Exclusive: Hackers acting in Turkey's interests believed to be behind recent cyberattacks - sources

reuters.com/article/us-cyber-attack-hijack-exclusive/exclusive-hackers-acting-in-turkeys-interests-believed-to-be-behind-recent-cyberattacks-sources-idUSKBN1ZQ10X

Jack Stubbs, Christopher Bing, Joseph Menn

Internet News
Updated

By Jack Stubbs, Christopher Bing, Joseph Menn

7 Min Read

LONDON (Reuters) - Sweeping cyberattacks targeting governments and other organizations in Europe and the Middle East are believed to be the work of hackers acting in the interests of the Turkish government, three senior Western security officials said.

FILE PHOTO: A man waves a Turkish flag at the courtyard of the Grand Camlica Mosque in Istanbul, Turkey, May 3, 2019. REUTERS/Murad Sezer

The hackers have attacked at least 30 organizations, including government ministries, embassies and security services as well as companies and other groups, according to a Reuters review of public internet records. Victims have included Cypriot and Greek government email services and the Iraqi government's national security advisor, the records show.

The attacks involve intercepting internet traffic to victim websites, potentially enabling hackers to obtain illicit access to the networks of government bodies and other organizations.

According to two British officials and one U.S. official, the activity bears the hallmarks of a state-backed cyber espionage operation conducted to advance Turkish interests.

The officials said that conclusion was based on three elements: the identities and locations of the victims, which included governments of countries that are geopolitically significant to Turkey; similarities to previous attacks that they say used infrastructure registered from Turkey; and information contained in confidential intelligence assessments that they declined to detail.

The officials said it wasn't clear which specific individuals or organizations were responsible but that they believed the waves of attacks were linked because they all used the same servers or other infrastructure.

Turkey's Interior Ministry declined to comment. A senior Turkish official did not respond directly to questions about the campaign but said Turkey was itself frequently a victim of cyberattacks.

The Cypriot government said in a statement that the "relevant agencies were immediately aware of the attacks and moved to contain" them. "We will not comment on specifics for reasons of national security," it added.

Officials in Athens said they had no evidence the Greek government email system was compromised. The Iraqi government did not respond to requests for comment.

The Cypriot, Greek and Iraqi attacks identified by Reuters all occurred in late 2018 or early 2019, according to the public internet records. The broader series of attacks is ongoing, according to the officials as well as private cybersecurity investigators.

A spokeswoman for the UK's National Cyber Security Centre, which is part of the GCHQ signals intelligence agency, declined to comment on who was behind the attacks. In the United States, the Office of the Director of National Intelligence declined to comment on who was behind the attacks and the Federal Bureau of Investigation did not respond to a request for comment.

HIJACKED

The attacks highlight a weakness in a core pillar of online infrastructure that can leave victims exposed to attacks that happen outside their own networks, making them difficult to detect and defend against, cybersecurity specialists said.

The hackers used a technique known as DNS hijacking, according to the Western officials and private cybersecurity experts. This involves tampering with the effective address book of the internet, called the Domain Name System (DNS), which enables computers to match website addresses with the correct server.

By reconfiguring parts of this system, hackers were able to redirect visitors to imposter websites, such as a fake email service, and capture passwords and other text entered there.

Reuters reviewed public DNS records, which showed when website traffic was redirected to servers identified by private cybersecurity firms as being controlled by the hackers. All of the victims identified by Reuters had traffic to their websites hijacked - often traffic visiting login portals for email services, cloud storage servers and online networks -- according to the records and cybersecurity experts who have studied the attacks.

The attacks have been occurring since at least early 2018, the records show.

While small-scale DNS attacks are relatively common, the scale of these attacks has alarmed Western intelligence agencies, said the three officials and two other U.S. intelligence officials. The officials said they believed the attacks were unrelated to a campaign using a similar attack method uncovered in late 2018.

As part of these attacks, hackers successfully breached some organizations that control top-level domains, which are the suffixes that appear at the end of web addresses immediately after the dot symbol, said James Shank, a researcher at U.S. cybersecurity firm Team Cymru, which notified some of the victims.

VICTIMS

Victims also included Albanian state intelligence, according to the public internet records. Albanian state intelligence had hundreds of usernames and passwords compromised as a result of the attacks, according to one of the private cybersecurity investigators, who was familiar with the intercepted web traffic.

The Albanian State Information Service said the attacks were on non-classified infrastructure, which does not store or process any “any information classified as ‘state secret’ of any level.”

Civilian organizations in Turkey have also been attacked, the records show, including a Turkish chapter of the Freemasons, which conservative Turkish media has said is linked to U.S.-based Muslim cleric Fethullah Gulen accused by Ankara of masterminding a failed coup

attempt in 2016.

The Great Liberal Lodge of Turkey said there were no records of cyberattacks against the hijacked domains identified by Reuters and that there had been “no data exfiltration.”

“Thanks to precautions, attacks against the sites are not possible,” a spokesman said, adding that the cleric has no affiliation with the organization.

The cleric has publicly denied masterminding the attempted coup, saying “it’s not possible,” and has said he is always against coups.

A spokesman for Gulen said Gulen was not involved in the coup attempt and has repeatedly condemned it and its perpetrators. Gulen has never been associated with the Freemason organization, the spokesman added.

Jack Stubbs reporting in London, Christopher Bing reporting in Washington and Joseph Menn reporting in San Francisco.; Additional reporting by Michele Kambas and Renee Maltezou in Athens, Ece Toksabay in Ankara, Can Sezer in Istanbul, John Davison in Baghdad and Benet Koleka in Tirana.; Editing by Cassell Bryan-Low and Jonathan Weber

Our Standards: The Thomson Reuters Trust Principles.