Fortinet Threat Landscape Research Finds Surprising Comeback in Lethic Spam Botnet

Report Also Discloses New Android Malware Hitting Phone Bills to the Tune of EUR 18.00

SUNNYVALE, CA -- (MARKET WIRE) -- 01/10/12 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today released its December research findings, which show Lethic botnet communication as one of the most prevalent botnet traffic observed in new locations.

Lethic was initially discovered in 2008 and was primarily used to distribute pharmaceutical spam. At one point, the botnet was alleged to be responsible for 8 to 10% of the spam generated worldwide. In early 2010, the botnet was severely disabled when Neustar employees contacted a number of Internet Service Providers in an attempt to disable the botnet's command and control servers. While that cooperative effort succeeded in significantly reducing the botnet's spam output, the owners managed to secure control of the botnet again by February. And by April, it had sputtered back to life and was again sending roughly two billion spam emails a day, about 1.5% share of the overall spam market.

"Lethic is a botnet that uses encryption when infected computers communicate to the command and control. In addition, Lethic uses its infected hosts (bots) as proxies, tasking them with reconnaissance missions to discover new spam routes," said Derek Manky, senior security strategist at Fortinet. "The dynamic approach used by this botnet has allowed it to survive over the years, despite takedown attempts. There are many different ways a botnet can be designed, and for total takedown, there must be a clear understanding of the anatomy of the botnet in question. Even after a seemingly successful takedown such as Lethic, new variants often crop up allowing the botnet to grow again from a new seed."

Foncy Android Malware Debuts in France
A new Android Trojan named Foncy, which was recently uncovered by Kaspersky's Denis Maslennikov and subsequently dissected by Fortinet's European-based labs, was developed and is currently spreading in France. This particular Trojan is a dialer, meaning it sends SMS messages to short numbers without a user's consent.

"Unsuspecting end-users have installed the malicious application on their mobile device, believing it to be the legitimate plan tracking application SuiConFo (SUIvi CONsommation FOrfait, French for 'Track Your Plan')," said Axelle Apvrille, senior mobile anti-virus researcher at Fortinet. "When a user installs the malware on their device, a SuiConFo icon appears in the device's launch menu. When the icon is pressed, the application displays an error message that reads: 'ERROR: Android version is not compatible,' while in the background, the Trojan surreptitiously sends four SMS messages to a list of short numbers. Those numbers can end up costing the user up to EUR 18.00."

If a user thinks they might be infected, FortiGuard Labs suggests they immediately check their bill, report any anomaly they find and uninstall the suspicious application. A legitimate version of the SuiConFo application can be downloaded from a developer named Alou, on the Android market.

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.

All Fortinet Threat reports can be found here. December's Security Minute video podcast, which features commentary on today's latest threats can be found here. 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 2011 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.

FTNT-O

Media Contacts:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media