Conquering Computer Zombies in Real Time

American Friends of Tel Aviv University

Tel Aviv — Cyber attacks are the primary domestic security threat facing the United States, FBI Director James Comey told the Senate Homeland Security Committee last year. In our brave new world, traditional warfare is now inextricably linked to economic and cyber warfare. In just one example, cyber strikes have the potential to derail a nation's power grid, causing widespread damage, chaos and loss of life. That's why surveillance programs must keep one step ahead of the perpetrators to secure civilian networks, cyberspace, and infrastructures essential to daily life.

*Prof. Yehuda Afek*and *Shir Landau-Feibish*of *Tel Aviv University's Blavatnik School of Computer Sciences* have joined forces with Prof. Anat Bremler-Barr of the Interdisciplinary Center in Herzliya to develop new technology that combats high-volume attacks by armies of "computer zombies." The researchers have devised an algorithm that identifies malicious content related to distributed denial of service (DDoS) attacks — attacks that direct high volume traffic to a single targeted site to shut down websites, banks, companies, and essential government and civil infrastructure functions.

The researchers' "double heavy hitters algorithm," presented last October at the annual Symposium on Architectures for Networking and Communications Systems conference in California and published in *IEEE Xplore*, is capable of finding even the smallest set of cyber clues or footprints (known as "signatures") required to detect attacks that may currently slip under the radar. Their work is supported by the Israeli Industry, Trade and Labor Ministry's Kabarnit-Cyber Consortium Magnet Program.

Zombies on the march

"Security is like electronic warfare. They get smarter, and we have to get smarter with them," says Landau-Feibish. "The only way to identify the signature of the new attackers is to devise new technology that will automatically review huge amounts of data in real time and find common patterns that the human eye would easily miss.

"We are focused on 'zero-day' attacks, attacks about which we have no prior knowledge, perpetrated by huge armies of computer zombies called 'botnets' — computers that have been unknowingly programmed to participate in a larger strike without their owners' knowledge," Landau-Feibish said. "In the past, source verification methods combined with traffic behavioral analysis were enough to identify and distinguish the source of the malicious attack. But now, in the face of huge zombie-armies, these methods are insufficient. A new method is required."

Security companies today painstakingly conduct real-time analysis of web traffic to identify cyber attackers. But, since terrorists now hide behind the guise of seemingly legitimate traffic and countless "innocent" computer sources, analysts are forced to change their tactics to become more efficient.

Malicious traffic

In their study, the researchers compared content extracted from normal traffic with content from attack traffic to identify the telltale footprints of attackers. The well-known "heavy hitters" streaming algorithm, which functions only with numerical values, served as a base for the new algorithm, which is able to detect frequent and varying sequences of characters in the traffic.

"A footprint can be so very small — even a single character that is out of place in a certain context," said Landau-Feibish. "Security companies need time to sift through traffic to identify these footprints. In the meantime, the customers' sites are gridlocked. We were able to cut down that time as well as decrease false positives, peaceful traffic misidentified as malicious, and false negatives — malicious traffic originally identified as safe."

The team is currently working on a "triple heavy hitter" algorithm, which will identify combinations of footprints to further improve the identification of DDoS strikes. The researchers are also exploring ways of expanding their methods to identify other types of attacks.