Fortinet Threat Landscape Research Shows Rise in Data Breaches, Attacks and Spam

Fraudload.OR Infection Run Continues for Second Month, Spam Bounces Back 3 Months After Rustock Takedown

SUNNYVALE, CA -- (MARKET WIRE) -- 07/06/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today released its latest Threat Landscape report, which details data breaches and attacks such as Sony Europe being hit by another SQL injection attack, the International Monetary Fund (IMF) suffering a critical data breach, hacktivism group LulzSec's continued attack on the U.S. government and the rise of spam despite a three month decline.

The most prominent virus FortiGuard® Labs detected during the month of June was, once again, Fraudload.OR, which frequently disguises itself in the form of fake antivirus software, though it also has the ability to download other Trojans and malware to an infected user's system. Fraudload.OR accounted for more than one third of new malware incidents during the last few weeks.

Fraudload.OR has been very active for nearly two months, no doubt fuelled by the success FakeAV loaders like Fraudload.OR have realized. Recently, bank accounts belonging to a FakeAV operator were frozen by the US District Attorney. Nearly $15M USD was in those accounts, highlighting the wealth such operators can achieve using a scam that is now well over three years old.

Also at the top of the attack charts was MS.IE.CSS.Self.Reference.Remote.Code.Execution (CVE-2010-3971). This vulnerability affects Internet Explorer 8 and earlier versions and is triggered simply by viewing a webpage that hosts a malicious CSS style sheet. Most activity for this attack was observed mid-month particularly in Algeria and South America.

"We are indeed entering a new era of cybersecurity, one where proactive measures are being put in place and this month's attacks show the importance of keeping patches up-to-date to help avoid exploitation by malicious code," said Derek Manky, senior security strategist at Fortinet. "It's also important to employ an IPS solution to help block malicious code looking to exploit vulnerable software and a Web application firewall to help protect your public facing digital assets."

About FortiGuard Labs
FortiGuard Labs compiled threat statistics and trends for this threat period based on data collected from FortiGate® network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Services should be protected against this vulnerability with the appropriate configuration parameters in place.

FortiGuard Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help protect 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.

The full Threat Landscape report, which includes the top threat rankings in several categories, is available now. Ongoing research can be found in the FortiGuardCenter or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the Fortinet Security Blog.

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.

FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties and Fortinet does not independently endorse such statements. Nothing in the news release constitutes a warranty, guaranty, or contractually binding commitment. This news release may contain forward-looking statements that involve uncertainties and assumptions. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements, including but not limited to, any statements related to expected trends in cybercriminal activity. These trends are difficult to predict and any stated expectations regarding these trends may not ultimately be correct. Fortinet assumes no obligation to update any forward-looking statements, and does not intend to update these forward-looking statements.

FTNT-O

Media Contacts:

Maeve Naughton

Fortinet, Inc.

408-486-7819

mnaughton@fortinet.com

Source: Fortinet