MITRE-ID: G0079

Name: DarkHydrus

Country: Iran

Description:

DarkHydrus is a threat group that has targeted government agencies and educational institutions in the Middle East since 2016. The group heavily leverages open-source tools and custom payloads for carrying out attacks.

TTPs:

1. The actors sent the spear-phishing emails to target. Each of the emails had a password protected RAR archive attached named credential.rar and include a password as well.
2. Users need to click to enable Microsoft Excel data connection to download the files like PowerShell scripts.
3. Its developer used many open-source tools, for example, to obfuscate PowerShell scripts.
4. The attack created back-door and made fake windows to capture user’s credential and upload to servers.
5. The payload relied on lot of domain names which looked like Microsoft website or applications.
6. This threat group not only used the Phishery (open source) tool to create these malicious Word documents, but also to host the C2 server to harvest credentials.
7. This threat later targeted Google Drive API
8. The new variant of the Trojan can use the Google Drive cloud service for its C2 channel, suggesting that DarkHydrus may be shifting to abusing legitimate cloud services for their infrastructure.

Reference:

https://unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/