The New York Times | https://nyti.ms/2yVSEU4

TECHNOLOGY

How Israel Caught Russian Hackers Scouring the World for U.S. Secrets

By NICOLE PERLROTH and SCOTT SHANE OCT. 10, 2017

It was a case of spies watching spies watching spies: Israeli intelligence officers looked on in real time as Russian government hackers searched computers around the world for the code names of American intelligence programs.

What gave the Russian hacking, detected more than two years ago, such global reach was its improvised search tool — antivirus software made by a Russian company, Kaspersky Lab, that is used by 400 million people worldwide, including by officials at some two dozen American government agencies.

The Israeli officials who had hacked into Kaspersky's own network alerted the United States to the broad Russian intrusion, which has not been previously reported, leading to a decision just last month to order Kaspersky software removed from government computers.

The Russian operation, described by multiple people who have been briefed on the matter, is known to have stolen classified documents from a National Security Agency employee who had improperly stored them on his home computer, on which Kaspersky's antivirus software was installed. What additional American secrets the Russian hackers may have gleaned from multiple agencies, by turning the Kaspersky software into a sort of Google search for sensitive information, is not yet publicly known.

The current and former government officials who described the episode spoke about it on condition of anonymity because of classification rules.

Like most security software, Kaspersky Lab's products require access to everything stored on a computer in order to scour it for viruses or other dangers. Its popular antivirus software scans for signatures of malicious software, or malware, then removes or neuters it before sending a report back to Kaspersky. That procedure, routine for such software, provided a perfect tool for Russian intelligence to exploit to survey the contents of computers and retrieve whatever they found of interest.

The National Security Agency and the White House declined to comment for this article. The Israeli Embassy declined to comment, and the Russian Embassy did not respond to requests for comment.

The Wall Street Journal reported last week that Russian hackers had stolen classified N.S.A. materials from a contractor using the Kaspersky software on his home computer. But the role of Israeli intelligence in uncovering that breach and the Russian hackers' use of Kaspersky software in the broader search for American secrets have not previously been disclosed.

Kaspersky Lab denied any knowledge of, or involvement in, the Russian hacking. "Kaspersky Lab has never helped, nor will help, any government in the world with its cyberespionage efforts," the company said in a statement Tuesday afternoon. Kaspersky Lab also said it "respectfully requests any relevant, verifiable information that would enable the company to begin an investigation at the earliest opportunity."

The Kaspersky-related breach is only the latest bad news for the security of American intelligence secrets. It does not appear to be related to a devastating leak of N.S.A. hacking tools last year to a group, still unidentified, calling itself the Shadow Brokers, which has placed many of them online. Nor is it evidently connected to a parallel leak of hacking data from the C.I.A. to WikiLeaks, which has posted classified C.I.A. documents regularly under the name Vault7.

For years, there has been speculation that Kaspersky's popular antivirus software might provide a back door for Russian intelligence. More than 60 percent, or $374 million, of the company's $633 million in annual sales come from customers in the United States and Western Europe. Among them have been nearly two dozen American government agencies — including the State

Department, the Department of Defense, Department of Energy, Justice Department, Treasury Department and the Army, Navy and Air Force.

The N.S.A. bans its analysts from using Kaspersky antivirus at the agency, in large part because the agency has exploited antivirus software for its own foreign hacking operations and knows the same technique is used by its adversaries.

"Antivirus is the ultimate back door," Blake Darché, a former N.S.A. operator and co-founder of Area 1 Security. "It provides consistent, reliable and remote access that can be used for any purpose, from launching a destructive attack to conducting espionage on thousands or even millions of users."

On Sept. 13, the Department of Homeland Security ordered all federal executive branch agencies to stop using Kaspersky products, giving agencies 90 days to remove the software. Acting Department of Homeland Security Secretary Elaine C. Duke cited the "information security risks" presented by Kaspersky and said the company's antivirus and other software "provide broad access to files" and "can be exploited by malicious cyber actors to compromise" federal computer systems.

That directive, which some officials thought was long overdue, was based, in large part, on intelligence gleaned from Israel's 2014 intrusion into Kaspersky's corporate systems. It followed months of discussions among intelligence officials, which included a study of how Kaspersky's software works and the company's suspected ties with the Kremlin.

"The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky," D.H.S. said in its statement, "could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security."

Kaspersky Lab did not discover the Israeli intrusion into its systems until mid-2015, when a Kaspersky engineer testing a new detection tool noticed unusual activity in the company's network. The company investigated and detailed its findings in June 2015 in a public report.

The report did not name Israel as the intruder but noted that the breach bore striking similarities to a previous attack, known as "Duqu," which researchers had attributed to the same nation states responsible for the infamous Stuxnet cyberweapon. Stuxnet was a joint American-Israeli operation that successfully infiltrated Iran’s Natanz nuclear facility, and used malicious code to destroy a fifth of Iran’s uranium centrifuges in 2010.

Kaspersky reported that its attackers had used the same algorithm and some of the same code as Duqu, but noted that in many ways it was even more sophisticated. So the company researchers named the new attack Duqu 2.0, noting that other victims of the attack were prime Israeli targets.

Among the targets Kaspersky uncovered were hotels and conference venues used for closed-door meetings by members of the United Nations Security Council to negotiate the terms of the Iran nuclear deal — negotiations from which Israel was excluded. Several targets were in the United States, which suggested that the operation was Israel’s alone, not a joint American-Israeli operation like Stuxnet.

Kaspersky’s researchers noted that attackers had managed to burrow deep into the company’s computers and evade detection for months. Investigators later discovered that the Israeli hackers had implanted multiple back doors into Kaspersky’s systems, employing sophisticated tools to steal passwords, take screenshots, and vacuum up emails and documents.

In its June 2015 report, Kaspersky noted that its attackers seemed primarily interested in the company’s work on nation-state attacks, particularly Kaspersky’s work on the “Equation Group” — its private industry term for the N.S.A. — and the “Regin” campaign, another industry term for a hacking unit inside the United Kingdom’s intelligence agency, the Government Communications Headquarters, or GCHQ.

Israeli intelligence officers informed the N.S.A. that in the course of their Kaspersky hack, they uncovered evidence that Russian government hackers were using Kaspersky’s access to aggressively scan for American government classified programs, and pulling any findings back to Russian intelligence systems. They provided their N.S.A. counterparts with solid evidence of the Kremlin campaign in the form of screenshots and other documentation, according to the people briefed on the events.

It is not clear whether, or to what degree, Eugene V. Kaspersky, the founder of Kaspersky Lab, and other company employees have been complicit in the hacking using their products. Technical experts say that at least in theory, Russian intelligence hackers could have exploited Kaspersky's worldwide deployment of software and sensors without the company's cooperation or knowledge. Another possibility is that Russian intelligence officers might have infiltrated the company without the knowledge of its executives.

But experts on Russia say that under President Vladimir V. Putin, a former K.G.B. officer, businesses asked for assistance by Russian spy agencies may feel they have no choice but to give it. To refuse might well invite hostile action from the government against the business or its leaders. Mr. Kaspersky, who attended an intelligence institute and served in Russia's Ministry of Defense, would have few illusions about the cost of refusing a Kremlin request.

Steven L. Hall, a former chief of Russian operations at the C.I.A., said his former agency never used Kaspersky software, but other federal agencies did. By 2013, he said, Kaspersky officials were "trying to do damage control and convince the U.S. government that it was just another security company."

He didn't buy it, Mr. Hall said. "I had the gravest concerns about Kaspersky, and anyone who worked on Russia or in counterintelligence shared those concerns," he said.

A version of this article appears in print on October 11, 2017, on Page A9 of the New York edition with the headline: How Israel Caught Russian Hackers Scouring for American Secrets.