Journalists investigating Russia targeted by cyberattacks: ProtonMail

July 28 2019, by Ben Simon

Investigations website Bellingcat helped unmask the Russian agents suspected of poisoning ex-spy Sergei Skripal

Reporters investigating Russian military intelligence have been targeted by highly sophisticated cyberattacks through their encrypted email accounts, with evidence suggesting Moscow was responsible, the email service provider ProtonMail and journalists said Saturday.

The phishing attack, which sought to dupe users into sharing their ProtonMail passwords, was aimed at journalists from the award-winning website Bellingcat, which helped identify the agents who poisoned former Russian spy Sergei Skripal in Britain.

Geneva-based ProtonMail said in a statement that "the evidence (along with independent third-party assessments) seem to suggest an attack of Russian origin."

The company's chief executive Andy Yen told AFP that the operation "was one of the best-run phishing attacks we have ever seen."

Bellingcat journalist Christo Grozev, who led the site's work on the Skripal case, said he had no doubt Russia's GRU military intelligence unit was responsible and that it marked "a quantum leap" in terms of their technical sophistication.

"It was very convincing," he told AFP, noting that no Bellingcat reporters gave up their passwords.

End-to-end encryption

ProtonMail, which describes itself as the world's most secure email provider, has become increasingly popular with journalists and others who handle sensitive information because user communications are protected by end-to-end encryption.

The Harvard-educated Yen, who worked at Europe's nuclear research lab CERN for five years before founding ProtonMail, told AFP that the company could not read users' emails even if it wanted to—in clear contrast with Google's Gmail.

The phishing attacks against Bellingcat reporters occurred this week,

with "emails sent to the targeted users claiming to be from the ProtonMail team, asking the targets to enter their... login credentials," the company said.

A Bellingcat journalist said he had no doubt Russia's GRU military intelligence unit was responsible for the cyberattacks

Grozev said that despite his technical savvy and awareness that he was a target, he "would have been fooled" if not for prior warning from a contact who had received a similar phishing email earlier this month.

While the assault on Bellingcat journalists was concentrated over the past few days, Grozen claimed that multiple investigators and researchers from other organisations that work on Russia have received phishing

emails in their ProtonMail accounts since April.

Yen told AFP that "putting a precise start date as to when other Russia journalists began to be targeted is a bit more complex and not something that we can confirm with full confidence right now."

'Has to be investigated'

Yen said that ProtonMail has alerted the Swiss Federal Police and the government's computer system security office, MELANI, about the events this week.

The company has not yet received any indication that an investigation will be launched, Yen said, noting that he was not optimistic the perpetrators would face justice, in part because Moscow was likely to protect them.

ProtonMail however is conducting its own investigation.

But Grozen said the Swiss had a duty to act, given that its .ch domain was used to carry out the phishing operation.

"It is essentially a crime within the digital territory of Switzerland," he said, stressing that the entities who registered the malicious .ch websites are "traceable for (Swiss) authorities".

Swiss Federal Police and MELANI did not immediately respond to a request for comment.

Bellingcat, a highly regarded Britain-based investigative website, has used open-source technology to break a series of stories, notably concerning Russia, including major revelations in the downing of MH17 flight over eastern Ukraine, which has also been linked to Russia's GRU

intelligence service.