Thursday, March 12, 2026

tomorrowsaffairs.com

TA Tomorrow's Affairs

Analysis of today
Assessment of tomorrow

By: TA | AP Insight

Attacks by pro-Iranian hackers are spreading in the West and the Middle East

Pro-Iranian hackers are targeting sites in the Middle East and starting to stretch into the United States during the war, raising the risk of American defense contractors, power stations and water plants being swept into a wave of digital chaos that could expand if Tehran's allies join the fray.

Hackers supporting Iran claimed responsibility for a significant cyberattack Wednesday against U.S. medical device company Stryker.

Since the war began Feb. 28, they also have tried to penetrate cameras in Middle Eastern countries to improve Iran's missile targeting.

They have targeted data centers in the region, as well as industrial facilities in Israel, a school in Saudi Arabia and an airport in Kuwait.

Iran has invested heavily in its offensive cyber capabilities while cultivating ties to hacking groups.

In recent years, groups working for Tehran have infiltrated the email system of President Donald Trump's campaign, targeted U.S. water plants and tried to breach the networks used by the military and defense contractors.

The goal is to wear down the American war effort, drive up the costs of energy, strain cyber resources and cause as much pain as possible for American companies that depend on the defense industry.

“Something is going to happen because the gloves are off," said Kevin Mandia, founder of the cybersecurity companies Mandiant and Armadin.

Who is being targeted

Pro-Iranian, pro-Palestinian hackers claimed credit for disrupting systems at Stryker, a Michigan-based medical technology company.

A group known as Handala said the attack was in retaliation for suspected U.S. strikes that killed Iranian schoolchildren.

Like other ideologically motivated hackers, profit is not Handala’s goal, according to Ismael Valenzuela, vice president of threat intelligence at the cybersecurity company Arctic Wolf.

“What distinguishes this group is its clear focus on data destruction rather than financial extortion,” he said in an email.

> Pro-Iranian hackers openly discuss their plans in Telegram and other online message boards

Polish authorities are investigating a recent cyberattack — on a nuclear research facility — that may have ties to Iran, though they acknowledge that another group could be behind the attack and using the Iran war to mask its identity.

Going forward, U.S. defense contractors, government vendors and businesses that work with Israel are likely targets, as is critical infrastructure such as hospitals, ports, water plants, power stations and railways.

Pro-Iranian hackers openly discuss their plans in Telegram and other online message boards.

“The datacenters need to be taken out,” wrote one user, as uncovered by researchers at U.S.-based SITE Intelligence Group. “They host the brains of USAs military communication and targeting systems.”

Cyber operations also gather intelligence — for example, Iran's effort to hack into cameras in neighboring countries to aid its missile targeting.

Infiltrating U.S. networks, meanwhile, would offer view into military planning or supply chains.

Going after easy targets

The strikes on Iran's military as well as internet outages may have limited Iran's cyberattacks in the short term.

But experts say Iranian hackers and their allies will aim for quick victories by targeting the weakest links in American cybersecurity.

Often, local water plants or health care facilities lack the funds and know-how to install the latest software patches or take other security steps.

That has made them a favorite target, both because of the relative ease of penetrating them and because of the panic these disruptions can cause.

> If a business or government agency has failed to keep up with its cybersecurity, it could pay a steep price

This can include denial-of-service attacks, in which hackers try to jam a network so legitimate users cannot use it, and website defacements, which can prevent a company from communicating with customers.

Hack-and-leak operations, where hackers threaten to release sensitive stolen material, are another possibility.

The attacks are not that sophisticated, according to Shaun Williams, a former FBI and CIA officer who is now a senior director at the cybersecurity firm SentinelOne.

But if a business or government agency has failed to keep up with its cybersecurity, it could pay a steep price, he said.

“Patch your systems. Ensure your firewalls and security solutions are up to date,” Williams said. “Remove your stale accounts. All the cyber hygiene that you should be doing, it’s more critical now than ever. Prepare for disruption.”

When it comes to cyber, Iran is considered a chaos agent

Russia and China present the greatest cyber threats to the U.S., while North Korea is a growing concern. But what Iran has lacked in resources it has made up for in ingenuity, experts say.

In recent years, Tehran's digital warriors have impersonated American activists online to covertly encourage protests against Israel on college campuses.

In 2024, Iranian hackers infiltrated the email system of the Trump campaign and later tried to disseminate files that the hackers said they stole

They have set up fake news websites and social media accounts primed to spread false and exaggerated claims before big U.S. elections.

In 2024, Iranian hackers infiltrated the email system of the Trump campaign and later tried to disseminate files that the hackers said they stole.

Hackers linked to Iran also tried to hack into the WhatsApp accounts of both Trump and his then-Democratic opponent, President Joe Biden.

The activity prompted the Department of Homeland Security to issue a public warning last year about Iranian cyber threats.

“Iran and especially the proxies don’t care how big or smart you are. This is about making an impact, about creating chaos,” said James Turgal, a cybersecurity expert who spent 22 years as an FBI agent and is now a vice president at Optiv, a Denver-based information security firm.

Next moves from Russia and China

Experts are watching closely to see if Russia, China or hacking groups allied with either country provide hacking assistance to Iran, mounting attacks intended to undermine American operations in Iran and make it harder for the U.S. to sustain its fight.

While China has so far taken a cautious approach, there is evidence that pro-Iranian hackers in Russia are already at work.

> The timing of the attack suggests the hackers were targeting U.S. interests because of the war in Iran

Researchers at the cybersecurity firm CrowdStrike detected a surge of activity from Russian hackers in support of Tehran since the war began.

One group known as Z-Pentest claimed responsibility for disrupting several U.S. networks, including some involved in closed-circuit video cameras.

The timing of the attack suggests the hackers were targeting U.S. interests because of the war in Iran, according to Adam Meyers, head of counter adversary operations at CrowdStrike.

“Western organizations should continue to remain on high-alert,” Meyers said.