Hive Pro

THREAT ADVISORY

Iranian APT is targeting Middle Eastern Aerospace and Telecommunications companies

TA202141

Threat Level AMBER

Publish Date – Oct 07, 2021

ShellClient is a powerful new Remote Access Trojan (RAT) that was used in highly targeted attacks on a select few Aerospace and Telecommunications firms, primarily in the Middle East, with other victims in the United States, Russia, and Europe. The attacks were carried out by a newly uncovered Iranian activity group known as MalKamak, which has been active since at least 2018 but has remained unknown until now. ShellClient follows the trend of abusing cloud-based storage services, in this case the popular Dropbox service. The programmers of ShellClient decided to leave their old C2 domain and replace the malware's C2 mechanism with a simpler C2 channel to exfiltrate stolen data and deliver commands to the malware.

The techniques used by ShellClient includes:

T1049 - System Network Connections Discovery
T1566 - Phishing
T1102 - Web Service
T1036 - Masquerading
T1003 - OS Credential Dumping
T1040 - Network Sniffing
T1543 - Create or Modify System Process
T1127 - Trusted Developer Utilities Proxy Execution
T1560 - Archive Collected Data

Actor Details

Name	Origin	Target Location	Target Sector
MalKamak	Iran	Middle East, USA, Russia and Europe.	Aerospace and Telecommunications

Indicators of Compromise(IoCs)

Type	Value
SHA-256 Hashes	21cc9c0ae5f97b66d69f1ff99a4fed264551edfe0a5ce8d5449942bf8f0aefb2 5d5ff74906d2666be0fbfe420c5d225684aa1cb516fffc32cfeee9e788e4b6e4 186ab2a5662c5e3994ee1cbfcf9e7842f1e41b1a4041c67f808914dfc8850706 A541afa0e73c3942b8c3645a3ba1ea59c4d6e1110e271be34fdb6a8c02a299e2 49c41771e8e348b30de43d1112221c71a6497794b541fead7f3b2eab706afba3 19e040305fb57592bb62b41c24e9b64162e1e082230a356a304a3193743b102d d7aa669de0f8a0cdb898cf33ac38ae65461de3c8c0c313c82ee8d48e408e4c4d 6b7b6e973779c1a07891cc1fa7b3e4078a1308c4114296eb3ea429e08793efe0
Domains	azure.ms-tech[.]us ms-tech[.].us
Service Names	WinDefUpd nhdService

References

https://www.cybereason.com/blog/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms