Fortinet October '09 Threatscape Report Shows Highest Malware Levels Detected all Year

Rogue Security Software Ups the Ante on Scareware to Celebrate Halloween

SUNNYVALE, Calif., Nov.5, 2009 - Fortinet® - a market-leading network security provider and worldwide leader of unified threat management (UTM) solutions - - today announced its October 2009 Threatscape report revealed the highest level of total malware detected in more than a year and four times greater than detected levels from the September Threatscape report. Mirroring the danger in last period's report, scareware tactics reached an all-time peak this month, with the worst attacks ever reported. In total, the seven malware variants listed in the top 10 malware list all point back to scareware, proving these attacks are occurring fast, hard and often. This unwelcomed news is in addition to recent scareware campaigns observed in the form of botnets, corrupted advertisements and SEO attacks. Key highlights of the October Threatscape report include:

- Scareware celebrates Halloween and masks malicious intent: Extending threat activity from September, scareware again dominates this period in the form of rogue security software, posing as the security suite AntiVirus Pro 2010. Users are schemed into purchasing the software to resolve their alleged problems, while more dangerous implications unfold: downloaders contact a remote server in order to obtain malicious payload and receive updated copies. Other components may be bundled with scareware, such as ransomware and bot agents; once an infection makes its way onto a system, the floodgates open up for cybercriminals. Such scareware activity pushed the pesky Virut and Netsky out of the top 10 malware list for the first time in over a year.
- Botnets make headway: The Trojan downloader Bredolab joined forces with scareware downloaders this period to add another element of surprise. Similar to the scareware framework, Bredolab reports to its network in order to obtain the latest components to download and this month downloaded the AntiVirus Pro 2010 installers. Through this download chain, Bredolab was also linked up to the notorious ZBot keylogger, bringing both a dangerous information-siphoning Trojan and a nasty scareware product together - a potent mix of threats, each one linking to different control sites. The two main Bredolab variants detected this month were W32/Bredo.G and W32/Bredolab.X, most notably included in fake DHL invoice spam campaigns.
- Affiliates extend scareware reach: No doubt scareware was the chart topper this month and the high threat levels can be attributed in part to the popular money-making affiliate programs that tempt participants with a handsome pay-out on each software download purchased. Tools and kits are readily available to participating affiliates, accelerating the distribution of scareware and other malicious components.

"We're seeing record levels of scareware building off volume from September, and the danger in these threats is only becoming more serious as the methods for delivery evolve and the blending of attacks bring more complexity," said Derek Manky, project manager, cyber security and threat research, Fortinet. "As we've seen in the consistency of repeated threats, the old schemes are still proving to be good methods. Enterprises and consumers must take equal responsibility in understanding the disguises of these threats and implementing a multi-pronged security solution that addresses the different and changing characteristics of tried and true tactics."

FortiGuard Labs compiled threat statistics and trends for October based on data collected from FortiGate® network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Subscription Services should already be protected against the threats outlined in this report.

To read the full October Threatscape report, which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_october_2009.html. For ongoing threat research, bookmark the FortiGuard Center (http://www.fortiguardcenter.com/) or add it to your RSS feed by going to

http://www.fortinet.com/FortiGuardCenter/rss/index.html. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog at http://blog.fortinet.com. To learn more about FortiGuard Subscription Services, visit http://www.fortinet.com/products/fortiguard.html.

FortiGuard Subscription Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help enable protection against threats on both application and network layers. FortiGuard Services are updated by FortiGuard Labs, which enables Fortinet to deliver a combination of multi-layered security intelligence and zero-day protection from new and emerging threats. For customers with a subscription to FortiGuard, these updates are delivered to all FortiGate, FortiMail™ and FortiClient™ products.

About Fortinet (www.fortinet.com)
Fortinet is a leading provider of network security appliances and the market leader in Unified Threat Management or UTM. Fortinet solutions were built from the ground up to integrate multiple levels of security protection -- including firewall, VPN, antivirus, intrusion prevention, Web content filtering, spyware prevention and antispam -- designed to help customers protect

against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in five programs by ICSA Labs: Firewall, Antivirus, IPSec VPN, Network IPS and Antispam. Fortinet is based in Sunnyvale, California.