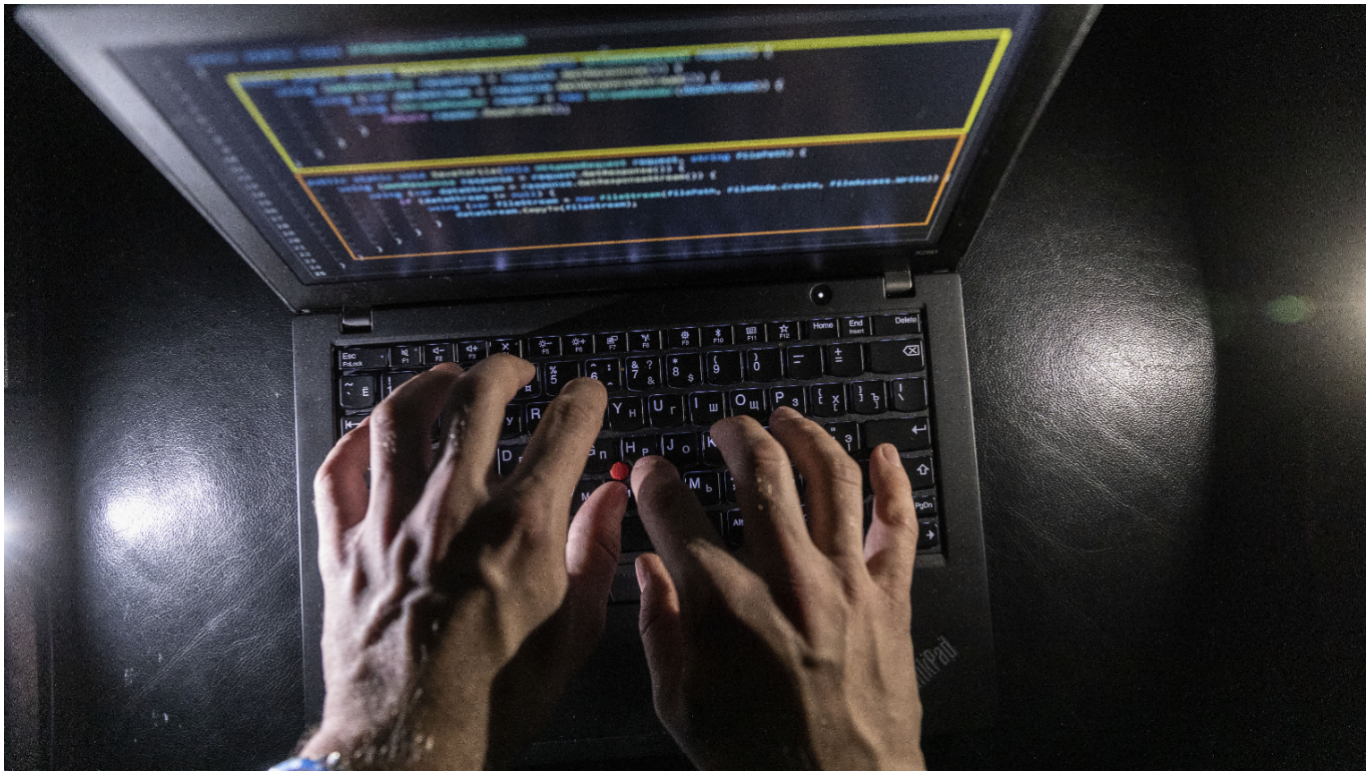
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Wanted Russian Cybercrime Group Resurfaces With Work-From-Home Attacks – NYT

June 26, 2020



Cybersecurity experts say Evil Corp is able to penetrate “some of the most well-protected corporations.”
Evgeny Razumny / TASS

A Russian cybercriminal group known as Evil Corp has resurfaced in the United States with attempts to hack into major corporations through employees who are working from home due to the coronavirus, The New York Times reported Thursday.

U.S. authorities indicted Evil Corp leader Maxim Yakubets and his associate in December on suspicion of stealing more than $100 million from U.S., British and other companies.

Related article: U.S. Cracks Down on Russian 'Evil Corp' Cybercrime Group

The computer security company Symantec said it identified a malicious ransomware program attributed to Evil Corp that had breached the networks of at least 31 major U.S. corporations

and were preparing to attack. Ransomware blocks access to users' computers until the victim pays a ransom.

"These hackers have a decade of experience and they aren't wasting time with small, two-bit outfits. They are going after the biggest American firms, and only American firms," Symantec's technical director Eric Chien told NYT.

Evil Corp hackers deploy malware on common websites that can identify whether visitors work for major corporations or governments, Chien said. They infect the visitors' personal computers and use them as a springboard to attack corporate systems once the users reconnect to their employers' networks via protected channels, he continued.

Symantec said Evil Corp is able to penetrate "some of the most well-protected corporations, stealing credentials and moving with ease across their networks." It warned that a successful attack could cause millions of U.S. dollars in damages and trigger "a domino effect on supply chains."

"A successful attack could cripple the victim's network, leading to significant disruption to their operations and a costly clean-up operation," it said.

Russia is unlikely to extradite the alleged hackers to the United States, meaning they are unlikely to stand trial there.

Britain has said it has arrested and convicted eight other members of Evil Corp. Photographs released by the British government in December showed Yakubets driving a custom Lamborghini and depicted other members enjoying a high-flying lifestyle.

This is at least the second time Evil Corp has resurfaced after a 2015 U.S. indictment against Yakubets and associate Igor Turashev failed to curb their attacks.

Original url:
https://www.themoscowtimes.com/2020/06/26/wanted-russian-cybercrime-group-resurfaces-with-work-from-home-attacks-nyt-a70714