Fortinet Threat Landscape Research Reveals Development of Highly-Evolved Android Malware

DroidKungFu Now Acts as Full-Fledged Botnet, Capable of Downloading Additional Malware, Opening Applications and Browsers at Will, Deleting Files and More

SUNNYVALE, CA -- (MARKET WIRE) -- 11/01/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today released its October research findings. This month, FortiGuard Labs observed ongoing development of the new DroidKungFu malware, which has been found to have multiple variants and behaves much like malware found on today's PCs.

"DroidKungFu clearly represents the next evolution in mobile malware," said Derek Manky, senior security strategist at Fortinet. "Where earlier attempts at Android malware, such as Zeus in the Mobile (Zitmo), are able to intercept the type of two-factor authentication that banks use to validate the identity of the account holder when logging in, DroidKungFu does much more. By disguising itself as a legitimate VPN client application, the malware quickly gains root access to the device using social engineering. Once executed, DroidKungFu has the ability to download further malware, open URLs in a browser, start programs and delete files on the system."

The Danger of URL Shortening Services
URL shortening services, such as TinyURL® offer a convenient way to package and transmit long and unwieldy Website addresses to specific recipients. When a user clicks on a shortened link, they are quickly redirected to the Website's original address. Because URL shortening services are able to reduce the number of characters in a typical Web address, they're a favorite among Twitter users. They're also frequently used for email purposes, because some email applications have the tendency to break longer links during transmit or arrival. However, the benefit of a URL shortening service is also its biggest weakness, as the service enables criminals to obfuscate malicious links that can infect a user's system. Historically, Fortinet has always recommended that users place their cursor over a questionable URL before clicking on it to see if that link is actually being redirected to a questionable page. This safety measure is not applicable to shortened URLs. There's no sure fire way to tell in advance when a user clicks on a shortened URL if they are about to be redirected to a malicious site.

"Advances in antispam techniques are catching much of today's shortened link malware," Manky continued. "However, we're now starting to see malicious software creators creating their own URL shortening services to circumvent the latest spam detection technology. This is yet another example of crime as a service (CaaS) that cybercriminals offer."

One way to determine if a shortened URL is pointing to a malicious site is to look at the domain at the end of the link. Most observed malicious URL shortening services have been recently using the .info domain. Another way to tell if a shortened URL is redirecting to a malicious site is to paste the questionable link into a URL filtering tool, such as Fortinet's URL Lookup. Finally, a proper Web filtering solution helps to protect against URL shortening services since the full domain is still resolved and checked.

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. October'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 2010 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