Hacking campaign combines attacks to target government, finance, and energy

By Written by Danny Palmer, Senior WriterSenior Writer July 26, 2018 at 3:02 a.m. PT

Archived: 2026-04-05 17:50:18 UTC

Video: Cyberwar: Nation-state cyber attacks threaten every company

Security

-
-
-
-

A newly-uncovered cyber espionage operation is combining known exploits with custom-built malware in a campaign that has targeted hundreds of organisations, particularly those in the government, finance, and energy sectors.

Discovered by researchers at Symantec, the group is called Leafminer and has been operating out of Iran since at least early 2017.

The malware and custom tools used by Leafminer have been detected across 44 systems in the Middle East: 28 in Saudi Arabia, eight in Lebanon, three in Israel, one in Kuwait, and four in unknown locations -- but the investigation into the campaign found a list of 809 targets.

The attackers' activity suggests the goal of their campaign is to steal data, including emails, credentials, files, and information on database servers operated by compromised targets.

Leafminer uses three main techniques for compromising target networks: watering hole attacks, vulnerabilities in network services, and brute-force dictionary attacks which attempt to crack passwords. Researchers said that phishing emails might also be used, but evidence for this hasn't yet been seen.

It's the watering hole attacks and the discovery of compromised websites which initially led Symantec to Leafminer. The watering hole attacks saw obfuscated JavaScript code left on targeted websites as a means of abusing SMB protocols to retrieve passwords.

Compromised targets included a Lebanese government site, a Saudi Arabian healthcare site, and an Azerbaijan university. Researchers note that the same technique was deployed by the DragonFly hacking group last year -- but rather than being a related attack group, Leafminer appears to be mimicking the earlier attack.

See also: Can Russian hackers be stopped? Here's why it might take 20 years[TechRepublic]

This isn't the only tactic which Leafminer has picked up of successful campaigns by other criminal groups. Leafminer uses EternalBlue -- the leaked NSA vulnerability which powered the WannaCry ransomware -- to move within targeted networks.

The attackers also attempt to scan for Heartbleed, an OpenSSL vulnerability which could allow attackers to see encrypted data. Heartbleed came to light in 2014, but thousands of sites still remain vulnerable.

Another known technique is lifted in order to help exfiltrate data. Known as doppelgänging, the process was revealed late last year and circumvents security tools by using process hollowing to make the malicious processes look benign.

The use of all the above leads Symantec to state that Leafminer actively monitors developers and publications of offensive techniques for ideas.

But the campaign isn't purely based on repurposed attacks deployed by others, as Leafminer has also deployed two strains of custom malware during their campaigns: Imecab and Sorgu.

Imecab is designed to set up persistent remote access to a target machine with a hard-coded password and is installed as a Windows service in order to ensure it remains available to the attacker.

Sorgu is used in a similar fashion, providing remote access to the infected machine and is also installed as a service in the Windows system via a shell command script.

But while the Leafminer group appears keen to learn from other successful espionage campaigns, one thing it has failed at is operational security: researchers uncovered a staging server used by the attackers to be publicly accessible, exposing the group's entire arsenal of tools, indicating inexperience by the attackers.

More: VPN services 2018: The ultimate guide to protecting your data on the internet (TechRepublic)

This public information also led to a list of over 800 potential targets in government, finance, and energy across the Middle East. The list is written in the Iranian Farsi language, leading researchers to conclude that the group is based in Iran, although there's currently no evidence of it being a state-backed campaign.

No matter who is behind the campaign, it's likely that the group will continue to develop offensive techniques -- and they could even widen the scope of malicious attacks.

"It's possible the group would keep adopting and adapting both new publicly available hacking tools and techniques, as well as proof-of-concept exploits for new and old vulnerabilities," Armin Buescher, threat researcher at Symantec, told ZDNet.

"In terms of targeting, the attackers might continue going after targets in the Middle East, perhaps even expanding to countries outside of the region."

Related coverage

Hacking campaign targets iPhone users with data-stealing, location-tracking malware

Campaign delivers fake versions of WhatsApp and Telegram to victims - and those behind it have tried to make it look like a Russian attack when it isn't.

Phishing alert: Hacking gang turns to new tactics in malware campaign

Security company warns 'SilverTerrier' group poses a threat to businesses.

Securing the power grid from hacking, sabotage, and other threats

Frank Gaffney, founder and president of the Center for Security Policy, talks about securing the power grid from EMP, hacking, sabotage, and solar flares. He thinks transformers are the key element.

READ MORE ON CYBER CRIME

- Fourth-generation Android espionage campaign targets Middle East
- China-based espionage campaign targets satellite, defense companies [CNET]
- Chafer: Hacking group expands espionage operation with new attacks
- Beware of Russian attackers impersonating LoJack security software to hack computers [TechRepublic]
- Espionage malware snoops for passwords, mines bitcoin on the side

---

Source: https://www.zdnet.com/article/hacking-campaign-combines-attacks-to-target-government-finance-and-energy/