FORTINET

Fortinet September '09 Threatscape Report Shows Scareware Anniversary Spike in Time for Halloween

Mass Mailing Scams Get Aggressive in Exploiting Money Mule Schemes

SUNNYVALE, Calif. - Sep 30, 2009 - Fortinet® - a market-leading network security provider and worldwide leader of unified threat management (UTM) solutions - today announced its September 2009 Threatscape Report uncovered a preponderance of scary tactics, showing continued strength one year after the initial cyberspace explosion of scareware in September 2008. Just in time for Halloween, cyber criminals are spooking the innocent with scams including email threats, botnet downloads and fraudulent software - ultimately aimed at scaring users into actions intended to exploit their pocketbooks. Additionally, newly uncovered vulnerabilities as well as exploits targeting new vulnerabilities remained high this period. Key highlights of the September Threatscape Report include:

- Bredolab and others spook users for scareware anniversary celebration: Marking the one year anniversary since the initial explosion of scareware across cyberspace, the Bredolab botnet (W32/Bredo.G), a Trojan downloader linked to rogue security software, was highly active this period. This is another example of the growing trend in broad distribution of fraudulent software (recent examples this month include SEO black hat campaigns, the NY Times malicious advertisements and a variant of Pushbot downloading such payloads). Bredolab variants were pushed out through a mass mailing campaign that sends fake DHL invoices; if opened, the machines are then recruited into a network of zombies. ZBot was again active this period, with the do-it-yourself botnet spreading through another mass mailing attack disguised as a tax scare from the IRS. The supplied link, which includes the recipient's name alongside an IRS sub-domain (formed to a malicious domain), is one way to identify and prevent infection from this attack.
- Spam pushes creative money mule hook: In line with the massive scareware tactics rampant this period, cybercriminals continued to roll out creative money mule hooks to lure in unsuspecting end-users with too-good-to-be-true offers. Similar to last period's Honeywell job listing, spammers pushed out another attractive job advertisement for Global Shipping Agency through a professional-looking email that requires the user's bank account to process customer payments.
- Zero-day attacks: One of two fresh remote-code execution vulnerabilities to make a stir this month was Microsoft Server Message Block (SMB2, CVE-2009-3103), which reported low but steadily increasing exploit activity. Additionally, a second vulnerability - Microsoft ISS FTP Service (CVE-2009-3023) - also popped up new this period, while Adobe Reader/Flash (CVE-2009-1862) continued with increasing levels of activity. Microsoft has released a temporary fix for CVE-2009-3103 (SMB2).

"We're seeing a steady if not rapid growth of scareware which - like other high-profile threats - will eventually begin to diminish in success and profitability once end-users become wise to them," said Derek Manky, project manager, cyber security and threat research, Fortinet. "However, it's clear that these get-rich-quick schemes are still proving to be successful today, and cybercriminals will undoubtedly continue to mine them until they are forced to move onto other innovative ways to exploit end-users. End-users should continue to be wary, and proceed online as they would offline with the notion that if it's too good to be true, it likely is."

The FortiGuard research team compiled threat statistics and trends for September 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 September Threatscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_september_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 the FortiGuard Global Security Research Team, 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, antivirus, intrusion prevention, VPN, 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.