localhost[.]herokuapp[.]com il1[.]000webhostapp[.]com a0w[.]herokuapp[.]com

References

https://mp.weixin.qq.com/s/s740Y3HaXBXkS5RJi9LaHQ

https://mp.weixin.qq.com/s/Jpw7TqyPzOy57RAZDQdlWA

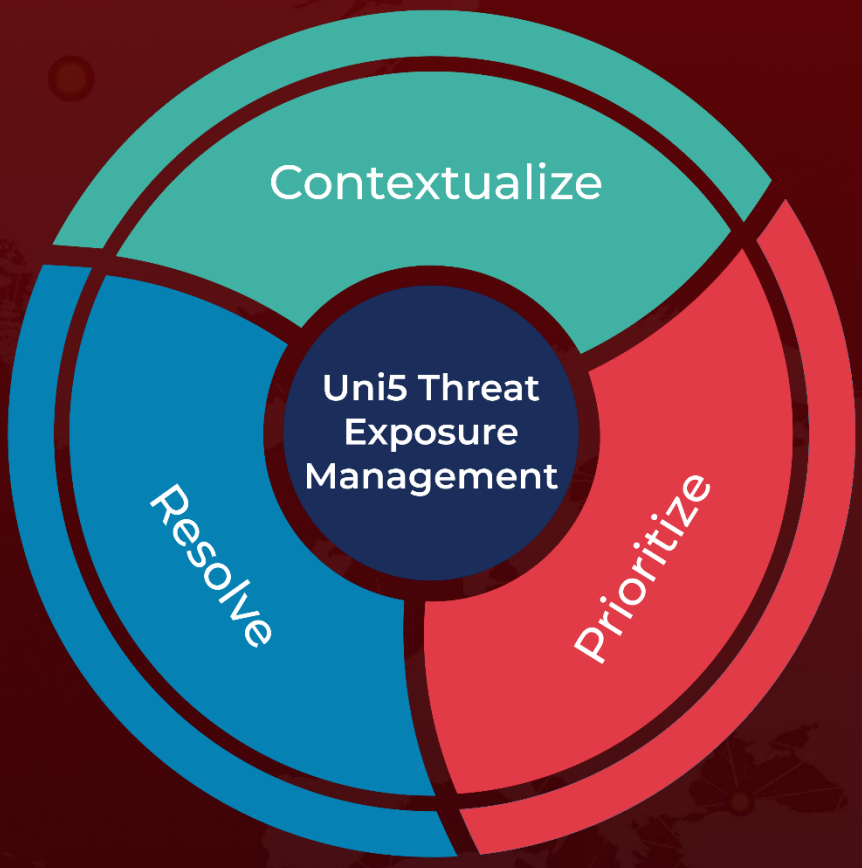
https://www.cirt.gov.bd/observed-apt-c-61-threat-actors-malicious-activities-targeting-bangladesh/

https://www.rewterz.com/rewterz-news/rewterz-threat-alert-apt-c-61-targeting-south-asian-countries

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 2, 2023 • 2:10 AM

More at www.hivepro.com