AP sources: US struck Iranian military computers this week

AP sources: US struck Iranian military computers this week

1. Top Stories

2. Topics
3. Video
4. Listen
5.

By TAMI ABDOLLAH56 minutes ago

FILE - In this Thursday, Aug. 31, 2017, file photo, a flame burns at the Shell Deer Park oil refinery in Deer Park, Texas. Iran has increased its offensive cyberattacks against the U.S. government and critical infrastructure as tensions have grown between the two nations, cybersecurity firms say. In recent weeks, hackers believed to be working for the Iranian government have targeted U.S. government agencies, as well as sectors of the economy, including oil and gas, sending waves of spear-phishing emails, according to representatives of cybersecurity companies CrowdStrike and FireEye, which regularly track such activity. (AP Photo/Gregory Bull, File)

WASHINGTON (AP) — U.S. military cyber forces launched a strike against Iranian military computer systems on Thursday as President Donald Trump backed away from plans for a more conventional military strike in response to Iran’s downing of a U.S. surveillance drone, U.S. officials said Saturday.

Two officials told The Associated Press that the strikes were conducted with approval from Trump. A third official confirmed the broad outlines of the strike. All spoke on condition of anonymity because they were not authorized to speak publicly about the operation.

The cyberattacks — a contingency plan developed over weeks amid escalating tensions — disabled Iranian computer systems that controlled its rocket and missile launchers, the officials said. Two of the officials said the attacks, which specifically targeted Iran’s Islamic Revolutionary Guard Corps computer system, were provided as options after Iranian forces blew up two oil tankers earlier this month.

The IRGC, which was designated a foreign terrorist group by the Trump administration earlier this year, is a branch of the Iranian military.

The action by U.S. Cyber Command was a demonstration of the U.S.’s increasingly mature cyber military capabilities and its more aggressive cyber strategy under the Trump administration. Over the last year U.S. officials have focused on persistently engaging with adversaries in cyberspace and undertaking more offensive operations.

There was no immediate reaction Sunday morning in Iran to the U.S. claims. Iran has hardened and disconnected much of its infrastructure from the internet after the Stuxnet computer virus, widely believed to be a joint U.S.-Israeli creation, disrupted thousands of Iranian centrifuges in the late 2000s.

Tensions have escalated between the two countries ever since the U.S. withdrew last year from the 2015 nuclear deal with Iran and began a policy of “maximum pressure.” Iran has since been hit by multiple rounds of sanctions. Tensions spiked this past week after Iran shot down an unmanned U.S. drone — an incident that nearly led to a U.S. military strike against Iran on Thursday evening.

The cyberattacks are the latest chapter in the U.S. and Iran's ongoing cyber operations targeting the other. Yahoo News first reported the cyber strike.

In recent weeks, hackers believed to be working for the Iranian government have targeted U.S. government agencies, as well as sectors of the economy, including finance, oil and gas, sending waves of spear-phishing emails, according to representatives of cybersecurity companies CrowdStrike and FireEye, which regularly track such activity. This new campaign appears to have started shortly after the Trump administration imposed sanctions on the Iranian petrochemical sector this month.

It was not known if any of the hackers managed to gain access to the targeted networks with the emails, which typically mimic legitimate emails but contain malicious software.

Tensions have run high between the two countries since the U.S. withdrew from the 2015 nuclear deal with Iran last year and began a policy of "maximum pressure." Iran has since been hit by multiple rounds of sanctions. Then Iran shot down an unmanned U.S. drone this week.

"Both sides are desperate to know what the other side is thinking," said John Hultquist, director of intelligence analysis at FireEye. "You can absolutely expect the regime to be leveraging every tool they have available to reduce the uncertainty about what's going to happen next, about what the U.S.'s next move will be."

CrowdStrike shared images of the spear-phishing emails with the AP.

One such email that was confirmed by FireEye appeared to come from the Executive Office of the President and seemed to be trying to recruit people for an economic adviser position. Another email was more generic and appeared to include details on updating Microsoft Outlook's global address book.

The Iranian actor involved in the cyberattack, dubbed "Refined Kitten" by CrowdStrike, has for years targeted the U.S. energy and defense sectors, as well as allies such as Saudi Arabia and the United Arab Emirates, said Adam Meyers, vice president of intelligence at CrowdStrike.

The Department of Homeland Security said in a statement released Saturday that its agency tasked with infrastructure security has been aware of a recent rise in malicious cyber activities directed at U.S. government agencies by Iranian regime actors and proxies.

Cybersecurity and Infrastructure Security Agency Director Christopher C. Krebs said the agency has been working with the intelligence community and cybersecurity partners to monitor Iranian cyber activity and ensure the U.S. and its allies are safe.

"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 said.

The National Security Agency would not discuss Iranian cyber actions specifically, but said in a statement to the AP on Friday that "there have been serious issues with malicious Iranian cyber actions in the past."

"In these times of heightened tensions, it is appropriate for everyone to be alert to signs of Iranian aggression in cyberspace and ensure appropriate defenses are in place," the NSA said.

Iran has long targeted the U.S. oil and gas sectors and other critical infrastructure, but those efforts dropped significantly after the nuclear agreement was signed. After Trump withdrew the U.S. from the deal in

May 2018, cyber experts said they have seen an increase in Iranian hacking efforts.

“This is not a remote war (anymore),” said Sergio Caltagirone, vice president of threat intelligence at Dragos Inc. “This is one where Iranians could quote unquote bring the war home to the United States.”

Caltagirone said as nations increase their abilities to engage offensively in cyberspace, the ability of the United States to pick a fight internationally and have that fight stay out of the United States physically is increasingly reduced.

The U.S. has had a contentious cyber history with Iran.

In 2010, the so-called Stuxnet virus disrupted the operation of thousands of centrifuges at a uranium enrichment facility in Iran. Iran accused the U.S. and Israel of trying to undermine its nuclear program through covert operations.

Iran has also shown a willingness to conduct destructive campaigns. Iranian hackers in 2012 launched an attack against state-owned oil company Saudi Aramco, releasing a virus that erased data on 30,000 computers and left an image of a burning American flag on screens.

In 2016, the U.S. indicted Iranian hackers for a series of punishing cyberattacks on U.S. banks and a small dam outside of New York City.

The Defense Department refused to comment on the latest Iranian activity. “As a matter of policy and for operational security, we do not discuss cyberspace operations, intelligence or planning,” Pentagon spokeswoman Heather Babb said in a statement. The White House did not respond to a request for comment.

Despite the apparent cyber campaign, experts say the Iranians would not necessarily immediately exploit any access they gain into computer systems and may seek to maintain future capabilities should their relationship with the U.S. further deteriorate.

“It’s important to remember that cyber is not some magic offensive nuke you can fly over and drop one day,” said Oren Falkowitz, a former National Security Agency analyst. It takes years of planning, he said, but as tensions increase, “cyber impact is going to be one of the tools they use and one of the hardest things to defend against.”

___

Associated Press writer Lolita C. Baldor in Washington and Jon Gambrell in Dubai contributed to this report. Follow Tami Abdollah on Twitter at https://twitter.com/latams