Leafminer cyber espionage group targets Middle East

July 27, 2018 By Pierluigi Paganini

Hackers belonging an Iran-linked APT group tracked as 'Leafminer' have targeted government and various organizations in the Middle East.

An Iran-linked APT group tracked as 'Leafminer' has targeted government and businesses in the Middle.

According to the experts from Symantec, the Leafminer group has been active at least since early 2017.

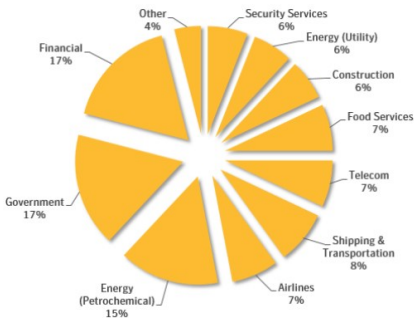
"Symantec has uncovered the operations of a threat actor named Leafminer that is targeting a broad list of government organizations and business verticals in various regions in the Middle East since at least early 2017." reads the analysis published by Symantec.

The experts detected malicious code and hacking tools associated with the cyber espionage group on 44 systems in Saudi Arabia, Lebanon, Israel, Kuwait and other countries.

The extent of the campaigns conducted by the group could be wider, the researchers uncovered a list, written in Iran's Farsi language, of 809 targets whose systems were scanned by the attackers.

The list groups each entry with organization of interest by geography and industry, in includes targets in the United Arab Emirates, Qatar, Bahrain, Egypt, and Afghanistan.

Most of the targets were in the financial, government and energy sectors.



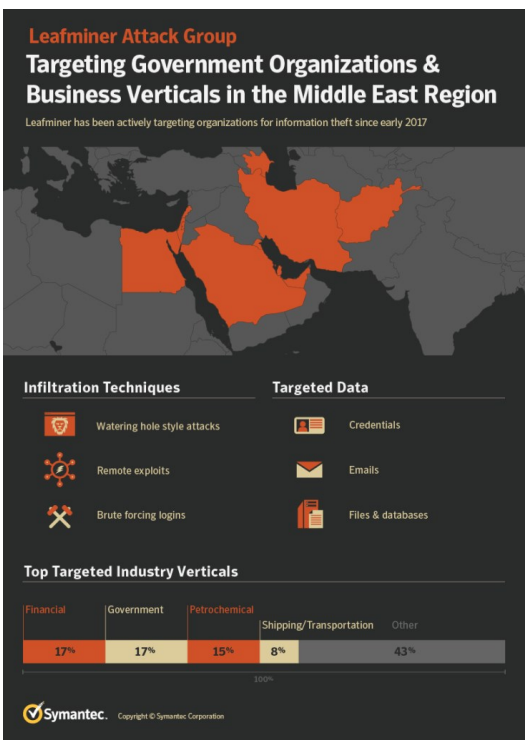
The hackers used publicly available tools and custom-malware in their attacks.

"On a broad level, it has followed the recent trend among targeted attack groups for "living off the land"—using a mixture of publicly available tools alongside its own custom malware." continues the report.

"More specifically, it mimicked Dragonfly's use of a watering hole to harvest network credentials. It also capitalized on the Shadow Brokers release of Inception Framework tools, making use of the leaked Fuzzbunch framework by developing its own exploit payloads for it."

Researchers discovered that hackers used three main techniques for initial intrusion of target networks:

- Compromised web servers used for watering hole attacks
- Scans/exploits for vulnerabilities of network services
- Dictionary attacks against logins of network services



While analyzing the attacks conducted by the group, the experts discovered a download URL for a malware payload used to compromise the victims. The URL pointed out to a compromised web server on the domain e-qht[.]az that had been used to distribute Leafminer malware, payloads, and tools within the group and make them available for download from victim machines.

"As of early June 2018, the server hosted 112 files in a subdirectory that could be accessed through a public web shell planted by the attackers. In addition to malware and tools, the served files also included uploads of log files seemingly originating from vulnerability scans and post-compromise tools." continues the report.

"The web shell is a modification of the PhpSpy backdoor and references the author MagicCoder while linking to the (deleted) domain magiccoder.ir. Researching the hacker handle MagicCoder results in references to the Iranian hacking forum Ashiyane as well as defacements by the Iranian hacker group Sun Army."

Symantec discovered two custom malware used by the Leafminer group, tracked as Trojan.Imecab and Backdoor.Sorgu, the former provides persistent access with a hardcoded password, the latter implements classic backdoor features.

The group also leveraged a modified version of the popular Mimikatz post-exploitation tool. To avoid detection, the group used a technique dubbed Process Doppelgänging, discovered in December 2017 by researchers from Ensilo security firm.

The technique is a fileless code injection method that exploits a built-in Windows function and an undocumented implementation of the Windows process loader.

"However, Leafminer's eagerness to learn from others suggests some inexperience on the part of the attackers, a conclusion that's supported by the group's poor operational security. It made a major blunder in leaving a staging server publicly accessible, exposing the group's entire arsenal of tools," concludes Symantec.

Pierluigi Paganini

(Security Affairs – *Leafminer, hacking*)

Share this...

cyber espionage | Hacking | Iran | Leafminer | Pierluigi Paganini | Security Affairs

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
US-CERT warns of ongoing cyber attacks aimed at ERP applications

NEXT ARTICLE
Dutch brothers sentenced to community service for involvement in CoinVault ransomware distribution

Yoroi Blog