Warning issued over attacks on internet infrastructure

February 23 2019, by Glenn Chapman

The internet's global address keeper is warning of large-scale attacks threatening key parts of the online infrastructure

Key parts of the internet infrastructure face large-scale attacks that threaten the global system of web traffic, the internet's address keeper

warned Friday.

The Internet Corporation for Assigned Names and Numbers (ICANN) declared after an emergency meeting "an ongoing and significant risk" to key parts of the infrastructure that affects the domains on which websites reside.

"They are going after the internet infrastructure itself," ICANN chief technology officer David Conrad told AFP.

"There have been targeted attacks in the past, but nothing like this."

The attacks could date back to 2017 but have sparked growing concerns from security researchers in recent weeks, which prompted the special meeting of ICANN.

The malicious activity targets the Domain Name System or DNS which routes traffic to intended online destinations.

ICANN specialists and others say these attacks have a potential to snoop on data along the way, sneakily send the traffic elsewhere or enable the attackers to impersonate or "spoof" critical websites.

"There isn't a single tool to address this," Conrad said, as ICANN called for an overall hardening of web defenses.

US authorities issued a similar warning last month about the DNS attacks.

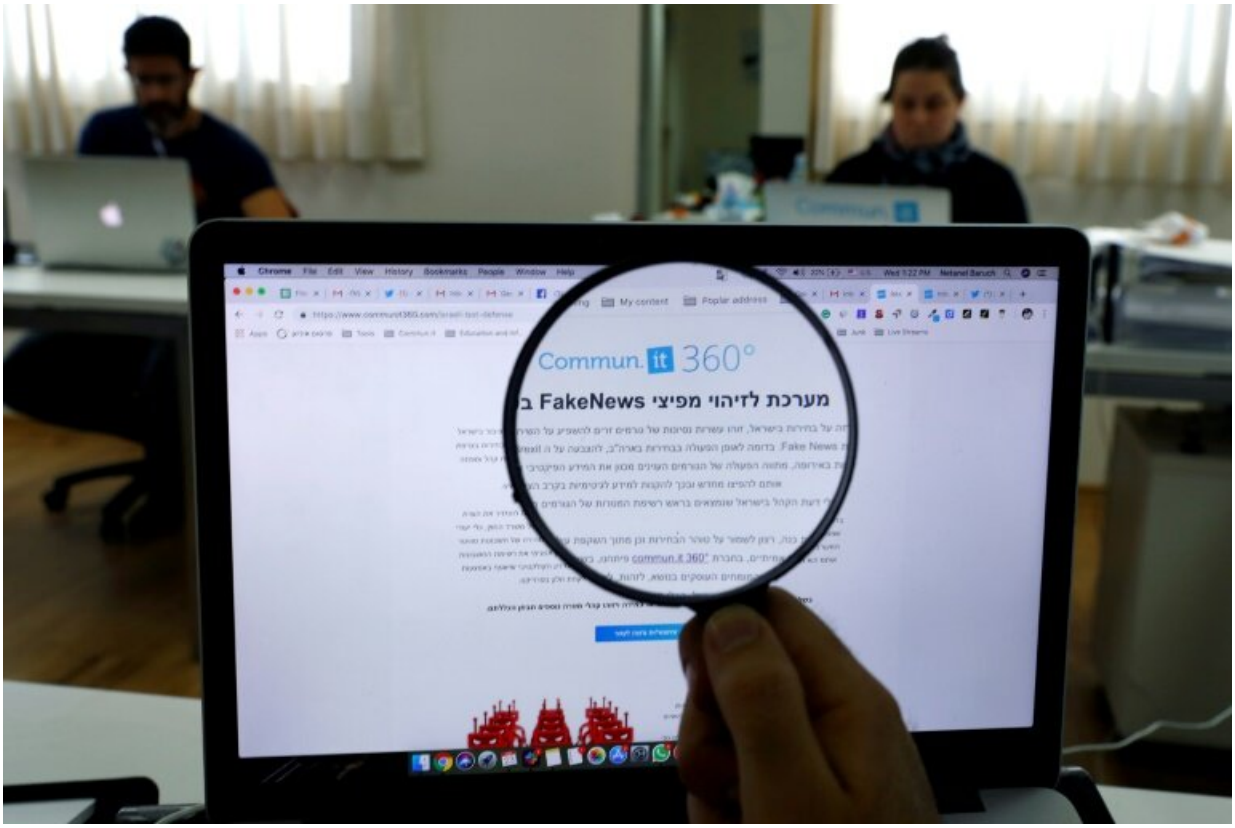
"This is roughly equivalent to someone lying to the post office about your address, checking your mail, and then hand delivering it to your mailbox," the US Department of Homeland Security said in a recent cybersecurity alert.

"Lots of harmful things could be done to you (or the senders) depending on the content of that mail."

Middle East targets

So-called "DNSpionage" attacks might date back to at least 2017, according to FireEye senior manager of cyber espionage analysis Ben Read.

The list of targets included website registrars and internet service providers, particularly in the Middle East.



So-called DNSpionage attacks have the potential to allow hackers to impersonate key websites and disrupt global internet traffic

"We've seen primarily targeting of email names and passwords," Read said.

"There is evidence that it is coming out of Iran and being done in support of Iran."

DNSpionage hackers appeared intent on stealing account credentials, such as email passwords, in Lebanon and the United Arab Emirates, according to Adam Meyers, vice president of intelligence at CrowdStrike cyber security firm.

Similar attacks took place in Europe and other parts of the Middle East, with targets including governments, intelligence services, police, airlines, and the oil industry, cybersecurity specialists said.

"You definitely need knowledge of how the internet works and you have to handle a lot of traffic being directed to you," Meyers said of the DNSpionage hackers.

"With that access, they could temporarily break portions of how the internet works. They chose to intercept and spy on folks."

The attack itself is technically simple, but its scope and targeting of internet service providers along with large government entities made it "a big deal," according to Meyers.

Digital signatures

ICANN is putting out word to website and online traffic handlers to ramp up security or leave users vulnerable to being tricked into trusting the wrong online venues.

The organization urged broader implementation of DNSSEC technology that adds digital signatures that act as virtual seals of sorts to expose when data moving online has been tampered with.

DNSSEC can also prevent internet users from being misdirected from intended websites, according to ICANN.

"It aims to assure that Internet users reach their desired online destination by helping to prevent so-called 'man in the middle' attacks where a user is unknowingly re-directed to a potentially malicious site," ICANN said in the release.

Part of the challenge to keeping the internet infrastructure safe is that website owners don't always grasp the imperative guarding against wily hackers, according to Conrad.

"We want to make sure people understand what it means to own a domain name and put it on the internet," Conrad said.

"Because, all of your customers are only as secure as you are."

Citation: Warning issued over attacks on internet infrastructure (2019, February 23) retrieved 24 April 2024 from https://phys.org/news/2019-02-issued-internet-infrastructure.html