



Virus Threats – September 2008

Two virus rankings have been compiled as a result of Kaspersky Security Network (KSN) activity in September.

The first ranking represents the most widespread malware, adware and potentially unwanted programs according to the number of computers they were detected on.

Position	Name
1	Rootkit.Win32.Agent.cvx
2	Trojan-Downloader.WMA.Wimad.n
3	Packed.Win32.Black.a
4	Trojan.Win32.Agent.abt
5	Trojan-Downloader.HTML.IFrame.sz
6	Trojan-Downloader.Win32.VB.eqj
7	Trojan-Downloader.JS.IstBar.cx
8	Trojan.Win32.Agent.tfc
9	not-a-virus:AdWare.Win32.BHO.ca
10	Trojan-Downloader.Win32.Small.aacq
11	not-a-virus:AdWare.Win32.Agent.cp
12	Trojan.Win32.Obfuscated.gen
13	not-a-virus:AdWare.Win32.BHO.sc
14	not-a-virus:AdWare.Win32.BHO.vp
15	Trojan.Win32.Chifrax.a
16	Trojan-Dropper.Win32.Agent.tbd
17	Trojan.RAR.Qfavorites.a
18	Email-Worm.Win32.Brontok.q



19	Trojan-Downloader.JS.Agent.cme
20	Trojan-Downloader.JS.Agent.chk

KSN recorded a change at the top of the rankings in September for the most widespread malicious and potentially unwanted programs. The former leader, Trojan.Win32.DNSChanger.ech, is nowhere to be seen and a wholly unexpected piece of code claimed first place.

The new leader turned out to be Rootkit.Win32.Agent.cvx. It was detected by our experts on 28 August and throughout the month it actively spread across the internet. Two factors have set the alarm bells ringing: first of all, rootkits are notoriously awkward customers for antivirus software and, secondly, very few antivirus programs, as yet, can detect this particular specimen.

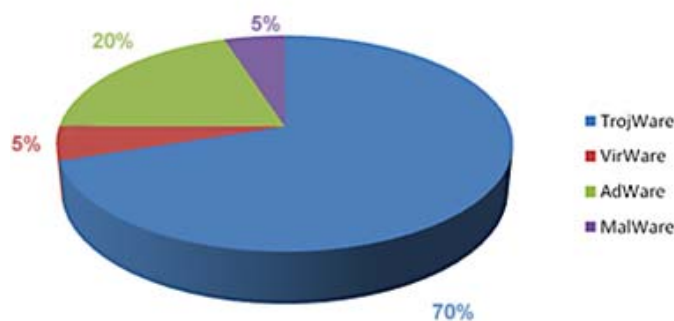
Another unusual malicious program, Trojan-Downloader.WMA.Wimad.n, returned to second place. This multimedia file exploits a vulnerability in Windows Media Player to download various Trojans.

A significant amount of the attacks on users stem from various script downloaders, with a total of four in September's rankings. These scripts act as the "trigger" for the majority of "drive-by download" attacks. By the way, Wimad.n functions by using exactly these types of Trojan Downloaders.

Interestingly, not only have all the adware programs from last month remained in the Top Twenty some of them have even consolidated their positions.

September's ranking only saw nine new entries (compared to 16 in August). Among them is the veteran worm of the virus world Brontok.q in eighteenth place. Attentive readers who have been following our monthly reports for some time will be familiar with this worm which has consistently figured in our rankings, even when they were compiled using different data sources and methodologies.

All the malware, adware and potentially unwanted programs from this ranking can be broken down into the four main categories of threats that we detect. Trojans remain the clear leader, but their share has fallen from 80 to 70%.



A total of 35103 different malicious and potentially unwanted programs were detected on users' computers in September. That represents another significant increase in the number of in-the-wild threats for the second month in a row (the figure for August was 28940).

The second table provides data about the most common malicious programs among all infected objects detected on users' computers. The majority of the programs listed below have file-infection capabilities.



Position	Name
1	Virus.Win32.Xorer.du
2	Net-Worm.Win32.Nimda
3	Worm.Win32.Mabezat.b
4	Virus.Win32.Alman.b
5	Virus.Win32.Sality.aa
6	Virus.Win32.Parite.b
7	Virus.Win32.Virut.n
8	Virus.Win32.Small.l
9	Virus.Win32.Virut.q
10	Virus.Win32.Parite.a
11	Email-Worm.Win32.Runouce.b
12	Virus.Win32.Sality.s
13	Virus.Win32.Hidrag.a
14	Virus.Win32.Sality.z
15	Trojan.Win32.Obfuscated.gen
16	Worm.Win32.Fujack.k
17	Virus.Win32.Tenga.a
18	Trojan-Downloader.WMA.GetCodec.d
19	Worm.VBS.Headtail.a
20	Virus.Win32.Sality.q

The changes to this ranking were minimal – only four new entries. But there was a change at the top. Nimda, which unexpectedly claimed first place in August, has fallen to second, making way for its nearest rival, the Xorer.du file virus.



September saw yet another member of the Sality family enter this ranking, bringing their number up to four, including Sality.aa in fifth place.

Mabezat.b has become another worm to be reckoned with. It initially showed no significant activity after being detected in November of last year, as it probably went about gradually increasing the number of infected machines and files. Now it has popped up in third place.

Overall, it has to be said that the state of virus and worm activity is rather stable and shows no signs of getting worse. According to KSN data, a number of malicious programs that infect files have been significantly curtailed over the last three months, which is borne out in the examples of the Allapple and Otwygal families falling off of our ranking.

Monthly Malware Statistics for September 2008 – Courtesy Kaspersky Lab



Toll Free Numbers

USA : +1-877-777-0368

India : +1-800-301-00013

APAC/MEA : +1-877-777-0368

Europe : +44-808-120-3958

Copyright © 1999 - 2008 Elitcore Technologies Ltd. All rights reserved.
Cyberoam and Cyberoam logo are registered trademarks of Elitcore Technologies Ltd. Although Elitcore has attempted to provide accurate information, Elitcore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitcore has the right to change, modify, transfer or otherwise revise the publication without notice.
PL-30-95435-080805

