Fortinet Threat Landscape Research Reveals Fake Antivirus Malware Accounted for 58 Percent of New Malware Activity This Period

Zeus Botnet Variant Takes 2nd Place in Monthly Malware Activity Due to Its Source Code Being Cracked and Leaked

SUNNYVALE, CA -- (MARKET WIRE) -- 09/09/11 -- 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 reveals the fake antivirus loader W32/FraudLoad.OR accounted for 58 percent of the new malware activity tracked this period.

"Traditionally, FraudLoad installs fake antivirus utilities on an unsuspecting user's system, but in our labs, we find that it is all too common for botnet loaders like this to download additional malware such as spam bots," said Derek Manky, senior security strategist at Fortinet.

Right behind FraudLoad, a newly discovered Zeus botnet variant was the second most active malware this period.

"The surge in Zeus activity doesn't surprise us given the botnet's popularity and the fact that its source code was hacked and subsequently leaked to the public last May," Manky continued. "We believe it's highly likely that we will continue to see Zeus and SpyEye -- another popular botnet whose source code was also recently cracked and leaked publicly -- to spread in waves in the coming months."

Additional News in Brief:
This period, the W32/Yakes botnet loader and four variants were observed spreading through spam emails using traditional major credit card manufacturer templates. The email that arrives at the victim's inbox typically carries the subject line "Credit card is blocked." Text within the email explains that the recipient's credit card was involved with illegal operations and has been disabled. The email then advises the recipient to open an attached file for details. When the user clicks on the attachment, the Yakes botnet is installed onto their computer.

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.

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