Latest U.S. Indictments Target Iranian Espionage Actors

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/elfin-indictments-iran-espionage

UPDATE September 22: *We have made some edits to this blog. An earlier version inaccurately described the links to the Elfin group as "strong".*

The U.S. government has indicted three Iranian nationals on charges related to cyber attacks against aerospace and satellite technology companies. Said Pourkarim Arabi, Mohammad Reza Espargham, and Mohammad Bayati are alleged to have carried out a string of attacks between 2015 and 2019 which resulted in the theft of sensitive commercial information, intellectual property, and personal data from targeted organizations.

According to the indictment, Arabi is a member of Iran's Islamic Revolutionary Guard Corps (IRGC) and carried out the attacks with Espargham and Bayati on behalf of the IRGC. Espargham is alleged to be the leader of an Iranian hacking group known as the Iranian Dark Coders Team, while Bayati is alleged to be a malware developer who shared tools with Arabi and Espargham.

The men are said to have obtained the names of individuals working in the aerospace and satellite industry, created fake accounts in their names, and used them to send spear-phishing emails to targeted organizations. If victims clicked on a malicious link within the email, malware would be installed on their computers. Once on the victim's network, the attackers would escalate privileges, steal credentials, move laterally across the network, and deploy further malware on computers before exfiltrating data.

Possible Elfin link?

Although not referenced specifically in the indictment, the attacks appear to have some links to the Elfin (aka APT33) cyber espionage group. Aside from the fact that the targets and tactics described in the indictment closely resemble Elfin activity observed by Symantec, there is also a commonality in tools used. According to the indictment, one of the main malware tools used in the attacks was the Nanocore RAT (Trojan.Nancrat). Although it was publicly available, Symantec has observed Elfin make extensive use of Nanocore. While we haven't observed any other Iranian group utilizing this tool, other vendors have found cases.

Who are Elfin?

Symantec has been tracking Elfin since late 2015. Aside from compromising its victims with spear-phishing emails, the group is also known for scanning for vulnerable websites, either for potential victims or for use as command and control (C&C) infrastructure. To date it has compromised a wide range of targets, including governments along with organizations in the research, chemical, engineering, manufacturing, consulting, finance, telecoms, and several other sectors. Aside from the U.S, Elfin is also heavily focused on targets in Saudi Arabia, which accounted for 42 percent of attacks observed by Symantec between the start of 2016 and March 2019. During this time, Symantec also identified possible links to the destructive Shamoon group.

Recent attacks

Symantec has observed multiple Elfin campaigns over the past 18 months. In February 2019, the group attempted to exploit a known vulnerability (CVE-2018-20250) in WinRAR in order to compromise an organization in the chemical sector in Saudi Arabia.

In June 2019, Elfin sent out a phishing email to hundreds of recipients across multiple countries in what appeared to be an opportunistic trawling attack. The link within the document led recipients to dynamic DNS infrastructure controlled by the group.

Subsequently, in late August 2019, Elfin compromised a victim in Saudi Arabia with a malicious HTA file. Following the initial compromise, Elfin continued to rely on the group's known tools, tactics, and procedures (TTPs) to strengthen its foothold. During the incident, the legitimate utility mshta.exe executed a malicious HTA file with a job application theme. The file was downloaded after a victim used Microsoft Edge to visit a malicious website. A PowerShell command then downloaded a JPG file from a dynamic DNS host spoofing a U.S. defense contractor.

Chafer alert and sanctions

In a separate announcement, the FBI has also issued a new cyber security advisory about an Iranian company called Rana Intelligence Computing Company, which it says is a front for the Chafer (aka APT39) cyber espionage group, which is linked to the Iranian Ministry of Intelligence and Security (MOIS). The FBI said Rana had systematically targeted and monitored Iranian citizens, dissidents, and journalists, along with government networks of Iran's neighboring countries, and foreign organizations in the travel, academic, and telecommunications sectors.

Simultaneously, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) imposed sanctions on Rana, Chafer, and a number of named individuals who work for MOIS.

Chafer has been active since at least July 2014 and its activities were first exposed by Symantec in December 2015, when it was found to be conducting targeted surveillance of domestic and international targets.

In 2018 Symantec observed it mounting a number of ambitious new attacks including the compromise of a major telecoms services provider in the Middle East.

Increased pressure

State-sponsored espionage actors appear to be firmly in the sights of the U.S. Justice and Treasury Departments. These indictments and sanctions may generate an unwelcome amount of publicity and disruption for groups that may have believed they were operating with a degree of anonymity.

Protection/Mitigation

Symantec has the following protection in place to protect customers against Elfin attacks:

File-based protection

- Backdoor.Notestuk
- Trojan.Stonedrill
- Backdoor.Remvio
- Backdoor.Breut
- Trojan.Quasar
- Backdoor.Patpoopy
- Trojan.Nancrat
- Trojan.Netweird.B
- Exp.CVE-2018-20250
- SecurityRisk.LaZagne
- Hacktool.Mimikatz
- SniffPass

Symantec has the following protection in place to protect customers against Chafer attacks:

File-based protection

- Backdoor.Remexi
- Backdoor.Remexi.B
- Hacktool.Mimikatz
- Pwdump

IPS: network-based protection

System Infected: Backdoor.Remexi Activity