

Global Threat Report June 07

The Next Generation of Bots Rears Its Head in High Profile Web Malware Incident on MySpace

In June, ScanSafe reported a high profile malware outbreak that used fast flux (aka flux bot) networks to seed a Web-based attack. Fast flux is used to hide malware delivery sites behind complex ever changing networks of proxy servers. A system infected with a flux bot will be used as one of these proxies. On June 28, ScanSafe identified fast flux being used to spread malware on MySpace. A flash movie installed on several compromised MySpace pages lead users to a spoofed MySpace login page. The login page hosts a number of exploits that download malware and attempt to make the user login to MySpace so that their credentials can be stolen and their MySpace page can then be updated to host malware. ScanSafe estimates that nearly 100,000 MySpace accounts may have been affected.

Fast flux networks represent a disturbing advance in the development and use of bot networks – networks of compromised ‘zombie’ PCs used to spread malware. Unlike traditional bots, which use IRC servers, PCs compromised by fast flux networks serve temporary hosts for malicious Websites. These hosting bots are constantly rotated, changing their DNS records to avoid detection. ScanSafe anticipates that fast flux networks will increasingly be used to seed malware.

About the ScanSafe Threat Center

2007The ScanSafe Threat Center monitors the global state of Web traffic, 24 hours a day, seven days a week. Combining technology as well as analysis from threat technicians, the ScanSafe Threat Center processes more than 7 billion Web requests each month from more than 30 countries around the world and provides unparalleled insight into real-time Web threats and usage. At the core of the ScanSafe Threat Center is Outbreak Intelligence, which leverages ScanSafe's position at the Internet-level to proactively identify threats, quickly develop heuristics, and test these against real data to quickly ensure accuracy and effectiveness. ScanSafe's ability to analyze threats proactively ensures that Outbreak Intelligence heuristics are created and updated for immediate protection from both known and unknown threats.

Web Virus

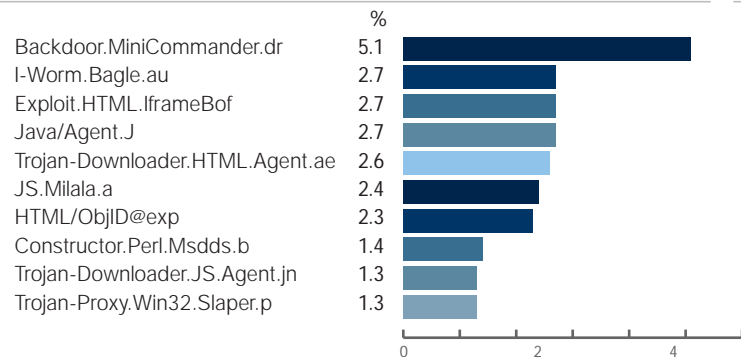
Key Data

Web Viruses	11.8% Decrease over May 2007
Unique Viruses Stopped	326
New Viruses Stopped	164

Key Trends

Web viruses decreased 12% in June after increasing 36% in May. ScanSafe blocked 324 unique viruses, half of which were new unique viruses – viruses seen and blocked for the first time by ScanSafe's network.

Top 10 Web Viruses Blocked



Percentage of Web Virus Blocks By Day



Spyware and Adware

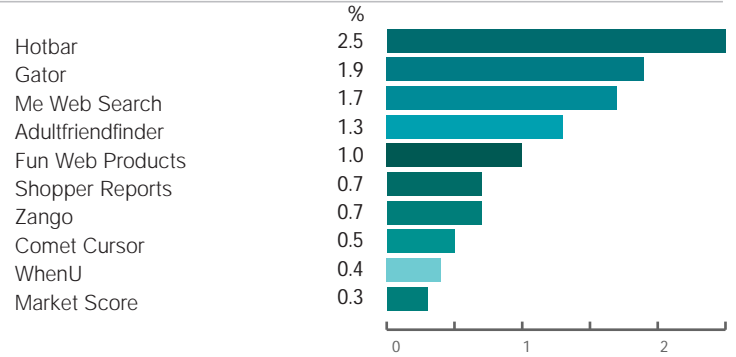
Key Data

Spyware/Adware	2.2% Decrease over May 2007
Trackers	54.68%
Adware/Browser Helper Object	39.20%
Spyware Calling Home	3.21%
Drive By Install Attempts	2.91%
	100%

Key Trends

Spyware and adware blocks decreased 2% in June following a 10% increase in May.

Top 10 Spyware, Adware & Ad-Sponsored Marketing Software Blocked



Percentage of Spyware, Adware & Ad-Sponsored Marketing Software Blocks By Day



