Botnets Battle for First Place in Fortinet's November '09 Threatscape Report

Trojan Downloaders Creep Into the Mainstream through a Flood of Spam Campaigns; Overall Malware Volume Continues to Peak

SUNNYVALE, CA, Dec 09, 2009 (MARKETWIRE via COMTEX News Network) -- Fortinet(R) (NASDAQ: FTNT) -- a leading network security provider and worldwide leader of unified threat management (UTM) solutions -- today announced its November 2009 Threatscape report showed consistent highs in overall malware detected, marking the third month of significantly increased activity. Contributing to the high volume this period were new variants of Pushdo/Cutwail, which pushed the rampant Bredolab loader from last period's report out of mainstream in order to secure the number one and two positions in the top 10 malware list. Not far behind, ZBot and Scareware still remained active, borrowing popular and successful social engineering and spam tactics to gain ground. iPhone threats were also very active in November with four new attacks reported. Key highlights of the November Threatscape report include:

-- Battle of the Bots -- Look Who Prevails: Pushdo is back. Bredolab may have taken the fame and glory with high placement in the October top malware list, but it lost the botnet fight to Pushdo/Cutwail during this period, which accounted for 30 percent of total malware activity, nearly double of last month's Bredolab and Scareware daily records. The Pushdo botnet is commonly known to download the Cutwail Trojan, among other components, and uses simple trickery in the form of social engineering hooks and spam to lure in victims. Once downloaded, Cutwail mass mails new spam templates -- pirated software and pharmacy spams -- which like scareware, comes with an alluring profit margin due to affiliate programs.

-- Spam Stirs up New Scams: Spam campaigns took on new forms this period, with ZBot driving high levels of activity for the second consecutive month and a new Trojan-seeding downloader, Sasfis, prevalent through at least three distinct spam campaigns. Ranking at number three and number 10 of the top malware list, Sasfis variants used the subjects 'payment request,' 'mailbox has been deactivated' and 'Facebook updated account agreement' to spam users with a .zip attachment that contains the Trojan. Multiple ZBot attacks were observed, each carrying distinct social engineering tactics: one used an H1N1 scare tactic to lure users to a web site serving ZBot, while another attached the malicious bot disguised as a balance-checking tool for Verizon Wireless. Combined with the prominence of Cutwail, November experienced a peak in spam activity.

-- New Attacks to Keep You on your Toes: iPhone threats were in full force this period with four new attacks exploiting jailbroken iPhone devices: (1) malware targeted at Dutch-speaking iPhone users for ransom money, (2) a tool that steals SMS contacts (HackerTool/iPhoneStealer), (3) a worm that changes the background image and (4) another concerning worm that attempts to steal banking credentials (iPhoneOS/Eeki).

"For the last few months we've reported record highs in the overall volume of malware and daily attacks, with threat levels continuing to top that of the previous month. Botnets like Pushdo/Cutwail continue to evolve, placing emphasis on obfuscation and encryption. In addition, old tricks simply leverage new layers of complexity to further penetrate systems while cyber criminals test the waters by exploiting smart phones," said Derek Manky, project manager, cyber security and threat research, Fortinet. "We're seeing innovation at its scariest, as hackers remain committed to evolving their scams and developing new approaches. Enterprises must bring the same level of commitment to security -- update software, employ valid intrusion prevention systems and layer security within and around the network -- in order to guard against the new vulnerabilities and zero-day attacks that rise to the surface each month."

FortiGuard Labs compiled threat statistics and trends for November based on data collected from FortiGate(R) 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 November Threatscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_november_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 are designed to enable 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(TM) and FortiClient(TM) products.

About Fortinet (www.fortinet.com)

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2009 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

FTNT-O

Media Contact:
Kim Nguyen
Fortinet, Inc.
408-486-5458
knguyen@fortinet.com

SOURCE: Fortinet

mailto:knguyen@fortinet.com