Researchers devise new method of detecting botnets

March 25 2011

(PhysOrg.com) -- With the threat of Botnets increasing, researchers in the Department of Electrical and Computer Engineering at Texas A&M University have devised a new method to detect their activity.

A botnet, or robot network, is a term used to describe a collection of computers that have been compromised by a worm or Trojan horse, allowing an attacker to remotely control the systems. Victims are typically unaware that they are infected or that their system is being controlled remotely by a botnet administrator.

Dr. Narasimha Reddy — in collaboration with his students Sandeep Yadav and Ashwath Reddy at Texas A&M and Supranamaya “Soups” Ranjan with Narus Inc. — came up with a method of detecting botnets like Conficker, Kraken and Torpig that use so-called DNS domain-fluxing for their command and control (C&C) infrastructure.

Domain-fluxing bots typically generate random domain names; a bot basically queries a series of domain names, but the domain owner registers just one. To get to the C&C, botnet researchers typically reverse-engineer the bot malware and figure out the domains that are generated on a regular basis, a time- and resource-intensive process, in an attempt to discern all of the domain names that would be registered by a botnet so they can jump ahead and register them in order gain a foothold in their investigation.

While there are other methods of detection, Reddy’s method basically looks at the pattern and distribution of alphabetic characters in a domain name to determine whether it’s malicious or legitimate. This allows them to spot botnets’ algorithmically generated (rather than generated by humans) domain names.

“Our method analyzes only DNS traffic and hence is easily scalable to large networks,” said Reddy, the J.W. Runyon, Jr. ’35 Professor I in the department. “It can detect previously unknown botnets by analyzing a small fraction of the network traffic.”

Botnets using both IP fast-flux and domain fast-flux can also be detected by the proposed technique. IP fast-flux is a round-robin method where malicious websites are constantly rotated across several IP addresses, changing their DNS records to prevent their discovery by researchers, ISPs or law enforcement. Reddy’s new detection method discovered two new botnets with their method. One of the new botnets generates 57 character long random names and the second botnet generates names using a concatenation of two dictionary words.

CERT, a nationwide network security coordination lab, is building a tool based on Reddy’s technique and this tool will be widely distributed for public use. Reddy expects this to be a useful tool because of its speed and simplicity.

More information: Further details on their research are available here.

Provided by Texas A&M University

Citation: Researchers devise new method of detecting botnets (2011, March 25) retrieved 18 April 2024 from https://phys.org/news/2011-03-method-botnets.html