Fortinet Threat Landscape Research Reveals FortiGuard Labs' Top 5 Android Malware Families

Report Also Discloses a New Android Root Level Vulnerability

SUNNYVALE, CA -- (MARKET WIRE) -- 12/06/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today released its November research findings. This month, FortiGuard Labs released its Top 5 Android Malware Families and tested a new vulnerability that affects Android phones at the root level.

Top 5 Android Malware
On November 15, the analyst firm Gartner issued a report that cited Google's Android mobile operating system had reached a global 52.5% smart phone market share, while iOS trailed in third, behind Symbian, with an 18% market share. FortiGuard Labs found interesting the disparity between the amount of malware found on the Android operating system compared to that found on iOS relative to their market share size.

"FortiGuard Labs has found approximately five times the amount of malicious families on the Android OS versus what we've found on iOS," said Axelle Apvrille, senior mobile anti-virus researcher at Fortinet. "We believe that this disparity can be attributed to the way Apple handles iOS application development and distribution. Unlike Android, which makes it fairly easy to place applications for people to download, iOS requires developers to undergo some strict screening from Apple before the application can make it to the Apple Store. That's not to say that Apple is totally immune from being infiltrated by malware -- the Eeki banking worm proves that -- but it is a testament to why we're seeing so little activity on the iOS platform."

"Unfortunately, we believe Android's higher market share and open development environment comes with a price; an almost six fold increase in malware targeting the operating system," Apvrille continued. "To date, our Labs have seen a 90% increase in Android malware families in 2011 compared to 2010, while malicious iOS families only increased by 25%. Of course, those statistics do not account for infection rates or dangerousness."

The Top 5 malware families for which FortiGuard Labs have received the most samples in 2011 are:

- Geinimi: Android's first botnet, which sends a victim's geographic location and controls his/her phone remotely. For example, Geinimi can force the infected phone call a given phone number.
- Hongtoutou: A Trojan live wallpaper that steals private information such as the victim's subscriber number (IMSI) and automatically visits Websites that the malware directs it to.
- DroidKungFu: Another botnet that has multiple capabilities such as remotely installing other malware, remotely starting specific applications and adding bookmarks.
- JiFake: A fake instant messenger application that sends SMS messages to premium phone numbers
- BaseBridge: A Trojan that sends SMS messages to premium numbers

The aforementioned malware and more are detected by Fortinet's antivirus engine. It should also be noted that malware such as BaseBridge was available on the Android Market but was later removed. Many times malicious software tries to pass itself off as a genuine application. However, malware has also been found within a legitimate application they have infected.

"DroidKungFu was an example of malware that was found repackaged in a legitimate VPN utility, whereas Geinimi was found within the legitimate application 'Sex Positions,'" said Karine de Ponteves, malware analyst at Fortinet.

Android Vulnerability
Last month, Jon Larimer and Jon Oberheide published vulnerability for Android platform 2.3.6 that revealed an easy way for hackers and malicious software developers to gain and exploit root access to an Android device.

"The mobile security trend is a familiar one: as operating systems mature and gain popularity, malware and vulnerabilities follow since there is focus and motivation from cyber criminals," observed Derek Manky, senior security strategist at Fortinet. "With root access, hackers can gain access to system files and change system settings that are typically authored to be read only. For example, a malware creator with root access to a vulnerable device could silently download and install additional malicious software, such as ransomware, spambots and keyloggers."

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. November'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