Fortinet Threat Landscape Research Shows Two New Malware Variants Targeting Facebook Users

Coreflood Botnet That Infected 2.3 Million Machines Dismantled by FBI in Largest U.S. Sting of Its Kind and Spam Levels Remain Down 15 Percent Month-Over-Month After the Recent Dismantling of the Rustock Botnet

SUNNYVALE, CA -- (MARKET WIRE) -- 05/05/11 -- 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 new malware variants targeting Facebook users. The malware, which is intended to look as though they're coming from Facebook, claim that the users' Facebook passwords have been reset and a malicious attachment has their new passwords. Clicking on the attachment can lead to immediate infection.

"The Facebook malware variants we examined are botnet loaders, which, upon execution, connect to a command and control server to download and display a document that reveals a bogus password in an effort to look legitimate," said Derek Manky, senior security strategist at Fortinet. "Afterwards, the botnet continues to run in the background and requests files to download and execute, one by one. Always beware of file attachments, never disclose information generated by an unsolicited request, and attempt to confirm identities of those who contact you."

Spam Activity Stays Down
On April 16, a large Coreflood (circa 2002) botnet operation was dismantled by the FBI in the largest enforcement action of its kind in U.S. history. Servers and domains controlled by an international group of cyber criminals were seized. This particular botnet had infected 2.3 million machines and millions of dollars were stolen from unsuspecting computer users.

"Coreflood comes off the heels of the Rustock botnet, which was taken offline mid-March with the help of Microsoft and a number of Federal agencies," Manky continued. "As a result, two major botnets have dwindled and global spam rates have remained about 15 percent lower than they were before Rustock's downfall."

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 FortiGuard Center or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the Fortinet Security Blog and Fortinet's monthly Security Minute videocast.

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. 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 Contact:

Rick Popko

Fortinet, Inc.

+1-408-486-7853

rpopko@fortinet.com

Source: Fortinet