# Iran sharpens cyber tools for foreign policy ends

Thursday, March 21, 2019

Iran's cyber capability has matured significantly, but sophistication does not automatically lead to increased threat

A statuette of the late Apple co-founder Steve Jobs is displayed next to Apple iPhone 4S packaging at a shop window in Payetakht (Capital) computer centre in northern Tehran January 19, 2012 (Reuters/Morteza Nikoubazl)

During the recent US government shutdown, the Department for Homeland Security (DHS) issued an emergency directive regarding a complex cyber espionage campaign probably linked to Iran against "multiple executive branch agencies". For many, this incident indicated a clear increase in the cyber threat posed by Iran.

## What next

Iran will primarily use its cyber tools to exfiltrate data rather than damage infrastructure. It will build its offensive capabilities but probably reserve them for a crisis or wider confrontation with adversaries such as the United States, Israel and the Gulf states.

## Subsidiary Impacts

◦ Iran will build on existing areas of individual expertise and proven technical tactics.

◦ It will seek to influence internet traffic.

◦ Espionage will be the main motivation behind Iranian cyberactivity.

## Analysis

In January, US Director for National Intelligence Daniel Coats identified three aspects of the cyber threat from Iran, claiming it:

- possessed increasingly sophisticated espionage techniques;
- had used online and social media influence campaigns against the United States and allied countries; and
- is developing the capability to attack critical infrastructure.

At least six US civilian agencies were reportedly affected by the espionage campaign.

The campaign was first publicly reported by cybersecurity company CISCO Talos in November 2018. Its claimed novelty and sophistication are due to its exploitation of the Domain Name System (DNS), the worldwide registry associating internet protocol (IP) addresses and web domains.

To access a particular domain, a device must first request the IP address for that domain from domain name servers, which are either specific servers within an organisation's infrastructure or provided by external hosting companies. Specific accredited companies provide the core DNS functions for generic (.com, .org) or country-level domains.

CISCO Talos identified two malicious uses of DNS:

- It found a new piece of malware communicating with servers controlled by the malicious actor via both HTTP (the standard internet protocol) and through DNS queries. These queries were crafted to communicate information about the infected device, and to execute new commands.
- It detailed the compromise of domain name servers in the victim's infrastructure that were then used to redirect traffic to servers controlled by the malicious actor. Victims included the Lebanese and UAE governments, and the Lebanese national airline.

A report by cybersecurity company FireEye in January 2019 identified similar activity beginning in January 2017, extending the victim list to companies and governments across the Middle East, North Africa, Europe and the United States.

FireEye concluded the campaign was conducted by Iranian state-linked actors.

Later analyses indicated that compromised organisations included foreign ministries, intelligence services, police bodies and embassies in several Arab states. The list includes states not necessarily hostile to Tehran but where intelligence on domestic developments would aid its regional strategy, including Iraq, Jordan, Lebanon and Egypt.

Targets included the Albanian police force and State Intelligence Service. Since 2013, Albania has been the base for the Iranian anti-government organisation Mojahedin-e Khalq, formerly designated a terrorist group by the US State Department, and an obvious target for Iranian cyberespionage.

## New sophistication

Such a sophisticated campaign requires a good understanding of DNS, DNS encryption and the particular characteristics of victim domains, implying widespread access to these domains.

Suspected Iranian state-linked actors have historically sought to obtain intelligence through compromised systems, notably through access to the Dutch certificate authority DigiNotar in 2011.

However, there was no indication that Iranian state-linked actors previously possessed the ability to manipulate DNS traffic in this way. It also required multiple intrusion vectors to compromise the victim organisations and DNS registrars.

## Espionage

The DNS-based espionage campaign follows several other cyberespionage activities by Iranian-linked groups.

In 2017, cybersecurity company Palo Alto Networks reported on the most prolific Iranian cyber espionage group up to that point. This group -- nicknamed Oilrig -- targeted a similarly broad list of organisations to the DNS-based campaign, and used similar techniques.

Other campaigns, identified by cybersecurity company Symantec, included one aimed at a range of private sector entities, particularly telecoms companies for surveillance of end users.

Symantec also identified a malware suite with references to Iranian hacking forums that combined custom malware with several standard publicly available network analysis and password-cracking tools.

This suggests that Iranian cyber espionage actors, like other mature cyber actors, recognise that publicly available tools can be equally effective and more deniable, and so are able to move up and down the scale of sophistication as required.

## Influence operations

Iran will increase social media influence operations

Google, Facebook and Twitter have closed hundreds of Iran-linked accounts engaged in coordinated influence campaigns. Reuters tracked a specific organisation, the International Union of Virtual Media, that promoted Iranian interests and had links to Iranian state-run news channels and websites affiliated with allies such as Hezbollah.

In coming years, Iran will increase such campaigns, taking a lead from the success of US adversaries and reciprocal struggles for online influence in neighbouring Gulf states.

## Influence internet traffic

Iran may also seek to influence internet traffic more widely. In August, a brief rearrangement of the Border Gateway Protocol (BGP), which decides international routes for internet traffic, redirected more than 100 prefixes including the encrypted messaging app Telegram through Iranian servers.

Although this could have been an error (similar issues occur frequently worldwide), actors including Russia and China are suspected of using BGP 'hijacking' to intercept internet traffic.

## Critical infrastructure

Iran has the capability to conduct damaging cyberattacks, as evidenced by the Shamoon malware attack against Saudi Aramco in 2012 and its reoccurrence across Saudi government networks in late 2016 and early 2017.

Yet there is no public indication that these capabilities have increased, and Coats's assessment relies on the Shamoon examples.

Moreover, critical infrastructure malware in Saudi Arabian companies that could override safety systems, reported in late 2017, has now been firmly attributed by FireEye to Russia, rather than Iran.

## Outlook

Iran's recent cyberactivity represents a broadening of Tehran's foreign policy-oriented cyber strategy. This trend is in line with other mature state cyber actors:

- Both the United States and its adversaries use complex espionage cybertools.
- Other states have also used DNS-based malware, while cyber criminals routinely exploit DNS weaknesses for extortion and spam.

### Defensive focus

> Iran is both a hostile actor and a victim in the cyber domain

Iran will continue to build its cyber capabilities for use in a crisis or conflict scenario for offensive and defensive purposes, especially given the recent sharpening of US cyber strategy (see UNITED STATES: Aggression risks deeper cyber conflict - October 4, 2018).

While the 2010 Stuxnet virus, widely attributed to the United States and Israel, was the first major incident of critical infrastructure damage through cyber means, in October 2018 Israeli news reports suggested that Iranian "strategic networks" had been damaged by a more severe virus than Stuxnet, with no indication of attribution.

Unlike critical infrastructure cyberattacks on Ukraine since 2015 by Russia, where malicious actors repeatedly targeted specific energy companies, Iranian actors are more likely to take a 'low-hanging fruit' approach: probing critical infrastructure companies widely and gaining access wherever there are vulnerabilities. The potential for damage therefore depends on intent, existing vulnerabilities and the crisis context (see IRAN: Tehran may prioritise cyber espionage - July 11, 2018).

### Targets

Iranian top targets for (offensive or defensive) cyberactivity include Lebanon, Israel and the Gulf, but also the United States and Europe. Iran is least likely to attack European states if their cooperation on preserving the 2014 nuclear deal continues, although this is unlikely to affect cyber espionage.