Georgia Tech releases cyber threats forecast for 2012

October 11 2011

The year ahead will feature new and increasingly sophisticated means to capture and exploit user data, as well as escalating battles over the control of online information that threatens to compromise content and erode public trust and privacy. Those were the findings announced by the Georgia Tech Information Security Center (GTISC) and the Georgia Tech Research Institute (GTRI) in today's release of the 'Georgia Tech Emerging Cyber Threats Report for 2012.' The report was released at the annual Georgia Tech Cyber Security Summit, a gathering of industry and academic leaders who have distinguished themselves in the field of cyber security.

According to GTISC, GTRI and the experts cited in the report, specific threats to follow over the coming year include, among others:

- Search Poisoning – Attackers will increasingly use SEO techniques to optimize malicious links among search results, so that users are more likely to click on a URL because it ranks highly on Google or other search engines.
- Mobile Web-based Attacks – Expect increased attacks aimed specifically against mobile Web browsers as the tension between usability and security, along with device constraints (including small screen size), make it difficult to solve mobile Web browser security flaws.
- Stolen Cyber Data Use for Marketing – The market for stolen cyber data will continue to evolve as botnets capture private user

information shared by social media platforms and sell it directly to legitimate business channels such as lead-generation and marketing.

The entire report is available at http://gtsecuritysummit.com/report.html.

"We continue to witness cyber attacks of unprecedented sophistication and reach, demonstrating that malicious actors have the ability to compromise and control millions of computers that belong to governments, private enterprises and ordinary citizens," said Mustaque Ahamad, director of GTISC. "If we are going to prevent motivated adversaries from attacking our systems, stealing our data and harming our critical infrastructure, the broader community of security researchers—including academia, the private sector and government—must work together to understand emerging threats and to develop proactive security solutions to safeguard the Internet and physical infrastructure that relies on it."

Today's Georgia Tech Cyber Security Summit is one forum where the IT security ecosystem can gather together to discuss and debate the evolving nature of cyber threats, and to chart the course for creating solutions through collaborations among industry, government and academia. The Summit was keynoted by Admiral William J. Fallon, U.S. Navy (retired) and included a panel of security experts from Equifax, The Financial Services Roundtable, Mobile Active Defense, Reputation.com and GTRI.

"Our adversaries, whether motivated by monetary gain, political/social ideology, or otherwise are becoming increasingly sophisticated and better funded," said Bo Rotoloni, director of GTRI's Cyber Technology and Information Security Laboratory (CTISL). "Acting as individuals or groups, these entities know no boundaries, making cyber security a

global problem. We can no longer assume our data is safe sitting behind perimeter-protected networks. Attacks penetrate our systems through ubiquitous protocols, mobile devices and social engineering, circumventing the network perimeter. Our best defense on the growing cyber warfront is found in cooperative education and awareness, best-of-breed tools and robust policy developed collaboratively by industry, academia and government."

Provided by Georgia Institute of Technology