



Fortinet Announces Top Australian Technology Threats for March 2007

Fortinet – the pioneer and leading provider of unified threat management (UTM) solutions – today announced the most threatening reported malware activities and top 10 threats for March 2007.

Top 10 Australian threats caught for March 2007 include:

Rank

Name

% of Detections

1

W32/Netsky.D@mm

10.3

2

W32/MyTob.EK@mm

9.1

3

HTML/Phishbank.BGU!phish

7.6

4

W32/Netsky.P@mm

6.8

5

HTML/Clicker.AC!tr

6.0

6

HTML/Iframe_CID!exploit

5.0

7

Adware/Boran

3.3

8

W32/Istbar.PK!tr.dldr

2.9

9

W32/Agent.BCD!tr.dldr

2.3

10

W32/KillAV.3B84!tr

2.2

The most common threat for March 2007 in Australia was W32/Netsky.P@mm and its variants. W32/Netsky.P@mm was first discovered in March 2004. The virus contains its own SMTP code to send itself by email, allowing it to rapidly spread via poorly protected computers connected to the Internet.

Charles Cote, Country Manager for Fortinet Australia commented, "Identity theft is a very serious danger for anybody using the Internet. Phishing attacks are a particular concern, as their purpose is usually to steal your identity in order to commit a crime. Businesses of all sizes need to move beyond relying solely on old fashioned anti-virus software running on Windows PCs, and deploy unified threat management systems which block threats before they reach your computers."

The malware report, compiled from all FortiGate® multi-threat security systems in production worldwide, is a service of the global security research team that supports Fortinet's FortiGuard Network®, which provides continuous updates to help protect against the latest threats around the clock and around the world.

Top 10 worldwide threats caught for March 2007 include:

Rank

Name

% of Detections

1

W32/Netsky.P@mm

4.62

2

W32/Bagle.DY@mm

4.44

3

HTML/Iframe_CID!exploit

3.93

4

W32/Grew.A!worm

2.87

5

W32/Bagle.GT@mm

2.47

6

HTML/BankFraud.BGU!phish

2.23

7

W32/Sality.Q

1.93

8

W32/Istbar.PK!tr.dldr

1.63

9

W32/Everda!tr

1.56

Adware/Solutions180

1.31

Worldwide, adware and more advanced phishing attacks focused on Web 2.0 sites such as MySpace.com are becoming more widespread.

Leveraging the popularity of Web 2.0 community sites, a new style of attack known as a Phisher Worm is making an appearance. Initially preying on MySpace users, the attack appears in the form of a message, with text encouraging the user to click on a link pointing to a seemingly funny video. The link directs novice users to a phishing site mimicking the MySpace login page, rather than to the advertised video. Anyone entering his or her credentials into that rogue login page hoping to see the video have their account details stolen, and then those credentials are used for spamming purposes. In addition, a server-side program on the rogue server then distributes the initial message carrying the rogue link to all the contacts of the freshly phished user, hence effectively propagating the Phisher Worm throughout the community.

To read the full March report, please visit http://www.fortiguardcenter.com/reports/roundup_mar_2007.html

For additional research from Fortinet's security response team, visit the FortiGuard Center at <http://www.fortiguardcenter.com/>.

About Fortinet (www.fortinet.com)

Fortinet is the pioneer and leading provider of ASIC-accelerated multi-threat security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and antispam--providing customers a way to protect multiple threats as well as blended threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified eight times over by the ICSA (firewall, antivirus, IPSec, SSL, IPS, client antivirus detection, cleaning and antispayware). Fortinet is privately held and based in Sunnyvale, California.

###

Fortinet is a registered trademark of Fortinet, Inc. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, and FortiReporter are trademarks of the Fortinet, Inc. in the United States and/or other countries. All other trademarks referred to herein are the property of their respective owners.