Cybersecurity Researchers Are Hunted from All Sides

Written by **ANDRADA FISCUTEAN**

December 14, 2015 // 09:00 AM EST

Cybersecurity researcher Peter Kruse, founder of CSIS Security Group in Denmark, thought his mother was calling. Her number appeared on his phone, but when he answered, it wasn't her. Instead, a male voice told him to stop what he was doing as a computer expert.

"They checked my family members," he said, referring to his anonymous tormenters. "They did their homework."

Security researcher Costin Raiu at Kaspersky Lab in Romania has a similar story. While he was analyzing Stuxnet, a worm written by the US and Israel and considered to be the first cyber weapon (http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html), someone broke into his house.

The intruder left behind a decision cube—a rubber die inscribed with conclusions like "yes," "no," "maybe"—on his living room table with the message "take a break" facing up.

These stories of being threatened are common throughout the tight-knit community of high-profile cybersecurity researchers, but few are willing to share them openly.

"If you are engaged in tracking cybercriminals, in research, you have to be really careful about your surroundings, your family, the people around you," said Righard Zwienenberg, ESET security expert. "People doing this kind of research take the risk knowingly and willingly."

Enemies on all sides

While this secretive lifestyle might be alluring to some, most cybersecurity researchers are, by nature, geeks. Computer science taught in high-school and at university level did not prepare them for what can only be described as spy games.

Pinpointing the people behind the threats is next to impossible, as evidence is scarce. Many of the incidents aren't even reported. "Nobody believes you if you go to the police and say a rubber cube appeared in your house," Raiu said.

> "For a while, it turned my life upside down. I understood it was serious. That my research annoyed some powerful people."

In some cases, researchers say they suspect intelligence agencies, who may be protecting state interests. In the case of Stuxnet, the fact that it had been authored by the US and Israel was secret for two years after its discovery. In other instances, there could be cybercriminals involved, wanting to get the researchers' data or to silence their detective work.

Attacks may also happen simply “for the lulz,” as hackers often want to challenge or amuse themselves.

Threats can include “subtle pressure, patriotic enlistment, bribery, compromise and blackmail, legal repercussions, threat to livelihood, threat to viability of life in the actor’s area of influence, threat of force, or elimination,”depending on the attacker, cybersecurity expert Juan Andres Guerrero-Saade wrote in a paper (http://media.kaspersky.com/pdf/Guerrero-Saade-VB2015.pdf) presented this fall at the Virus Bulletin Conference in Prague.

The scariest threats may come from governments, he said.

“The researcher as a private individual faces unique challenges when in cross-hairs of a nation-state actor,” he wrote. “The operator of an espionage campaign is not a common criminal nor a simple citizen and his resources are truly manifold.”

Even “vague threats carry weight,” he noted.

“Take a break”

For this story, we spoke to 18 security researchers, most of whom declined to be named.

These threats are real, these researchers said, and not just paranoia inspired by their line of work—although they admit that living in fear can change your perception of the world.

“I arrived home at 7 PM. I saw the decision cube on the center of the table with the “take a break” side up,” Costin Raiu said. “We had the cube at Kaspersky Lab in Bucharest. It disappeared from there, and later showed up in my house.”

He said he doesn’t remember taking the cube home, and even had breakfast on that table in the morning. He said he cleared the table afterwards, before leaving for work. The date was November 29, 2010

He connects this incident to a strange feeling he had on September 30, the same year, during the Virus Bulletin Conference in Vancouver, where he gave a speech on Stuxnet (https://www.virusbtn.com/conference/vb2010/programme/index), filling in for his colleague Alexander Gostev, who didn’t get a visa for Canada.

“At that conference, we had three last-minute participants. They paid in cash several thousand dollars. All three of them wrote on the form that they were from GOI,” he said.

Raiu said he doesn't know what GOI stands for. He claimed, though, that judging by their appearance, they seemed to be coming from a Middle Eastern country. His was the only presentation the three attended, he said.

After the rubber cube incident, Costin Raiu did take a break from Stuxnet. "For a while, it turned my life upside down," he said. "I understood it was serious. That my research annoyed some powerful people."

A year and a half later, he reconsidered. His team was actively involved in analyzing Flame, a cyber weapon from the same family as Stuxnet, also aimed at attacking Middle Eastern countries, especially Iran. This sophisticated malware was, again, allegedly developed by the US and Israel, the Washington Post reported (https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html).

"Letting yourself be intimidated is a mistake," Raiu said. "What we do is important."

Intimidating phone calls

Peter Kruse did report his incident to the police back late 2011 when it happened. The Danish researcher explained he received threats by phone, and that the attacker appeared to be calling from his mother's number.

"The police told me that the call was made from the UK. I've never heard from the investigators again," he said. He still doesn't know who threatened him.

He believes the threat was likely related to his work on Multibanker/Patcher Trojan, which attacked online banks. The malware quietly harvested data from thousands of infected computers, many in Denmark. The hackers behind the malware probably didn't like him poking around, he said.

This isn't his only incident. "I've received threats on the internet many times, by email," he said. At some point, wrongdoers even used his name to spread malware (http://blog.check-and-secure.com/peter-kruse-csis-dk-scam-cyberkriminelle-warnen-vor-virengefahr/). "They sent emails on my behalf, with a file attached."

It's impossible to be 100 percent secure, no matter who you are, he said.

Bombs

Sometimes, the source of attacks is easier to identify. Russian security company Dr. Web, whose products are used by banking, telecom and oil companies, was bombed with Molotov cocktails after its researchers revealed that a gang created and sold a Trojan able to steal money from ATMs.

Dr. Web received a threat by email (https://antifraud.drweb.com/atm_trojs/drweb/?lng=en) saying the company had a week to delete all references to the group posted online. "Otherwise syndicate will stop cash-out transactions and send criminal for your programmers' heads," the note read. "The end of Doctor Web will be tragic."

CEO Boris Sharov decided not to satisfy the demand.

In March 2014, a company in St. Petersburg that distributed Dr. Web's ATM Shield software was attacked three times with Molotov cocktails, with limited damage. There have also been two physical intrusions into Dr. Web's office in Moscow.

The security company believes that the Molotov cocktail attacks were executed by strangers paid over the internet by a group of developers who sold software to several gangs specialized in cashing out hacked ATM cards. A bank in Moscow was able to confirm that the team was operating from Kiev, Ukraine, the CEO Boris Sharov told cybersecurity journalist (http://krebsonsecurity.com/2015/09/atm-skimmer-gang-firebombed-antivirus-firm/) Brian Krebs.

Swatting

Krebs, the reporter Sharov spoke to, has his own stories of being harassed for cybersecurity research.

In the spring of 2013, police received a phony emergency call from his house, a practice known as "swatting," or calling in a false 911 emergency that will bring a SWAT (Special Weapons Attack Team) force to a victim's home.

> Cybersecurity researchers know how to guard themselves in the digital world. What they are worried about more is their real lives, and those of their families

“[T]he caller claimed to be me, reporting that Russians had broken into the home and shot my wife,” Krebs wrote on his blog (http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/).

He has made many enemies in the course of his reporting on hackers, and he figured something like this would happen to him eventually. The journalist had alerted his local police six months before, but the police still took the threat seriously. Officers came to Krebs’s house, pointed shotguns and assault rifles at him, and handcuffed him, before letting him go and apologizing.

The swatting incident happened together with a DDoS attack on his blog.

Then in the summer of 2013, Krebs received a heroin package (http://krebsonsecurity.com/2013/07/mail-from-the-velvet-cybercrime-underground/) from “the administrator of an exclusive cybercrime forum” who wanted to frame him. The journalist saw the scam being planned on a forum in real time and called the police before the delivery was even made. The hacker responsible is now being charged

Latest Videos

Documentaries (/tag/documentaries?trk_source=nav)

Interviews (/tag/interviews?trk_source=nav)

nsecurity.com/2015/10/hacker-who-sent-me-heroin-faces-charges-in-u-s/).

reported that hackers have opened new lines of credit on his behalf, paid his

n credit cards, and used his name and likeness online.

Paranoia

any groups want access to their findings, cybersecurity experts must secure

hones, and conversations.

“Cybersecurity researchers are paranoid by nature. All my communication is encrypted,” Kruse said.

These researchers take extra measures while attending cybersecurity conferences, for example. Whenever they leave a laptop unattended in a hotel room, they close it and spread some cables on top of it. And then, they take a picture. “If someone opens the laptop, it’s virtually impossible to rearrange the cables in the same way,” Raiu said.

At one such cybersecurity conference, Raiu said, he left his laptop in a hotel room to get a coffee. When he came back, he realized someone else had been there: The intruder didn’t even bother to close the laptop.

Two experts who prefer to remain anonymous confessed that they exchange messages by hiding them in the code they post online. They use the internet to share information and try to avoid the GSM cellular infrastructure. Some even stay in Faraday cages, which block electric fields and radio signals, to avoid being snooped on when they have face to face conversations.

Cybersecurity researchers know what to do to safeguard themselves in the digital world. What they are worried about more is their real lives, and those of their families.

“People snooping on me will know that I’m vulnerable in some ways in the physical world,” Kruse said.

That means cybersecurity researchers will have to get used to a James Bond lifestyle.

“I don’t think there’s anything anyone can do to protect people working in this field,” Raiu said.

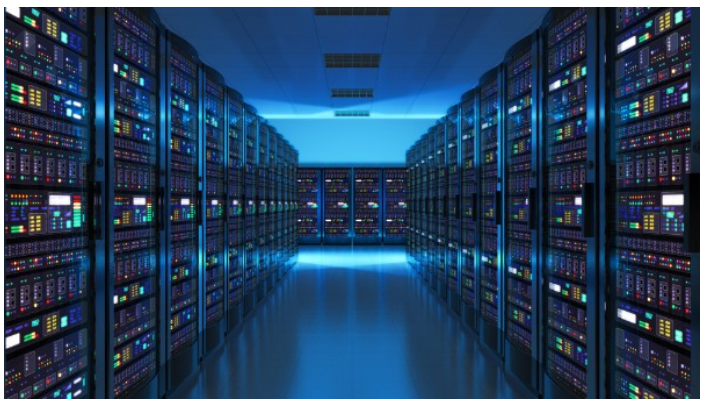
Contact the author: andradaf@gmail.com (mailto:andradaf@gmail.com) **(PGP** (https://pgp.mit.edu/pks/lookup?op=get&search=0xFC1A72769ECECACA)**)**

--

TOPICS: security (/tag/security), infosec (/tag/infosec), peter kruse (/tag/peter+kruse), costin raiu (/tag/costin+raiu), kaspersky lab (/tag/kaspersky+lab), stuxnet (/tag/stuxnet), harassment (/tag/harassment), intimidation (/tag/intimidation)

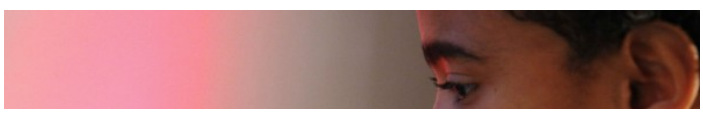
to see other people talking about Motherboard? Check out our letters to the editor (http://motherboard.vice.com/tag/letters+to+the+editor).

RECOMMENDED



How Databases with Personal Info Get Accidentally Left Open on the Public Web (/read/how-databases-with-personal-info-get-accidentally-left-open-on-the-public-web?trk_source=recommended)

Twitter Told a Bunch of Users They May Be Targets of a 'State Sponsored Attack' (/read/twitter-told-a-bunch-of-users-they-may-be-targets-of-a-state-sponsored-attack?trk_source=recommended)



British Cops Arrested a Man They Suspect of Hacking VTech (/read/british-cops-arrested-a-man-they-suspect-of-hacking-vtech?trk_source=recommended)

The Sweeping OPM Hack Also Compromised White House Journalists (/read/the-sweeping-opm-hack-also-compromised-white-house-journalists?trk_source=recommended)

MOST POPULAR

(/read/yahoo-had-a-party?trk_source=popular)

Yahoo Had a Party (/read/yahoo-had-a-party?trk_source=popular)

(/read/star-wars-fan-explains-what-he-was-thinking-in-his-phantom-menace-tv-interview?

trk_source=popular)

Star Wars Fan Explains What He Was Thinking in His ‘Phantom Menace’ TV Interview (/read/star-wars-fan-explains-what-he-was-thinking-in-his-phantom-menace-tv-interview?trk_source=popular)

(/read/weezers-bizarre-copyright-crackdown-on-hash-pipe?trk_source=popular)

Weezer's Bizarre Copyright Crackdown on 'Hash Pipe' (/read/weezers-bizarre-copyright-crackdown-on-hash-pipe?trk_source=popular)

(/read/ill-register-my-drone-when-you-have-to-register-your-gun?trk_source=popular)

I'll Register My Drone When You Have to Register Your Gun (/read/ill-register-my-drone-when-you-have-to-register-your-gun?trk_source=popular)

(/read/jose-cansecos-guide-to-terraforming-mars?trk_source=popular)

We Asked Astrobiologists About Jose Canseco's Plan to Terraform Mars (/read/jose-cansecos-guide-to-terraforming-mars?trk_source=popular)

(/read/rollercoaster-tycoon-sadist-creates-210-day-long-hell-coaster?trk_source=popular)

‘Rollercoaster Tycoon' Sadist Creates 210 Day-Long Hell Coaster (/read/rollercoaster-tycoon-sadist-creates-210-day-long-hell-coaster?trk_source=popular)

---

print