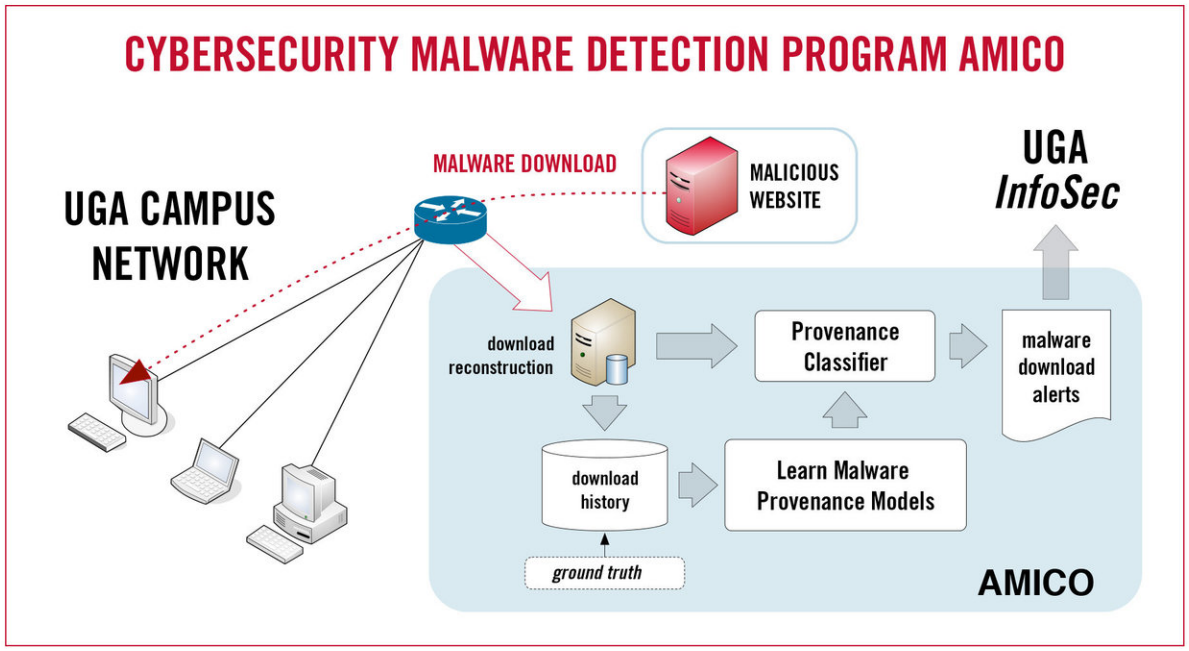
Georgia malware, cybersecurity research helps make internet safer

June 25 2018



Credit: University of Georgia

The internet has made many things easier.

You can buy just about anything, make bank transactions and find information on almost any topic all without leaving the comfort of your living room couch.

With the increased connectivity, though, comes a new and ever-evolving threat: cybercrime.

The University of Georgia is fighting back with its recently established Institute for Cybersecurity and Privacy, a state hub for cybersecurity research and education.

The university is already reaping rewards from establishing the center, by using the anti-malware software developed by the institute's network security expert, Roberto Perdisci, to detect malware downloads on its own networks. The University of Alabama-Birmingham is also using Georgia's tool to monitor its systems.

"Your antivirus software installed on your computer to protect against malware attacks will always be behind," Perdisci says. Such software scans downloads for malicious code, but cybercriminals have found ways to disguise malware as legitimate-looking code, enabling them to evade traditional security measures. "I'm not saying the antivirus products are useless—they're not useless—but they're much less useful than they used to be."

That's why he created AMICO, the open-source software system that analyzes where downloads are sourced from online and detects malware downloads with startling accuracy, flagging 95 percent of malicious downloads on a network serving tens of thousands of users and alerting network security personnel to malware other defenses missed.

Grants from the Department of Homeland Security and the National Science Foundation are helping take AMICO to the next level with grants to get the software to a wider market than just institutes of higher education.

The goal for Perdisci is to make the internet a more secure place.

"Ideally," he says, "users may not even notice that we've done something to improve cybersecurity because they will just go about their business without having to deal with malware infections, not having to deal with scams, not having to deal with anything else that is a potential threat."

What complicates cybersecurity efforts is the rapidly evolving nature of both the internet and types of online crime.

"The problem is that we're dealing with human beings, and human beings are very intelligent and creative so the threats to our cybersecurity change all the time," says Perdisci. "The services and technologies people use change all the time as well, so you have this combination of two rapidly changing factors that makes cybersecurity really, really challenging."

As Perdisci points out, cybercrime isn't really that different from traditional crime. Both involve people who are determined to exploit vulnerabilities in systems and other people and profit from doing so. But one takes place in cyberspace, making it slightly more intricate to track than crimes with physical evidence left behind. His work on understanding the mechanisms behind cyberattacks and the distribution of malicious software, however, is helping inform new ways of fighting back.

"Cybercrime will never go away completely," Perdisci says. "But the investments in cybersecurity that universities like UGA are making are helping us get much, much better at fighting it. We may not eliminate it completely, but the important thing is to make cybercriminal activities less impactful, less damaging to normal users. That's, I think, a realistic goal that we can and are working toward."

Provided by University of Georgia