April 10, 2013

Fortinet(R)'s FortiGuard Threat Landscape Research Team Reports That Bitcoin Botnet, ZeroAccess, Was the Number One Threat This Quarter

Team Also Reveals Information on South Korea Attacks and Two New Android Adware Variants

SUNNYVALE, CA -- (Marketwired) -- 04/10/13 -- 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 - March 31, 2013. FortiGuard® Labs observed that the Bitcoin mining botnet, ZeroAccess, was the number one threat this quarter as reported by FortiGate devices worldwide. The report also reveals analysis of the South Korea cyberattacks and two new Android adware variants that have climbed the watch list in the last 90 days.

ZeroAccess Shows No Signs of Slowing
"In the first quarter of 2013, we have seen owners of the ZeroAccess botnet maintain and expand the number of bots under its control," said Richard Henderson, security strategist and threat researcher for Fortinet's FortiGuard Labs. "In the last 90 days, the owners of ZeroAccess have sent their infected hosts 20 software updates."

Based on reporting from FortiGate devices worldwide, ZeroAccess is the number one botnet threat the team is seeing. ZeroAccess is used primarily for click fraud and Bitcoin mining. The value of the decentralized, open source-based digital currency continues to skyrocket, which likely means the amount of money being made by ZeroAccess is in the millions of dollars or more.

"As Bitcoin's popularity and value increases, we may see other botnet owners attempt to utilize their botnets in similar fashions or to disrupt the Bitcoin market," Henderson continued.

In March and into April, Mt. Gox, the largest Bitcoin Exchange in the world, battled a continued Distributed Denial of Service (DDoS) attack in an attempt to destabilize the currency and/or profit from it. FortiGuard Labs' analysis of ZeroAccess, which has the capability to load DDoS modules onto infected machines, revealed that the botnet does not currently have a DDoS module attached to its arsenal. This suggests other botnet owners are attempting to profit from fluctuations in the Bitcoin currency.

The growth of new ZeroAccess infections has remained constant in the last 90 days. Since FortiGuard Labs began actively monitoring ZeroAccess in August 2012, the team has seen a virtually linear amount of growth in new infections. Most recently, the team is seeing a staggering 100,000 new infections per week and almost 3 million unique IP addresses reporting infections. It's estimated that ZeroAccess may be generating its owners up to $100,000 per day in fraudulent advertising revenue alone.

Wiper Attack Hits South Korea Companies
A massive malware attack on South Korean television networks and financial institutions in March caused wide-scale damage, wiping thousands of hard drives. FortiGuard Labs, leveraging its partnerships with both the public and private sector in South Korea, has uncovered information relating to the nature of the attack and how the malware was spread. The team's research shows the attackers were able to seize control of patch management systems and use the trusted nature of those systems to distribute malware within their targets' networks.

"During out investigation of the attacks, we discovered that a version of the wiper malware was able to infect internal security management servers and use the trusted nature of that internal server to spread infections inside the victim's network," said Kyle Yang, Senior Manager of Antivirus at FortiGuard Labs.

Cleanup and restoration continues, and the perpetrators responsible remain unidentified.

Two New Adware Variants Propagating on Android
Two new Android adware variants, Android.NewyearL.B and Android.Plankton.B have seen a large number of global infections in the past 90 days.

"The new advertising kits we are monitoring suggest that the authors behind this are working very hard to remain undetected," said David Maciejak, senior researcher for Fortinet's FortiGuard Labs. "It's also possible that Newyear and Plankton are being written by the same author, but being maintained separately in order to generate more infections."

Both pieces of malware are embedded into various applications and have the ability to display advertisements, track users

through the phone's unique IMEI number, and modify the phone's desktop.

"The surge in Android adware can most likely be attributed to users installing what they believe are legitimate applications that contain the embedded adware code," said Guillaume Lovet, Senior Manager at FortiGuard Labs. "It suggests that someone or some group has been able to monetize these infections, most likely through illicit advertising affiliate programs."

Users can protect themselves by paying close attention to the rights asked by an application at the point of installation. It is also recommended to download mobile applications that have been highly rated and reviewed.

Q1 Threat Recap:

NBC.com
In February, using a popular cybercrime toolkit available in the cyber underground, attackers were able to leverage recently patched exploits in Oracle's Java and Adobe's PDF platforms to install the Citadel banking Trojan and ZeroAccess botnet onto systems that visited a number of NBC's digital properties. At the time of the attack, only three out of 46 popular antivirus applications were able to detect and mitigate this threat, and Fortinet's FortiClient was one of them.

"The reports of signature-based antivirus' death have been greatly exaggerated," said Derek Manky, global security strategist for Fortinet's FortiGuard Labs. "A signature is often used loosely to refer to a simple pattern to match a virus. But, as we've seen recently, that's not always the case. Fortinet signatures, for example, are highly intelligent, as they work with our antivirus engine to identify the intent of a virus. In a case like the NBC.com attack, advanced signatures are proven to be proactive and can help in the fight against advanced persistent threats (APTs) and zero-day attacks."

Today's APTs are able to defeat many technologies, including next generation firewalls. Building a network defense strategy that includes multiple layers of security is the best way to protect an infrastructure from attack. In the case of NBC, layers of security beyond traditional NGFW apply here -- Webfiltering, antivirus, intrusion prevision and application control all were involved.

Spamhaus
In March, global spam fighter The Spamhaus Project placed CyberBunker on their spam blacklist, which caused some groups sympathetic to the Dutch Web hosting provider to launch a sustained DDoS attack on Spamhaus. Content delivery provider CloudFlare was recruited to assist Spamhaus to help keep their blacklisting services available, but they, too, came under attack. At its peak, the attack on Spamhaus, CloudFlare and other groups reached a whopping 300 billion bits per second (Gbps), the largest online attack ever recorded. In what is referred to as a DNS Amplification attack, an attacking bot sends a spoofed request to an open DNS server and asks it to send back a large DNS file.

"As long as misconfigured or intentionally left open DNS servers exist, these types of attacks will continue and be difficult to protect against," Henderson maintained. "As botnet owners grow the size of their armies and diversify the ways in which they launch attacks, we're likely to see even larger attacks like this in the future," Henderson said.

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.

Follow Fortinet Online: Twitter at: www.twitter.com/fortinet; Facebook at: www.facebook.com/fortinet; YouTube at: http://www.youtube.com/user/SecureNetworks.

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a 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 2012 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 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