Hive Pro

THREAT ADVISORY

Airline industry affected by supply-chain attack allegedly done by Chinese espionage group APT-41.

TA202120

Threat Level Red

Publish Date – June 14, 2021

A supply chain attack was carried out on the airline industry, which started with SITA being compromised, allegedly done by Chinese espionage group APT-41. SITA is responsible for providing software solutions to 90% of airlines in the world. The attack was carried forward by deploying Cobalt Strike beacons in the infrastructure of airlines using the SITA data processing server and BadPotato malware is used for privilege escalation. The attackers later used hash dump and mimikatz to exfiltrate NTLM hashes and plain-text passwords.

The Techniques used by the APT41 includes:

- T1195 - Supply Chain Compromise,
- T1059 - Command and Scripting Interpreter,
- T1569.002 - Service Execution,
- T1543.003 - Windows Service,
- T1134 - Access Token Manipulation,
- T1055 - Process Injection,
- T1070 - Indicator Removal on Host,
- T1550 - Use Alternate Authentication Material,
- T1021 - Remote Services,
- T1003 - OS Credential Dumping,
- T1046 - Network Service Scanning,
- T1005 - Data from Local System,
- T1071.004 - DNS,
- T1029 - Scheduled Transfer,
- T1550.002 - Pass the Hash,
- T1021.002 - SMB/Windows Admin Shares,
- T1070.004 - File Deletion,
- T1055.012 - Process Hollowing

Threat Actor

Name	Known as	Origin	Target Locations	Target sectors
APT 41	WICKED SPIDER (PANDA), Winnti Umbrella, and BARIUM	China	Australia, Canada, Denmark, Finland, France, India, Italy, Japan, Malaysia, Mexico, Philippines, Poland, Qatar, Saudi Arabia, Singapore, Sweden, Switzerland, UAE, UK and USA	Banking/Finance, Construction, Defense Industrial Base, Government, Healthcare, High Technology, Higher Education, Legal, Manufacturing, Media, Non-profit, Oil & Gas, Petrochemical, Pharmaceutical, Real Estate, Telecommunications, Transportation, Airline, and Utility

Indicators of Compromise

Type	Value
Ipv4	185.118.164[.]198; 104.224.169[.]214; 45.61.136[.]199; 185.118.166[.]66; 149.28.134[.]209;
Hash(SHA!)	B3038101fd0e8b11c519f739f12c7e9b60234d3b 7185bb6f1dddca0e6b5a07b357529e2397cdee44
Hash(MD5)	20aebf6e20c46b6bfe44f2828adf3b91 b6b06a95cfeeee0efe8bc0cd54eac71d 83249cff833182b3299cbd4aac539c9a 143278845a3f5276a1dd5860e7488313 559b7150d936fffe728092b160c14d28 9337952aa3be0dacfc12898df3180f02 212784cf25f0adfaf9ba46db41c373d5 d414c7ede5a9d6d30e6d3fe547e27484 83e6da9cd8ccf9b0c04f00416b091076 7b501402c843034cd79151257aca189e 69f5c5f67850acdb373ddd106adce48c b071a62d2dd745743c6de5f115d633b1 019122b1d783646f99c73a3c399cc334 f61dbac694d34c96830f184658610261 fc208a4d04c085edcea1ec5f402057f9 5528bb928e02926179fca52dd388b1f0 b8ecab09b7bfb42b9ace3666edf867a7 c4be6b466807540a22f62ffa6829540f a00ab8ac0f11c3fcd5c557729afcbf89
URLs	service04.dns04.com service.dns22.ml server04.dns04.com ns2.colunm.tk ns1.colunm.tk cs.colunm.tk colunm.tk

References

https://blog.group-ib.com/colunmtk_apt41
https://www.cnbctv18.com/aviation/china-backed-apt41-behind-sita-and-air-india-cyber-attacks-9634641.html
https://threatpost.com/supply-chain-attack-airlines-state-actor/166842/