

WEB VIRUSES INCREASE 36%; LEGITIMATE WEBSITES INCREASINGLY HIJACKED TO UNKNOWINGLY DISTRIBUTE MALWARE VIA 3RD PARTY PROVIDED CONTENT

For the second consecutive month ScanSafe reported a large increase in Web viruses (36%). The ANI (animated cursor) vulnerability, reported in late March, may be responsible for part of the recent increase in Web viruses. While a patch has been available since early April, millions of PCs remain unpatched and vulnerable to ANI exploits. ScanSafe expects to see ANI exploits for months to come.

ScanSafe also cautioned that it is increasingly seeing legitimate websites unknowingly host malware as the result of malicious content provided to sites by 3rd parties or through compromised servers. This includes content from ad servers, user contributed content, and widgets – interesting content from 3rd party sites. Even more troubling, when hosting companies are compromised, all of their customers' websites are at risk.

In early June, hackers gained access to passwords for FTP accounts for 3,500 websites hosted by DreamHost. As a result, ScanSafe identified 2 high profile U.K industry sites (www.clintons.co.uk and www.nationwidemercurys.com) that unknowingly hosted an iFrame that loaded Trojan-Downloader.JS.Psyme.fq. It then redirected to a malicious website, where a second piece of malware, Trojan-Downloader.Win32.Small.mi, was executed. The entire attack was completely invisible to users—including the iFrame which was just 1 pixel wide.

This followed an instance in early May, when a compromised ad server was used to distribute ANI exploit on www.tomshardware.com, a popular technical product review site.

ABOUT THE SCANSAFE THREAT CENTER

The 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

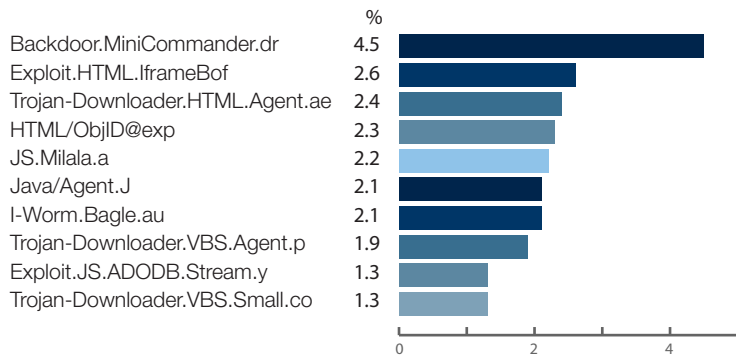
Key Data

Web Viruses	↑ 36.2% Increase over Apr 2007
Unique Viruses Stopped	265
New Viruses Stopped	130

Key Trends

Web viruses increased 36% in May after increasing 26% in April. ScanSafe blocked 265 unique viruses, 49% 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

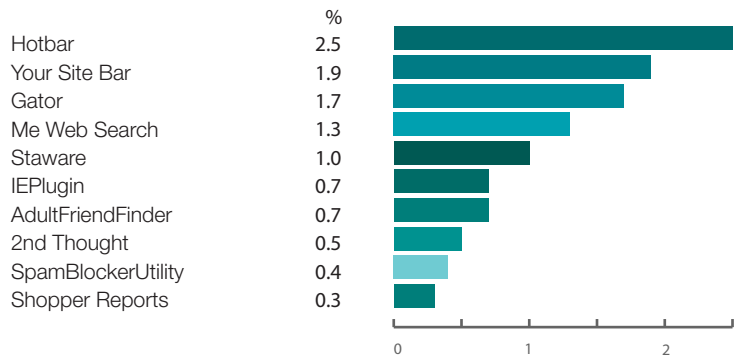
Key Data

Spyware/Adware	↑ 9.8% Increase over Apr 2007
Trackers	59.14%
Adware/Browser Helper Object	34.26%
Spyware Calling Home	3.88%
Drive By Install Attempts	2.72%
	100.00%

Key Trends

Spyware and adware blocks increased 10% in May following an 8% increase in April.

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



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

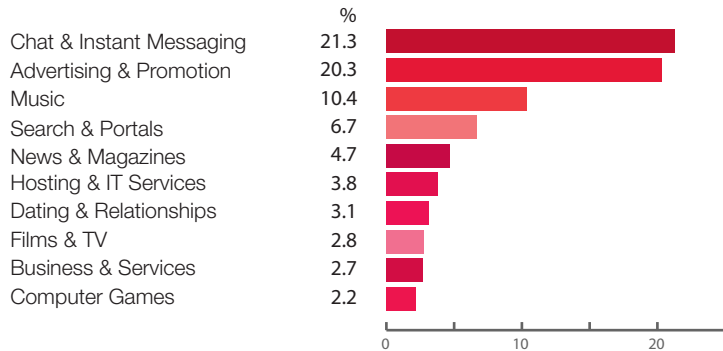


WEB FILTERING

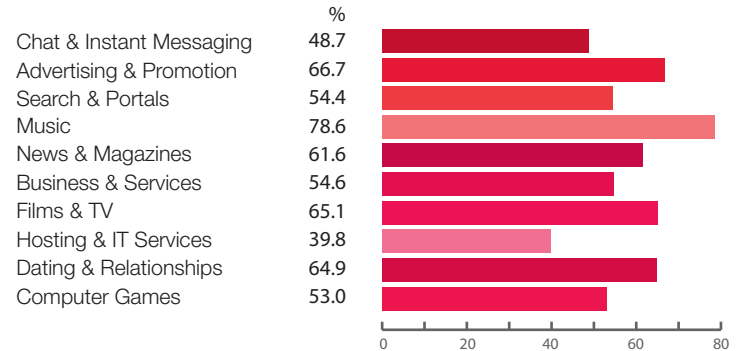
Key Trends

Web filtering blocks increased 49% in May following an 8% increase in April. For the third consecutive month, Online Chat and Instant Messaging accounted for the largest percentage of Web Filtering Blocks (21%) followed by Advertising & Promotion (20%) and Music (10%).

Top 10 Blocks By Category



% of Companies with Users Attempting to Access Blocked URL Categories



IM CONTROL

Key Trends

IM blocks decreased 25% in May following a 9% increase in April. ScanSafe identified and blocked 18 new IM threats. MSN Messenger remained the most targeted IM platform with 50% of blocked IM threats targeting it compared to 28% that affected Yahoo! and 17% that affected AIM.

Key Data

New Unique IM Threats	↓ 25% decrease over Apr 2007
New Unique IM Threats	18
Last Month	24

Top 10 recent IM Threats

Malware Name	Networks Affected				
	Total	MSN	AOL	Yahoo!	Generic
W32/Rbot-KPH	1	0	1	1	0
W32/Culler	1	0	1	0	0
W32.Posse	1	0	1	0	0
W32/Hakaglan.worm.gen	1	0	0	1	0
W32/Spybot-NR	1	0	1	1	0
Troj/PWS-AMY	1	0	0	1	0
Worm/TermX.A	1	1	1	1	0
W32/Culler-Gen	1	0	1	0	0
MSNDiablo.A	1	0	1	0	0
W32/Sohana-V	1	0	0	0	1

NOTE TO READERS

Spyware, Adware & Ad-Sponsored Marketing Software Blocked

ScanSafe Web Malware Scanning service is designed to help businesses maximize productivity by blocking a range of programs that some users might consider unwanted. ScanSafe recognizes that there may be legitimate uses of these applications in environments where an authorized administrator has knowingly installed this application.

Disclaimer

The statistics contained in this report are based on data generated by ScanSafe from analysis of over 7 billion individual Web requests each month from 30+ countries. While ScanSafe believes that this is a reasonably representative statistical sample, and conforms to the corresponding level of validity testing, Internet content and usage will inevitably change over time and ScanSafe accepts no liability in respect to the accuracy or completeness of the statistics.

ScanSafe seeks to encourage and facilitate the safe and productive use of the Internet through the use of its Web security solutions. However, nothing in this report is intended as a criticism of any specific website, and Internet users should form their own view as to the risks involved in visiting specific websites.

Contact ScanSafe

ScanSafe US
 999 Baker Way, Suite 410
 San Mateo, CA 94404
 T: +1 650 294 3450
 F: +1 650 294 3451
 E: ussales@scansafe.com

ScanSafe EMEA
 The Connection, 198 High Holborn
 London, WC1V 7BD
 T: +44 (0) 20 7959 0630
 F: +44 (0) 20 7959 0631
 E: emeasales@scansafe.com