https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036

BUSINESS

Iranian Hackers Have Hit Hundreds of Companies in Past Two Years

Cyberattack campaign has caused damages estimated at hundreds of millions of dollars, focusing on Middle East but also affecting U.S.

Italian oil company Saipem was hit by the hackers. **PHOTO:** IGOR GOLOVNIOV/SOPA IMAGES/ZUMA PRESS

By Robert McMillan

Updated March 6, 2019 7:28 pm ET

Cyberattacks linked to Iranian hackers have targeted thousands of people at more than 200 companies over the past two years, Microsoft Corp. MSFT **0.01%** ▲ said, part of a wave of computer intrusions from the country that researchers say has hit businesses and government entities around the globe.

The campaign, the scope of which hadn't previously been reported, stole corporate secrets and wiped data from computers. It caused damages estimated at hundreds of millions of dollars in lost productivity and affected oil-and-gas companies, heavy-machinery manufacturers and international conglomerates in more than a half-dozen countries including Saudi Arabia, Germany, the U.K., India and the U.S., according to researchers at Microsoft, which deployed incident-response teams to some of the affected companies.

“These destructive attacks...are massively destabilizing events,” said John Lambert, the head of Microsoft’s Threat Intelligence Center.

Microsoft traced the attacks to a group it calls Holmium. It is one of several linked by other researchers over the past year to hackers in Iran, a country that many security researchers say aspires to join Russia and China as one of the world’s premier cyber powers. Some of Holmium’s hacking was done by a group that other security companies call APT33, Microsoft said.

Iran “denies any involvement in cyber crimes against any nation,” said a spokesman for Iran’s mission to the United Nations in an email. He called the cybersecurity research by Microsoft and other companies “essentially ads, not independent or academic studies,” that should not be taken at face value.

While American and European companies have been hit, security researchers say the attacks from Iran have focused heavily on the Middle East.

But they say Iran’s growing cyber strength poses a potential threat to the U.S. at a time of intensified tension between the two countries.

“They’re definitely sharpening their skills and moving up their capabilities,” said John Hultquist, director of intelligence analysis at the cybersecurity firm FireEye Inc. “When they turn their attention back to the United States, we may be surprised by how much more advanced they are.”

One target hit by APT33 is Italian oil company Saipem SPM **-1.05%** ▼ SpA. A December attack wiped data and affected computer infrastructure at company facilities in the Middle East, India, Scotland and Italy, according to Saipem.

Microsoft has been tracking Holmium for nearly four years. Activity surged in late 2018, according to Microsoft and other companies following the group.

To date, Mr. Lambert and his researchers have seen Holmium target more than 2,200 people across about 200 organizations with phishing emails that, if clicked, can install code that steals information or wipes data from computers on the victim’s network.

In a phishing email sent to a victim and viewed by The Wall Street Journal, Holmium attackers copied a legitimate job advertisement from a Saudi Arabian oil-and-gas company and sent it to a worker with oil-industry expertise. When clicked on, the email led to a website that then attempted to download malicious software onto the victim’s computer.

In January, FireEye warned that Iran-linked hackers were using another technique to break into corporate networks, hitting an “almost unprecedented” number of victims world-wide with a high degree of success.

FireEye said in a blog post that the hackers had been manipulating the critical DNS, or domain name service, records of companies—often telecommunications and internet service providers based in the Middle East—monitoring targets' internet traffic to read email messages and steal usernames and passwords.

FireEye observed at least 50 entities—including corporations, universities and government agencies—hit by this attack, but said it suspected many more victims.

Two weeks after FireEye's warning, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency issued a warning about this type of attack, saying the technique, called DNS hijacking, was also being used against the U.S. government.

However, security researchers, including FireEye, say there isn't enough evidence to know whether Iran was involved in the U.S.-focused attacks or hackers from a different country launched them using the same techniques.

Researchers agree that the Iran-linked attacks don't rely on "zero day" exploits, or those leveraging previously undisclosed flaws in computer products. Zero-day attacks are the hallmark of elite hacking groups.

While the attacks tied to Iran use less sophisticated tactics, they often cast a wide net.

Last year, Facebook Inc. removed dozens of pages that it had tied to an Iranian influence operation. Months before that, federal authorities charged nine Iranians with launching cyberattacks that hit 144 American universities, 36 U.S. companies and five American government agencies between 2013 and 2017.

Symantec Corp. tracked another campaign it linked to Iran in which hackers went after 800 organizations over the course of the past two years. The unusually large target list shows that the hackers aren't using the kind of precise targeting typically associated with a nation-state attacker, said Vikram Thakur, a researcher with Symantec. Typical nation-state campaigns would focus on fewer than 100 entities, he said.

"No one attacks 800 organizations on purpose," he said. "It just shows that these people were being very opportunistic."

Another Iranian-linked group also has hit more than 200 government agencies, oil-and-gas companies and technology companies including Citrix Systems Inc., according to the security firm Resecurity International Inc. Using a technique described in an alert issued by the Department of Homeland Security last year, the hackers guess the passwords for corporate email accounts, then steal data that they use to burrow further into corporate networks.

A Citrix spokesman confirmed that a single employee account was compromised in 2018 due to a weak password and that the hacker then used that access to obtain "an old version of a list containing Citrix employee work contact information."

The Citrix attack is worrying because the software maker builds widely used remote-access products that could be misused by hackers to gain unauthorized access to other corporate networks. Citrix says it has seen no evidence of any compromise beyond that single account. The company has also "not found any evidence of state-sponsored activity," the spokesman said in an email.

Write to Robert McMillan at Robert.Mcmillan@wsj.com