ADVISORY FOR ICM SECTORS

APT41 cyber-espionage campaign targeting media sector in Asia

Original report published on: July 19, 2024[1]

Executive Summary

Recently, APT41, a Chinese-nexus threat actor was observed to have performed cyber-espionage campaign targeting the media and entertainment sector in Asia. In the recent campaign, they were seen mainly using in-memory droppers and plugins to successfully infiltrate and maintain prolonged, unauthorised access to numerous victims' networks, enabling them to extract sensitive data over an extended period.

Background

Mandiant researchers observed Chinese-nexus threat actor APT41 (Double Dragon, BARIUM, Wicked Panda, Winnti, Brass Typhoon) performing cyber-espionage campaigns targeting the media and entertainment sector in Asia as well as other sectors and countries. APT41, initially observed in 2012, focused on financially motivated operations targeting video game industry before expanding into state-sponsored activities in 2014.[2]

In recent campaigns, ANTSWORD and BLUEBEAM web shells were seen on exposed Tomcat Apache Manager server to execute certutil.exe and download the DUSTPAN dropper which loads BEACON. DUSTPAN is an in-memory dropper that decrypts and executes an embedded payload and may be injected into another process or spawn on its own. DUSTPAN was disguised as a Windows binary by executing the malicious file as w3wp.exe or conn.exe. Additionally, DUSTPAN was made persistent via Windows services, such as "Windows Defend" masquerading as a legitimate Windows Defender service. It also loads an encrypted BEACON payloads into memory and once executed, communicate to its configured Command and Control (C2) server.

DUSTTRAP dropper, a multi-stage plugin framework decrypts its Portable Executable (PE) file to execute in memory and may be used to download additional plugins to discover file and process operations, system information gathering, active directory manipulation, data exfiltration, network probing, and RDP session enumeration.

Furthermore, they utilised SQLULDR2 to extract data from Oracle Databases and used PINEGROVE to efficiently copy large volumes of sensitive information from compromised networks, transferring to OneDrive for further exfiltration and analysis.

Detection and Mitigation

IMDA recommends organisations 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:

- Refer to the MITRE ATT&CK techniques in this advisory:
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.

- Validate and add malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR) on endpoints including servers.
- Keep all operating system, software, especially on public facing systems up to date.
- Deploy Web Application Firewalls (WAFs) to detect and block web shell payloads.
- Deploy data loss prevention (DLP) solution to monitor and block unauthorised data exfiltration especially to unapproved cloud storage services.

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

Indicators of Compromise

Malware Hashes – SHA256	Remarks
4bd3dccb1537af5c4102eddae83c85c83afb8653f61e901d186a322f66a7ae4e	SQLULDR2
c40db0438a906eb0bec55093f1a0f2cc4cdc38104af0b4b4b3f18200a635c443	PINEGROVE
c3efcb6efad675613721910a783389a646b2d138c7721df9849b28952d25bcfc	DUSTPAN
069ca8ae8a3909aa4717832d911d646c536fed4c907866724f74daf4d740f41a	DUSTTRAP
22a50cea6ad67a7e8582d2cd4cdc3eaaf57c0fbe8cd062a9b15710166e255a86	DUSTTRAP
073b35ecbd1833575fbfb1307654fc532fd938482e09426cfb0541ad87a04f75	DUSTTRAP
7586e58a569c2a07d0b3a710616f48833a040bf3fc57628bbdec7fcb462d565a	DUSTTRAP
c7dce6c950735bfcf2125be8eb1f3dd468eeb56a1c615c34f95bf38cb58b7d3a	DUSTTRAP
6b37e0e0b0586769bc7b32ae3e0bc2f29e8ad2a1d3de07d50bb3e5489e2dd136	DUSTTRAP
c6a3a1ea84251aed908702a1f2a565496d583239c5f467f5dcd0cfc5bfb1a6db	DUSTTRAP
33fd050760e251ab932e5ca4311b494ef72cee157b20537ce773420845302e49	DUSTTRAP
8407defe0cc29d04b8d0f519b5008d30c09783fe0c63aad5ccb0950fc9a98406	DUSTTRAP
cdc619734f4e2aba0137b5fe9faf36896b85dff7cd4a93de562de770777d181a	DUSTTRAP
e5c7089eb3297b204aaabdb4a660d125a948ba869d2a7cf3cf7c0098125b5ef5	DUSTTRAP
bd058a6fd20347f21c38115490aef858d06f26b49b9d7be357297e60bd2934cc	DUSTTRAP
b0890685b25c6736827573e9536b2bf8c42dbaf36760fc947d461efdb6309aec	DUSTTRAP

Malware Hashes – MD5	Remarks
0e74285f3359393e57f5d49c156aca47	DUSTTRAP
35f650c94faf6a2068e8238dd99edbea	DUSTPAN
3bb44c0dd7f424864d76d4df09538cb6	DUSTPAN
aca5c6daecf463012a09564764584937	DUSTTRAP
6bc4a92ff4d2cfc9da91ae6a5d2ad3d5	DUSTTRAP

Domain	Remarks
ns2[.]akacur[.]tk	BEACON
ns1[.]akacur[.]tk	BEACON
orange-breeze-66bb[.]tezsfsoikdvd[.]workers[.]dev	BEACON
www[.]eloples[.]com	DUSTRAP

IP Address	Remarks
95[.]164[.]16[.]231	Related to www[.]eloples[.]com
152[.]89[.]244[.]185	Used to deliver DUSTPAN
hxxp://152.89.244[.]185/conn.exe	conn.exe

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Reconnaissance	T1593.002	Search Open Website/Domains: Search Engines
	T1594	Search Victim-Owned Websites
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1569.002	System Services: Service Execution
Persistence	T1543.003	Create or Modify System Process: Windows Service
	T1574.001	Hijack Execution Flow: DDL Search Order Hijacking
	T1574.002	Hijack Execution Flow: DLL Side-loading
	T1505.003	Server Software Component: Web Shell
Defense Evasion	T1070.004	Indicator Removal: File Deletion
	T1036.005	Masquerading: Match Legitimate Name or Location
	T1027.013	Obfuscated Files or Information: Encrypted/Encoded File
Collection	T1560.001	Archive Collected Data: Archive via Utility
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage

References

1. ^ “APT41 Has Arisen From the DUST” .
2. ^ “APT41, A Dual Espionage and Cyber Crime Operation” .