NB researcher launches project to help track authors of malware

The Canadian Press

October 7, 2015

Share this article f Facebook Twitter Email

Natalia Stakhanova, centre, the NB Innovation Research Chair in Cyber Security at the University of New Brunswick, has begun a five-year research project aimed at trying to determine the digital profile of people developing certain types of malicious software, or malware. Photo: Rob Blanchard/ Submitted

FREDERICTON • As use of the Internet has exploded, so has the number of malware attacks around the world and now a researcher at the University of New Brunswick is trying to unlock the digital fingerprints of hackers who are after your money and personal information.

“A typical computer user can host a lot of profitable things for a hacker,” said Natalia Stakhanova, a professor at the school’s Information Security Centre of Excellence.

Stakhanova has begun a five-year research project aimed at trying to determine the digital profile of people developing certain types of malicious software, or malware.

She is focusing on the binary side of existing malware to look for clues about the source of an infection and the kinds of tools used to develop it. Her team will also try to determine whether the malware was targeting a specific person or if it is more random.

“We hope to at some time to be able identify where it comes from. So we’ll know who wrote it, why he wrote it, how it was written, and where that person lives,” she said.

“It’s probably going to take us a while.”

According to a 2014 report by Intel Security, the estimated annual cost to the global economy from cybercrime is more than $400 billion.

In recent years there have been a number of major malware attacks on large retailers, such as Target and Home Depot, giving the malware creators access to the personal information of shoppers.

Doug Cooke, director of sales engineering at Intel Security Canada, said the work of researchers like Stakhanova is very important.

“If they are starting to understand the attributes of those types of people or what motivates them, then maybe all of us can start ferreting them out a little bit easier and help to put a dent in this,” he said.

Cooke said the hackers have become more sophisticated and quickly launch variants of their malware once earlier versions are detected and defences put in place.

“It has been an increasing arms race over time,” he said, noting that more than 400 million different pieces of malware have been detected around the world.

“They’re looking to make money and use your computer for some gain, such as launching a spam campaign which could result in dollars, or to gain information off your computer that could be of value.”

According to the McAfee Labs Threats Report for August 2015, the threat of malware spreads well beyond home and business computers as we adopt new technology connected to the Internet, such as smartphones and other devices.

It suggests technology linked to healthcare, energy, retail, cities and transportation are also vulnerable.

“Attackers are not after the devices themselves but the data or gateway capability that they enable,” it said.

“Cloud adoption has changed the nature of some attacks, as devices are attacked not for the small amount of data that they store, but as a path to where the important data resides.”

Cooke said companies need to be more proactive in building a full program for thwarting malware, which goes beyond just having protective software to being able to react quickly in the event of an attack.

“If you have a breach, how do you handle that from a media perspective, but also how you’re going to react technically to minimize its impact,” he said.

Stakhanova said individuals also need to protect themselves by encrypting personal information and keeping it on an external drive, and ensuring you have updated malware protection.

“You need passwords that are long and complicated and don’t contain the name of your dog or your spouse,” she said.

Share this article Facebook Twitter Email