Fortinet's FortiGuard Labs Reveals 2012 Threat Predictions

Expected Threats Include Mobile Ransomware, Android Worms and Increased Hacktivism

SUNNYVALE, CA -- (MARKET WIRE) -- 12/13/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today revealed FortiGuard Labs' 2012 threat predictions, highlighting eight threats to watch out for next year.

Top 8 Security Predictions for 2012
1. Ransomware to Take Mobile Devices Hostage
"Ransomware," an infection that holds a device "hostage" until a "ransom" payment is delivered, has been around on PCs for years. Mobile malware that utilize exploits have also been observed, along with social engineering tricks that lead to root access on the infected device. With root access comes more control and elevated privileges, suitable for the likes of ransomware. FortiGuard predicts we'll see the first instances of ransomware on a mobile device in the coming year.

2. Worming into Android
Worms, malware that is able to quickly propagate from one device to another, have by and large remained absent from the Android operating system, but FortiGuard Labs believes that will change in 2012. Unlike Cabir, the first Symbian worm discovered in 2004, Android malware developers most likely won't be using Bluetooth or computer sync to spread out because of their limited ranges. Instead, the team believes the threat will come from either poisoned SMS messages that include a link that contains the worm or through infected links on social networks, such as Facebook and Twitter.

3. Polymorphism Want a Cracker?
In the last year, FortiGuard Labs has seen Android malware use encryption, embed exploits, detect emulators and implement botnets. But what they haven't seen yet is an example of polymorphism. Polymorphism is malware that is capable of automatically mutating, making it extremely difficult to identify and thus destroy. The team has previously encountered polymorphism on Windows Mobile phones and believes it's only a matter of time before the malware appears on Android devices.

4. Clampdown on Network-Based Money Laundering
Using anonymous fund transferring services, human networks and payment processor safe havens, cybercriminal syndicates have pretty much operated with impunity for years. However, FortiGuard Labs believes more people will be tracked and captured in 2012. The recent arrest of ChronoPay CEO Pavel Vrublevsky's on the grounds of hacking Aerfolot's Website and preventing visitors from buying tickets, is a good example of the type of takedowns the team expects to see in the coming year.

5. Public-Private Relationships in Security
In 2011, FortiGuard Labs saw an increase in global collaborative botnet takedowns including Rustock and DNS Changer. Meanwhile, arrests were made against international members of Anonymous and LulzSec hacktivist groups. This crackdown will continue in 2012, and the team believes that much of it will be aided by Defense Advanced Research Projects Agency's (DARPA's) public defense initiative. DARPA was recently granted $188 million budget and plans to use part of the money on initiatives to build a cyber defense team in the private sector. It seems likely that in 2012 similar relationships will be formed worldwide.

6. SCADA Under the Scope
For over a decade, Supervisory Control and Data Acquisition- (SCADA) based threats have been a concern, because they are often connected to critical infrastructure such as power and water grids, which are not always operating on a closed circuit. Many new human machine interface (HMI) devices that interact with these systems have Web interfaces for logging in that can be circumvented to access back end systems. Groups such as Anonymous have already found an assortment of Web-based vulnerabilities simply by picking targets and scouring code. In 2012, FortiGuard predicts new SCADA vulnerabilities will be discovered and exploited with potentially devastating consequences.

7. Sponsored Attacks
The FortiGuard team often talks about Crime as a Service (CaaS) to describe how criminal syndicates are offering though the Internet illegal and detrimental services, such as infecting large quantities of computers, sending spam and even launching direct denial of service (DDoS) attacks. In 2012, FortiGuard Labs expects to see CaaS leveraged for more strategic and targeted attacks on companies and individuals to include state or corporate sponsorship.

8. Hacking a Good Cause
While Anonymous formed on 4Chan.org in 2003, only in the last year have the loosely organized anarchists started using their

power to attack large, high profile targets such as Sony or, like towards the end of the year, using their power for "good." Case in point, they've recently threatened to unmask Mexican drug cartel members and they recently helped authorities break up a child porn ring. FortiGuard expects to see more examples of "hacktivist" justice meted out throughout 2012 along with a mix of attacks that border or cross the line of justice.

About FortiGuard Labs
FortiGuard Labs compiled threat statistics and trends data for these predictions 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 many of the vulnerabilities discussed in these predictions.

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.

Last year's threat predictions 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.

Fortinet has not independently verified statements or certifications herein attributed to third parties and Fortinet does not independently endorse such statements. Nothing in the news release constitutes a warranty, guaranty, or contractually binding commitment. This news release may contain forward-looking statements that involve uncertainties and assumptions. 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, including but not limited to, any statements related to expected trends in threat activity. These trends are difficult to predict and any stated expectations regarding these trends may not ultimately be correct. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements.

FTNT-O

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contacts:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media