Georgia Research Alliance

25 Breakthroughs in Georgia

NO. 18:

Algorithms to detect cyber invaders

Zombie armies aren't just science fiction. They're also a major type of computer security threat – vast networks of infected laptops, phones and other devices known as "bot nets."

These compromised devices number up into the millions, and they helplessly follow the "bot master's" commands to carry out cyber crimes, unbeknownst to the owner of the device.

Although bot nets are well known today, they were a novel concept back in 2005. Computer science professor Wenke Lee and his research group at Georgia Tech were among the first to study this next-generation threat and sound the alarm about their danger.

Their breakthrough came when they discovered that the key to stopping bot nets was recognizing the unique patterns of web traffic they spawned — and tracing these communications back to the source.

Lee and his group developed algorithms to identify the key signatures of communication between bot nets and their master: characteristics like the pattern and number of queries, or even the time of day. Using these algorithms, they could monitor an entire network for the suspicious communications that suggested a bot was phoning home to its controlling source.

With their research results in high demand, Lee and his Georgia Tech colleague Merrick Furst and postdoc student David Dagon launched Damballa. In summer 2016, Damballa was acquired by Core Security, an industry-leading network security company.

The war against malicious cyber threats may never end, but the ingenuity of Georgia Tech researchers gives the "good guys" a major advantage.

"25 Breakthroughs in Georgia" celebrates 25 years of the Georgia Research Alliance. GRA expands research and commercialization capacity in Georgia's universities to launch new companies, create high-value jobs and transform lives. More: GRA.org