DHS cyber director warns of surge in Iranian “wiper” hack attacks



Enlarge / An effective wiper of sorts.
Getty Images

reader comments

51 with 32 posters participating, including story author

Share this story

With tensions between the US and Iran on the rise following the downing of a US military drone last week, the director of the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency is warning that Iran is elevating its efforts to do damage to US interests through destructive malware attacks on industrial and government

networks.

In a statement issued on Saturday, June 22, CISA Director Christopher C. Krebs said:

> *CISA is aware of a recent rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies. Iranian regime actors and proxies are increasingly using destructive "wiper" attacks, looking to do much more than just steal data and money. These efforts are often enabled through common tactics like spear phishing, password spraying, and credential stuffing. What might start as an account compromise, where you think you might just lose data, can quickly become a situation where you've lost your whole network.*

Krebs urged businesses and agencies to take steps to improve their security hygiene, including implementing multi-factor authentication for user credentials to prevent brute-force attempts to connect to exposed network and cloud applications.

A brief history of Iranian(?) wipers

There have been allegations of Iranian-backed wiper attacks in the past—the most infamous of which is Shamoon, a family of malware that first emerged in an attack against Saudi Aramco in August of 2012.

Shamoon, which in its first outing took down approximately 30,000 workstations, was launched after a state-sponsored wiper attack against Iran in April of that year. It's believed to be connected to the same (US-Israeli) state-sponsored development team that built the Stuxnet malware that attacked Iranian nuclear labs. Tied to the suspected Iranian "threat group" APT33, Shamoon was refreshed for another attack against multiple Saudi targets in December 2016.

Other wiper attacks from Iran have been somewhat less sophisticated. In January of 2014 after Las Vegas Sands Corp. majority owner Sheldon Adelson called for a nuclear attack on Iran, Iranian hacktivists used a Visual Basic-based malware attack to wipe the drives of Sands' computers.

Most other recent Iran-attributed attacks have focused on data theft—including attacks focused on aviation and energy companies. In 2015, a group tied to the Iranian Revolutionary Guard Corps used spear-phishing attacks to compromise computers at the US State Department, stealing data that may have led to the arrest of multiple Iranians holding dual US citizenship. Other attacks attributed to Iran have focused on taking down Web servers at financial institutions.

Cyber-escalation

While President Donald Trump called off a planned military strike last Friday in response to the downing of the drone, the Department of Defense has reportedly gone ahead with cyber attacks against an Iranian intelligence group connected to attacks against oil tankers in the Persian Gulf. Another cyber attack reportedly targeted Iranian missile fire control systems.

It's not clear the form these attacks took. And in a post to Twitter today, Iran's Minister for Information Mohammad Javad Azari Jahromi claimed that the cyber attacks were unsuccessful, Reuters reports.

https://arstechnica.com/?p=1526641