Hive Pro

THREAT ADVISORY

DarkHotel APT group targeting the Hospitality Industry in China

TA2022071

Threat Level RED

Publish Date – Mar 22, 2022

DarkHotel, a South Korean advanced persistent threat (APT), has been targeting premium hotels in Macao, China, since November 2021. The APT group is active since 2007 and has been actively targeting critical sectors such as hotels, government, automotive, and pharmaceutical industries, focusing on surveillance and data theft, with company and industry leaders identified as targets.

The group carried out the attack with a spear phishing email that seemed to be from the "Macao Government Tourism Office" and was directed to management personnel of luxury hotels, including front office and HR employees. The emails featured an Excel sheet bait demanding the completion of a form for a guest query, and if the victim enables macros in order to read the document, the macros activate the download and execution of malware payloads. The malware function is meant to generate a scheduled task for persistence and the execution of VBS and PowerShell scripts for establishing a connection to a hard-coded command-and-control (C2) server disguised as a web server.

The Mitre TTPs used by DarkHotel are:
TA0001 - Initial Access
TA0003 - Persistence
TA0007 - Discovery
TA0005 - Defense Evasion
TA0002 - Execution
TA0011 - Command and Control
T1566.001: Phishing: Spearphishing Attachment
T1204.002: User Execution: Malicious File
T1059.005: Command and Scripting Interpreter: Visual Basic
T1070.004: Indicator Removal on Host: File Deletion
T1106: Native API
T1012: Query Registry
T1053: Scheduled Task
T1064: Scripting
T1071: Standard Application Layer Protocol
T1059.001: Command and Scripting Interpreter: PowerShell

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
DarkHotel (APT-C-06, SIG25, Dubnium, Fallout Team, Shadow Crane, CTG-1948, Tungsten Bridge, ATK 52, Higaisa, T-APT-02, Luder)	South Korea	Afghanistan, Armenia, Bangladesh, Belgium, China, Ethiopia, Germany, Greece, Hong Kong, India, Indonesia, Malaysia, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Lebanon, Malaysia, Mexico, Mozambique, North Korea, Pakistan, Philippines, Russia, Saudi Arabia, Serbia, Singapore, South Korea, Taiwan, Tajikistan, Thailand, Turkey, UAE, UK, USA, Vietnam	Defense, Energy, Government, Healthcare, Hospitality, NGOs, Pharmaceutical, Research, Technology	Information theft and espionage

Indicators of Compromise (IoCs)

Type	Value
SHA-256	163c386598e1826b0d81a93d2ca0dc615265473b66d4521c359991828b725c14, a251ac8cec78ac4f39fc5536996bed66c3436f8c16d377922187ea61722c71f8

References

https://www.trellix.com/en-hk/about/newsroom/stories/threat-labs/suspected-darkhotel-apt-activity-update.html