APT39: An Iranian Cyber Espionage Group Focused on Personal Information

January 29, 2019

Sarah Hawley, Ben Read, Cristiana Brafman-Kittner, Nalani Fraser, Andrew Thompson, Yuri Rozhansky, Sanaz Yashar

Original report available at https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html

In December 2018, FireEye identified APT39 as an Iranian cyber espionage group responsible for widespread theft of personal information. We have tracked activity linked to this group since November 2014 in order to protect organizations from APT39 activity to date. APT39's focus on the widespread theft of personal information sets it apart from other Iranian groups FireEye tracks, which have been linked to influence operations, disruptive attacks, and other threats. APT39 likely focuses on personal information to support monitoring, tracking, or surveillance operations that serve Iran's national priorities, or potentially to create additional accesses and vectors to facilitate future campaigns.

APT39 was created to bring together previous activities and methods used by this actor, and its activities largely align with a group publicly referred to as "Chafer." However, there are differences in what has been publicly reported due to the variances in how organizations track activity. APT39 primarily leverages the SEAWEED and CACHEMONEY backdoors along with a specific variant of the POWBAT backdoor. While APT39's targeting scope is global, its activities are concentrated in the Middle East. APT39 has prioritized the telecommunications sector, with additional targeting of the travel industry and IT firms that support it and the high-tech industry. The countries and industries targeted by APT39 are depicted in Figure 1.

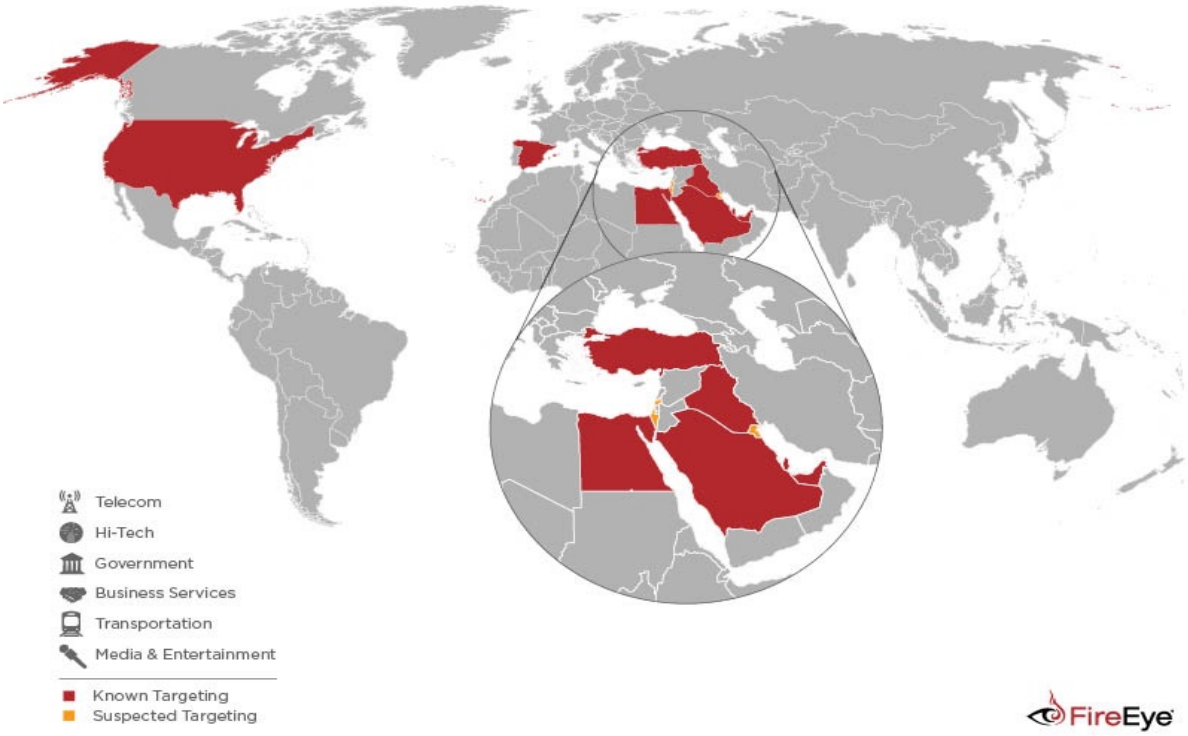

Figure 1: Countries and industries targeted by APT39

Operational Intent

APT39's focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns. Government entities targeting suggests a potential secondary intent to collect geopolitical data that may benefit nation-state decision making. Targeting data supports the belief that APT39's key mission is to track or monitor targets of interest, collect personal information, including travel itineraries, and gather customer data from telecommunications firms.

Iran Nexus Indicators

We have moderate confidence APT39 operations are conducted in support of Iranian national interests based on regional targeting patterns focused in the Middle East, infrastructure, timing, and similarities to APT34, a group that loosely aligns with activity publicly reported as “OilRig”. While APT39 and APT34 share some similarities, including malware distribution methods, POWBAT backdoor use, infrastructure nomenclature, and targeting overlaps, we consider APT39 to be distinct from APT34 given its use of a different POWBAT variant. It is possible that these groups work together or share resources at some level.

Attack Lifecycle

APT39 uses a variety of custom and publicly available malware and tools at all stages of the attack lifecycle.

1. Initial Access - Spearphishing Attachment (T1193)
2. Initial Access - Spearphishing Link (T1192)
3. Execution - User Execution (T1204)

Initial Compromise

For initial compromise, FireEye Intelligence has observed APT39 leverage spear phishing emails with malicious attachments and/or hyperlinks typically resulting in a POWBAT infection. APT39 frequently registers and leverages domains that masquerade as legitimate web services and organizations that are relevant to the intended target.

Furthermore, this gro 4. Persistence - Web Shell (T1100) ed vulnerable web servers of targeted organizations to install web shells, such as ANTAK and ASPXSPY, and used stolen legitimate credentials to compromise externally facing Outlook Web Access (OWA)

5. Initial Access - Valid Account (T1078)

Establish Foothold, Escalate Privileges, and Internal Reconnaissance

6. Credential Access - Credential Dumping (T1003)

Post-compromise, APT39 leverages custom backdoors such as SEAWEED, CACHEMONEY, and a unique variant of POWBAT to establish a foothold in a ta environment. During privilege escalation, freely available tools such as Mimikatz Ncrack have been observed, in addition to legitimate tools such as Windows Credential Editor and ProcDump. Internal reconnaissance has been performed using custom scripts and both freely available and custom tools such as the port scanner, BLUETORCH.

7. Execution - Scripting (T1064)

8. Discovery - Network Service Scanning (T1046)

L *Presence, and Complete Mission*

A ment through myriad tools such as Remote Desktop Protocol (RDP), Secure Shell (SSH), PsExec, RemCom, and xCmdSvc. Custom tools such as REDTRIP, PINKTRIP, and BLUETRIP have also been used to create SOCKS5 proxies between infected hosts. In addition to using RDP for lateral movement, APT39 has used this protocol to maintain persistence in a victim environment. To complete its mission, APT39 typically archives stolen data with compression tools such as WinRAR or 7-Zip.

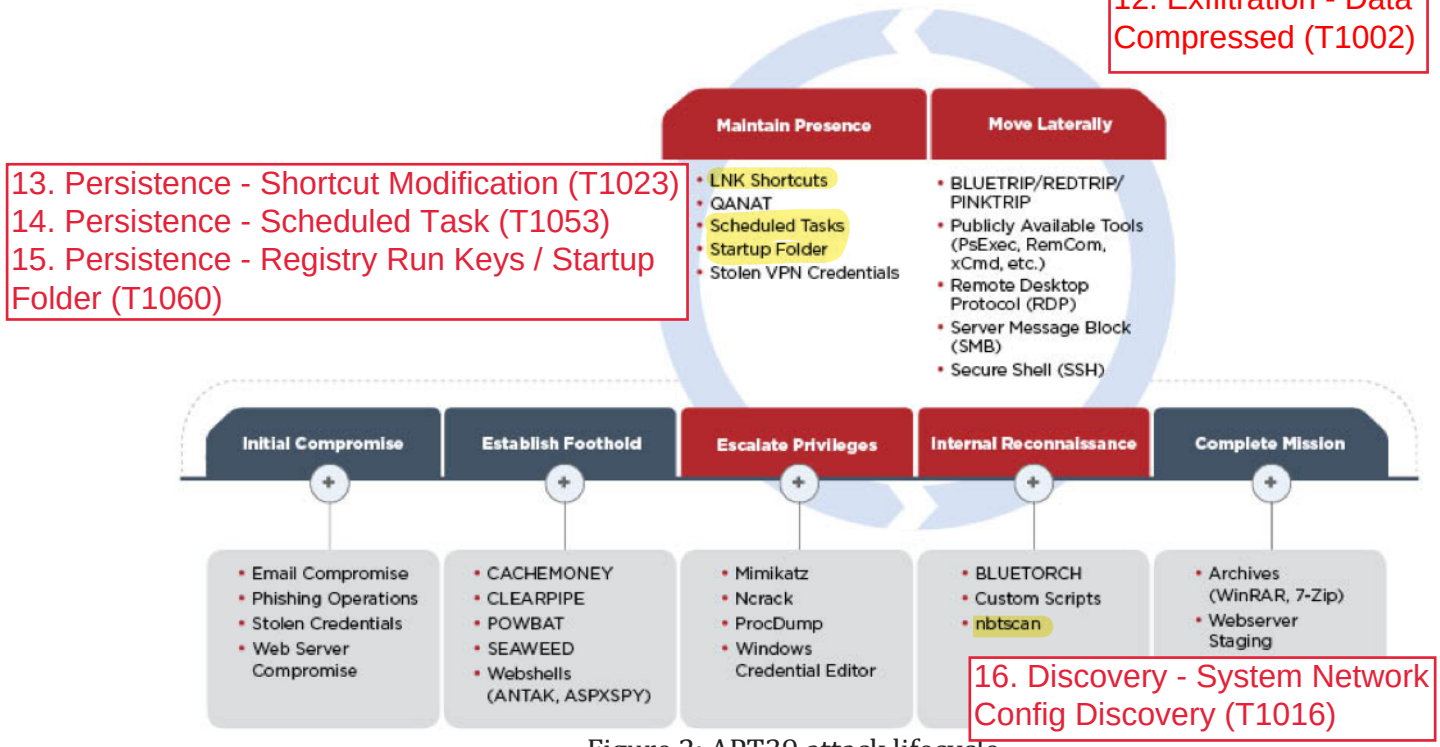

Figure 2: APT39 attack lifecycle

There are some indications that APT39 demonstrated a penchant for operational security to bypass det e of a modified version of Mimikatz that was repacked to thwart anti-virus detection in one case, as well as another instance when after gaining initial access APT39 performed credential harvesting outside of a compromised entity's environment to avoid detection.

Outlook

We believe APT39's significant targeting of the telecommunications and travel industries reflects efforts to collect personal information on targets of interest and customer data for the purposes of surveillance to facilitate future operations. Telecommunications firms are attractive targets given that they store large amounts of personal and customer information, provide access to critical infrastructure used for communications, and enable access to a wide range of potential targets across multiple verticals. APT39's targeting not only represents a threat to known targeted industries, but it extends to these organizations' clientele, which includes a wide variety of sectors and individuals on a global scale. APT39's activity showcases Iran's potential global operational reach and how it uses cyber operations as a low-cost and effective tool to facilitate the collection of key data on perceived national security threats and gain advantages against regional and global rivals.