Fortinet's March Threatscape Report Shows Domination of Ransomware and Troublesome Zero-Day

Rise of Ransomware Is Primarily Driven by Bredolab and Pushdo Botnets

SUNNYVALE, CA, Apr 01, 2010 (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 March 2010 Threatscape report showed domination of ransomware threats with nine of the detections in the malware top ten list resulting in either scareware or ransomware infesting the victim's PC. Fortinet observed the primary drivers behind these threats to be two of the most notorious botnet "loaders" -- Bredolab and Pushdo. Another important finding is the aggressive entrance of a new zero-day threat in FortiGuard's top ten attack list, MS.IE.Userdata.Behavior.Code.Execution, which accounted for 25 percent of the detected activity last month.

Key threat activities for the month of March include:

-- SMS-based Ransomware High Activity: A new ransomware threat -- W32/DigiPog.EP -- appeared in Fortinet's top ten malware list. DigiPog is an SMS blocker using Russian language, locking out a system and aggressively killing off popular applications like Internet Explorer and Firefox until an appropriate code is entered into a field provided to the user. To obtain the code, a user must send an SMS message to the provided number, receiving a code in return. Upon execution, DigiPog registers the user's MAC address with its server. It is the first time that SMS-based ransomware enters Fortinet's top ten list, showing that the rise of ransomware is well on its way.

-- Botnets -- the competition gets tough: While the infamous Bredolab and Pushdo botnets can be identified behind the strong ransomware activity this month, a challenger has been particularly active this month. Sasfis, another botnet loader, moved up eight positions in our Top 100 attack list from last month, landing just behind Gumblar & Conficker network activity in the fifth position. Sasfis is just the latest example of simplified botnets, which are used heavily for malicious business services (crime as a service).

-- Zero-day attack forces in: A new zero-day threat aggressively entered FortiGuard's top ten attack list: MS.IE.Userdata.Behavior.Code.Execution (CVE-2010-0806, FortiGuard Advisory 2010-14). This exploit triggers a vulnerability in Internet Explorer, making remote code execution through a drive-by download (no user interaction required) possible. Accounting for one fourth of the detected activity in March, this exploit was ranked number two in our top ten attacks last month and remains very active, predominantly in Japan, Korea and the U.S.

"As we predicted for 2010, cybercriminals are clearly pursuing new ways to lure consumers and threaten the enterprise at large. Troublesome zero-day exploits continue to attack popular client-side software, while methods such as ransomware and crime as a service help them increase their reach and make their attacks more effective against end users," said Derek Manky, project manager, cyber security and threat research, Fortinet. "With cybercrime techniques getting more sophisticated every day, it is critical to educate users on the importance of having the right security software and patches in place. Robust security services and safe practice can help protect consumers and organizations against known vulnerabilities, but also unknown ones such as zero-day threats."

FortiGuard Labs compiled threat statistics and trends for March 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 March Threatscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_march_2010.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(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 Contacts:
Barbara Maigret
Fortinet, Inc.
+33 (0)4 8987 0552
bmaigret@fortinet.com

SOURCE: Fortinet

mailto:bmaigret@fortinet.com