Iranian state hackers reload their domains, release off-the-shelf RAT malware

Enlarge / Iran’s hacking groups are scaling up, hitting Saudi companies and other organizations, according to a Recorded Future report.

reader comments

29 with 22 posters participating

Share this story

A new report from the threat research firm Recorded Future finds that activity from APT33—the Iranian “threat group” previously tied to the Shamoon wiper attack and other Iranian cyber-espionage and destructive malware attacks—has risen dramatically, with the organization creating over 1,200 domains for use in controlling and spreading malware. The research, conducted by Recorded Future’s Insikt Group threat intelligence service, found with some confidence that individuals tied to APT33 (also known as “Elfin”) had launched attacks on multiple Saudi companies, including two healthcare organizations—as well as an Indian media company and a “delegation from a diplomatic institution.”

The majority of these attacks have involved “commodity” malware—well-known remote access tools (RATs). According to the report:

> *APT33, or a closely aligned threat actor, continues to control C2 domains in bulk. Over 1,200 domains have been in use since March 28, 2019, alone. Seven hundred twenty-eight*

> *of these were identified communicating with infected hosts. Five hundred seventy-five of the 728 domains were observed communicating with hosts infected by one of 19 mostly publicly available RATs. Almost 60% of the suspected APT33 domains that were classified to malware families related to njRAT infections, a RAT not previously associated with APT33 activity. Other commodity RAT malware families, such as AdwindRAT and RevengeRAT, were also linked to suspected APT33 domain activity.*

After Symantec revealed much of the infrastructure used by APT33 in March, the Iranian group parked a majority of its existing domains and registered over 1,200 new ones, with only a few remaining active. In addition to the collection of RATs, about a quarter of the domains are tied to unknown activity—and a half-percent are connected to StoneDrill, the upgraded Shamoon wiper first seen in 2017.

Can't tell the players without a scorecard

The use of publicly available malware is a common part of APT33's operations, as is the operation of massive command and control infrastructures. Much of Iran's cyber-operations are apparently contracted out through a hierarchy that is managed by the Nasr Institute, Iran's state organization overseeing computing and networking. The institute acts on behalf of the Iranian Government and Iranian Revolutionary Guard Corps.

According to the Insikt Group research, operations are divided into compartmentalized operations across about 50 different contracted organizations. As a result, there's some overlap between APT33's activities and other Iranian state-sponsored threat groups. These organizations "conducted activities such as vulnerability research, exploit development, reconnaissance, and the conducting of network intrusions or

attacks," according to data from an Iniskit Group source, and "each of these discrete components, in developing an offensive cyber capability, were purposefully assigned to different contracting groups to protect the integrity of overarching operations," the researchers reported.

One of these contractors, the research determined, is the Kavosh Security Center, an information security organization tied to the "Muddywater" threat group responsible for espionage against a Turkish military supplier.

The use of commodity malware makes many of these operations technically indistinguishable from criminal activity aside from infrastructure—and intent. Many of the attacks are based on phishing, brute-force attacks such as "credential stuffing" and other common criminal tactics.

"Organizations in industries that have been historically targeted by APT33″—such as aviation, military, and energy companies—"should be increasing the scrutiny of operational security controls focusing on detection and remediation of initial unauthorized access, specifically from phishing campaigns, webshells, and third-party (vendor and supplier) relationships," the Iniskit researchers noted. That statement matches up with the warnings issued recently by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

https://arstechnica.com/?p=1528015