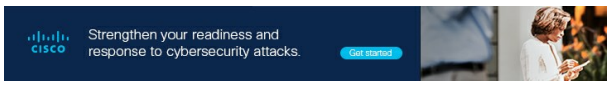


GOVERNMENT

Roy Moore scandal used for phishing schemes aimed at U.S. law firms

(Roy moore for senate)

Written by Chris Bing

DEC 4, 2017 | CYBERSCOOP

Since at least June, Chinese hackers have been actively targeting a shortlist of multinational law firms in an apparent effort to spy on lawyers and steal confidential information, according to cybersecurity firm FireEye.

The hacking group, which is known as APT19, will often design phishing campaigns that contain references to pertinent, high-profile U.S. news stories. Most recently, these booby-trapped emails have separately mentioned U.S. Senate candidate Roy Moore, disgraced Hollywood producer Harvey Weinstein and former presidential candidate Hillary Clinton.

The hacking group has been loosely linked to China.

FireEye says APT19 crafted the subject line "FW: Roy Moore scandal ignites fundraising explosion for Democratic challenger Doug Jones" to seemingly capitalize on the contentious campaign to fill the vacant senate seat in Alabama. Moore, 70, has been accused of making unwanted sexual advances toward multiple teenage girls when he was in his 30s.

It's relatively common for hackers to leverage public events to lure targets into clicking a suspicious email or link. Other groups known to leverage this technique include Russian groups APT28 and APT29, more commonly known as "Fancy Bear" and "Cozy Bear." APT28 used the technique in the aftermath of a terrorist attack in New York City earlier this year.

FireEye has evidence of at least three law firms being repeatedly and continuously targeted as part of APT19's latest activity. These organizations are based in the U.S. but have offices globally, including in China. All three boast business internationally, offering various different legal practices.

Ben Read, an analyst with FireEye, told CyberScoop the most recent wave of APT19's phishing emails had been detected last week. It is the fourth known wave of related malicious emails following a barrage of similar messages in June, October and then again in mid-November.

In each case, the emails carried malware inside a Microsoft word document, Read said. When opened, the document would covertly download an open-source backdoor onto the victim's computer

before then establishing a connection to the attacker's own server. This backdoor can provide APT19 with wide-access to a compromised device as well as the network it is connected to.

All four identified waves of phishing emails targeted the same group of law firms. FireEye's visibility into the threat is limited to its customer base, meaning that a variety of other APT19 targets may exist.

"It's difficult to say what they're after because the lures are so broadly written and we're stopping them at the perimeter, before they really get a chance to do much," said Read. "It's feasible that APT19 is looking to steal financial documents, including information about business mergers and acquisitions which could be worth a lot."

FireEye first detailed APT19's interest in law firms in June. Read says the group has continued to use the same toolset since June although in some instances they've slightly tweaked their intrusion techniques to avoid detection. The original sighting in June saw APT19 use a well-known and outdated Microsoft office vulnerability (CVE-2017-0199) to deliver malware.

"Based on what we can observe, the targets are mostly the same every time (major U.S.-based law firms)," said FireEye analyst Ian Ahl. "The emails all originate from an APT19 owned domain, but the sender username is often changed."

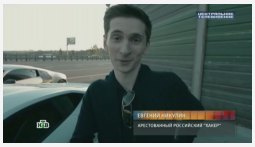
Read said it remains unclear whether APT19 is in any way affiliated with the Chinese government.

Last week, the Justice Department indicted three Chinese hackers who were at one point connected to a group also tracked by FireEye, named APT3. While there's some indication those indicted individuals worked for a state run intelligence agency, the trio regularly used what appeared to be a Chinese shell company to obfuscate the nature of their offensive operations. Experts say it's typical for Beijing to use a mix of contractors and fake companies to hide traditional intelligence gathering efforts which are in reality led by state agencies.

-In this Story-

advanced persistent threat (APT), APT19, breaches, China, FireEye, government, hacking, Intelligence, law firms, legal, security research

RELATED NEWS



GOVERNMENT

FSB asset introduced...

by **Jeff Stone** • 2 days ago

GOVERNMENT

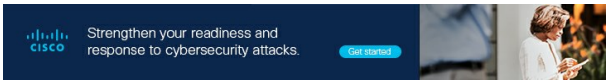
Election commission hires...

by **Sean Lyngaas** • 3 days ago

GOVERNMENT

What to expect from the...

by **Shannon Vavra** • 4 days ago



Privacy Policy

© 2020 Scoop News Group | All Rights Reserved

We use cookies to provide you with the best experience across all Scoop News Group websites. By using Scoop News Group websites, you consent to the use of cookies. *Learn more*

GOT IT!