February 24, 2014

Fortinet's FortiGuard Labs Reports 96.5% of All Mobile Malware Tracked Is Android Based, Symbian Is Distant Second at 3.45%; iOS, BlackBerry, PalmOS, and Windows Together Represent Less Than 1%

Team Also Reveals Top 10 Mobile Malware Families, Top 10 Botnets, Top 10 Countries Responsible for the Majority of the World's Spam and Top 10 Malware Families

SUNNYVALE, CA -- (Marketwired) -- 02/24/14 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today announced the findings of its FortiGuard threat landscape research for the period of January 1, 2013 - December 31, 2013. The complete report can be downloaded here: http://www.fortinet.com/resource_center/whitepapers/threat-landscape-report-2014.html

Android OS Dominates Mobile Malware Landscape
2013 was a bumper crop for malware targeting mobile devices. Looking back at the entire year FortiGuard® Labs observed Android was the dominant platform of choice for malware developers, representing 96.5% of all mobile malware infections detected by FortiGuard Labs. Symbian was a distant second at 3.45% and iOS, BlackBerry, PalmOS and Windows together don't even warrant 1%.

"The rapid growth of malware targeting Android continues to be of concern to system administrators who have implemented a mobile device strategy on their networks," said Axelle Apvrille, senior mobile antivirus researcher with Fortinet's FortiGuard Labs. "FortiGuard Labs detected over 1,800 new distinct families of viruses in the past year, and the majority of those are targeting Google's Android platform. Looking at the growth of Android malware, we can see that there is much to be concerned about in 2014. The growth shows no signs of slowing; in fact, the growth seems to be accelerating. As more Android-based devices are purchased and taken online, the opportunities for attackers to infect increases as well."

While attacks on platforms such as Symbian wane, attackers have made Android the number one mobile target. The NewyearL.B Android malware, which was bundled inside seemingly harmless downloads like a flashlight application, continued to target millions of devices and was the number one mobile malware family seen all year. Unwitting or unaware users looking to try out the latest games or apps find themselves unknowingly sharing a wealth of personal information with an attacker, leading to obtrusive advertisements and other negative effects, such as allowing NewyearL.B permission to add and remove system icons and modify and delete the contents of any external storage. And the distribution of Android malware continues to accelerate.

"Clearly cybercriminals are putting a substantial amount of effort into churning out hundreds of thousands of new variants daily in the hopes that some of them will be successfully implanted on a target device," Apvrille concluded.

Top 10 Mobile Malware Families based on Reported Incidents

1. Android/NewyearL.B
2. Android/DrdLight.D
3. Android/DrdDream
4. Android/SMSSend Family
5. Android/OpFake Family
6. Android/Basebridge.A
7. Android/Agent Family
8. Android/AndCom.A
9. Android/Lotoor Family
10. Android/Qdplugin.A

ZeroAccess: The Most Prolific Botnet of the Year
Earlier in 2013, FortiGuard Labs reported on the ZeroAccess botnet and how its controllers were systematically adding about 100,000 new infections weekly, leading researchers to believe that the person or persons behind it were not only paying a substantial amount of money weekly to generate new affiliate infections, but that they were able to make a significant amount of money doing so.

"Like other cybercriminals, ZeroAccess's owners have taken pages from the playbooks of legitimate businesses and made successful attempts to diversify their income generation," said Richard Henderson, security strategist with Fortinet's FortiGuard

Labs. "We saw 32- and 64-bit versions of ZeroAccess being used to commit click fraud, search engine poisoning and to mine Bitcoin. With the dramatic rise in Bitcoin value over 2013, it's likely that the owners of ZeroAccess have profited substantially on the backs of their victims."

Top 10 Botnets Based on Reported Incidents with Percentage of Overall Dominance

1. ZeroAccess (88.65%)
2. Andromeda (3.76%)
3. Jeefo (3.58%)
4. Smoke (2.03%)
5. Morto (0.91%)
6. Mariposa (0.43%)
7. Waledac (0.18%)
8. IMDDOS (0.18%)
9. Mazben (0.15%)
10. Torpig (0.10%)

India Leads the World in Spam Delivery

Fortinet antispam appliances around the world last year blocked billions of spam emails.

"Spammers will try multiple methods to foil scanners and to entice users to click on the links inside their messages including fake fax messages, pharmaceutical ads, e-cards and malicious attachments or links designed to deliver malware," Henderson continued. "Perhaps what is most interesting is how diversified spammers are globally when it comes to sending their messages: our statistics shows that while about half of all total messages we saw in 2013 came from Eastern Europe and Russia, the remaining countries in our top 10 are located all over the globe."

Top 10 Country IPs Sending Spam on a Monthly Basis Based on Number of Reported Incidents with Percentage of Overall Dominance

1. India (22.66%)
2. China (18.39%)
3. Belarus (12.40%)
4. Russia (10.27%)
5. USA (10.06%)
6. Kazakhstan (6.14%)
7. Spain (5.37%)
8. Argentina (5.00%)
9. Ukraine (4.93%)
10. Taiwan (4.78%)

ZeuS is Still the King of the Malware Hill

In terms of general PC malware, the ZeuS trojan took the top spot in 2013, with over 20 million attempts to infect FortiGate-protected networks. ZeuS first showed up on computers in 2007 and has been a thorn in the side of Internet users ever since. The 2011 leak of ZeuS' source code led to an explosion of copy cat variants by aspiring cybercriminals looking to make their fortunes on the backs of innocent victims.

"An interesting and nefarious development late in 2013 saw ZeuS infections being used in a new way," Henderson continued. "While ZeuS was often used as a financial trojan, a significant number of ZeuS infections were used to deliver and execute the Cryptolocker ransomware. Cryptolocker put a new spin on ransomware in that it used uniquely generated cryptographic key pairs to fully encrypt the contents of a victim's computer, and any mapped drive the victim had the ability to write to. Cryptolocker would then inform the victim they had a short period of time to pay a significant ransom -- sometimes as much as a few hundred dollars, and typically only paid using the Bitcoin cryptocurrency -- before the encryption key used to encrypt the victim's computer was deleted, making the victim's files completely unrecoverable."

Victims ranged from home users losing thousands of personally significant files such as photographs and home movies, to businesses of all sizes and public agencies. Cryptolocker was also seen to infect users via other methods, including infected flash drives, often in combination with fake program activation tools commonly spread through file sharing sites and through infected email attachments.

Top 10 Malware Families Basis Based on Number of Reported Incidents

1. W32/ZeuS(Zbot) Family
2. W32/Tepfer Family
3. JS/FBJack.A

4. PDF/Script.JS
5. W32/ZeroAccess Family
6. W32/Kryptik Family
7. JS/IFrame Family
8. W32/Yakes.B
9. X97M/Agent.F
10. W32/Blocker Family

Zero Day Vulnerabilities

FortiGuard Labs actively research and discover zero-day vulnerabilities in products that are likely candidates that a hacker would also uncover. Once the flaw is discovered, it is confidentially disclosed to the affected vendor under the Labs' Responsible Disclosure protocols. Since research began in 2006, FortiGuard Labs has discovered 142 zero-day vulnerabilities. To date, 14 remain unpatched. In 2013, the Labs discovered and responsibly disclosed 18 new zero-days, 12 of which remain unpatched. The majority of these vulnerabilities were classified as Important or Critical.

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 the vulnerabilities outlined in this report as long as the appropriate configuration parameters are 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.

Ongoing research can be found in the FortiGuard Center or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog.

About Fortinet

Fortinet (NASDAQ: FTNT) helps protect networks, users and data from continually evolving threats. As a global leader in high-performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low-performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content. Learn more at www.fortinet.com.

Copyright © 2013 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiAP, FortiDB, FortiVoice and FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties, and Fortinet does not independently endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release contains forward-looking statements that involve uncertainties and assumptions. Changes of circumstances, product release delays, or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release. If the uncertainties materialize or the assumptions prove 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. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements.

FTNT-O

Media Contact:
Rick Popko
Fortinet, Inc.
408-486-7853
rpopko@fortinet.com

Investor Contact:
Michelle Spolver
Fortinet, Inc.

408-486-7837
mspolver@fortinet.com

Source: Fortinet

News Provided by Acquire Media