

EVENT FLASH

Trend Micro Announces InterCloud Security Service: Botnets Beware

Brian E. Burke

IN THIS EVENT FLASH

This IDC Flash discusses Trend Micro's InterCloud Security Service and analyzes its impact on the IT security market.

SITUATION OVERVIEW

On September 25, 2006, Trend Micro Inc., a leader in network antivirus and content security software and services, announced the release of InterCloud Security Service, a unique solution for identifying botnet activity and offering customers the ability to quarantine and optionally clean bot-infected PCs. InterCloud Security Service is designed to meet the performance and scalability requirements of Internet service providers (ISPs), universities, and other large network providers. The solution incorporates the InterCloud Service Delivery Platform and a service subscription that leverages Trend Micro's expertise in threat identification, analysis, mitigation, and remediation.

InterCloud Security Service specifically addresses the mounting threat posed by botnets — networks of compromised machines that can be remotely controlled by an attacker. Threats associated with botnets include click fraud, distributed denial-of-service (DDoS) attacks, spam, identity theft via phishing and pharming techniques, and other crimeware-related activity. Trend Micro's new service relies on patent-pending behavioral analysis technology known as Behavioral Analysis Security Engine (BASE). BASE technology analyzes aggregated application and network infrastructure data, including DNS queries and Border Gateway Protocol (BGP) routing tables, to detect aberrant botnet-related behavior. As a result, Trend Micro's InterCloud Security Service can effectively identify and isolate bots in real time, derailing their ability to initiate attacks or spread infection.

FUTURE OUTLOOK

Botnets are a collection of computers that, although their owners are unaware of it, have been set up to distribute malware such as spam and viruses to other computers on the Internet. IDC believes the growth of malicious botnets has been fueled by the growing number of consumers with high-speed connections who either do not have security solutions (i.e., antivirus, firewall, antispymware) installed or do not keep their security signatures up to date. Botnets are designed to create multiple threats to enterprise environments and consumer alike, including:

- Botnets are becoming the distribution vector of choice for spammers. IDC believes more than 75% of all spam is currently sent from a botnet of compromised zombie machines.
- Botnets are quickly becoming an ideal platform for launching DDoS attacks. Botnets allow hackers to control a very large number of zombie machines in order to attack a targeted site.
- Botnets increasingly expose users, especially consumers, to identity theft. Botnets can install keyloggers and sniffers to capture personal information such as passwords, social security numbers, credit card information, financial account information, and other sensitive personal data.
- Botnets are also using zombie machines to host illegal material such as pirated software and adult content.

As botnet attacks become more malicious and sophisticated, solutions such as Trend Micro's InterCloud Security Service will play an increasingly valuable role in protecting both consumer and enterprise environments. We expect botnet attacks to increase in volume, sophistication, and severity. IDC believes the InterCloud Security Service is an ideal solution to help ISPs identify and quarantine customers whose PCs have been infected.

Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights. Visit us on the Web at www.idc.com. To view a list of IDC offices worldwide, visit www.idc.com/offices.

Copyright 2006 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Filing Information: October 2006, IDC #204156, Volume: 1, Tab: Vendors

Secure Content and Threat Management Products: Event Flash