



Virus Threats - August 2009

Two malware ratings have been compiled from data generated by the Kaspersky Security Network (KSN) in August 2009.

The first Top Twenty lists malicious programs, adware and potentially unwanted programs that were detected and neutralized when accessed for the first time, i.e. by using the on-access scanner.

Position	Name
1	Net-Worm.Win32.Kido.ih
2	Virus.Win32.Sality.aa
3	not-a-virus:AdWare.Win32.Boran.z
4	Trojan-Downloader.Win32.VB.eql
5	Trojan.Win32.Autoit.ci
6	Virus.Win32.Virut.ce
7	Worm.Win32.AutoRun.dui
8	Net-Worm.Win32.Kido.jq
9	Virus.Win32.Sality.z
10	Virus.Win32.Induc.a
11	Worm.Win32.Mabezat.b
12	Net-Worm.Win32.Kido.ix
13	Packed.Win32.Klone.bj
14	Trojan.Win32.Swizzor.b
15	Packed.Win32.Katusha.b
16	Worm.Win32.AutoIt.i
17	not-a-virus:AdWare.Win32.Shopper.v
18	Trojan-Dropper.Win32.Flystud.yo



19	Email-Worm.Win32.Brontok.q
20	P2P-Worm.Win32.Palevo.jaj

Net-Worm.Win32.Kido.ih and Virus.Win32.Sality.aa, our two long-standing leaders, are still at the top of the rating.

There are six newcomers to this month's Top Twenty and some of them deserve a special mention.

By far the most interesting is Virus.Win32.Induc.a, which we've written about a number of times in recent weeks [in news](#) and [in weblog](#). To recap: in order to replicate, Virus.Win32.Induc.a makes use of the fact that Delphi has a two stage method for creating executable files - the application source code is first compiled into intermediate DCU modules which are then assembled into Windows executable files. Software products compiled on machines which had infected versions of Delphi were consequently infected with the virus when they were compiled; as there were a lot of these products, it's no surprise that Induc went straight into tenth place.

Another newcomer, not-a-virus:AdWare.Win32.Boran.z, entered the ratings even higher, coming straight in at third place. This program is a component of the Baidu Toolbar for Internet Explorer, which is popular in China. It uses a range of rootkit technologies to prevent users from removing the toolbar using standard methods.

Trojan.Win32.Swizzor.b and Packed.Win32.Katusha.b claimed 14th and 15th positions respectively. These two replace earlier versions of the same programs which previously figured in our ratings. In comparison to the previous versions, both these programs use very sophisticated and innovative obfuscation methods.

Palevo.jaj took last place in the Top Twenty, taking over from its relative P2P-Worm.Win32.Palevo.ddm that emerged back in May. As this version of Palevo spreads via file exchange networks, infects removable media, can also be spread by IM, and includes a backdoor which gives an attacker the ability to control infected computers, this malware poses quite a threat.

Overall, the appearance of Virus.Win32.Induc was the highlight of the month, as this malware does use a truly innovative approach to infecting users' computers.

Overall, there were no significant changes to the first Top Twenty in August, unlike our second Top Twenty.

Our second Top Twenty presents data generated by the web antivirus component, and reflects the online threat landscape. This ranking includes malicious programs detected on web pages and malware is downloaded to victim machines from web pages.

Position	Name
1	not-a-virus:AdWare.Win32.Boran.z
2	Trojan-Downloader.HTML.IFrame.sz
3	Trojan.JS.Redirector.l
4	Trojan-Downloader.JS.Gumblar.a
5	Trojan-Clicker.HTML.Agent.w
6	Exploit.JS.DirektShow.k



7	Trojan-GameThief.Win32.Magania.biht
8	Trojan-Downloader.JS.LuckySploit.q
9	Trojan-Clicker.HTML.IFrame.kr
10	Trojan-Downloader.JS.Major.c
11	Exploit.JS.Sheat.c
12	Trojan-Downloader.JS.FraudLoad.d
13	Trojan-Clicker.HTML.IFrame.mq
14	Trojan.JS.Agent.aat
15	Exploit.JS.DirektShow.j
16	Trojan-Downloader.JS.IstBar.bh
17	Trojan-Downloader.JS.Iframe.bmu
18	Exploit.JS.DirektShow.l
19	Exploit.JS.DirektShow.q
20	Trojan-Downloader.Win32.Agent.ckwd

More than half the entries in August's second Top Twenty are new examples of cybercriminals' creativity.

AdWare.Win32.Boran.z, which has already been described, took first place in this rating.

A month ago we [wrote](#) about [a vulnerability in Internet Explorer](#). The script that exploits this vulnerability is detected by Kaspersky Lab products as Exploit.JS.DirektShow. The July Top Twenty included three modifications of this exploit: .a, .j and .o. This month, there are four versions in the rankings, showing that exploiting this vulnerability is apparently still a very popular approach. It seems that cybercriminals assume that lots of users won't have installed the security patch, and so they keep trying to attack systems via this loophole.

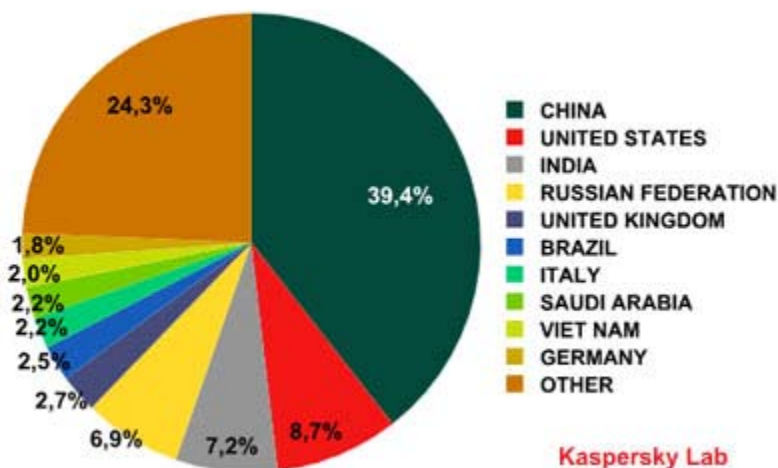
[Another vulnerability](#), this time in Microsoft Office, was also actively exploited by cybercriminals in August. One modification of an exploit for this vulnerability – Exploit.JS.Sheat - took 11th place in the rating.

Fake, or rogue antivirus applications are spread from a number of web pages and one of the scripts that facilitates this took 12th place in our rating. Kaspersky Anti-Virus detects it as Trojan-Downloader.JS.FraudLoad.d. If a user visits a website infected with this script, they are notified that their computer is infected with lots of malicious programs and that these programs can be removed. If the user agrees to this, a rogue antivirus (classified as FraudTool) is then downloaded to their computer.

The Trojan Redirector.I works by redirecting user search requests to specific servers in order to increase the hit rate for these servers. The Trojan-Downloader program Iframe.bmu is a typical example of malware which contains a range of different exploits, in this case exploits for Adobe products.

The trends seen in July are continuing, with cybercriminals still actively exploiting vulnerabilities in popular software products. Rogue antivirus applications and basic iframe-clickers are also spreading fast. It's unlikely that this situation will change next month, as cybercriminals have tried and tested these approaches and found them to be successful.

Countries where most attempts to infect computers via the web were recorded:



Monthly Malware Statistics for August 2009 - Courtesy Kaspersky Lab



USA - Sales Toll Free: +1- 866-663-2927 | Support Toll Free: +1-877-380-8531
 India - Sales: +91-79-66065606 | Support Toll Free: 1-800-301-00013
 EMEA/APAC - Sales: +91-79-66065787 | Support: +91-79-66065777

Copyright © 1999 - 2008 Elitecore Technologies Ltd. All rights reserved. Elitecore and Cyberoam logo are registered trademarks of Elitecore Technologies Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice.

