

TRACK: IT Security Advanced
SESSION #: ITA#5
DATE: Tuesday April 20, 2010
TIME: 8:30-9:45am
SESSION TITLE: "It Takes an EcoSystem To Effectively Defend Against Modern Malware"
SPEAKER(S): Dr. Fengmin Gong – Chief Scientist, Network Security
ORGANIZATION: HuaweiSymantec

ABSTRACT: "It Takes an EcoSystem To Effectively Defend Against Modern Malware"

Botnet has become the preferred infrastructure for cyber crimes. Botnet infection has become a global pandemic threatening the privacy of citizens, the profitability of businesses, and the national security of our nation. Besides the direct loss it causes businesses, Botnet attacks are shaking people's confidence in E-commerce. Not only that specific Botnets have been found to be used for industrial espionage or political activism, Botnet-based "software as a service" has been offered for spamming, DDoS, and spear-phishing.

Botnet is a network-distributed threat technology by design. It has a coherent strategy for robust infection, stealthy growth and operation, and for surviving countermeasures. To its credit, Botnet uses command and control (C&C) structure to support automated operation which allows great flexibility and adaptability; it uses multiple vectors of infection, multiple methods of malware installation, and multiple C&C servers, which makes it difficult to detect and take down. Existing security solutions are inadequate at mitigating Botnet threats. Two fundamental problems account for this failure of the existing solutions. First, the basic detection technologies are not keeping up with the evasive multi-vector techniques used by the Botnet to spread and conduct attacks. Signature-based detection does not work well unless accurate signatures are available timely; Memory-violation based detection, which has been used in many host-based security solutions can be bypassed through new techniques of control-flow redirection or social engineering; Moreover, host-based solutions also suffered from the lack of consistent deployment. Enforcing patching and configuration policies on desktops have always been a challenge for large enterprises, adding mobile workforce to the mix has made the matter worse. Second, existing solutions are mostly designed as a "point solution" for some threats, so they are typically deployed in isolation. A firewall by itself cannot recognize a Botnet infection, although it could block Botnet if given accurate C&C server information; An IPS deployed at a given location may not see an infection attack at all, but it could block the Botnet activities if given accurate signatures for them; An AV gateway can protect many hosts behind it from a new malware, if intelligence information is extracted from the first detection and distributed to the gateway in a timely fashion.

What's the lesson? We need an anti-Botnet ecosystem, consisting of enforcement devices such as switches/routers, firewalls, and UTM etc, powered by an effective intelligence creation and distribution network. The intelligence will contain information for detecting infection, for identifying bots and C&C servers, and for cleaning up infected hosts. The best strategy is to extract accurate and complete intelligence about a Botnet on the first sight, to feed the intelligence throughout the ecosystem as quickly as possible, and for all the enforcement devices to take control actions.

SPEAKER BIO(S): As Chief Scientist in Network Security, Gong is responsible for defining the direction and leading the R&D effort to bring advanced security capabilities to HuaweiSymantec products. He brings over 25 years of security expertise formerly serving as Chief Security Content Officer at FireEye, founder & Chief Scientist at Palo Alto Networks, Chief Scientist at McAfee, and founder of IntruVert Networks (acquired by McAfee), and Director of Advanced Networking Research at MCNC. He's an inventor of 7 awarded patents in security areas and has published over 40 papers.

His academic background includes professorial appointment North Carolina State University and research roles at Washington University. Gong holds a D.Sc. and M.S. in Computer Science from Washington University in St. Louis and a B.Eng. and M.Eng. in Computer Science from Xi'an Jiaotong University.