‘e Scan™

Malware Report

(Jan'11 - Jun'11)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

Malware Report

The complexity and the growth of malware have more than just tripled in the last six months. What we have witnessed and will be witnessing is a change in the threat landscape. Clever new ways have cropped up to compromise new devices of which, fake antivirus are on the rise and password stealing malware are showing a sudden surge in the level of activity. Their ability to adapt to avoid detection is one aspect that needs to be taken into consideration. Moreover, the growing complexity in malware show that cybercriminals are posing challenges to security vendors. The ever growing functionality of the World Wide Web has put users at a greater risk as the ease of gaining users personal information, credit card, bank account numbers have greatly increased. The last couple of years have seen a surge in malware threats and it has now turned into a profitable business for cyber criminals and has formed into highly organized, profit-motivated crime rings. Having said that, cyber attacks can take any form and adopt various different methods such as phishing, compromised URLs, drive by downloads, and vulnerabilities.

In what got to be known as Operation Payback, 2011 saw the rise in DDoS attacks against some well known companies. These attacks were in response to corporations that froze donations to WikiLeaks due to political pressures. As a result companies such as Swiss PostFinance, Mastercard, Visa, Paypal and Amazon were made unavailable. With the beginning of such an outcry, followers of WikiLeaks have literally shown the effectiveness of such attacks on IT infrastructure. Taking to the streets or rioting seems to be a thing of the past. The very fact that the web can be used as a medium to get one's message across is extremely thought provoking. However, there is more to it than meets the eye. Cyber espionage, industrial sabotage and hacktism are a growing threat to our IT infrastructure. Moreover, the campaigns that were initially started by followers of WikiLeaks can and will in fact lead to a rise in the number of attacks – be it towards businesses, political parties, governments or institutions.

Top 10 Malware Threats
(Jan 2011- June 2011)

- Backdoor.IRCBot.ADCD
- Gen:Variant.Kazy.14119
- Gen:Variant.Kazy.7494
- Trojan.JS.Iframe.AEW
- Trojan.JS.Agent.ECM
- Trojan.Dropper.RYF
- Trojan.Generic.KD.295209
- Backdoor.PHP.IRCBot.AC
- Gen:Variant.Kazy.32687
- Dropped:Trojan.Downloader.JODP

With that being said, social networks are and still will be a focal point for hackers as far as targeted attacks are concerned. What make hackers favour social networks is the access to information along with the intertwined services (such as Facebook) that come with their respective applications make for a more effective approach to attacks – be it on individuals or organizations. In addition, to further help in the distribution of malware, location based services and URL shortening services will be used to a much larger extent.

The use of common accounts across various platforms is also a growing concern. For instance, Google's seamless integration across platforms provides users to access not only Gmail but also their newly launched social hub – Google+. In addition, this also perfectly integrates with all Android platforms. While this greatly enhances usability it also comes as a risk of the highest degree as a compromise of one account will compromise all connected accounts. This would include his email account and personal identity. In addition, his Google Checkout account can be used to make un-called for online purchases.

Exploits or application vulnerabilities are major concerns that need to be patched every now and then. With over 85% of PCs (worldwide) using some sort of Java plugins and with the prevalence of security holes it becomes inevitable for hackers to overlook such a gaping hole. Therefore there will be a significant rise in Java based attacks in the months that will follow. However, keeping your system patched with the latest security updates will help in thwarting such attacks.

The following report is generated to give you an in-depth analysis of the overall malware statistics that is prevalent around the world. We have broken them down into 7 different sections to help you get a better analysis of the report.

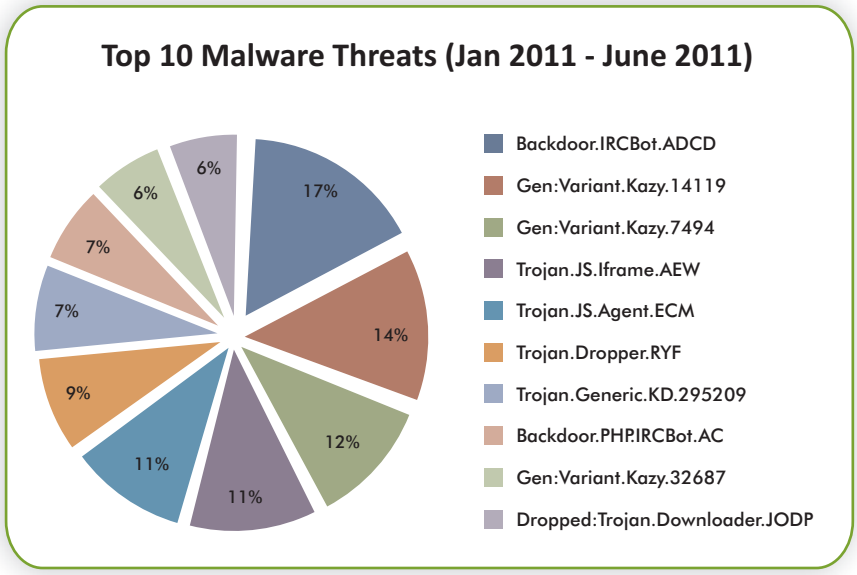
The sections will include:

- Top 10 Malware Threats
- Malware URL Count (Hosted Countries)
- Malware Count by Extension
- Malware Count (Month Wise)
- Malware Count (Day Wise)
- Domain Wise Malware Hosting

Top 10 Malware Threats

Torjans have always been categorized as the highest as far as malware is concerned. The main reason behind their popularity is mainly because they allow hackers remote access to a target computer. Once installed, the Trojan allows the hacker to perform various operations. Operations could include anything from –

- Use of the machine as part of a botnet (e.g. to perform automated spamming or to distribute Denial-of-service attacks)
- Data theft (e.g. retrieving passwords or credit card information)
- Installation of software, including third-party malware
- Downloading or uploading of files on the user's computer
- Modification or deletion of files
- Keystroke logging
- Screen capturing
- Crashing the computer
- Anonymizing Internet viewing



Malware URL Count (Hosted Countries)

Infected webpages play a big role in the spreading of malware. Moreover, hacked sites, more often than not, come with a payload that either leads to malwartized content or drive by downloads.

The following research is based on analysis of threats found in the last 6 months. The figures shown is a basic study of malware hosting web sites that focus on stealing everything from credit card information to an individual's identity to banking credentials to spreading malware via links or even social networking sites.

The figures clearly show that 29% (22,040) of malwartized links are hosted in the US followed by Latvia, China and Germany at 20% (15,608), 11% (8,249)

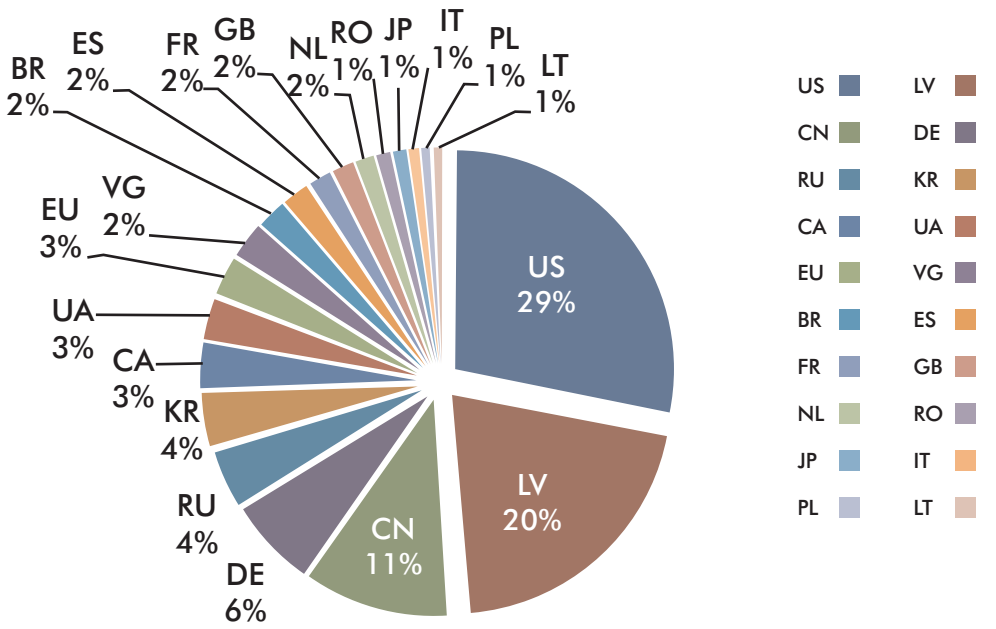
and 6% (4,919) respectively. However, it would be good to know that many of these malwartized servers or links are compromised by hackers and then are cooked up to serve malware.

The main reason for the US to lead the race is mainly due to its rich infrastructure. Not only are they great in number but can also be easily be compromised by an experienced hacker. And with the average hackers techniques multiplying by the day, it becomes almost impossible for the average user to be able to detect a flawed or compromised website.

To eliminate over-inflated numbers we have not considered malware that come with the same virus string. Therefore, the overall percentage or count might seem less than expected.

All figures are approximate values.

Malware URL Count (Hosted Countries)

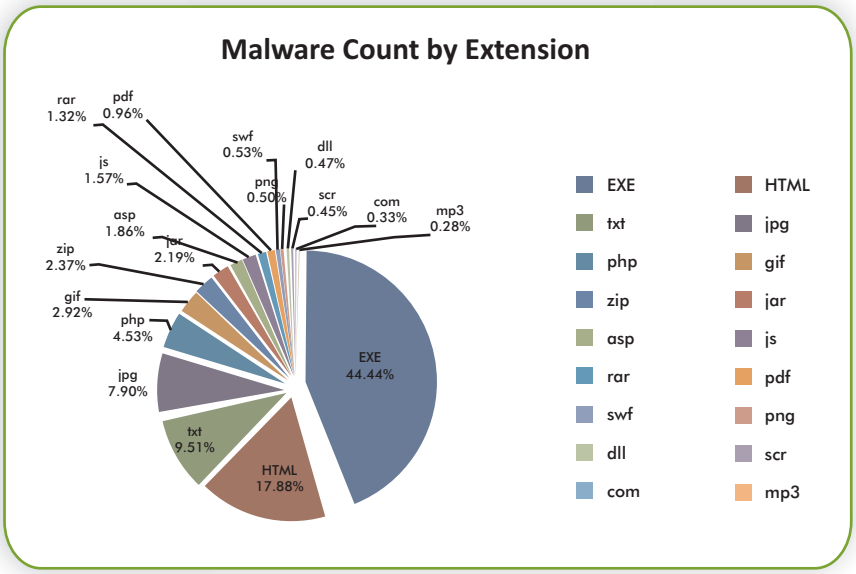


Malware Count by Extension

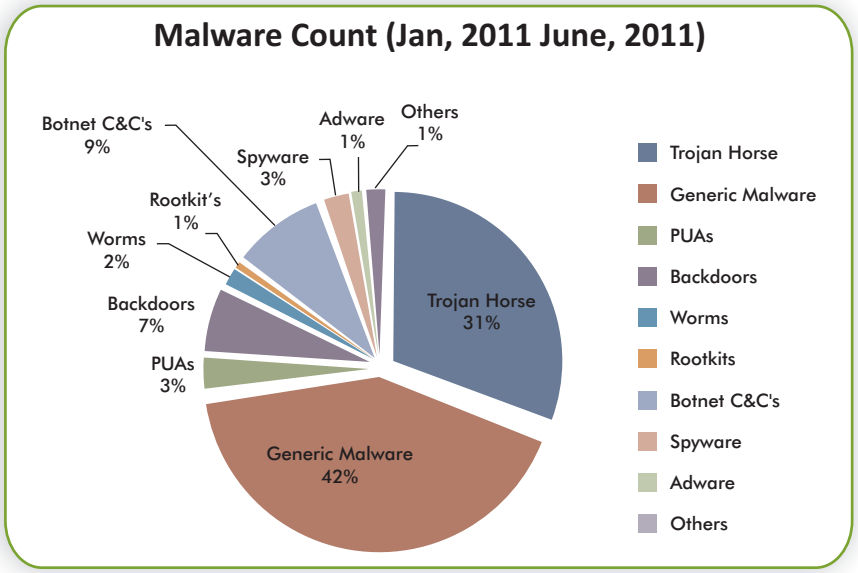
In the last few years the security industry has seen a number of changes in the way malware is coded. Malware writers have become more complex and have developed a sense of maturity as far as malware coding is concerned. For instance, Stuxnet was the first complex malware that went on to infect and sabotage industrial systems in Iran. That, followed by the virtually indestructable TDL-4 goes on to prove their overall efficacy. However, the programming skills they are acquiring over time is not the only worrying factor. Their overall proficiency in English have also risen dramatically so-much-so that the content generated can also fool a well trained eye. So what do hackers gain out of this? The ability to convince the user of the authenticity of the content is what they gain.

For instance, Facebook has been the most widely used social networking platform to spread malware. Click-

jacking, drive-by-downloads, are a mentioned few that are used to compromise the users machine. The latest discovery of a new breed of Fake AV clearly shows the complexity used to convince unsuspecting users. Targeted specifically at Facebook users, this new Trojan comes in as a YouTube video



wrapped with multiple fake comments from your Facebook friends. The speciality of this Trojan lies in its ability to copy the look and feel of 16 different security solutions currently on the market. Having said that, the Fake AV acts as both a



downloader and a bot that help it in spreading. The current scenario itself says a lot about the progress of malware writers and we won't be seeing a decrease in trend anytime soon.

In addition, there has also been a sudden jump in the number of hijacked links that are hosted by legitimate websites. There has also been an increase in the number of phishing sites that have mostly been found to be targetted at banks and other payment gateways. The increase is proportional to the number of smartphones and tablets being made available. Moreover with smartphones surpassing PC sales it is inevitable not to see a rise in attacks that are based on phishing and Cross Site Scripting.

March 21st 2011, saw the demise of probably the worlds largest botnet – "Rustock". With a rough estimation of over a billion infected computers capable of mailing billions of spam related mails a day, Rustock was responsible for whopping 80% (peak) of junk email worldwide. The whole process of taking this bot down was made easier mainly due to technical details learned when tackling the Waledac bot. However, a slightly different approach was required as Rustock didn't just use DNS to identify control servers, it in-fact relied on a list of hard-coded IP addresses to fall back on. Therefore, to effectively cut off all links from control servers, all aspects (P2P networks, HTTP-based control systems, DNS and IP addresses) needed to be taken down at the same time. Any delay caused would open the possibility of creation of new domain names or IP addresses, nullifying the whole process.

In addition, the takedown of major Command & Control centers will definitely hinder but not stop the increase in the number of zombie PCs. The count appended to the text files not only signifies the number of active Command and Control centers but they are also a summation of the number of updates that are received by various bots and malware.

Malware Count (Month Wise)

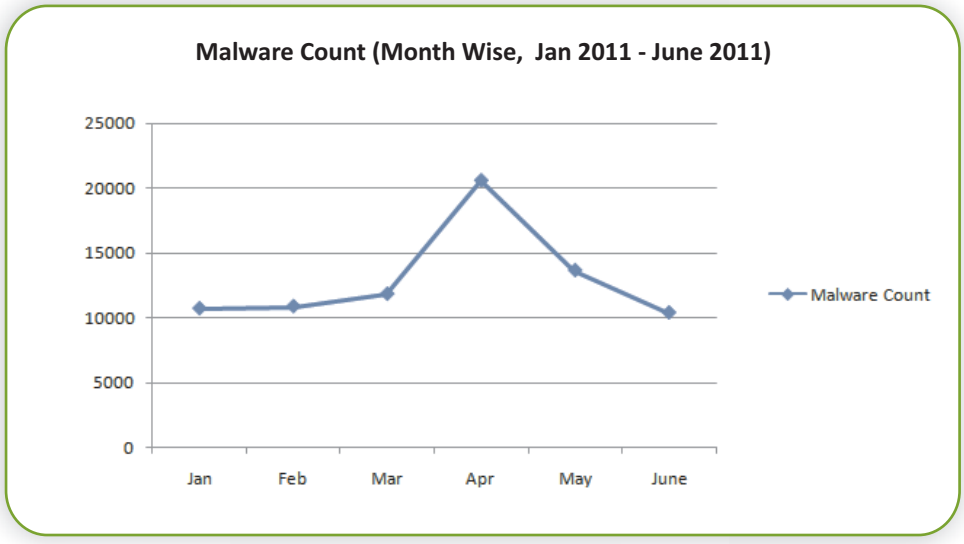
It goes without saying that 2011 will see a rise in the overall sophistication and volume of malicious activity. As seen earlier, Stuxnet was the first piece of code to have used multiple exploits along with the ability to hinder the functionality of physical devices. However the regularity of creating such malware is higly unlikely mainly because of the immense amount of resources it requires. The very aspect of its complexity states that organized crime will definitely see a rise. 2011 will also see a shift in the tactics used to lure unsuspecting web users into providing personal information. Fake AVs will rise in number, as we are slowly witnessing a change in the way they are being presented. In fact they have given a whole new dimension to Fake Antiviruses. The overall effectiveness of the recently detected 'Trojan.FakeAV.LVT' doesn't only lie in its ability to evade most security suites but its ability to be identically similar to previously installed security suite is an aspect that is totally new.

Having said that, 2011 will see a significant rise in attacks. They are as follows.

Targetted Attacks: Stuxnet was definitely an eye-opener as far as targeted attaks were concerned. While the use of vulnerabilities play a big role in gaining access to information, it is the ability to exploit the trust of users that give it a much bigger role in siphoning critical information.

Social Networking: Whatever be the medium, Social Networks are slowly becoming a playground for hackers. Social networks have in-fact made it easy for hackers to learn of our interests, gain our trust and masquerade as friends. The days of unusual and strange email addresses are slowly dying out along with the use of bad grammar. It's no more about pride within the hacking community but it all lies in the ability to gain access to information. Moreover, the hacking communiy has made progress such that – spotting a social engineering attack is becoming close to impossible.

Zero-Day Vulnerabilities & Rootkits: Making use of zero-day vulnerabilities is one of the key concepts in avoiding detection. They are specifically designed to exploit computer application vulnerabilities that are unknown to the developer. A good example of this would be that of the Stuxnet worm that was built mainly to sabotage Iranian nuclear facilities. Rootkits on the other hand are deployed either by exploiting a known vulnerability or through social engineering. For instance, the rootkit implemented by TDL4 allowed it to conseal itself from most security products while it also had the ability to remove most other bots and malware written programs. To go undetected and to be able to self-launch itself, the program infects the MBR – ensuring a safe run of the



malicious code prior to the launch of the operating system. With both sides being equally innovative, attacks such as these will certainly be good examples to learn from. However, their techniques will definitely be copied and altered for massive attacks.

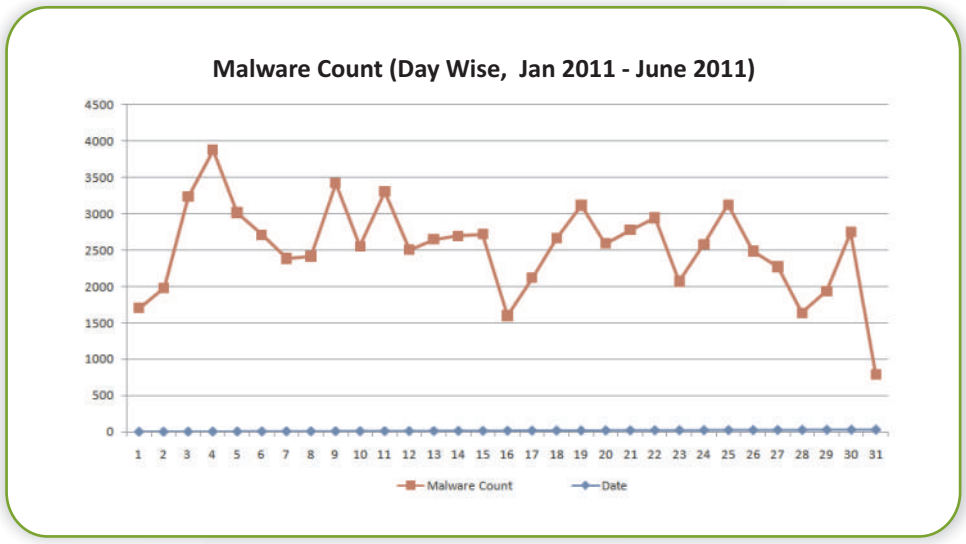
Portable Document Format: PDFs are one of the most commonly used file formats that are used across various platforms. It is their overall popularity that makes them the most used in terms of malware attack. Statistically speaking, compromised PDFs account for at least 68% of all exploits.

Attack Kits: The main reason for mass distribution of these threats are due to attack kits. This further helps distributing zero-day vulnerabilities into regularly implemented vulnerabilities. Inevitably such vulnerabilities find their way into such attack kits which are sold in the underground community.

Malware Count from Jan '11 – Jun '11 (Day Wise)

The first half of 2011 has been quite a show in terms of malware productivity. With an average detection rate of approximately 4000 uncategorized malware per day, 2011 has definitely been the most active in the history of malware. The following report reveals the significant impact that malware has had in the last six months. The first week shows a relative increase in the number of spams that were sent out. However, the graph is not limited to spam but also includes a significant number of malware on a daily basis spread across the first six months. Having said that, the takedown of the Rustock botnet resulted in the fall of many command and control centers which caused spam to drop drastically. However, the gap was soon filled up by other botnets which would include Maazben, Bobaz, Lethic, Cutwail and Grum.

Having said that, the merging of the Zeus source code with the SpyEye botnet brought in a new breed of threats that effected most banking and online transactions. It has also been detected that the SpyEye botnet is capable of thriving on over 150 modules – such as USB drives, Instant Messengers and various other browser certificates.



Domain Wise Malware Hosting

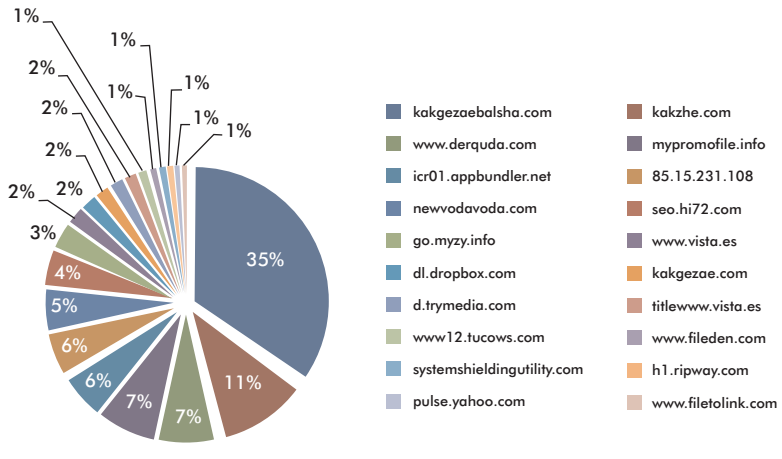
We all love downloading content – be it media players, songs, or even applications. However, most of us download content from sites we don't even recognise. So what is the chance of us downloading infected content? Almost 80%, of content available on the web is malicious. In fact SEO poisoning has risen to such an extent that the chances of clicking an infected link has significantly risen in the last year.

In lieu to the above statement, the takedown of the rustock botnet saw a major decrease in the number of spams sent out per day. With an average of approximately 53 billion spams per day, rustock was probably the deadliest of the bots around. So much so that the overall spam count dropped to 30 billion. 44% decrease is a significant drop as far as spam is concerned.
However, to be able to register domains cyber crooks are pretty smart in getting what they need. Here is what they look out for, however not limited to:
Low prices
Ease of registration
Lack of regularizing policies
Fewer the number of questions asked the better

However, it isn't necessary for malware to spread directly via malware hosting domains. A malware infection could either happen via a compromised link/webpage or using a drive by download technique – all pointing to the infected domains. Cross site scripting is a well known technique that allow hackers to bypass client-side security mechanisms normally enforced on web content by modern day browsers. A successful hack can allow attackers gain access to content, session cookies along with a handful of other information which most browsers maintain on behalf of the user.

Social networks will continue to be a security concern for organizations. While social networks are observed as a great tool towards marketing ones product, the dangers posed by the overall exposure of sensitive and exploitable information is quite high. With that said, malicious code that uses social networking sites to spread remains considerably high. The information used is then used by attackers to exploit profile information to mount targeted attacks. While it might seem safe to divulge such information it provides the hacker to create a convincing scam to dupe the victim. This might come in the form of an email message from a co-worker containing links pointing to pictures from a recent vacation. That along with a clever subject line, makes the malware surprisingly difficult for people to resist. While adjusting the privacy settings can reduce the the probability of a profile from being spoofed, the user still stands a chance of being exploited via a compromised friend. In addition, there have been steady increase in the use of shortened URLs as the destination always remains hidden from the user. Also, of all links posted within social networks nearly 75% of them are reported as malicious.

Domain Wise malware Hosting (Jan 2011 - June 2011)



Disclaimer

The above report is based on malware URL collected between 1st January 2011 & 31st June 2011 and is a representation of the growth in malware infected URLs in the span of 6 months. The domains mentioned were found infected at the time of report creation. However, the domain/site/URL might be safe now as the infection may have been removed by the host. MicroWorld Technologies Inc. is not liable to any party for any direct, indirect, special or other consequential damages caused.

Our Offices

USA:
MicroWorld Technologies Inc.
31700 W 13 Mile Rd, Ste 98
Farmington Hills, MI 48334,
USA.

Tel: +1 248 855 2020/2021
Fax: +1 248 855 2024.
TOLL FREE: 1-877-EZ-VIRUS
(USA Only)

E-mail: sales@escanav.com
Web site: www.escanav.com

India:
MicroWorld Software Services Pvt. Ltd.
Plot No.80, Road No.15, MIDC,
Marol, Andheri (E),
Mumbai- 400 093, India.

Tel: +91 22 2826 5701
Fax: +91 22 2830 4750

E-mail: sales@escanav.com
Web site: www.escanav.com

Germany:
MicroWorld Technologies GmbH
Drosselweg 1,
76327 Pfinztal,
Germany.

Tel: +49 72 40 94 49 0920
Fax: +49 72 40 94 49 0992

E-mail: sales@escanav.de
Web site: www.escanav.de

Malaysia:
MicroWorld Technologies Sdn Bhd.
(722338-A)
E-8-6, Megan Avenue 1,
189, Jalan Tun Razak,
50400 Kuala Lumpur, Malaysia.

Tel: +603 2333 8909 / 8910
Fax: +603 2333 8911

E-mail: sales@escanav.com
Web site: www.escanav.com

South Africa:
MicroWorld Technologies South
Africa (Pty) Ltd.
376 Oak Avenue, Block C
(Entrance at 372 Oak Avenue),
Ferndale, Randburg, Gauteng,
South Africa.

Tel: Local 08610 eScan (37226)
International: +27 11 781 4235
Fax: +086 502 0482

E-mail: sales@escan.co.za
Web site: www.escan.co.za