

# Fortinet's April Threatscape Report Shows Botnets Battling for Digital Real Estate

## Gumblar and Sasis Continue to Gain Momentum

**SUNNYVALE, Calif., May 3, 2010** - Fortinet® (NASDAQ: FTNT) - a leading network security provider and worldwide leader of unified threat management (UTM) solutions - today announced its April 2010 Threatscape report showed high activity from multiple botnets, namely Gumblar and Sasis. While Gumblar remained in the No. 1 position in Fortinet's Top 10 Network Attacks list, the Sasis botnet ranking was bolstered by two of its executables prevalent in Fortinet's Antivirus Top 10 listing. Like Bredolab, Sasis is a botnet loader that reports statistics and retrieves/executes files upon check-in. However, Sasis differs since it is newer and does not employ encryption (all communications are sent through HTTP unencrypted). Nonetheless, Sasis continues to spread aggressively and typically loads banking trojans among other malicious files.

Additional key threat activities for the month of April include:

- **Microsoft Vulnerabilities:** The Internet Explorer vulnerability MS.IE.Userdata.Behavior.Code.Execution (CVE-2010-0806) was the second-most detected malicious network activity for the second report in a row. While in its zero-day state, Fortinet observed an attack on this vulnerability that installed the infamous Gh0st RAT spy-trojan, a fully-functioning remote administration tool that also streams Webcam video and audio feeds. Secondly, FortiGuard Labs also discovered two memory corruption vulnerabilities in Microsoft Office Visio that allow a remote attacker to compromise a system through a malicious document. The vulnerabilities are triggered when opening and rendering a Visio file. A remote attacker could craft a malicious document that exploits either one of these vulnerabilities, allowing them to compromise a system.
- **Adobe Acrobat vulnerabilities:** Fortinet's FortiGuard Labs also discovered two memory corruption vulnerabilities in Adobe Reader / Acrobat, which allow a remote attacker to compromise a system through a malicious document. The vulnerabilities are triggered when opening and rendering a PDF document. A remote attacker could craft a malicious document which exploits either one of these vulnerabilities, allowing them to compromise a system.
- **Ransomware and Scareware still top virus detection:** This is no surprise, as Scareware has been consistently prevalent since September 2008. Ransomware, on the other hand, began making headway in 2010 due to incentives from affiliate-backed programs that pay out when victims purchase the fake products.
- **Cutwail spambot leveraged for money mule recruitment:** Fortinet continues to observe the Cutwail spambot, which has been active for years, send various spam campaigns for its customers. The spam sent by Cutwail this month typically included malicious links to eCard binaries or emails with the binaries themselves attached. There were various money mule recruitment themes observed in spam emails this report, showing a growing demand for jobs on the black market.

"Money mules are essentially money laundering vehicles utilized by cyber criminals to handle and transfer illicit funds," said Derek Manky, project manager, cyber security and threat research, Fortinet. "The mule receives a commission for doing the transfer. These transfers are typically done in batches of \$10,000 USD or less. Money mule positions are, more times than not, crafted as legitimate sounding jobs, such as accounts receivable positions. If something seems too good to be true, it generally is."

FortiGuard Labs compiled threat statistics and trends for April 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.

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

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.

*Copyright © 2010 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiDB, FortiWeb and FortiAP. 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. This press release contains forward-looking statements that involve risks and uncertainties. These statements include statements regarding the functionality and benefits of our FortiOS maintenance release 2. Future circumstances might differ from the assumptions on which such statements are based and results may differ from such forward-looking statements. All forward-looking statements reflect our opinions only as of the date of this release, and we undertake no obligation to revise or publicly release the results of any revision of these forward-looking statements in light of new information or future events.*

## About GEOBRIDGE

Since 1997, GEOBRIDGE has been providing information security solutions to global clients. Today our client list includes Fortune 500 companies, financial institutions, health care, government agencies and defense clients across North America and internationally. GEOBRIDGE helps clients mitigate risk and realize significant value from their IT investments while allowing clients to focus on the growth and profitability of their company. Our team provides solutions, integration services and consultancy in the areas of encryption, network security, identity management, transaction security, and compliance. Due to the increased needs for compliance with internal governance, and external legal and regulatory requirements, we have expanded our compliance and security best-practices offerings to address information assurance. GEOBRIDGE is a Qualified Security Assessor company (QSAC) certified by the Payment Card Industry (PCI) and a TG-3 Assessor recognized by the Electronic Funds Transfer (EFT) networks.