Cybersecurity firm: US Senate in Russian hackers' crosshairs

January 12 2018, by Raphael Satter

In this Friday, Jan. 20, 2017 file photo, the U.S. Capitol Building is illuminated during sunrise in Washington. The same Russian government-aligned hackers who penetrated the Democratic Party have spent the past few months laying the groundwork for an espionage campaign against the U.S. Senate, the cybersecurity firm Trend Micro said Friday, Jan. 12, 2018. (AP Photo/John Minchillo)

The same Russian government-aligned hackers who penetrated the

Democratic Party have spent the past few months laying the groundwork for an espionage campaign against the U.S. Senate, a cybersecurity firm said Friday.

The revelation suggests the group often nicknamed Fancy Bear, whose hacking campaign scrambled the 2016 U.S. electoral contest, is still busy trying to gather the emails of America's political elite.

"They're still very active—in making preparations at least—to influence public opinion again," said Feike Hacquebord, a security researcher at Trend Micro Inc., which published the report . "They are looking for information they might leak later."

The Senate Sergeant at Arms office, which is responsible for the upper house's security, declined to comment.

Hacquebord said he based his report on the discovery of a clutch of suspicious-looking websites dressed up to look like the U.S. Senate's internal email system. He then cross-referenced digital fingerprints associated with those sites to ones used almost exclusively by Fancy Bear, which his Tokyo-based firm dubs "Pawn Storm."

Trend Micro previously drew international attention when it used an identical technique to uncover a set of decoy websites apparently set up to harvest emails from the French presidential candidate Emmanuel Macron's campaign in April 2017. The sites' discovery was followed two months later by a still-unexplained publication of private emails from several Macron staffers in the final days of the race.

Hacquebord said the rogue Senate sites—which were set up in June and September of 2017—matched their French counterparts.

"That is exactly the way they attacked the Macron campaign in France,"

he said.

Attribution is extremely tricky in the world of cybersecurity, where hackers routinely use misdirection and red herrings to fool their adversaries. But Tend Micro, which has followed Fancy Bear for years, said there could be no doubt.

In this Jan. 3, 2018 photo, the Capitol is seen in Washington. Newly published research shows that the same Russian government-aligned hackers who penetrated the Democratic Party have spent the past six months laying the groundwork for an espionage campaign against an unknown number of U.S. Senate staffers, including Republicans. (AP Photo/J. Scott Applewhite)

"We are 100 percent sure that it can attributed to the Pawn Storm group," said Rik Ferguson, one of the Hacquebord's colleagues.

Like many cybersecurity companies, Trend Micro refuses to speculate publicly on who is behind such groups, referring to Pawn Storm only as having "Russia-related interests." But the U.S. intelligence community alleges that Russia's military intelligence service pulls the hackers' strings and a months-long Associated Press investigation into the group, drawing on a vast database of targets supplied by the cybersecurity firm Secureworks, has determined that the group is closely attuned to the Kremlin's objectives.

If Fancy Bear has targeted the Senate over the past few months, it wouldn't be the first time. An AP analysis of Secureworks' list shows that several staffers there were targeted between 2015 and 2016.

Among them: Robert Zarate, now the foreign policy adviser to Florida Senator Marco Rubio; Josh Holmes, a former chief of staff to Senate Majority Leader Mitch McConnell who now runs a Washington consultancy; and Jason Thielman, the chief of staff to Montana Senator Steve Daines. A Congressional researcher specializing in national security issues was also targeted.

Fancy Bear's interests aren't limited to U.S. politics; the group also appears to have the Olympics in mind.

Trend Micro's report said the group had set up infrastructure aimed at collecting emails from a series of Olympic winter sports federations, including the International Ski Federation, the International Ice Hockey Federation, the International Bobsleigh & Skeleton Federation, the International Luge Federation and the International Biathlon Union.

The targeting of Olympic groups comes as relations between Russia and the International Olympic Committee are particularly fraught. Russian athletes are being forced to compete under a neutral flag in the upcoming Pyeongchang Olympics following an extraordinary doping

scandal that has seen 43 athletes and several Russian officials banned for life. Amid speculation that Russia could retaliate by orchestrating the leak of prominent Olympic officials' emails, cybersecurity firms including McAfee and ThreatConnect have picked up on signs that state-backed hackers are making moves against winter sports staff and anti-doping officials.

On Wednesday, a group that has brazenly adopted the Fancy Bear nickname began publishing what appeared to be Olympics and doping-related emails from between September 2016 and March 2017. The contents were largely unremarkable but their publication was covered extensively by Russian state media and some read the leak as a warning to Olympic officials not to press Moscow too hard over the doping scandal.

Whether any Senate emails could be published in such a way isn't clear. Previous warnings that German lawmakers' correspondence might be leaked by Fancy Bear ahead of last year's election there appear to have come to nothing.

In this Wednesday, May 11, 2011 file photo, Colorado State Rep. Andy Kerr, left, speaks on the last day of the legislative session at the Capitol in Denver. According to data supplied by the cybersecurity firm Secureworks, Kerr – who is now a state senator – was one of the targets of the hacking group Fancy Bear. Kerr says thousands of his emails were posted to an obscure section of the website DCLeaks before the site fell offline in 2017. (AP Photo/Ed Andrieski)

On the other hand, the group has previously dumped at least one U.S. legislator's correspondence onto the web.

One of the targets on Secureworks' list was Colorado State Senator Andy Kerr, who said thousands of his emails were posted to an obscure section of the website DCLeaks—a web portal better known for publishing emails belonging to retired Gen. Colin Powell and various members of Hillary Clinton's campaign—in late 2016.

Kerr said he was still bewildered as to why he was targeted. He said that

while he supported transparency, "there should be some process and some system to it.

"It shouldn't be up to a foreign government or some hacker to say what gets released and what shouldn't."