Fortinet Threat Landscape Research Reveals New Android Botnet

W32/Exchanger Trojan Malware Downloader Observed Downloading Ten Different Pieces of Malware Within a Day of Initial Infection

SUNNYVALE, CA -- (MARKET WIRE) -- 08/03/11 -- 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 a new variant of Zitmo (Zeus in the mobile) that was written to run on the Android operating system, allowing the malware to continue its expansion across mobile platforms beyond the Windows Mobile, Symbian and BlackBerry operating systems. The first variant of Zitmo on Symbian OS (SymbOS/Zitmo.A!tr) was found in September 2010 and was based on commercial, Russian spyware for Symbian 3rd and 5th editions (SMS Monitor Lite). Zitmo has since evolved and is now capable of intercepting two-factor authentication that banks use to validate the identity of the account holder when logging in (it is a one-time password that is sent to a mobile device via SMS). Even if a mobile user does not rely on the two-factor authentication method for banking activities, Zitmo can forward and spy on all SMS messages, making it a valid threat.

Trojan Malware Downloader W32/Exchanger
On July 24, FortiGuard Labs observed a surge of activity from the W32/Exchanger Trojan downloader, which downloaded and installed ten different malware families within the course of a day onto the lab's test system. This type of rapid mass infection can cause a system to become unstable and ultimately crash.

"Most infections we see like this in our labs serve a similar purpose to W32/Exchanger and are known in the digital underground as 'loaders,'" said Derek Manky, senior security strategist at Fortinet. "Loaders are botnets with simple functionality. They report status, such as uptime, operating system version, geographic location, etc., and receive download commands from their controllers. Such statistics help cyber criminals manage their infections, bill customers for installing malware on a given number of systems and provide reports to their clients as a quality of service metric."

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.

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 Contacts:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media