Researchers have discovered multiple botnets

January 27 2016

Ben-Gurion University of the Negev cyber security researchers have discovered and traced approximately six botnets by analyzing data collected from past cyber attacks. The research was conducted at Deutsche Telekom Innovation Labs@BGU and was announced at Cybertech 2016 in Tel Aviv today.

Botnets are networks of malicious, remotely updatable code that covertly lurk on infected computers. Using botnets, which until now were largely untraceable, hackers and cyber criminals can carry out powerful attacks, spread viruses, generate spam, and commit other types of online crime.

Deutsche Telekom Innovation Labs@BGU is an innovative research facility staffed by BGU faculty and student teams that conduct cutting-edge cyber security research.

Led by BGU Prof. Bracha Shapira and Prof. Lior Roach, the team analyzed data captured by a "honeypot" network run by Deutsche Telekom, the worldwide telecommunications company. The team developed and implemented advanced algorithms to identify the botnet by finding similar attack patterns that can then be traced back to its administrator. They were able to identify six distinct botnets, each capable of inflicting serious criminal and monetary damage.

Dudu Mimran, chief technology officer of Deutsche Telekom Innovation Labs@BGU, said, "This is the first time such a comprehensive study has been carried out and returned with unique findings. In addition, we were able to identify whether the attack

emanated from a real person or from a robot and predict future attacks."

In 2014, law enforcement agencies revealed that they had disrupted a Russian botnet that targeted personal bank accounts and stole $100 million.

Ben-Gurion University of the Negev is the academic sponsor of CyberTech, Israel's largest cyber security event, organized by the Israel Defense Forces (IDF).

Provided by American Associates, Ben-Gurion University of the Negev

Citation: Researchers have discovered multiple botnets (2016, January 27) retrieved 19 April 2024 from https://phys.org/news/2016-01-multiple-botnets.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.