The New York Times https://nyti.ms/2CAaL98

Russian Criminal Group Finds New Target: Americans Working at Home

A hacking group calling itself Evil Corp., indicted in December, has shown up in corporate networks with sophisticated ransomware. American officials worry election infrastructure could be next.

By David E. Sanger and Nicole Perlroth

Published June 25, 2020 Updated June 26, 2020, 12:07 a.m. ET

A Russian ransomware group whose leaders were indicted by the Justice Department in December is retaliating against the U.S. government, many of America's largest companies and a major news organization, identifying employees working from home during the pandemic and attempting to get inside their networks with malware intended to cripple their operations.

Sophisticated new attacks by the hacking group — which the Treasury Department claims has at times worked for Russian intelligence — were identified in recent days by Symantec Corporation, a division of Broadcom, one of the many firms that monitors corporate and government networks.

In an urgent warning issued Thursday night, the company reported that Russian hackers had exploited the sudden change in American work habits to inject code into corporate networks with a speed and breadth not previously witnessed.

Ransomware allows the hackers to demand that companies pay millions to have access to their own data restored.

While ransomware has long been a concern for American officials, after devastating attacks on the cities of Atlanta and Baltimore and towns across Texas and Florida, it has taken on new dimensions in an election year. The Department of Homeland Security has been racing to harden the voter registration systems run by cities and states, fearing that they, too, could be frozen, and voter rolls made inaccessible, in an effort to throw the Nov. 3 election into chaos.

"Security firms have been accused of crying wolf, but what we have seen in the past few weeks is remarkable," said Eric Chien, Symantec's technical director, who was known as one of the engineers who first identified the Stuxnet code that the United States and Israel used to cripple Iran's nuclear centrifuges a decade ago. "Right now this is all about making money, but the infrastructure they are deploying could be used to wipe out a lot of data — and not just at corporations."

A leaked May 1 F.B.I. warning said ransomware attacks on American corporations were threatening to take out election infrastructure. "The F.B.I. assesses that ransomware infections delivered through M.S.P.s," the abbreviation for internet service providers, "to U.S. county and state government networks will likely threaten the availability of data on interconnected election servers, even if that is not the actors' intention," it said.

A cyberattack attack late last year on a Louisiana internet services company allowed hackers to target the Louisiana secretary of state and nine court clerk offices the week before an election. And in Tillamook County, Ore., in January, ransomware attackers prevented voter registration personnel from accessing voter registration data as they readied the data for the May primaries.

Symantec declined to name the companies that were the targets of the Russian hackers, citing the usual confidentiality of its client base. But it said it had already identified 31, including major American brands and Fortune 500 firms. It is unclear whether any of those companies have received ransomware demands, which would only come if the malicious code was activated by its authors. Mr. Chien said the warning was issued because "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."

The hackers call themselves "Evil Corp.," a play off the "Mr. Robot" television series. In December, the Justice Department said they had "been engaged in cybercrime on an almost unimaginable scale," deploying malware to steal tens of millions of dollars from online banking systems. The Treasury Department placed sanctions on them, and the State Department offered $5 million for information leading to the arrest or conviction of the group's leader.

The indictment is one of many in the past few years against Russian groups, including intelligence agents and the Internet Research Agency, accused of interfering in the 2016 election. Those indictments were intended as a deterrent. But Moscow has protected Evil Corp.'s hackers from extradition, and they are unlikely to stand trial in the United States. In the Treasury Department sanctions announcement, the United States contended that some of the group's leaders have done work for the F.S.B., the successor to the Soviet K.G.B.

The December indictment and the sanctions both named Maksim V. Yakubets, said by the Treasury Department to be "working for the Russian F.S.B." three years ago, and "tasked to work on projects for the Russian state, to include acquiring confidential documents through cyber-enabled means and conducting cyber-enabled operations on its behalf."

Symantec said it had briefed federal officials on the findings, which are echoed by at least one other company monitoring corporate networks. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency did not immediately respond to questions about whether it had seen the same activity, or planned to issue a parallel warning.

But the attack's methodology suggests it was intended for the work-at-home era.

The malware, Mr. Chien said, was deployed on common websites and even one news site. But it did not infect every computer used to go shopping or read about the day's events. Instead, the code looked for a sign that the computer was part of a major corporate or government network. For example, many firms have their employees use a "virtual private network," or V.P.N., a protected channel that allows workers sitting in their basements or attics to tunnel into their corporate computer systems as if they were at the office.

"These attacks do not try to get into the V.P.N.," Mr. Chien said. "They just use it to identify who the user works for." Then the systems wait for the worker to go to a public or commercial website, and use that moment to infect their computer. Once the machine is reconnected to the corporate network, the code is deployed, in hopes of gaining access to corporate systems.

The indictment was intended to put Evil Corp. out of business. It failed. In the month after the indictment, Evil Corp.'s hackers dropped off the map, but they picked up again in May, according to security researchers at Symantec and Fox-IT, another security company that is a division of the NCC Group. For the past month, they have been successfully breaking into organizations using custom ransomware tools.

Evil Corp.'s hackers managed to disable the antivirus software on victims' systems and take out backup systems, in what Fox-IT's researchers said was a clear attempt to thwart victims' ability to recover their data, and in some cases prevent "the ability to recover at all."

While Symantec did not say how much money Evil Corp. was generating from its recent attacks, Fox-IT researchers said they had previously seen the Russian hackers demand more than $10 million to unlock data on a single victim's network.

"We've seen them ramp up their ransom demands over the past few years, into the millions of dollars as they hit bigger targets," said Maarten van Dantzig, a threat analyst at Fox-IT. "They are the most professional group we see deploying attacks on this scale today."