Extortion extinction: Researchers develop a way to stop ransomware

July 8 2016, by Steve Orlando

Credit: University of Florida

Ransomware - what hackers use to encrypt your computer files and demand money in exchange for freeing those contents - is an exploding global problem with few solutions, but a team of University of Florida researchers says it has developed a way to stop it dead in its tracks.

The answer, they say, lies not in keeping it out of a computer but rather in confronting it once it's there and, counterintuitively, actually letting it lock up a few files before clamping down on it.

"Our system is more of an early-warning system. It doesn't prevent the ransomware from starting ... it prevents the ransomware from completing its task ... so you lose only a couple of pictures or a couple of documents rather than everything that's on your hard drive, and it relieves you of the burden of having to pay the ransom," said Nolen Scaife, a UF doctoral student and founding member of UF's Florida Institute for Cybersecurity Research.

Scaife is part of the team that has come up with the ransomware solution, which it calls CryptoDrop.

Ransomware attacks have become one of the most urgent problems in the digital world. The FBI issued a warning in May saying the number of attacks has doubled in the past year and is expected to grow even more rapidly this year.

It said it received more than 2,400 complaints last year and estimated losses from such attacks at $24 million last year for individuals and businesses.

Attackers are typically shadowy figures from other countries lurking on the Dark Web and difficult, if not impossible, to find. Victims include not only individuals but also governments, industry, health care providers, educational institutions and financials entities.

Attacks most often show up in the form of an email that appears to be from someone familiar. The recipient clicks on a link in the email and unknowingly unleashes malware that encrypts his or her data. The next thing to appear is a message demanding the ransom, typically anywhere from a few hundred to a few thousand dollars.

"It's an incredibly easy way to monetize a bad use of software," said Patrick Traynor, an associate professor in UF's department of computer and information science and engineering at UF and also a member of the Florida Institute for Cybersecurity Research. He and Scaife worked together on developing CryptoDrop.

Some companies have simply resigned themselves to that inevitability and budgeted money to cover ransoms, which usually must be paid in Bitcoin, a digital currency that defies tracing.

Ransomware attacks are effective because, quite simply, they work.

Antivirus software is successful at stopping them when it recognizes ransomware malware, but therein lies the problem.

"These attacks are tailored and unique every time they get installed on someone's system," Scaife said. "Antivirus is really good at stopping things it's seen before ... That's where our solution is better than traditional anti-viruses. If something that's benign starts to behave maliciously, then what we can do is take action against that based on what we see is happening to your data. So we can stop, for example, all of your pictures form being encrypted."

Scaife, Traynor and colleagues Kevin Butler at UF and Henry Carter at Villanova University lay out the solution in a paper accepted for publication at the IEEE International Conference on Distributed Computing Systems and scheduled to be presented June 29 in Nara, Japan.

The results, they said, were impressive.

"We ran our detector against several hundred ransomware samples that were live," Scaife said, "and in those case it detected 100 percent of those malware samples and it did so after only a median of 10 files were encrypted."

And CryptoDrop works seamlessly with antivirus software.

"About one-tenth of 1 percent of the files were lost," Traynor said, "but the advantage is that it's flexible. We don't have to wait for that anti-virus update. If you have a new version of your ransomware, our system can detect that."

The team currently has a functioning prototype that works with Windows-based systems and is seeking a partner to commercialize it and make it available publicly.

Provided by University of Florida