Improved technology aids criminals in brazen cyber attacks

October 6 2015, by Brian L. Huchel

Computer viruses and malware are obsolete scams for the latest wave of increasingly aggressive computer criminals, says a top cyber forensics expert at Purdue University.

Marcus Rogers, director of Purdue's Cyber Forensics Lab, said past reports of cyber attacks—allegedly by foreign nations—have opened the floodgates for computer criminals to launch their own illegal efforts.

"They figure it is open season now," said Rogers, a former police investigator working in the area of fraud and computer investigations, who still works with law enforcement. "There are going to be less resources law enforcement and the intelligence community can put to bear on these cases when they're spread so thin."

October is National Cyber Security Awareness Month.

Improved technology, in part, has led to more brazen criminal efforts. Phishing attacks— emails disguised as various entities to obtain sensitive information—are on the rise. Rogers said a new kind of attack called "ransomware" has surfaced. It encrypts parts of a computer or the entire system until the user pays to get a decryption password from the criminal.

There have been reports of businesses being hit by ransomware, but any computer user faces the risk. A person could see 10 years of family pictures encrypted.

"They're using pretty sophisticated encryption, so it's not practical for most people to try to break it on their own," said Rogers, a professor in the Purdue Polytechnic Institute. "It's hitting everybody."

It's a race to utilize the most sophisticated technology, Rogers says, and right now the bad guys have the best tech. It puts more responsibility on the users to police the emails coming into their computers every day.

"You now have to be your own cyber cop," he said. "You have to take responsibility for paying attention to what's going on yourself. The technology is not going to do it for you. The attacks are slicing right through our technology."

With estimates that at least 95 percent of email traffic in the world consists of spam and phishing, it's obvious another solution is necessary, Rogers said. Artificial intelligence is among the next steps being considered, combining technology and the human ability to look at information quickly and make a decision.

Rogers said Google, Amazon and Windows are all making strides in that regard, with the possibility of a solution being on the market in five years.

Until then, however, cyber criminals are targeting anyone who logs onto a computer. Rogers urges users to practice caution.

"You don't want to mistrust everything you get," he said. "Trust it but verify it first."

Provided by Rutgers University