PHYS.ORG

A system that identifies malicious patterns in network traffic

November 1 2017

The majority of cyber-security solutions that stand between us and increasingly sophisticated malware, target only specific attacks or subsets of attacks, meaning that users may have to buy and install many different products to protect themselves. Now, A*STAR researchers have developed a system that instead gathers evidence across a wide stream of internet traffic, and identifies links and correlations related to suspicious activity.

"Our aim is to develop a framework to gather as much evidence as possible from a set of traffic, and indicate malicious anomalies, regardless of the type of attacks," says Vrizlynn Thing at the A*STAR Institute for Infocomm Research, who led the study.

Thing and her team designed their new framework to look out for the fundamental characteristics of the malicious activities that stalk unsuspecting users through the evolving cyber landscape. Through this approach, the framework is robust against new threatening software and gathers only relevant evidence on the threats. For example, the system looks out for data flows that arrive at fixed time intervals, because attack bots are much less random than ordinary human-generated internet activities. The model also identifies sources that try to communicate with a large number of destinations in a short time, which is indicative of a botnet.

"The main challenge was devising ways to build up a large set of possible patterns which could serve as potential evidence for detecting a wide variety of anomalies," says Thing. "We capture the persistent characteristics of the malicious activities in transit, and represent them in observable sequential forms. This has allowed us to detect very fundamental patterns related to malicious traffic."

The team tested their new evidence-gathering system on recorded internet traffic, and found it could quickly identify many notorious botnets such as Andromeda, Zeus and Sality, with very few false positives. Given this success, Thing is hopeful that by improving their detection patterns, their system could defend networks against a much wider variety of attacks than has previously been possible.

"If we can detect malware infections by analyzing network traffic, we can prevent malware from further spreading," she says. "We could also trigger the disconnection of infected hosts, thereby curbing the rampant growth of botnets."

More information: Dinil Mon Divakaran et al. Evidence gathering for network security and forensics, *Digital Investigation* (2017). DOI: 10.1016/j.diin.2017.02.001

Provided by Agency for Science, Technology and Research (A*STAR), Singapore

Citation: A system that identifies malicious patterns in network traffic (2017, November 1) retrieved 10 April 2024 from https://phys.org/news/2017-11-malicious-patterns-network-traffic.html