The New York Times | https://nyti.ms/2v0QQXH

EUROPE

In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking

By ANDREW E. KRAMER and ANDREW HIGGINS AUG. 16, 2017

KIEV, Ukraine — The hacker, known only by his online alias "Profexer," kept a low profile. He wrote computer code alone in an apartment and quietly sold his handiwork on the anonymous portion of the internet known as the dark web. Last winter, he suddenly went dark entirely.

Profexer's posts, already accessible only to a small band of fellow hackers and cybercriminals looking for software tips, blinked out in January — just days after American intelligence agencies publicly identified a program he had written as one tool used in Russian hacking in the United States. American intelligence agencies have determined Russian hackers were behind the electronic break-in of the Democratic National Committee.

But while Profexer's online persona vanished, a flesh-and-blood person has emerged: a fearful man who the Ukrainian police said turned himself in early this year, and has now become a witness for the F.B.I.

"I don't know what will happen," he wrote in one of his last messages posted on a restricted-access website before going to the police. "It won't be pleasant. But I'm

still alive."

It is the first known instance of a living witness emerging from the arid mass of technical detail that has so far shaped the investigation into the election hacking and the heated debate it has stirred. The Ukrainian police declined to divulge the man's name or other details, other than that he is living in Ukraine and has not been arrested.

There is no evidence that Profexer worked, at least knowingly, for Russia's intelligence services, but his malware apparently did.

That a hacking operation that Washington is convinced was orchestrated by Moscow would obtain malware from a source in Ukraine — perhaps the Kremlin's most bitter enemy — sheds considerable light on the Russian security services' modus operandi in what Western intelligence agencies say is their clandestine cyberwar against the United States and Europe.

It does not suggest a compact team of government employees who write all their own code and carry out attacks during office hours in Moscow or St. Petersburg, but rather a far looser enterprise that draws on talent and hacking tools wherever they can be found.

Also emerging from Ukraine is a sharper picture of what the United States believes is a Russian government hacking group known as Advanced Persistent Threat 28 or Fancy Bear. It is this group, which American intelligence agencies believe is operated by Russian military intelligence, that has been blamed, along with a second Russian outfit known as Cozy Bear, for the D.N.C. intrusion.

Rather than training, arming and deploying hackers to carry out a specific mission like just another military unit, Fancy Bear and its twin Cozy Bear have operated more as centers for organization and financing; much of the hard work like coding is outsourced to private and often crime-tainted vendors.

Russia's Testing Ground

In more than a decade of tracking suspected Russian-directed cyberattacks against a host of targets in the West and in former Soviet territories — NATO, electrical grids, research groups, journalists critical of Russia and political parties, to name a few — security services around the world have identified only a handful of people who are directly involved in either carrying out such attacks or providing the cyberweapons that were used.

This absence of reliable witnesses has left ample room for President Trump and others to raise doubts about whether Russia really was involved in the D.N.C. hack.

“There is not now and never has been a single piece of technical evidence produced that connects the malware used in the D.N.C. attack to the G.R.U., F.S.B. or any agency of the Russian government,” said Jeffrey Carr, the author of a book on cyberwarfare. The G.R.U. is Russia’s military intelligence agency, and the F.S.B. its federal security service.

United States intelligence agencies, however, have been unequivocal in pointing a finger at Russia.

Seeking a path out of this fog, cybersecurity researchers and Western law enforcement officers have turned to Ukraine, a country that Russia has used for years as a laboratory for a range of politicized operations that later cropped up elsewhere, including electoral hacking in the United States.

In several instances, certain types of computer intrusions, like the use of malware to knock out crucial infrastructure or to pilfer email messages later released to tilt public opinion, occurred in Ukraine first. Only later were the same techniques used in Western Europe and the United States.

So, not surprisingly, those studying cyberwar in Ukraine are now turning up clues in the investigation of the D.N.C. break-in and related hacking, including the discovery of a rare witness.

Security experts were initially left scratching their heads when the Department of Homeland Security on Dec. 29 released technical evidence of Russian hacking that seemed to point not to Russia, but rather to Ukraine.

In this initial report, the department released only one sample of malware said to be an indicator of Russian state-sponsored hacking, though outside experts said a variety of malicious programs were used in Russian electoral hacking.

The sample pointed to a malware program, called the P.A.S. web shell, a hacking tool advertised on Russian-language dark web forums and used by cybercriminals throughout the former Soviet Union. The author, Profexer, is a well-regarded technical expert among hackers, spoken about with awe and respect in Kiev.

He had made it available to download, free, from a website that asked only for donations, ranging from $3 to $250. The real money was made by selling customized versions and by guiding his hacker clients in its effective use. It remains unclear how extensively he interacted with the Russian hacking team.

After the Department of Homeland Security identified his creation, he quickly shut down his website and posted on a closed forum for hackers, called Exploit, that "I'm not interested in excessive attention to me personally."

Soon, a hint of panic appeared, and he posted a note saying that, six days on, he was still alive.

Another hacker, with the nickname Zloi Santa, or Bad Santa, suggested the Americans would certainly find him, and place him under arrest, perhaps during a layover at an airport.

"It could be, or it could not be, it depends only on politics," Profexer responded. "If U.S. law enforcement wants to take me down, they will not wait for me in some country's airport. Relations between our countries are so tight I would be arrested in my kitchen, at the first request."

In fact, Serhiy Demediuk, chief of the Ukrainian Cyber Police, said in an interview that Profexer went to the authorities himself. As the cooperation began, Profexer went dark on hacker forums. He last posted online on Jan. 9. Mr. Demediuk said he had made the witness available to the F.B.I., which has posted a full-time cybersecurity expert in Kiev as one of four bureau agents stationed at the United States Embassy there. The F.B.I. declined to comment.

Profexer was not arrested because his activities fell in a legal gray zone, as an author but not a user of malware, the Ukrainian police say. But he did know the users, at least by their online handles. “He told us he didn’t create it to be used in the way it was,” Mr. Demediuk said.

A member of Ukraine’s Parliament with close ties to the security services, Anton Gerashchenko, said that the interaction was online or by phone and that the Ukrainian programmer had been paid to write customized malware without knowing its purpose, only later learning it was used in Russian hacking.

Mr. Gerashchenko described the author only in broad strokes, to protect his safety, as a young man from a provincial Ukrainian city. He confirmed that the author turned himself in to the police and was cooperating as a witness in the D.N.C. investigation. “He was a freelancer and now he is a valuable witness,” Mr. Gerashchenko said.

It is not clear whether the specific malware the programmer created was used to hack the D.N.C. servers, but it was identified in other Russian hacking efforts in the United States.

A Bear’s Lair

While it is not known what Profexer has told Ukrainian investigators and the F.B.I. about Russia’s hacking efforts, evidence emanating from Ukraine has again provided some of the clearest pictures yet about Fancy Bear, or Advanced Persistent Threat 28, which is run by the G.R.U.

Fancy Bear has been identified mostly by what it does, not by who does it. One of its recurring features has been the theft of emails and its close collaboration with the Russian state news media.

Tracking the bear to its lair, however, has so far proved impossible, not least because many experts believe that no such single place exists.

Even for a sophisticated tech company like Microsoft, singling out individuals in the digital miasma has proved just about impossible. To curtail the damage to

clients' operating systems, the company filed a complaint against Fancy Bear last year with the United States District Court for the Eastern District of Virginia but found itself boxing with shadows.

As Microsoft lawyers reported to the court, "because defendants used fake contact information, anonymous Bitcoin and prepaid credit cards and false identities, and sophisticated technical means to conceal their identities, when setting up and using the relevant internet domains, defendants' true identities remain unknown."

Nevertheless, Ukrainian officials, though wary of upsetting the Trump administration, have been quietly cooperating with American investigators to try to figure out who stands behind all the disguises.

Included in this sharing of information were copies of the server hard drives of Ukraine's Central Election Commission, which were targeted during a presidential election in May 2014. That the F.B.I. had obtained evidence of this earlier, Russian-linked electoral hack has not been previously reported.

Traces of the same malicious code, this time a program called Sofacy, were seen in the 2014 attack in Ukraine and later in the D.N.C. intrusion in the United States.

Intriguingly, in the cyberattack during the Ukrainian election, what appears to have been a bungle by Channel 1, a Russian state television station, inadvertently implicated the government authorities in Moscow.

Hackers had loaded onto a Ukrainian election commission server a graphic mimicking the page for displaying results. This phony page showed a shocker of an outcome: an election win for a fiercely anti-Russian, ultraright candidate, Dmytro Yarosh. Mr. Yarosh in reality received less than 1 percent of the vote.

The false result would have played into a Russian propaganda narrative that Ukraine today is ruled by hard-right, even fascist, figures.

The fake image was programmed to display when polls closed, at 8 p.m., but a Ukrainian cybersecurity company, InfoSafe, discovered it just minutes earlier and unplugged the server.

State television in Russia nevertheless reported that Mr. Yarosh had won and broadcast the fake graphic, citing the election commission's website, even though the image had never appeared there. The hacker had clearly provided Channel 1 with the same image in advance, but the reporters had failed to check that the hack actually worked.

"For me, this is an obvious link between the hackers and Russian officials," said Victor Zhora, director of InfoSafe, the cybersecurity company that first found the fake graphic.

A Ukrainian government researcher who studied the hack, Nikolai Koval, published his findings in a 2015 book, "Cyberwar in Perspective," and identified the Sofacy malware on the server.

The mirror of the hard drive went to the F.B.I., which had this forensic sample when the cybersecurity company CrowdStrike identified the same malware two years later, on the D.N.C. servers.

"It was the first strike," Mr. Zhora said of the earlier hack of Ukraine's electoral computers. Ukraine's Cyber Police have also provided the F.B.I. with copies of server hard drives showing the possible origins of some phishing emails targeting the Democratic Party during the election.

In 2016, two years after the election hack in Ukraine, hackers using some of the same techniques plundered the email system of the World Anti-Doping Agency, or WADA, which had accused Russian athletes of systematic drug use.

That raid, too, seems to have been closely coordinated with Russian state television, which began airing well-prepared reports about WADA's hacked emails just minutes after they were made public. The emails appeared on a website that announced that WADA had been hacked by a group calling itself the "Fancy Bears' Hack Team."

It was the first time Fancy Bear had broken cover.

Fancy Bear remains extraordinarily elusive, however. To throw investigators off its scent, the group has undergone various makeovers, restocking its arsenal of

malware and sometimes hiding under different guises. One of its alter egos, cyberexperts believe, is Cyber Berkut, an outfit supposedly set up in Ukraine by supporters of the country's pro-Russian president, Viktor F. Yanukovych, who was ousted in 2014.

After lying dormant for many months, Cyber Berkut jumped back into action this summer just as multiple investigations in Washington into whether the Trump campaign colluded with Moscow shifted into high gear. Cyber Berkut released stolen emails that it and Russian state news media said had exposed the real story: Hillary Clinton had colluded with Ukraine.

Correction: August 16, 2017

An earlier version of this article misstated how a type of malware known as P.A.S. was used in Russian hacking efforts in the United States that included the electronic break-in at the Democratic National Committee. The agencies identified the malware as a tool used in Russian hacking, but they did not specify in which attacks it was used.

A version of this article appears in print on August 17, 2017, on Page A1 of the New York edition with the headline: Code Writer in Ukraine Could Blow Whistle on Russian Hacking.
