



Fortinet Announces Top Reported Technology Threats for Aug 2007

Fortinet – the pioneer and leading provider of unified threat management (UTM) solutions – today announced the top 10 most reported high-risk threats for August 2007. The report, compiled from all FortiGate® multi-threat security systems in production worldwide, is a service of Fortinet’s FortiGuard Global Security Research Team.

August 2007’s top 10 threats, as determined by the degree of prevalence are:

Rank

Threat Name

Threat Type

% of Detections

1

W32/Dloader.K!tr

Trojan

10.17

2

W32/Netsky.P@mm

Mass mailer

9.53

3

HTML/Iframe_CID!exploit

Exploit

7.84

4

Adware/CashOn

Spyware

6.68

5

W32/Dialer.PZ!tr

Trojan

4.29

6

W32/ANI07.A!exploit

Exploit

4.00

7

HTML/Obscured!exploit

Exploit

3.70

8

W32/Grew.A!worm

Worm

3.42

9

W32/Bagle.DY@mm

Mass mailer

3.28

10

The August top 10 highlights the following:

More than 89% of malware activity volume was observed in Korea this month, with Dloader.K!tr (aka Small), a downloader loading malware on personal computers, at the top of the chart. Dloader.K!tr displayed large spikes of activity in Korea, indicating that the source of the distribution campaign resides there. In parallel, with a growth rate of activity at 80%, the CashOn adware, installed via a toolbar plug-in for a Korean Website, was also very active, exceeding 750,000 hits. The FortiGuard Global Security Research Team noticed a parallel trend between those two malware, with similar distribution spikes on Mondays and Thursdays.

Obscured!Exploit gained momentum, joining the top ten list for the first time. Its activity has increased by 20% since July 2007, and by 75% since June 2007.

Dialer.PZ, which has been part of the top 10 threats for the past few months, remained active with consistent production waves, although its volume has dropped around 80% since it was first identified in May. This dialer still targets Mexico and the USA.

Another trend in August was the rise of service-luring Websites created to attract additional users and ultimately drive higher online advertising revenues. A service-luring (aka: sluring) site is a site that performs ID-theft by prompting users to provide personal information in order to access an online service – a service they will never actually get.

As an example, a site called Scan Messenger prompts the user to enter his or her Messenger login and password, and offers to use that information to determine if other Messenger contacts have blocked or deleted the user from their contact list. Not only does this not happen but the user's nickname is replaced by the Website URL in order to "promote it" to the user's contacts, driving them, in turn, to the Website too. This "worm-like" method of driving Website traffic has proved successful, given that this particular site was registered three months ago and has been translated into 20 languages.

"Service-luring sites are less likely to be shut down than phishing sites, given that there is no actual infringement taking place and these sites tend to have unique terms and conditions," said Guillaume Lovet, manager for the FortiGuard Global Security Research Team. "But like phishing sites, users giving their login and password information don't realize that it can be easily used for wrong purposes. As a rule, users should never give out any login credentials to an online service, regardless of the reason for the request."

To read the full August report, please visit http://www.fortiguardcenter.com/reports/roundup_aug_2007.html. For ongoing threat research, bookmark the FortiGuard Center (<http://www.fortiguardcenter.com/>) or add it to your RSS feed by going to

<http://www.fortinet.com/FortiGuardCenter/rss/index.html>. To learn more about FortiGuard Subscription Services, visit

<http://www.fortinet.com/products/fortiguard.html>.

About Fortinet (www.fortinet.com)

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, 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 anti-spam -- designed to help customers protect against network and content level 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 ICSA Labs (firewall, antivirus, IPSec, SSL, IPS, client antivirus detection, cleaning and antispymware). 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.

Contacts

Sebastian Rice
+61 2 9959 1991
mailto: seb@silverspan.com