ADVISORY FOR ICM SECTORS

Chinese APT Groups Target ASEAN Entities

Original report published on: March 26, 2024[1]

Executive Summary

Palo Alto Unit 42 researchers identified and published an advisory in March 2024 highlighting activities and campaigns of Advanced Persistent Threat ("APT") groups that conduct cyberespionage activities against entities and member countries affiliated with the Association of Southeast Asian Nations ("ASEAN").

Two groups have been identified: Stately Taurus (aka Mustang Panda, BRONZE PRESIDENT, RedDelta, TA416) and an unidentified actor. Both groups pose significant threat due to their potential to exfiltrate sensitive information.

Background

Two APT groups have been observed targeting ASEAN entities:

- Stately Taurus: This group created malware packages aimed at organisations in Myanmar, the Philippines, Japan, and Singapore. The timing suggests a possible connection to the ASEAN-Australia Special Summit held from 4 to 6 March 2024.

- Second Unidentified Group: This group compromised an ASEAN-affiliated entity, highlighting their interest in cyber-espionage activities. The researchers identified threat actor activities throughout January and February 2024.

Recent cyberespionage activities against entities and member countries affiliated to ASEAN demonstrated how organisations are targeted to fulfil the mission objective of collecting intelligence of geopolitical interests within the region.

Stately Taurus was observed to have targeted Non-Governmental Organisations ("NGOs"), Think Tanks, and Telecommunications sectors in European and Asian regions based on past campaigns.

Detection and Mitigation

IMDA recommends organisations in the infocomm and media sectors to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Deploy a multi-layered protection solution that includes email sandboxing, domain URL filtering, endpoint detection and response protection, and network security measures to detect and block phishing attempts and other threats at various entry points.

- Implement and enforce strong password policies and multi-factor authentication (MFA).
- Deploy data loss prevention solution to monitor that data remains within the enterprise or approved networks.
- Refer to MITRE ATT&CK techniques in this advisory to create detection rules and harden system configuration controls that have no business need. Ensure systems are up to date with the latest security updates.
- Be alert for suspicious emails, particularly those containing phishing attempts or malicious attachment and educate employees on social engineering tactics used by APTs.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess potential impacts prior to deploying defensive measures.

Indicators of Compromise[1]

Malware Hashes - SHA256	Remarks
a16a40d0182a87fc6219693ac66428673832922298 3bd9e70b455f198e124ba2	Stately Taurus Campaigns
316541143187acff1404b98659c6d9c8566107bd652310705214777f03ea10c8	
02f4186b532b3e33a5cd6d9a39d9469b8d9c12df7cb45dba6dcab912b03e3cb8	
5cd4003ccaa479734c7f5a01c8ff95891831a29d857757bbd7fe4294f3c5c126	

IP Address	Remarks
103[.]27[.]109[.]157	Stately Taurus Campaigns
123[.]253[.]32[.]71	
146[.]70[.]149[.]36	
65[.]20[.]103[.]231	ASEAN Affiliated Activity

139[.]59[.]46[.]88	
193[.]149[.]129[.]93	
192[.]153[.]57[.]98	

Domain	Remarks
www[.]openservername[.]com	ASEAN Affiliated Activity
ai[.]nerdnooks[.]com	
web[.]daydreamdew[.]net	

MITRE ATT&CK Tactics and Techniques[2]

Tactic	Technique	ID
Reconnaissance	Spearphishing Link	T1598.003
Resource Development	Domains	T1583.001
	Email Accounts	T1585.002
	Stage Capability: Upload Malware	T1608.001
Initial Access	Spearphishing Attachment	T1566.001
	Spearphishing Link	T1566.002

	Replication Through Removable Media	T1091
Execution	Command and Scripting Interpreter: PowerShell	T1059.001
	Command and Scripting Interpreter: Windows Command Shell	T1059.003
	Command and Scripting Interpreter: Visual Basic	T1059.005
	Exploitation for Client Execution	T1203
	Scheduled Task/Job: Scheduled Task	T1053.005
	User Execution: Malicious Link	T1204.001
	User Execution: Malicious File	T1204.002
	Windows Management Instrumentation	T1047
Persistence	Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder	T1547.001
	Event Triggered Execution: Windows Management Instrumentation Even Subscription	T1546.003
	Hijack Execution Flow: DLL Side-Loading	T1547.002
Defence Evasion	Hide Artifacts: Hidden Files and Directories	T1564.001
	Indicator Removal: File Deletion	T1070.004

	Masquerading: Match Legitimate Name or Location	T1036.005
	Masquerading: Double File Extension	T1036.007
	Obfuscated Files or Information: Binary Padding	T1027.001
	System Binary Proxy: InstallUtil	T1218.004
	System Binary Proxy: Mshta	T1218.005
Credential Access	OS Credential Dumping: NTDS	T1003.003
Discovery	File and Directory Discovery	T1083
	Process Discovery	T1057
	Software Discovery	T1518
	System Information Discovery	T1082
	System Network Configuration Discovery	T1016
	System Network Connections Discovery	T1049
Collection	Automated Collection	T1119
	Archive Collected Data: Archive via Utility	T1560.003
	Archive Collected Data: Archive via Custom Method	T1560.001
	Data Staged: Local Data Staging	T1074.001
	Application Layer Protocol: Web Protocols	TT1071.001

Command and Control	Encrypted Channel: Symmetric Cryptography	T1573.001
	Ingress Tool Transfer	T1105
	Remote Access Software	T1219
	Web Service	T1102
Exfiltration	Exfiltration Over Physical Medium: Exfiltration over USB	T1052.001

References

1. ^ "ASEAN Entities in the Spotlight: Chinese APT Group Targeting" .
2. ^ "Mustang Panda - MITRE" .