Russian hacker group Evil Corp targets US workers at home

bbc.com/news/world-us-canada-53195749

BBC News

Published
26 June 2020

Image source, Reuters

Image caption,
One Russian national is accused of carrying out attacks on behalf of the Russian state

A Russian hacking group is launching ransomware attacks against a number of US companies, targeting employees who are working from home due to Covid-19.

Evil Corp hackers have tried to access at least 31 organisations' networks in order to cripple systems and demand millions of dollars in ransom.

The group's two alleged leaders were indicted by the US Justice Department in December 2019.

There are concerns that US voting systems could also be targeted.

Last year, US authorities filed charges against Evil Corp's alleged leaders Maksim Yakubets and Igor Turashev, accusing them of using malware to steal millions of dollars from groups including schools and religious organisations in over 40 countries.

Officials announced a $5m reward for information leading to their arrest, which they said was the largest amount ever offered for a cyber criminal. Both men are still at large.

Image source, US Department of Justice

Image caption,
Maksim Yakubets (L) and Igor Turashev are accused of running Evil Corp

The threat comes as the majority of Americans have been working from home due to the coronavirus pandemic - 62% according to a Gallup poll.

The US presidential election is also just months away, and federal and local officials have been working to put measures in place to protect voter records as well as manage safe voting practices amid the pandemic.

What do we know about the attack?

Symantec Corporation, a firm that monitors corporate and government networks released a notice warning of the threat it identified on Thursday night.

The attacks used what Symantec described as a relatively new type of ransomware called WastedLocker, which has been attributed to Evil Corp. Ransomware are computer viruses that threaten to delete files unless the ransom is paid. The WastedLocker ransomware virus demands ransoms of $500,000 to $1m to unlock computer files it seizes.

Symantec said the "vast majority of targets are major corporations, including many household names", and eight targets were Fortune 500 companies. All are US-owned but one, which is a US-based subsidiary.

Most targeted companies were in the manufacturing, information technology and media sectors.

Media caption,
Technology explained: what is ransomware?

Symantec said the hackers had breached the networks of these companies and were "laying the groundwork" for future ransomware attacks that would let them block access to data and demand millions of dollars.

Symantec technical director Eric Chien told the New York Times the hackers take advantage of employees now using virtual private networks (VPNs) to access work systems.

They use VPNs to identify which company a user works for, and then infect the user's computer when they visit a public or commercial site. When the user next connects to their employer's system, the hackers can attack.

What's the context?

There have been a number of recent cyber-attacks on local governments across the US.

Cities and towns in Louisiana, Oregon, Maryland, Georgia, Texas and Florida were hit by ransomware attacks last year.

The Department of Homeland Security is looking into safeguarding voter registration databases ahead of November 3's general election. In February, the agency's head of cyber-security said this was a key election security concern.

These attacks by foreign cyber-criminals are far from a new threat.

During the impeachment inquiry last year, former White House security adviser and Russia expert Fiona Hill testified that "Russia's security services and their proxies have geared up to repeat their interference in the 2020 election".

In 2018, the justice department charged 12 Russian intelligence officers with hacking Democratic officials in the 2016 US elections, using spear phishing emails and malicious software.

The hackers also stole data on half a million voters from a state election board site. Moscow has said there is no evidence linking the 12 to military intelligence or hacking.