Fortinet Threat Landscape Research Shows 64-Bit Malware Family Spreading

Fake Antivirus Fraudload.OR Was the Most Prominent Virus Detected in This Report With Majority of Detections Coming From Africa

SUNNYVALE, CA -- (MARKET WIRE) -- 06/09/11 -- 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 two prominent detections belonging to the TDSS family of rootkits that are capable of infecting 64-bit Windows operating systems. The TDSS rootkit, which is difficult to detect and remove, has full access to any system it infects and can mask its activity to administrators and end users.

"Microsoft issued a security advisory in mid-April to fix a vulnerability with driver signing enforcement that the TDSS family of rootkits have been known to exploit," said Derek Manky, senior security strategist at Fortinet. "Since TDSS is still active and potent, we strongly recommend applying this critical update if you are running an affected x64 edition of Microsoft Windows. These rootkits spread through common infection methods like malicious Websites that host exploit kits, and we have recently seen a new 64-bit rootkit emerge that uses an entirely different method to subvert x64 based systems."

Fake Antivirus Detections Up and Targeting the Mac
The most prominent virus FortiGuard Labs detected during the month of May was Fraudload.OR, which frequently disguises itself in the form of fake antivirus software, though Fraudload also has the ability to download other Trojans and malware to an infected user's system.

"Fake antivirus software is a tried and true model for cyber criminals, often operating on a pay-per-purchase basis where the criminals who infect a user's system receive a commission for every victim that orders a version of the fake software," Manky continued. "Recently, this type of malware has started to make its way to the Mac OSX platform in the form of MacDefender and MacGuard."

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'sFortiGuard 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.

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

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contacts:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media