



CERT-In Monthly Security Bulletin December 2007

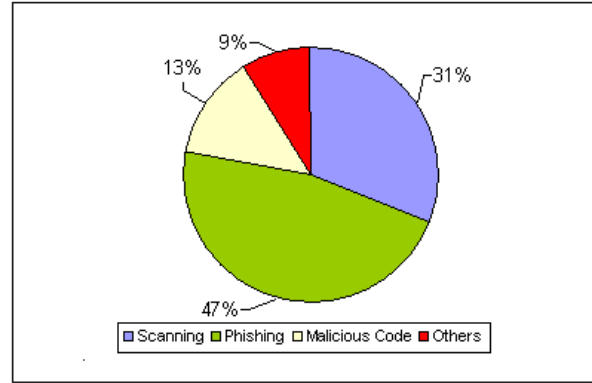
Cyber Intrusion Trends

In this month 45 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 47% phishing incidents were reported in this month. 31% unauthorized scanning, 13% incidents related to virus/worm under the Malicious code category and 9 % incidents related to technical help under the Others category were reported in this month. As compared to previous month the number of phishing and scanning incidents have decreased while incidents related to technical help under the Others category have increased.

In this month CERT-In tracked 2 C&C (Command & Control) servers and 1020 bot-infected computers existing in India. The concerned ISPs were intimated to dis-infect the bot infected systems and C&C servers to mitigate botnets.

It has been observed that new variants of 'Storm Worm' were circulating via e-mails purporting to be [Christmas Greetings](#) and [Happy New Year e-mail Greetings](#).

Cyber Intrusion during December 2007



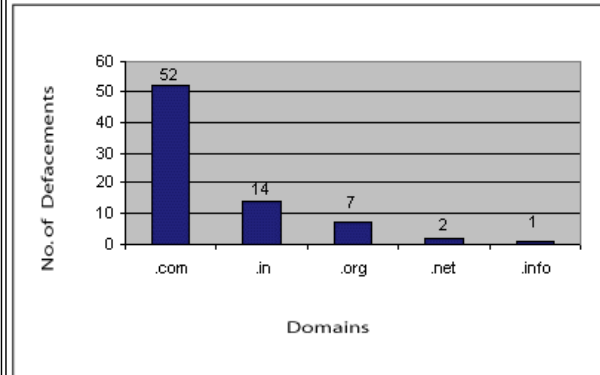
Indian Websites Defacement

In total 76 Indian websites were defaced during december 2007. A chart depicting Top Level Domain(TLD) wise defacements is shown in the figure.

The vulnerabilities which might have been exploited for the defacements are:

1. Cross Site Scripting Vulnerability in Apache mod_imap Module [CIVN-2007-163](#)

Statistics of Defaced Indian Websites in December 2007

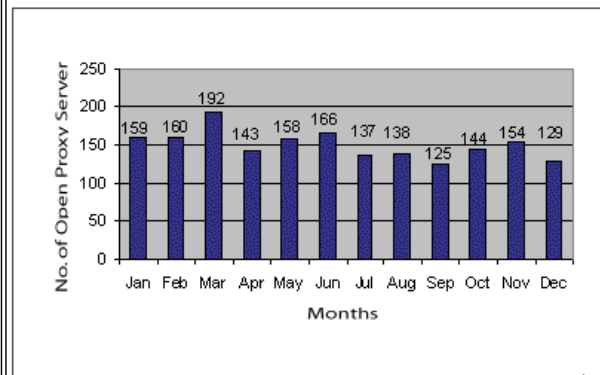


Open proxy servers

Any proxy server that doesn't restrict its client base to its own set of clients and allows any other client to connect to it, is known as an open proxy server. An open proxy server will accept client connections from any IP address and make connections to any Internet resource.

CERT-In tracked 46 open proxy servers functioning in India during December 2007. All the concerned ISPs were alerted immediately to shut down the open proxy servers. A bar chart of open proxy servers tracked during this year is shown in the figure.

Statistics of Open Proxy Servers tracked during Jan - Dec 2007



Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during December 2007 and their countermeasures alongwith wide-spreading malicious code like virus/ worm/Trojan are given below:

High Vulnerabilities

Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
	Multiple Vulnerabilities in various components of Microsoft		

Microsoft Windows	Products: Microsoft Windows Vista, Microsoft Windows 2000 Server, Internet Explorer , Microsoft Windows SMBv2 Code Signing, Microsoft DirectX, Microsoft Windows Macrovision SafeDisc secdrv.sys driver, Microsoft Windows Media File Format	December 12,2007	CIAD-2007-65		
Microsoft DirectX SAMI/WAV/AVI File	Microsoft DirectX SAMI/WAV/AVI File Parsing Vulnerabilities	December 12,2007	CIVN-2007-152		
Microsoft Windows	Message Queuing Service Remote Code Execution Vulnerability	December 12,2007	CIVN-2007-153		
Microsoft Windows	Microsoft Windows Media File Format Remote Code Execution vulnerability	December 12,2007	CIVN-2007-156		
Internet Explorer	Internet Explorer Multiple Code Execution Vulnerabilities	December 12,2007	CIVN-2007-157		
Microsoft Jet Database Engine	Microsoft Jet Database Engine MDB File Parsing Remote Buffer Overflow Vulnerability	December 19,2007	CIVN-2007-159		
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
MIT - Kerberos 5	Multiple Vulnerabilities in Kerberos	December 05,2007	CVE-2007-5894,CVE-2007-5901,CVE-2007-5902, CVE-2007-5971,CVE-2007-5972		
Wireshark	Multiple Vulnerabilities in Wireshark	December 19,2007	CVE-2007-6439,CVE-2007-6441,CVE-2007-6444, CVE-2007-6445,CVE-2007-6447,CVE-2007-6448,CVE-2007-6450,CVE-2007-6451,CVE-2007-6438,CVE-2007-6440,CVE-2007-6442,CVE-2007-6443,CVE-2007-6446		
Opera Browser	Multiple Vulnerabilities in Opera Browser	December 28, 2007	CIAD-2007-66		
Database	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Oracle Database	Oracle Database Server Installation Security Bypass Vulnerability	December 14, 2007	CIVN-2007-158		
Cisco	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Cisco	Cisco Security Agent for Windows System Driver Remote Buffer Overflow Vulnerability	December 07 , 2007	CIVN-2007-148		
Cisco	CiscoWorks Server XSS Vulnerability	December 11 , 2007	CIVN-2007-149		
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Adobe Flash Player	Adobe Flash Player Cross-Site Scripting Vulnerability	December 26 , 2007	CIVN-2007-162		
Medium Vulnerabilities					
Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Microsoft Web Proxy Auto-Discovery (WPAD)	Information Disclosure Vulnerability in Microsoft Web Proxy Auto-Discovery (WPAD)	December 05,2007	CIVN-2007-147		
Microsoft Windows Media Player	Microsoft Windows Media Player 11 AIFF Parsing Divide-By-Zero Denial of service Vulnerability	December 12,2007	CIVN-2007-150		
Microsoft Windows SMBv2	Remote Code Execution Vulnerability in Microsoft Windows SMBv2 Code Signing	December 12,2007	CIVN-2007-151		
Microsoft Windows	Local Privilege Escalation Vulnerability in Microsoft Windows Vista Kernel ALPC	December 12,2007	CIVN-2007-154		
Microsoft Windows	Microsoft Windows Macrovision SafeDisc secdrv.sys driver Local Elevation of Privilege vulnerability	December 12,2007	CIVN-2007-155		
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
OpenOffice	HSQldb Database Engine Code Execution Vulnerability in OpenOffice	December 19 , 2007	CIVN-2007-160		
Samba	"send_mailslot()" Buffer Overflow Vulnerability in Samba	December 19 , 2007	CIVN-2007-161		
Apache	Cross Site Scripting Vulnerability in Apache mod_imap Module	December 26, 2007	CIVN-2007-163		
Malicious Code Threats					
Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References

BZub Trojan	Trojan	This trojan has the logging routine on the infected system to capture keystrokes made by the user visiting respective online banking websites.	Trojan-Spy:W32/BZub [F-Secure], Spy-Agent.ba [McAfee]	December 13 , 2007	http://www.cert-in.org.in/virus/BZub-Trojan.htm
JS_ORKUT.A	JavaScript	This malicious JavaScript spreads via the popular social networking site <i>Orkut</i> . It searches for target recipients in a compromised <i>Orkut</i> account. It then sends a scrap object to its target recipients.	No Alias	December 19 , 2007	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=JS%5FORKUT%2EA&Vsect=P
EXPL_REALPLAY.H	Exploit	This exploit code is hosted on a Web site and runs when a user accesses the said Web site. It takes advantage of a known vulnerability in several versions of the media player <i>RealPlayer</i> described in CVE-2007-5601	No Alias	December 20 , 2007	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=EXPL%5FREALPLAY%2EH
Storm Worm Variants	Trojan/Bot Virus	New variants of 'Storm Worm' are circulating via e-mails purporting to be Happy New Year e-mail Greetings.	TROJ_SMALL.EDW [Trend Micro], Trojan.Peacomm [Symantec]	December 26 , 2007	http://www.cert-in.org.in/currentacts/currentact07.htm#SWHNY
JS_AGENT.AEVE	JavaScript	This malicious JavaScript may be downloaded unknowingly by a user when visiting compromised Web pages that have a certain IFrame tag.	No Alias	December 27 , 2007	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=JS%5FAGENT%2EAEVE&Vsect=P

Security News

MALWARE DOUBLED IN 2007; NEXT YEAR ISN'T LOOKING BETTER

[Source: www.informationweek.com]

December 05, 2007

At the start of 2007, computer security firm F-Secure had about 250,000 malware signatures in its database, the result of almost 20 years of antivirus research. Now, near the end of 2007, the company has about 500,000 malware signatures. "We added as many detections this year as for the previous 20 years combined," said Patrik Runald, security response manager at F-Secure. F-Secure's report on 2007 threats isn't a pretty picture. Beyond the explosive growth of malware, the year also saw the emergence of the Storm worm, a catch-all term for a series of related backdoor Trojans and e-mail worms that have been distributed to create a massive peer-to-peer botnet. Shortly, F-secure expects the gang behind the Storm worm to open its botnet for business, renting access to other cyber criminals.

[\[More\]](#)

2007: A YEAR OF SOPHISTICATED WEB THREATS

[Source: www.computerweekly.com]

December 10, 2007

This year has seen even more sophisticated and targeted web attacks come of age, says the MessageLabs Intelligence 2007 Annual Security Report. The web security firm says 2007 has been a year of diversity, because of the vast number of new tactics, techniques and trojans entering the security market during the last 12 months. Spam retains the title of "dominant menace" with annual spam levels reaching 84.6% of messages sent. But rather than just playing the volume game, the spammers also introduced an additional 10% of new and previously unknown spam attacks from 2006. The notorious Storm botnet, which appeared early in 2007, is likely to take some credit for the increased innovation, said MessageLabs, especially through its distribution of 15 million e-mails, with MP3 attachments, new to the market in October.

[More]

THEFT OF PERSONAL DATA IN '07 GROWS MORE THAN 3 TIMES 3 Dec 07

[Source: www.hartfordbusiness.com]

December 03, 2007

More than 162 million personal records have been reported lost or stolen in 2007; triple the 49.7 million that went missing in 2006, according to USA Today's analysis of data losses reported over the past two years. This year, news stories have been written about data losses disclosed by 98 companies, 85 schools, 80 government agencies, and 39 hospitals and clinics, according to a database at tech security web site Attrition.org; arrests or prosecutions have been reported in just 19 cases. Names, birth dates, account numbers, and Social Security numbers have increased in value in the cyber crime underground. Meanwhile, organizations expose rich veins of such data as they convert paper documents into digital records. Business data worldwide are expected to swell to 988 billion gigabytes by 2010, up from 161 billion gigabytes in 2006, says researcher IDC. As they "cram more and more data into a single place," companies and agencies present thieves with more opportunities for a big score, says the vice president of technology at Cryptography Research.

[More]

Top-secret US labs penetrated by phishers

[Source: www.channelregister.co.uk]

December 12, 2007

One of the most sensitive science and technology labs in the US has been hacked as part of what it called "a sophisticated cyber attack that now appears to be part of a coordinated attempt to gain access to computer networks at numerous laboratories and other institutions across the country." The unknown attackers managed to access a non-classified computer maintained by the Oak Ridge National Laboratory by sending employees hoax emails that contained malicious attachments. That allowed them to access a database containing the personal information of people who visited the lab over a 14-year period starting in 1990. The institution, which has a staff of about 3,800, conducts top-secret research that is used for homeland security and military purposes. "At this point we have determined that the thieves made approximately 1,100 attempts to steal data with a very sophisticated strategy that involved sending staff a total of seven 'phishing' emails, all of which at first glance appeared legitimate," Thom Mason, the lab's director, wrote in an email sent to employees on Monday. "At present we believe that about 11 staff opened the attachments, which enabled the hackers to infiltrate the system and remove data."

[More]

DNS Attack Could Signal Phishing 2.0

[Source: www.pcvorld.com]

December 11, 2007

Researchers uncovered an attack targeting 'open-recursive' DNS servers that controls where phishing victims go on the Internet. Researchers at Google and the Georgia Institute of Technology are studying a virtually undetectable form of attack that quietly controls where victims go on the Internet. The study, set to be published in February, takes a close look at "open recursive" DNS servers, which are used to tell computers how to find each other on the Internet by translating domain names like google.com into numerical Internet Protocol addresses. Criminals are using these servers in combination with new attack techniques to develop a new generation of phishing attacks. The researchers estimate that there are 17 million open-recursive DNS servers on the Internet, the vast majority of which give accurate information. Unlike other DNS servers, open-recursive systems will answer all DNS lookup requests from any computer on the Internet, a feature that makes them particularly useful for hackers.

[More]

Shorter URLs help phishers hook more victims

[Source: www.news.com]

December 03, 2007

Phishers are using shorter URLs for malicious sites in a bid to lend an air of legitimacy to threatening links. Internet Security Services, IBM's online-security division, claims to have noticed a significant drop in the number of characters used by fraudsters in their phishing URLs. A post on ISS's Frequency X blog stated that "analysts have been observing host names within fraudulent phishing URLs consistently arrive with lengths of between 30 and 37 characters"; observers "have noted a significant change" as phishing host names have shrunk down to an average of only 17 characters in recent weeks. Ralf Iffert, researcher for ISS's X-Force threat analysis team and author of the Frequency X blog, believes this is another step in the increasingly sophisticated social-engineering measures adopted by cybercriminals. Phishers "appear to have adopted shorter URLs to avoid the suspicion of their potential victims," he said. Steve Reddock, senior IT specialist for ISS, believes that this is a developing trend. "This is a pattern we've noticed over several months; it's not just a blip."

[More]

Hackers and zombies

[Source: www.crime-research.org]

December 13, 2007

While doing research on a suspicious neighbor, Ben Sayre went to a website that seemed fishy and later noticed extra buttons showing up on his computer screen. Sayre, a UW-Madison journalism graduate student and victim of a computer virus, said he doesn't do much to protect his computer from future viruses and other malware, or software used for malicious attacks and intrusions. "I worry about it a little, but I feel I can just reinstall the OS [operating system] if it actually makes it hard to use my computer," Sayre said. The downsides to not protecting your computer can reach far beyond the annoyance of reinstalling an operating system, however: unprotected computers leave

themselves vulnerable to botnets, or "robot networks."Using a botnet, a hacker or spammer can remotely control a "zombie army" of computers, according to the government computer-protection website OnGuard Online, and the owners might not even realize their computers have been compromised.

[More]

Peer-to-peer botnets pose fresh network threat

[Source: www.computerweekly.com]

December 13, 2007

Businesses, governments and internet service providers face dangerous new network disruption and malware attacks from botnets based on peer-to-peer technology (P2P) instead of the more common hierarchical structure. Eugene Kaspersky, CEO of Kaspersky Laboratories, the Russian antivirus company that identified the new method, said the new method had already succeeded in strangling internet communications in Krasnodar and Astrakhan for several weeks. "We do not know who was behind these attacks," he said. "It may have been a test." Alex Gostev, senior virus analyst at Kaspersky, said the P2P nature of the new botnet meant that each infected machine needed to know only its neighbours. An instruction to activate the botnet could be sent to any of the machines in the network which would then propagate from machine to machine to build an attack.

[More]

New Year's Eve greetings disguise Storm Worm attacks

[Source: www.theregister.co.uk]

December 27, 2007

The Storm Worm gang are spreading seasonal ill-will. Security watchers have spotted New Year greeting spam runs that attempt to direct recipients to a malicious web site called uhavepostcard.com. Anti-virus firm F-Secure warns that although the site remains free of exploits (for now) the spam run is likely to be a prelude for a New Year's Eve-themed Storm Worm attack. Malware miscreants are making early preparations for the New Year after they left it too late for Christmas, only striking on Christmas Eve. A widely-circulated email first distributed on December 24 pointed to a website containing a malicious Santa Claus-themed striptease. The emails, which have varied subject lines including "Your Secret Santa", "Santa Said, HO HO HO", "Warm Up this Christmas" and "Mrs. Clause Is Out Tonight!" attempt to entice prospective marks into visiting a website containing images of scantily clad young women in a Santa suits. The images and "Download for free now!" button both linked to a variant of the Storm Worm, anti-virus firm Sophos reports.

[More]

Worm Hits Google's Orkut

[Source: www.pcworld.com]

December 19, 2007

Google's Orkut social networking site appeared to have been hit by a relatively harmless worm, but one that demonstrated the continuing vulnerability of Web applications. Some Orkut users received an e-mail telling them they had been sent a new scrapbook entry -- a type of Orkut message -- on their profile from another Orkut user. They only had to view their profile to become infected by the worm, which added them to an Orkut group, "Infectados pelo Virus do Orkut," wrote the blogger Kee Hinckley on his site TechnoSocial. The name of the group, in Portuguese, roughly translates to "infected by the Orkut virus." Orkut is popular in Brazil, as well as India, but has not caught on as well outside those countries compared to MySpace and Facebook.

[More]

Serious Flash vulns menace at least 10,000 websites

[Source: www.theregister.co.uk]

December 21, 2007

Researchers from Google and a well-known security firm have documented serious vulnerabilities in Adobe Flash content which leave tens of thousands of websites susceptible to attacks that steal the personal details of visitors. The security bugs reside in Flash applets, the ubiquitous building blocks for movies and graphics that animate sites across the web. Also known as SWF files, they are vulnerable to attacks in which malicious strings are injected into the legitimate code through a technique known as cross-site scripting, or XSS. Currently there are no patches for the vulnerabilities, which are found in sites operated by financial institutions, government agencies and other organizations. The vulnerabilities are laid out in the book Hacking Exposed Web 2.0: Web 2.0 Security Secrets and Solutions. It is due to hit store shelves soon, but is already in the hands of many security professionals. The book's authors, who work for penetration testing firm ISEC Partners as well as for Google, say a web search reveals more than 500,000 vulnerable applets on major corporate, government and media sites.

[More]

Cyber crime: Two youths arrested in Rajasthan

[Source: www.crime-research.org]

December 30, 2007

Two youths allegedly involved in withdrawing and transferring money over the Internet were today arrested by police in Ajmer. The Special Task Force of UP police along with Special Operation Group here arrested Abdul Kadir (22) and Abdul Qadir (23), who were wanted in several cases of cyber frauds, Superintendent of Police (SOG) A Punoohammy said. Asked if the youths had any hand in the November UP blasts or any other terrorist incidents, he said, "I don't know much about it. As far as we are concerned STF had sought our assistance and we gave them."

[More]

Ad hijacking Trojan targets Google

[Source: www.theregister.co.uk]

December 21, 2007

Security researchers have identified a Trojan that hijacks Google text advertisements, replacing them with "ads" from a different provider that are likely to be laced with spyware. The Qhost-WU modifies an infected computer's hosts file, thereby poisoning systems with bogus DNS lookup records. The hosts file matches

domain names of websites with corresponding IP addresses. By corrupting the file hackers can redirect surfers to domains controlled by hackers even when users visit a trusted location. In this case, the modified file contains a line redirecting the host "page2.google syndication.com" from a server run by Google to an imposter, potentially depriving web masters of revenue while leaving infected punters in a pickle.

[\[More\]](#)

Gmail exploit aids domain hijack

[\[Source: www.theregister.co.uk\]](http://www.theregister.co.uk)

December 28, 2007

Web designer David Airey has succeeded in recovering his domain after hackers exploited flaws in Gmail to trick his hosts into authorising a fraudulent transfer. Airey's woes began when he took his girlfriend for a month-long holiday to India on 21 November, a trip he mentioned in his blog. The holiday was a break from work and he only occasionally checked his emails. All seemed well until shortly before his return when Airey received an email from a friend informing him that his website, Davidairey.com, had "disappeared". At first Airey thought he'd made a mistake and allowed his domain name to expire and a domain poacher had snapped it up before he got the chance to renew it. Subsequent digging revealed a darker truth: hackers had posted a bogus transfer request on his web host support panel the day Airey left for India.

This, alongside an attack on a Gmail account run by Airey, allowed them to seize his domain and hold it for ransom. Initially crooks demanded \$650 before dropping their offer down to \$250.

[\[More\]](#)

ID sales sites start loss leader marketing programme

[\[Source: www.theregister.co.uk\]](http://www.theregister.co.uk)

December 03, 2007

The Information Commissioners' in-tray got a little bigger today as it confirmed it would be investigating a series of ID trading sites unearthed by journalists. The Times screamed today that "the financial details of tens of thousands of Britons" were being sold on the internet. The paper detailed how it had been able to download banking information for 32 people, including account numbers, PINS, and security codes, "without spending a single penny". The data, including that of a deputy judge, was apparently offered as a free taster by the ID traders. It's no secret that personal details are being traded online, although the fact that criminals are now offering free samples is a new wrinkle. A spokeswoman for the Information Commissioner's Office (ICO) confirmed the paper had passed on the details of its investigation, and said: "We'll be looking at the evidence." She pointed out the ICO had previously called for custodial sentences for criminal trading of details. Given the ICO's remit, the organisation's interest would presumably be in how the data escaped into the wild in the first place.

[\[More\]](#)

Cybercrooks lurk in shadows of big-name websites

[\[Source: www.theregister.co.uk\]](http://www.theregister.co.uk)

December 12, 2007

A small team of security researchers has documented how many high-profile websites are unwittingly helping phishing fraudsters. Phishing scams often use "open redirector" exploits on major sites to make their attack URL look more legitimate. The trick also makes it more likely that fraudulent emails that form the basis of phishing attacks will slip past spam filters. Typically, security flaws on exploited high-profile sites allow a phisher to provide a link which appears to be a legitimate URL, but actually redirects to a fraudulent site. Previous Register stories have covered examples of the ruse practiced on websites including Barclays Bank (story here), eBay (here), and others.

To date, most of the information about the topic has been anecdotal. SiteTruth aims to shed light on the scope of the problem by collecting hard numbers as part a project that ultimately aims to provide a search engine that will allow clued-up surfers to check on the legitimacy of sites. SiteTruth's search service isn't limited to sites that have paid a fee. Nor is it selling "seals of approval".

[\[More\]](#)

Dutch arrest 14 mules in ABN AMRO scam

[\[Source: www.channelregister.co.uk\]](http://www.channelregister.co.uk)

December 12, 2007

Dutch police have arrested 14 suspects who allegedly lent their bank accounts at ABN Amro to cybercriminals in Russia and Ukraine. After being recruited by the fraudsters, the mules received funds taken from phishing scams, which they transferred overseas. The twelve men and two women were bailed today. Customers of ABN Amro were lured to bogus websites in Hong Kong which were set up to gather security details. Money stolen from their accounts was then transferred to Russia and other countries. The collaborators were generously remunerated, the Prosecutor's Office said today.

The cybercriminals often used IP addresses through Russian Business Network based in St Petersburg, an ISP notorious for hosting illegal and dubious businesses, including child pornography, phishing and malware distribution sites.

[\[More\]](#)