JUNIPER NETWORKS MOBILE THREAT CENTER THIRD ANNUAL MOBILE THREATS REPORT: MARCH 2012 THROUGH MARCH 2013

Faster, better, cheaper: mobile malware creators take lessons from business to improve profitability through faster go-to-market strategies

Over the past year, the Juniper Networks Mobile Threat Center (MTC) found rapid mobile malware growth and increased sophistication of cyber criminals, turning attacks into an increasingly profit-driven business.

Mobile devices and apps are becoming ubiquitous to both personal and professional lives, allowing for near anytime access to critical information. It's no wonder that adoption of smartphones and tablets, which offer Internet connectivity and densely populated application ecosystems for add-on features, is growing at a torrid pace. According to Gartner, "Of the 1.875 billion mobile phones to be sold in 2013, 1 billion units will be smartphones, compared with 675 million units in 2012."[1] **IDC expects** tablet shipments alone to outpace the entire PC market by 2015.[2]

The increasing reliance of smart devices has proven to be an irresistible target for attackers as they are quickly eclipsing computers in the post-PC era. From March 2012 through March 2013, the total amount of malware the MTC sampled across all mobile platforms grew 614 percent to 276,259 total malicious apps, compared with a 155 percent increase reported in 2011. This trend suggests that more attackers are shifting part of their efforts to mobile.

Developments in the threat landscape also point to malware professionals increasingly behaving like calculated business professionals when devising attacks. Juniper Networks observed that similar to legitimate developers focused on the rise of mobile, cyber criminals are looking to maximize their return on investment (ROI) with their attacks. Through targeting threats at Google Android with its commanding global market share, leveraging loosely regulated third-party marketplaces to distribute their illicit wares and developing threats that yield profits, it's clear that the mobile malware writers are more sophisticated and chasing higher rewards for their efforts.

Findings from the MTC in its third annual Mobile Threats Report, compiled by Juniper security researchers, show several indicators of a shift in mobile malware from cottage industry to developed market:

- **Targeting Markets with Greatest ROI:** According to analyst firm **Canalys**, Android devices accounted for 67.7 percent of all smartphones shipped in 2012 and is projected to ship over 1 billion smartphones in 2017.[3] Just as commercial sales teams have learned to "fish where the fish are," cyber criminals are focusing the vast majority of threats on Android and its open ecosystem for apps and developers. By March 2013, Android was the target of 92 percent of all detected mobile malware threats by the MTC. This is a significant uptick from 2011 when Android made up 47 percent of all detected threats and 2010 where just 24 percent targeted the platform.

- **Shortened Supply Chains and Distribution:** Attackers made strides to shorten the supply chain and find more agile methods to distribute their wares around the world. The MTC identified more than 500 third-party application stores hosting mobile malware. These third-party alternatives to official marketplaces often have low levels of accountability, allowing for malicious commodities to have a near infinite shelf life. These stores are also a concern for the several million "jailbroken" iOS devices that rely on them to "side load" apps. Of these third-party stores, MTC research shows that three out of five originate from two emerging markets infamous for malware in the PC space: China and Russia.

- **Multiple Paths to Market:** Less sophisticated mobile criminals are exploiting holes in mobile payments to make a quick and easy profit by proliferating SMS Trojan and Fake Installer malware. These types of attacks make up 73 percent of all malware sampled by the MTC. According to MTC researchers each successful download provides attackers around $10 USD in immediate profit.[4] At the high-end of the market, more sophisticated attackers are using botnets and threats targeting high-value data on corporate networks in the enterprise.

- **Operating System Fragmentation Causes Issues:** Attackers continue to benefit from the largely fragmented Android ecosystem that keeps the vast majority of devices from receiving new security measures provided by Google, leaving users exposed to even well-known and documented threats. Google provides protection against SMS threats – *which make up 77 percent of Android malware* – in its latest OS version, yet according to Google, only four percent of Android phones have it as of June 3, 2013.[5] This threat could be largely eliminated if the Android ecosystem of OEMs and carriers found a way to regularly update devices.

The MTC examined more than 1.85 million mobile applications and vulnerabilities across major mobile operating system platforms to inform this report. Key findings and guidance, along with predictions about the evolving threat landscape, follow in this report.

The Business of Mobile Malware:
From Cottage Industry to Developed Market
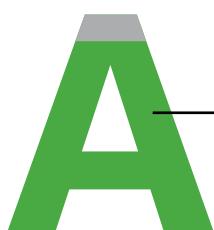A snapshot from the third annual Mobile Threats Report from Juniper Networks

Mobile malware grew

155% in 2011

614%
from March 2012 to March 2013

73% of all malware exploit holes in mobile payments by sending fraudulent premium SMS messages, each generating around **$10** USD in immediate profit

Android is responsible for **92%** of all known mobile malware. An increase from **47%** in 2012...
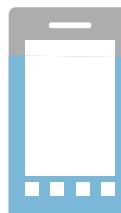
...a significant threat given more than

1 BILLION
Android-based smart phones are estimated to be shipped in 2017

Source: Canalys Smart Phone Report, June 2013

There are more than

500
third-party app stores containing malicious apps

77% of Android threats could be largely eliminated today if all Android devices had the latest OS. Currently only **4%** do

REFERENCES

1   "Gartner press release: "Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 billion units by 2013"; Full report: "Forecast: Devices by Operating System and User Type, Worldwide, 2010-2017, 1Q13 Update," by Carolina Milanesi, Lillian Tay, Roberta Cozza, Ranjit Atwal, Tuong Huy Nguyen, Tracy Tsai, Annette Zimmerman, CK Lu; March 28, 2013. **http://www.gartner.com/newsroom/id/2408515**

2   IDC Forecasts Worldwide Tablet Shipments to Surpass Portable PC Shipments in 2013, Total PC Shipments in 2015, doc #prUS24129713, May 2013.

3   "Over 1 billion Android-based smart phones to ship in 2017," Canalys, June 4, 2013.
    http://www.canalys.com/newsroom/over-1-billion-android-based-smart-phones-ship-2017#sthash.jc9ZyC7y.dpuf

4   "2011 Mobile Threats Report," pg. 16, Juniper Networks, Feb. 2012.
    http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf

5   Google Android Developer Page: **http://developer.android.com/about/dashboards/index.html#Screens**