

# Information Warfare Center's Cyber Intelligence Report (CIR)

Author: Jeremy Martin, CISSP-ISSMP/ISSAP, CISM, CEH/LPT/CHFI, CREA/CEPT/CSSA/CCFE

[www.informationwarfarecenter.com](http://www.informationwarfarecenter.com)

**October 10, 2012**

The IWC CIR is a weekly OSINT resource focusing on advanced persistent threats and other digital dangers. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage.

## Top News

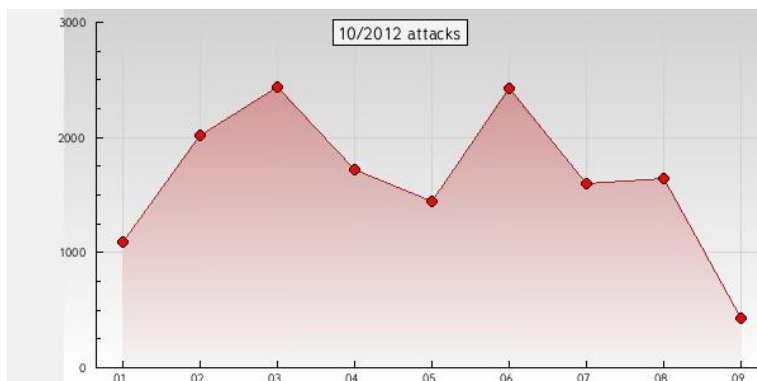
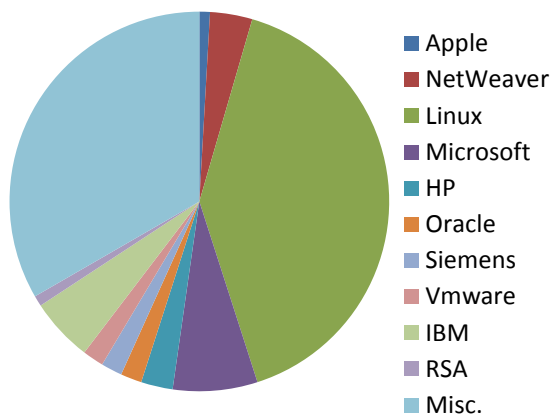
State sponsored attacks are not just non-kinetic perpetrated by employees of a country. If "cybercrime" consistently occurs with traffic or product outside of the country and the government actively knows about said activity, they are passively sponsoring the actions of the bad guys. Well, the Chinese Nitel Botnet has been propagated by corrupt Chinese resellers to help create one of history's largest zombie network. This should come as no surprise to anyone who has seen the counterfeit products and information leakage when dealing with foreign countries, especially China. State sponsored doesn't have to be funded by a government if the said government doesn't lift a finger to stop the cyber-attacks.

Now we have technology companies such as Huawei trying to get a foothold into countries including America. There are several recent "instances" of information leakage that are now being claimed by the company and even the U.S. government is not telling the technology sector that this may not be the best choice for company cyber security or national security. The UK has already started to learn this lesson AFTER allowing Huawei into the infrastructure and now they have the additional expense to secure data after the fact.

In 2010, 6 out of the top 7 Industrial Espionage cases, costing the United States hundreds of billions of dollars in damages, were found that either the Chinese government or Chinese industry was directly responsible for the loses. This doesn't even include the massive and well known Intellectual Property (IP) piracy/theft that occurs on a daily basis. Feds are even warning about dangerous Chinese counterfeit airbags (that can easily kill the driver) that have been installed in thousands of U.S. cars. Needless to say, any country that competes is a threat. The companies that reside in that country will have at least some sort of influence pushed on them. Be it full blown government involvement or the regulations (or lack thereof) on how they can do business and "secure" information and ideas.

| Section             | Page | #   | Country       | Gov't Defaced sites | OS defaced | #   |
|---------------------|------|-----|---------------|---------------------|------------|-----|
| In the News         | 2    | 77  | United States | 5                   | Unix       | NA  |
| Papers              | 5    | 5   | Australia     | 2                   | Linux      | 202 |
| Discussions         | NA   | NA  | China         | 60                  | Unknown    | NA  |
| Advisories          | 5    | 110 | Mexico        | 3                   | Windows    | 140 |
| Tools released      | 16   | 8   | Turkey        | 22                  |            |     |
| Exploits published  | 17   | 54  | India         | 25                  |            |     |
| Vulnerable websites | NA   | NA  | Brazil        | 16                  |            |     |
| Websites defaced    | 18   | 342 | Indonesia     | 3                   |            |     |

## Alerts



## In the news

### China Focus

- Chinese Nitro Botnet Host Back Up After Microsoft Settles Lawsuit
- Huawei customers defend their security after congressional report
- Huawei calls for cybersecurity cooperation - Worldnews.com
- Huawei corruption allegations given to FBI
- Huawei and ZTE respond to U.S. *security concerns* - Digital Trends
- Feds to warn of counterfeit replacement *air bags*: auto execs

### Government

- After FTC crackdown, users chronicle tech support scam calls
- CACI Awarded \$36 Million contract by Lockheed Martin to Support Defense Cyber Crime Center
- Emergence of Cyber crime and our Ghanaian police
- Feds Charge 11 Over \$50m Secret Tech Exports To Russia
- Google Warning About More State-Sponsored Attacks
- Influence of federal cyber workforce roadmap growing
- Iran Linked To al-Qaeda's Web Jihadi Crew By X.25
- Iran's cyberattack claims difficult to judge, experts say
- NEW: #Anonymous #OpPedoChat takes down another 27 websites that supplied CP
- Philippines Cyber Crime Law Suspended For Making Online Libel A Crime, Too
- Phillipine cyber-crime law threatens free speech, says Amnesty
- The Center for Internet Security Boosts Government Cybersecurity (VIDEO)
- U.S. Should Lead Cybersecurity Efforts, NSA Director Says
- US agencies seize 686 websites accused of selling fake drugs
- Wash. National Guard focuses on cyber-attacks
- White House to meet with House staffers over cybersecurity order

### Security alerts

- Cyber-Criminals Plan Massive Trojan Attack on 30 Banks
- Fake Rovio games for Chrome hijack browser
- Malware-infected computers rented as proxy servers on the black market
- Proxy service users download malware, unknowingly join botnet
- Skype IM ransomware worm spreading quickly
- Trojan disguised as image delivered via Skype messages
- Zitmo Growing More Sophisticated, Prevalent in Android

### Legal

- Lieberman: Obama could issue cybersecurity order in the next month
- Lawmaker threatens to impeach Aquino over anti-cybercrime law
- New cybersecurity threat could revive legislation
- 'People's victory' netizens declare after High Court issues TRO against Cybercrime Law
- Supreme Court Terminates Warrantless Electronic Spying Case
- The Legal Perils Of Cyber-Insurance For Retailers

## CIR

### Forensics

- Electronic Evidence Heard in Rogue Trader Trial
- Interview with Lindy Sheppard, F3 (First Forensic Forum) Secretary
- KRyS Global launches suite of forensic tools
- NIST November Symposium focuses on forensics
- Old Laptops Give Historians a Digital Paper Trial
- Review: Malware Forensics Field Guide for Windows Systems
- Rimkus Analytics Adds New Services to Digital Forensics Division

### Mobile

- Cloud Security Alliance outlines top mobile threats
- iPhone-controlled keyless lock
- Surge in Android adware

### News, Technologies and Techniques

- 25 critical updates in Adobe Flash fix
- All Eyes on User Security as Cyber Criminals Up Their Game
- Assange Backers Ordered to Pay Up after Asylum Bid
- Break Office 2013 Passwords
- Can we trust the code that increasingly runs our lives?
- Cyber crime costs UK organisations £2.1m a year
- Cyberattacks on the upswing
- Cybercrime Costs Jumped 6 Percent in 2012
- DDoS Attacks on Major US Banks are No Stuxnet
- Global Action Takes Down Tech Support Scam
- Microsoft Issues Office Fix in Patch Tuesday Releases
- Microsoft speeds up IE10 Flash patching, matches Google
- Otaki firms global fight against cyber-crime
- Predicting Malicious Behavior
- Proof-of-Concept Exploits HTML5 Fullscreen API for Social Engineering
- The dangers of delaying heightened cybersecurity
- Theres Nothing Virtual about Cyberattacks
- Trend Micro takes aim at targeted attacks with custom-designed security service
- UNIVERSITY OF JOHANNESBURG: Cyber criminals 'targeting SA's small companies'
- USBGuru simulated attack service
- Windows 7 malware infection rate soars in 2012

## CIR

### FBI news

#### Gov

- Customs and Border Protection Officer Pleads Guilty to Concealing Fugitive from Law Enforcement
- Russian Agent, 10 Others Indicted for Exports to Russian Military
- Three Alleged International Terrorists Extradited from Great Britain
- Two Extradited British Nationals to Appear in New Haven Federal Court to Face Terrorism-Related Charges

#### Cyber

- FBI Cincinnati Warns of Malware That Continues to Infect Computers, Extort Money
- Federal Grand Jury Charges Dallas Resident with Making an Internet Threat and Other Felony Offenses
- Payment Processor for Internet Poker Companies Sentenced in Manhattan Federal Court
- Software Company CEO Charged in Manhattan Federal Court for \$2 Million Securities Fraud Scheme

#### CPKP

- Charlotte Man Sentenced to More Than 10 Years in Prison for Transporting 13-Year-Old Girl Across State Lines for Purposes of Prostitution
- El Paso Man Pleads Guilty to Federal Child Pornography Solicitation Charge
- Erie Man Pleads Guilty to Possessing, Distributing Child Pornography
- Former Groton Man Convicted and Sentenced on Child Pornography Charges
- Houston Man Ordered to Serve 60 Years for Producing and Advertising Child Pornography
- Houston Resident Sentenced for Possessing Child Pornography
- Jury Convicts Modesto Man for Receiving Child Pornography
- Kansas City Man Sentenced in Sex Trafficking Case
- Maryland MS-13 Member Arrested for Child Sex Trafficking
- Morris County Man Sentenced to More Than Five Years for Distributing Child Pornography
- Norco Man Charged with Receipt of Child Pornography
- Pennsylvania Man Sentenced to Eight+ Years in Prison for Distribution of Child Pornography
- Pittsburgh Man Pleads Guilty to Possessing Pornographic Images and Videos of Children
- Producer of Child Pornography Sentenced to 40 Years, Followed by Supervision
- Remaining Defendants Convicted in District's Largest Domestic Sex Trafficking Case
- Suspected Child Sexual Abuser Sought by Honolulu FBI
- Sword-Wielding Palm Coast Man Pleads Guilty to Federal Charge of Receiving Child Pornography
- Tohajiilee Man Pleads Guilty to Federal Child Sex Abuse Charge
- Twice-Convicted Sex Offender Pleads Guilty to Eight Counts of Production of Child Pornography
- Wayne County Man Sentenced in Child Pornography Case

**Papers:**

- [MS IE CVE-2012-4969 Analysis](#)
- [PHP Fuzzing In Action](#)

**Advisories for the week of October 10, 2012**

**Apple (1)**

[Secunia Security Advisory 50859](#)

Secunia Security Advisory - Some vulnerabilities have been reported in Apple OS X Server, which can be exploited by malicious people to disclose certain sensitive information, bypass certain security restrictions, and compromise a user's system.

**HP (3)**

[HP Security Bulletin HPSBOV02822 SSRT100966](#)

HP Security Bulletin HPSBOV02822 SSRT100966 - Potential vulnerabilities have been identified with HP Secure Web Server (SWS) for OpenVMS. The vulnerabilities could be remotely exploited to create a Denial of Service (DoS), unauthorized access, or unauthorized disclosure of information. Revision 1 of this advisory.

[Secunia Security Advisory 50861](#)

Secunia Security Advisory - A weakness has been reported in HP Network Node Manager i, which can be exploited by malicious people to disclose certain sensitive information.

[HP Security Bulletin HPSBMU02817 SSRT100950](#)

HP Security Bulletin HPSBMU02817 SSRT100950 - A potential security vulnerability has been identified with HP Network Node Manager i (NNMi) for HP-UX, Linux, Solaris, and Windows. The vulnerability could be remotely exploited resulting in disclosure of information. Revision 1 of this advisory.

**IBM (6)**

[IBM Informix Dynamic Server 11.50 Stack Overflow](#)

IBM Informix Dynamic Server version 11.50 suffers from a stack overflow vulnerability. The specific flaw exists within the oninit process bound to TCP port 9088 when processing the arguments to the COLLATION option in a SQL query. User-supplied data is copied into a stack-based buffer without proper bounds checking resulting in an overflow.

[Secunia Security Advisory 50881](#)

Secunia Security Advisory - A security issue and two vulnerabilities have been reported in IBM Tivoli Directory Server, which can be exploited by malicious people to conduct spoofing attacks and cause a DoS (Denial of Service).

[Secunia Security Advisory 50818](#)

Secunia Security Advisory - A security issue has been reported in IBM Tivoli Access Manager for e-business, which can be exploited by malicious people to conduct spoofing attacks.

[Secunia Security Advisory 50794](#)

Secunia Security Advisory - MustLive has reported a weakness and some vulnerabilities in IBM Lotus Notes Traveler, which can be exploited by malicious people to conduct spoofing and cross-site scripting attacks.

## CIR

### [IBM DB2 LUW 9.x / 10.1 XML File Disclosure](#)

Team SHATTER Security Advisory - Two system stored procedures executable by PUBLIC allow reading of files with xml extensions in IBM DB2 LUW versions 9.1, 9.5, 9.7, and 10.1.

### [IBM DB2 LUW 9.x / 10.1 JAR File Overwrite](#)

Team SHATTER Security Advisory - System stored procedure SQLJ.DB2\_INSTALL\_JAR executable by PUBLIC allows JAR file overwrite to any authenticated user in IBM DB2 LUW versions 9.1, 9.5, 9.7, and 10.1.

## Microsoft (8)

### [Microsoft Security Bulletin Summary For October 2012](#)

This bulletin summary lists 7 released Microsoft security bulletins for October, 2012.

### [Technical Cyber Security Alert 2012-283A](#)

Technical Cyber Security Alert 2012-283A - Select Microsoft software products contain multiple vulnerabilities. Microsoft has released updates to address these vulnerabilities.

### [Secunia Security Advisory 50901](#)

Secunia Security Advisory - A vulnerability has been reported in Microsoft SQL Server, which can be exploited by malicious people to conduct cross-site scripting attacks.

### [Secunia Security Advisory 50867](#)

Secunia Security Advisory - A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious users to cause a DoS (Denial of Service).

### [Secunia Security Advisory 50862](#)

Secunia Security Advisory - A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious, local users to gain escalated privileges.

### [Secunia Security Advisory 50855](#)

Secunia Security Advisory - A vulnerability has been reported in multiple Microsoft products, which can be exploited by malicious people to conduct cross-site scripting attacks.

### [Secunia Security Advisory 50844](#)

Secunia Security Advisory - A vulnerability has been reported in Microsoft Works, which can be exploited by malicious people to compromise a user's system.

### [Secunia Security Advisory 50835](#)

Secunia Security Advisory - Two vulnerabilities have been reported in multiple Microsoft products, which can be exploited by malicious people to compromise a user's system.

## Novel (1)

### [Secunia Security Advisory 50797](#)

Secunia Security Advisory - A vulnerability has been reported in Novell Sentinel Log Manager, which can be exploited by malicious users to bypass certain security restrictions.

**Oracle (2)**

[Oracle Enterprise Manager 11.x SQL Injection](#)

Team SHATTER Security Advisory - There are multiple SQL Injection vulnerabilities in components of SQL Tuning Sets that can be abused to perform attacks to execute SQL statements with elevated privileges in Oracle Enterprise Manager Database Control versions 11.1.07, 11.2.0.3, and previous patch sets.

[Secunia Security Advisory 50845](#)

Secunia Security Advisory - Oracle has acknowledged a vulnerability in Perl included in Solaris, which can be exploited by malicious people to conduct HTTP response splitting attacks in an application using the library.

**RSA (1)**

[RSA Adaptive Authentication Information Disclosure](#)

RSA Adaptive Authentication (On-Premise) version 6.0.2.1 contains a vulnerability that can potentially lead to sensitive information disclosure.

**Siemens (2)**

[Secunia Security Advisory 50900](#)

Secunia Security Advisory - A vulnerability has been reported in Siemens SiPass Integrated, which can be exploited by malicious people to compromise a vulnerable system.

[Secunia Security Advisory 50816](#)

Secunia Security Advisory - A vulnerability has been reported in Siemens SIMATIC S7-1200, which can be exploited by malicious people to conduct cross-site scripting attacks.

**Vmware (2)**

[VMware Security Advisory 2012-0014](#)

VMware Security Advisory 2012-0014 - VMware has provided an upgrade path for vCenter Operations and CapacityIQ and an update for Movie Decoder. These updates address multiple security vulnerabilities.

[Secunia Security Advisory 50798](#)

Secunia Security Advisory - A vulnerability has been reported in VMware vCenter CapacityIQ, which can be exploited by malicious people to disclose potentially sensitive system information.

**Linux (2)**

[Secunia Security Advisory 50849](#)

Secunia Security Advisory - A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to potentially gain escalated privileges.

[Secunia Security Advisory 50790](#)

Secunia Security Advisory - A weakness has been reported in Linux Kernel, which can be exploited by malicious, local users to disclose system information and cause a DoS (Denial of Service).

## Debian

### [Secunia Security Advisory 50808](#)

Secunia Security Advisory - Debian has issued an update for bacula. This fixes a security issue, which can be exploited by malicious users to bypass certain security restrictions.

### [Debian Security Advisory 2558-1](#)

Debian Linux Security Advisory 2558-1 - It was discovered that bacula, a network backup service, does not properly enforce console ACLs. This could allow information about resources to be dumped by an otherwise-restricted client.

### [Debian Security Advisory 2557-1](#)

Debian Linux Security Advisory 2557-1 - Timo Warns discovered that the internal authentication server of hostapd, a user space IEEE 802.11 AP and IEEE 802.1X/WPA/WPA2/EAP Authenticator, is vulnerable to a buffer overflow when processing fragmented EAP-TLS messages. As a result, an internal overflow checking routine terminates the process. An attacker can abuse this flaw to conduct denial of service attacks via crafted EAP-TLS messages prior to any authentication.

### [Debian Security Advisory 2556-1](#)

Debian Linux Security Advisory 2556-1 - Several vulnerabilities were discovered in Icedove, Debian's version of the Mozilla Thunderbird mail and news client.

### [Secunia Security Advisory 50810](#)

Secunia Security Advisory - Debian has issued an update for icedove. This fixes multiple vulnerabilities, which can be exploited by malicious people to bypass certain security restrictions and compromise a user's system.

### [Secunia Security Advisory 50805](#)

Secunia Security Advisory - Debian has issued an update for hostapd. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service).

### [Secunia Security Advisory 50838](#)

Secunia Security Advisory - Debian has issued an update for libxslt. This fixes multiple vulnerabilities, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise an application using the library.

### [Debian Security Advisory 2555-1](#)

Debian Linux Security Advisory 2555-1 - Nicholas Gregoire and Cris Neckar discovered several memory handling bugs in libxslt, which could lead to denial of service or the execution of arbitrary code if a malformed document is processed.

## Mandriva

### [Mandriva Linux Security Advisory 2012-161](#)

Mandriva Linux Security Advisory 2012-161 - Directory traversal vulnerability in html2ps before 1.0b7 allows remote attackers to read arbitrary files via directory traversal sequences in SSI directives. The updated packages have been upgraded to the 1.0b7 version which is not affected by this issue.



[Mandriva Linux Security Advisory 2012-160](#)

Mandriva Linux Security Advisory 2012-160 - The Magick\_png\_malloc function in coders/png.c in ImageMagick 6.7.8-6 does not use the proper variable type for the allocation size, which might allow remote attackers to cause a denial of service via a crafted PNG file that triggers incorrect memory allocation. The updated packages have been patched to correct this issue.

[Mandriva Linux Security Advisory 2012-150-1](#)

Mandriva Linux Security Advisory 2012-150 - Multiple security issues were identified and fixed in OpenJDK (icedtea6). Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE 7 Update 6 and earlier, and 6 Update 34 and earlier, has no impact and remote attack vectors involving AWT and a security-in-depth issue that is not directly exploitable but which can be used to aggravate security vulnerabilities that can be directly exploited. The updated packages provides icedtea6-1.11.4 which is not vulnerable to these issues.

[Mandriva Linux Security Advisory 2012-151-1](#)

Mandriva Linux Security Advisory 2012-151 - An integer overflow flaw, leading to a heap-based buffer overflow, was found in Ghostscript's International Color Consortium Format library (icclicb). An attacker could create a specially-crafted PostScript or PDF file with embedded images that would cause Ghostscript to crash or, potentially, execute arbitrary code with the privileges of the user running Ghostscript. The updated packages have been patched to correct this issue.

[Mandriva Linux Security Advisory 2012-159](#)

Mandriva Linux Security Advisory 2012-159 - Stack-based buffer overflow in the cbtls\_verify function in FreeRADIUS 2.1.10 through 2.1.12, when using TLS-based EAP methods, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a long not after timestamp in a client certificate. The updated packages have been patched to correct this issue.

[Mandriva Linux Security Advisory 2012-158](#)

Mandriva Linux Security Advisory 2012-158 - Multiple integer overflows in the calloc functions in malloc.c, and the GC\_generic\_malloc\_ignore\_off\_page function in mallocx.c in Boehm-Demers-Weiser GC before 7.2 make it easier for context-dependent attackers to perform memory-related attacks such as buffer overflows via a large size value, which causes less memory to be allocated than expected. The updated packages have been patched to correct this issue.

[Mandriva Linux Security Advisory 2012-157](#)

Mandriva Linux Security Advisory 2012-157 - A heap-based buffer overflow was found in the way OpenJPEG, an open-source JPEG 2000 codec written in C language, performed parsing of JPEG2000 image files. A remote attacker could provide a specially crafted JPEG 2000 file, which when opened in an application linked against openjpeg would lead to that application crash, or, potentially arbitrary code execution with the privileges of the user running the application. The updated packages have been patched to correct this issue.

**Redhat**

[Red Hat Security Advisory 2012-1346-01](#)

Red Hat Security Advisory 2012-1346-01 - The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in. This update fixes several vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed on the Adobe security page APSB12-22, listed in the References section. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

[Red Hat Security Advisory 2012-1350-01](#)

Red Hat Security Advisory 2012-1350-01 - Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox. Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. Two flaws in Firefox could allow a malicious website to bypass intended restrictions, possibly leading to information disclosure, or Firefox executing arbitrary code. Note that the information disclosure issue could possibly be combined with other flaws to achieve arbitrary code execution.

[Red Hat Security Advisory 2012-1351-01](#)

Red Hat Security Advisory 2012-1351-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird. Two flaws in Thunderbird could allow malicious content to bypass intended restrictions, possibly leading to information disclosure, or Thunderbird executing arbitrary code. Note that the information disclosure issue could possibly be combined with other flaws to achieve arbitrary code execution.

[Red Hat Security Advisory 2012-1347-01](#)

Red Hat Security Advisory 2012-1347-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. A flaw was found in the way socket buffers requiring TSO were handled by the sfc driver. If the skb did not fit within the minimum-size of the transmission queue, the network card could repeatedly reset itself. A remote attacker could use this flaw to cause a denial of service.

[Secunia Security Advisory 50820](#)

Secunia Security Advisory - Red Hat has issued an update for flash-plugin. This fixes multiple vulnerabilities, which can be exploited by malicious people to compromise a user's system.

[Red Hat Security Advisory 2012-1344-01](#)

Red Hat Security Advisory 2012-1344-01 - JBoss Enterprise Portal Platform is the open source implementation of the Java EE suite of services and Portal services running atop JBoss Enterprise Application Platform. It comprises a set of offerings for enterprise customers who are looking for pre-configured profiles of JBoss Enterprise Middleware components that have been tested and certified together to provide an integrated experience. An attack technique was found against the W3C XML Encryption Standard when block ciphers were used in cipher-block chaining mode. A remote attacker could use this flaw to conduct chosen-ciphertext attacks, leading to the recovery of the entire plain text of a particular cryptogram by examining the differences between SOAP responses sent from JBoss Web Services.

[Red Hat Security Advisory 2012-1332-01](#)

Red Hat Security Advisory 2012-1332-01 - IBM J2SE version 1.4.2 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit.

[Red Hat Security Advisory 2012-1330-01](#)

Red Hat Security Advisory 2012-1330-01 - JBoss Enterprise SOA Platform is the next-generation ESB and business process automation infrastructure. JBoss Enterprise SOA Platform allows IT to leverage existing, modern, and future integration methodologies to dramatically improve business process execution speed and quality. An attack technique was found against the W3C XML Encryption Standard when block ciphers were used in cipher-block chaining mode. A remote attacker could use this flaw to conduct chosen-ciphertext attacks, leading to the recovery of the entire plain text of a particular cryptogram by examining the differences between SOAP responses sent from JBoss Web Services.

[Red Hat Security Advisory 2012-1331-01](#)

Red Hat Security Advisory 2012-1331-01 - JBoss Operations Network is a middleware management solution that provides a single point of control to deploy, manage, and monitor JBoss Enterprise Middleware, applications, and services. This JBoss ON 3.1.1 release serves as a replacement for JBoss ON 3.1.0, and includes several bug fixes and enhancements.

[Secunia Security Advisory 50813](#)

Secunia Security Advisory - Red Hat has issued an update for freeradius2. This fixes a vulnerability, which can be exploited by malicious people to compromise a vulnerable system.

[Secunia Security Advisory 50811](#)

Secunia Security Advisory - Red Hat has issued an update for the kernel. This fixes multiple vulnerabilities, which can be exploited by malicious, local users to cause a DoS (Denial of Service), disclose potentially sensitive information, or to potentially gain escalated privileges.

**Ubuntu**

[Ubuntu Security Notice USN-1599-1](#)

Ubuntu Security Notice 1599-1 - Pablo Neira Ayuso discovered a flaw in the credentials of netlink messages. An unprivileged local attacker could exploit this by getting a netlink based service, that relies on netlink credentials, to perform privileged actions.

[Ubuntu Security Notice USN-1598-1](#)

Ubuntu Security Notice 1598-1 - An error was discovered in the Linux kernel's network TUN/TAP device implementation. A local user with access to the TUN/TAP interface (which is not available to unprivileged users until granted by a root user) could exploit this flaw to crash the system or potential gain administrative privileges.

[Ubuntu Security Notice USN-1600-1](#)

Ubuntu Security Notice 1600-1 - Henrik Skupin, Jesse Ruderman, Christian Holler, Soroush Dalili and others discovered several memory corruption flaws in Firefox. If a user were tricked into opening a specially crafted web page, a remote attacker could cause Firefox to crash or potentially execute arbitrary code as the user invoking the program. David Bloom and Jordi Chancel discovered that Firefox did not always properly handle the select element. A remote attacker could exploit this to conduct URL spoofing and clickjacking attacks. Various other issues were also addressed.

[Secunia Security Advisory 50848](#)

Secunia Security Advisory - Ubuntu has issued an update for kernel. This fixes a vulnerability, which can be exploited by malicious, local users to perform certain actions with escalated privileges.

[Ubuntu Security Notice USN-1597-1](#)

Ubuntu Security Notice 1597-1 - A flaw was found in how the Linux kernel passed the replacement session keyring to a child process. An unprivileged local user could exploit this flaw to cause a denial of service (panic).

[Secunia Security Advisory 50869](#)

Secunia Security Advisory - Ubuntu has issued an update for libxslt. This fixes multiple vulnerabilities, which can be exploited by malicious people to disclose potentially sensitive information, cause a DoS (Denial of Service), and potentially compromise an application using the library.

[Secunia Security Advisory 50853](#)

Secunia Security Advisory - Ubuntu has issued an update for kernel. This fixes a vulnerability, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

[Secunia Security Advisory 50858](#)

Secunia Security Advisory - Ubuntu has issued an update for python. This fixes multiple vulnerabilities, which can be exploited by malicious, local users to potentially disclose sensitive information and malicious people to conduct cross-site scripting attacks, disclose potentially sensitive information, cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

[Ubuntu Security Notice USN-1595-1](#)

Ubuntu Security Notice 1595-1 - Chris Evans discovered that libxslt incorrectly handled generate-id XPath functions. If a user or automated system were tricked into processing a specially crafted XSLT document, a remote attacker could obtain potentially sensitive information. This issue only affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS and Ubuntu 11.04. It was discovered that libxslt incorrectly parsed certain patterns. If a user or automated system were tricked into processing a specially crafted XSLT document, a remote attacker could cause libxslt to crash, causing a denial of service. Various other issues were also addressed.

[Ubuntu Security Notice USN-1576-2](#)

Ubuntu Security Notice 1576-2 - USN-1576-1 fixed vulnerabilities in DBus. The update caused a regression for certain services launched from the activation helper, and caused an unclean shutdown on upgrade. This update fixes the problem. Sebastian Krahmer discovered that DBus incorrectly handled environment variables when running with elevated privileges. A local attacker could possibly exploit this flaw with a setuid binary and gain root privileges. Various other issues were also addressed.

[Ubuntu Security Notice USN-1596-1](#)

Ubuntu Security Notice 1596-1 - It was discovered that Python would prepend an empty string to sys.path under certain circumstances. A local attacker with write access to the current working directory could exploit this to execute arbitrary code. It was discovered that the audioop module did not correctly perform input validation. If a user or automated system were tricked into opening a crafted audio file, an attacker could cause a denial of service via application crash. Various other issues were also addressed.

[Secunia Security Advisory 50846](#)

Secunia Security Advisory - Ubuntu has issued an update for kernel. This fixes two vulnerabilities, which can be exploited by malicious, local users in a guest virtual machine to cause a DoS (Denial of Service) and potentially gain escalated privileges and by malicious people to cause a DoS (Denial of Service).

[Ubuntu Security Notice USN-1594-1](#)

Ubuntu Security Notice 1594-1 - Vadim Ponomarev discovered a flaw in the Linux kernel causing a reference leak when PID namespaces are used. A remote attacker could exploit this flaw causing a denial of service. A flaw was found in how the Linux kernel's KVM (Kernel-based Virtual Machine) subsystem handled MSI (Message Signaled Interrupts). A local unprivileged user could exploit this flaw to cause a denial of service or potentially elevate privileges. Various other issues were also addressed.

[Secunia Security Advisory 50850](#)

Secunia Security Advisory - Ubuntu has issued an update for python. This fixes multiple vulnerabilities, which can be exploited by malicious, local users to disclose potentially sensitive information and by malicious people to conduct cross-site scripting attacks, disclose potentially sensitive information, and cause a DoS (Denial of Service).

[Secunia Security Advisory 50854](#)

Secunia Security Advisory - Ubuntu has issued an update for xdiagnose. This fixes a security issue, which can be exploited by malicious, local users to perform certain actions with escalated privileges.

[Secunia Security Advisory 50851](#)

Secunia Security Advisory - Ubuntu has issued an update for devscripts. This fixes some weaknesses, which can be exploited by malicious, local users to cause a DoS (Denial of Service) and by malicious people to cause a DoS (Denial of Service) and compromise a vulnerable system.

[Secunia Security Advisory 50860](#)

Secunia Security Advisory - Ubuntu has issued an update for qemu. This fixes a vulnerability, which can be exploited by malicious, local users in a guest virtual machine to potentially gain escalated privileges.

**Misc**

[Logica HotScan SWIFT Alliance Access Interface Buffer Overflow](#)

The Hotscan Listener interface is prone to a buffer overflow vulnerability because the application fails to perform adequate boundary checks on user-supplied input. This allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.

[Wing FTP Server 4.x Denial Of Service](#)

Wing FTP server versions prior to 4.1.1 suffer from a denial of service vulnerability.

[Secunia Security Advisory 50890](#)

Secunia Security Advisory - A vulnerability has been discovered in Icy Phoenix, which can be exploited by malicious people to conduct cross-site scripting attacks.

[Secunia Security Advisory 50840](#)

Secunia Security Advisory - Fujitsu has acknowledged a vulnerability in Interstage HTTP Server, which can be exploited by malicious people to disclose potentially sensitive information.

[Secunia Security Advisory 50817](#)

Secunia Security Advisory - Multiple vulnerabilities with an unknown impact have been reported in Pale Moon.

[Hostapd Missing EAP-TLS Message Length Validation](#)

## CIR

Hostapd versions 0.6 through 1.0 fail to validate EAP-TLS message length allowing for a possible denial of service condition.

### [Secunia Security Advisory 50888](#)

Secunia Security Advisory - A vulnerability has been reported in hostapd, which can be exploited by malicious people to cause a DoS (Denial of Service).

### [Secunia Security Advisory 50796](#)

Secunia Security Advisory - Multiple vulnerabilities have been reported in SRWare Iron, where some have an unknown impact and others can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting attacks, and compromise a user's system.

### [Secunia Security Advisory 50886](#)

Secunia Security Advisory - ERPScan has reported a vulnerability in SAP NetWeaver Process Integration, which can be exploited by malicious people to bypass certain security restrictions.

### [Secunia Security Advisory 50883](#)

Secunia Security Advisory - ERPScan has reported a vulnerability in SAP NetWeaver Business Warehouse, which can be exploited by malicious people to disclose potentially sensitive information.

### [Secunia Security Advisory 50795](#)

Secunia Security Advisory - A vulnerability has been reported in VMware vCenter Operations, which can be exploited by malicious people to conduct cross-site scripting attacks.

### [Secunia Security Advisory 50866](#)

Secunia Security Advisory - Some vulnerabilities with an unknown impact have been reported in LetoDMS.

### [Secunia Security Advisory 50882](#)

Secunia Security Advisory - ERPScan has reported two vulnerabilities in SAP NetWeaver, which can be exploited by malicious people to disclose potentially sensitive information and conduct cross-site scripting attacks.

### [Secunia Security Advisory 50884](#)

Secunia Security Advisory - ERPScan has reported a vulnerability in SAP NetWeaver, which can be exploited by malicious people to conduct cross-site scripting attacks.

### [Secunia Security Advisory 50868](#)

Secunia Security Advisory - Some vulnerabilities with an unknown impact have been reported in the Pinterest Pin It Button Lite plugin for WordPress.

### [Sybase ASE 15.x Java Command Execution](#)

Team SHATTER Security Advisory - It is possible to execute Operating System commands using the Java call Runtime.getRuntime().exec() in Sybase ASE versions 15.0, 15.5, and 15.7.

### [Sybase ASE 15.x Role Elevation](#)

Authenticated users can elevate privileges to any role via SQL injection in one of the DBCC commands in Sybase ASE versions 15.0, 15.5, and 15.7.

[Ogg DirectShow Vulnerable Libraries](#)

Ogg DirectShow filters are distributed and installed with vulnerable MSVC++ 2008 runtime libraries.

[Secunia Security Advisory 50865](#)

Secunia Security Advisory - Ibrahim M. El-Sayed has reported some vulnerabilities in OSSIM, which can be exploited by malicious people to conduct cross-site scripting attacks.

[Secunia Security Advisory 50802](#)

Secunia Security Advisory - A vulnerability has been reported in the Commerce extra panes module for Drupal, which can be exploited by malicious people to conduct cross-site request forgery attacks.

[Secunia Security Advisory 50792](#)

Secunia Security Advisory - Ibrahim El-Sayed has reported two vulnerabilities in Omnistar Mailer, which can be exploited by malicious people to conduct SQL injection attacks.

[Secunia Security Advisory 50852](#)

Secunia Security Advisory - McAfee has acknowledged a vulnerability in McAfee Firewall Enterprise, which can be exploited by malicious people to cause a DoS (Denial of Service).

[Secunia Security Advisory 50803](#)

Secunia Security Advisory - High-Tech Bridge has discovered two vulnerabilities in Template CMS, which can be exploited by malicious people to conduct cross-site scripting and request forgery attacks.

[Secunia Security Advisory 50841](#)

Secunia Security Advisory - A vulnerability has been reported in the MijoFTP component for Joomla!, which can be exploited by malicious people to compromise a vulnerable system.

[Secunia Security Advisory 50863](#)

Secunia Security Advisory - Red Hat has issued an update for JBoss Operations Network. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service).

[Secunia Security Advisory 50825](#)

Secunia Security Advisory - Reaction Information Security has discovered a vulnerability in XnView, which can be exploited by malicious people to compromise a user's system.

[Secunia Security Advisory 50812](#)

Secunia Security Advisory - Two vulnerabilities have been discovered in Spider Calendar plugin for WordPress, which can be exploited by malicious people to conduct cross-site scripting and SQL injection attacks.

[Secunia Security Advisory 50799](#)

Secunia Security Advisory - Scott Herbert has discovered a vulnerability in Zenphoto, which can be exploited by malicious people to conduct cross-site scripting attacks.

[Drupal Hostip 6.x / 7.x Cross Site Scripting](#)

Drupal Hostip third party module versions 6.x and 7.x suffer from a cross site scripting vulnerability.

[Drupal Commerce Extra Panes 7.x Cross Site Request Forgery](#)



## CIR

Drupal Commerce Extra Panes third party module version 7.x suffers from a cross site request forgery vulnerability.

### [Drupal Twitter Pull 6.x / 7.x Cross Site Scripting](#)

Drupal Twitter Pull third party module versions 6.x and 7.x suffer from a cross site scripting vulnerability.

### [Secunia Security Advisory 50839](#)

Secunia Security Advisory - catatonicprime has discovered a vulnerability in PowerTCP WebServer for ActiveX, which can be exploited by malicious people to cause a DoS (Denial of Service).

### [Secunia Security Advisory 50864](#)

Secunia Security Advisory - Some vulnerabilities have been reported in libxslt, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise an application using the library.

### [Secunia Security Advisory 50843](#)

Secunia Security Advisory - Multiple vulnerabilities have been reported in Wireshark, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

### [Secunia Security Advisory 50826](#)

Secunia Security Advisory - A vulnerability has been discovered in ProjectPier, which can be exploited by malicious people to compromise a vulnerable system.

### [Secunia Security Advisory 50595](#)

Secunia Security Advisory - Zhao Liang has discovered a vulnerability in TurboFTP Server, which can be exploited by malicious users to compromise a vulnerable system.

### [Secunia Security Advisory 48430](#)

Secunia Security Advisory - Francis Provencher has discovered a vulnerability in CYME, which can be exploited by malicious people to compromise a user's system.

## Tools released this week:

- [Contrack Tools 1.4.0](#)
- [Linux IPTables Firewall 1.4.16.2](#)
- [MySQL Login Scanner](#)
- [Reverse Shell 1.0](#)
- [RFIDIoT Python Library For RFID Readers 1.0d](#)
- [Rubilyn 0.0.1](#)
- [strongSwan IPsec Implementation 5.0.1](#)
- [Suricata IDPE 1.3.2](#)



**Exploits released this week (9):**

- [Apple iOS Default SSH Password](#)
- [Arctic Torrent 1.2.3 Memory Corruption](#)
- [Avaya IP Office Customer Call Reporter Command Execution](#)
- [Avaya WinPMD UniteHostRouter Buffer Overflow](#)
- [Cyme ChartFX Client Server ActiveX Control Array Indexing Vulnerability](#)
- [FastStone Image Viewer 4.6 Arbitrary Code Execution](#)
- [FastStone Image Viewer 4.6 Proof Of Concept](#)
- [FL Studio 10 Producer Edition Buffer Overflow](#)
- [Hardcorereview WriteAV Arbitrary Code Execution](#)
- [HCView WriteAV Crash Proof Of Concept](#)
- [JPEGsnoop <= 1.5.2 WriteAV Arbitrary Code Execution](#)
- [JPEGsnoop 1.5.2 Code Execution](#)
- [Key Systems Electronic Key Lockers Command Injection](#)
- [Microsoft Windows Privilege Escalation](#)
- [PHP 5.3.4 com\\_event\\_sink 0-Day](#)
- [PLIB 1.8.5 Buffer Overflow](#)
- [VLC Player 2.0.3 ReadAV Arbitrary Code Execution](#)
- [Windows Escalate UAC Protection Bypass](#)
- [XnView 1.99.1 JLS File Decompression Heap Overflow](#)
- [XnView JLS File Decompression Heap Overflow](#)

**Web Exploits released this week (9):**

- [23rdweb Studio SQL Injection](#)
- [Blog Mod 0.1.9 SQL Injection](#)
- [Breviloquent SQL Injection](#)
- [Cyme ChartFX Client Server Array Indexing](#)
- [Dark Comet RAT SQL Injection / Arbitrary File Access](#)
- [Easy Fast Admin SQL Injection](#)
- [Endpoint Protector 4.0.4.0 Cross Site Scripting](#)
- [Et-Chat Rank SQL Injection](#)
- [et-chat SQL Injection](#)
- [Exploit: NCMedia Sound Editor Pro v7.5.1 SEH&DEP](#)
- [Icy Phoenix 2.0 Cross Site Scripting](#)
- [InduSoft Web Studio Arbitrary Upload Remote Code Execution](#)
- [InduSoft Web Studio Arbitrary Upload Remote Code Execution](#)
- [Interspire Email Marketer 6.0.1 XSS / SQL Injection](#)
- [Latihan Ilmiah 2.3 Cross Site Scripting / SQL Injection](#)
- [Megapolis.Portal Manager Cross Site Scripting](#)
- [MS11-080 AfdJoinLeaf Privilege Escalation](#)
- [MyAuth3 Blind SQL Injection](#)
- [MyBB Remote Command Execution](#)
- [MyFreePost Cross Site Scripting](#)

## CIR

- [Novell Sentinel Log Manager <=1.2.0.2 Retention Policy Vulnerability](#)
- [Novell Sentinel Log Manager 1.2.0.2 Bypass](#)
- [Number Nine Design SQL Injection](#)
- [Omnistar Mailer 7.2 SQL Injection / Cross Site Scripting](#)
- [Omnistar Mailer v7.2 Multiple Vulnerabilities](#)
- [Open-Realty 2.5.6 Local File Inclusion](#)
- [Opera 12.02 Cross Site Scripting](#)
- [Oracle Identity Management 10g Cross Site Scripting](#)
- [Paypal BugBounty 5 Cross Site Scripting](#)
- [phpMyBitTorrent 2.04 Multiple Vulnerabilities](#)
- [phpMyBitTorrent 2.04 SQL Injection / Local File Inclusion](#)
- [phpMyChat Plus 1.94 RC1 LFI / XSS / RFI / SQL Injection](#)
- [phpMyChat Plus v1.94 RC1 Multiple Remote Vulnerabilities](#)
- [PhpTax pfilez Parameter Exec Remote Code Injection](#)
- [QNX QCONN Remote Command Execution](#)
- [Template CMS 2.1.1 Cross Site Request Forgery / Cross Site Scripting](#)
- [Template CMS 2.1.1 Multiple Vulnerabilities](#)
- [TinyCMS 1.4 Local File Inclusion](#)
- [TP-LINK TD-W8151N Cross Site Request Forgery](#)
- [Utempter Fake Entry Manipulation](#)
- [Web Help Desk 11.0.7 Cross Site Scripting](#)
- [Wordpress Plugin spider calendar Multiple Vulnerabilities](#)
- [WordPress Remote Command Execution](#)
- [WordPress Shopp 1.0.17 XSS / Shell Upload / Disclosure](#)
- [WordPress Spider 1.0.1 SQL Injection / XSS](#)
- [XnView JLS File Decompression Heap Overflow](#)
- [YourArcadeScript 2.4 Cross Site Request Forgery](#)

### Denial of Service (PoC)

- [Arctic Torrent 1.2.3 Memory Corruption \(DoS\)](#)
- [Cyme ChartFX Client Server ActiveX Control Array Indexing Vulnerability](#)
- [FastStone Image Viewer 4.6 <= ReadAVonIP Crash PoC](#)
- [FL Studio 10 Producer Edition SEH Based Buffer Overflow PoC](#)
- [Gom Player 2.1.44.5123 \(Unicode\) NULL Pointer Dereference](#)
- [HCView WriteAV Crash PoC](#)
- [JPEGsnoop <= 1.5.2 WriteAV Crash PoC](#)
- [XnView 1.99.1 JLS File Decompression Heap Overflow](#)



CIR

|                                 |   |   |          |                        |
|---------------------------------|---|---|----------|------------------------|
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">gtj.fangcheng.gov.cn</a>              | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">jh.yclgb.gov.cn</a>                   | Win 2008 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">xqzx.xncx.gov.cn</a>                  | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.xhxz.gov.cn/data/</a>             | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.taetn.gov.cn</a>                  | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.chenxi.gov.cn</a>                 | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.czei.gov.cn</a>                   | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.luyi.gov.cn</a>                   | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.qyfbz.gov.cn</a>                  | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.jcgaj.gov.cn</a>                  | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.ytws.gov.cn</a>                   | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.tydj.gov.cn</a>                   | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.bjmwr.gov.cn</a>                  | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.bbstyj.gov.cn</a>                 | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Barbaros-DZ</a>     |   | <a href="#">www.yxhb.gov.cn</a>                   | Win 2003 | <a href="#">mirror</a> |
| <a href="#">billy cyber</a>     | <a href="#">Borneo Attacker</a>         | <a href="#">spaq.daqing.gov.cn</a>                | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">Black Angels</a>    |   | <a href="#">disnakkan.boyalalikab.go.id/ID...</a> | Linux    | <a href="#">mirror</a> |
| <a href="#">Black Angels</a>    |   | <a href="#">disbudpar.boyalalikab.go.id/ID...</a> | Linux    | <a href="#">mirror</a> |
| <a href="#">Black Angels</a>    |   | <a href="#">boyalalikab.go.id/index.php</a>       | Linux    | <a href="#">mirror</a> |
| <a href="#">Black Angels</a>    | <a href="#">Marco-Exploit-Community</a> | <a href="#">www.mu.ac.zm/sbs/templates/...</a>    | Linux    | <a href="#">Mirror</a> |
| <a href="#">Black Angels</a>    | <a href="#">Marco-Exploit-Community</a> | <a href="#">guide.lbtech.ac.th/index.php</a>      | Linux    | <a href="#">Mirror</a> |
| <a href="#">c0d3-X-1337</a>     | <a href="#">Under Ground Hacker</a>     | <a href="#">tarek.in/1337.html</a>                | Linux    | <a href="#">Mirror</a> |
| <a href="#">c0d3-X-1337</a>     | <a href="#">Under Ground Hacker</a>     | <a href="#">spi.gov.bd/1337.html</a>              | Linux    | <a href="#">Mirror</a> |
| <a href="#">catalyst71</a>      | <a href="#">The Crows Crew</a>          | <a href="#">nutritionnext.in</a>                  | Linux    | <a href="#">Mirror</a> |
| <a href="#">Computer Korner</a> | <a href="#">Computer Korner</a>         | <a href="#">www.cobaw.vic.gov.au/computerk...</a> | Linux    | <a href="#">Mirror</a> |
| <a href="#">Computer Korner</a> |   | <a href="#">orner.html</a>                        |          |                        |
| <a href="#">Computer Korner</a> | <a href="#">Computer Korner</a>         | <a href="#">ordumemarge.gov.tr</a>                | Linux    | <a href="#">Mirror</a> |
| <a href="#">Cr4ck-Br4iN</a>     | <a href="#">Computer Korner</a>         | <a href="#">www.orduab.gov.tr</a>                 | Linux    | <a href="#">Mirror</a> |
| <a href="#">Cr4ck-Br4iN</a>     | <a href="#">BD GREY HAT HACKERS</a>     | <a href="#">dhaulagirizonalhospital.gov.np/</a>   | Linux    | <a href="#">Mirror</a> |
| <a href="#">Cr4ck-Br4iN</a>     | <a href="#">BD GREY HAT HACKERS</a>     | <a href="#">www.cip.gov.np/cb.html</a>            | Linux    | <a href="#">Mirror</a> |
| <a href="#">Cyb3r.BI@d3r</a>    | <a href="#">BD GREY HAT HACKERS</a>     | <a href="#">www.chrdu.gov.np/cb.html</a>          | Linux    | <a href="#">Mirror</a> |
| <a href="#">DaiLexX</a>         | <a href="#">BD BLACK HAT</a>            | <a href="#">www.eduhub.in</a>                     | Linux    | <a href="#">Mirror</a> |
| <a href="#">DaiLexX</a>         |   | <a href="#">spitalitepelene.gov.al</a>            | Linux    | <a href="#">mirror</a> |
| <a href="#">DaiLexX</a>         |   | <a href="#">drshelbasan.gov.al</a>                | Linux    | <a href="#">mirror</a> |
| <a href="#">DaiLexX</a>         |   | <a href="#">spitalipogradec.gov.al</a>            | Linux    | <a href="#">mirror</a> |
| <a href="#">DaiLexX</a>         |   | <a href="#">dshpkolonje.gov.al</a>                | Linux    | <a href="#">mirror</a> |
| <a href="#">DaiLexX</a>         |   | <a href="#">dshppeqin.gov.al</a>                  | Linux    | <a href="#">mirror</a> |
| <a href="#">DaiLexX</a>         |   | <a href="#">dshpkucove.gov.al</a>                 | Linux    | <a href="#">mirror</a> |
| <a href="#">DaiLexX</a>         |   | <a href="#">spitalipeqin.gov.al</a>               | Linux    | <a href="#">mirror</a> |
| <a href="#">Dark Knight</a>     | <a href="#">AnonymousPakistan</a>       | <a href="#">samplepapersbook.in</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">Dark Knight</a>     | <a href="#">AnonymousPakistan</a>       | <a href="#">procapital.in</a>                     | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">Dark Knight</a>     | <a href="#">AnonymousPakistan</a>       | <a href="#">aiuonline.in</a>                      | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">Dark Knight</a>     | <a href="#">AnonymousPakistan</a>       | <a href="#">gandhibuilders.in</a>                 | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">Dark Knight</a>     | <a href="#">AnonymousPakistan</a>       | <a href="#">conference.bitmesra.ac.in</a>         | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">Dark Knight</a>     | <a href="#">AnonymousPakistan</a>       | <a href="#">bitmesra.ac.in</a>                    | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">Dark Knight</a>     | <a href="#">AnonymousPakistan</a>       | <a href="#">funelement.co.in</a>                  | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">Dbuzz</a>           |   | <a href="#">bpp426.go.th</a>                      | Linux    | <a href="#">mirror</a> |
| <a href="#">Dbuzz</a>           |   | <a href="#">bpp145.go.th</a>                      | Linux    | <a href="#">mirror</a> |
| <a href="#">Dbuzz</a>           |   | <a href="#">bpp11.go.th</a>                       | Linux    | <a href="#">mirror</a> |
| <a href="#">Dbuzz</a>           |   | <a href="#">www.aoleukpolice.go.th</a>            | Linux    | <a href="#">mirror</a> |
| <a href="#">Deep Sparrow</a>    | <a href="#">Single Attacker Crew</a>    | <a href="#">www.studio3.co.il/blog/</a>           | Linux    | <a href="#">Mirror</a> |
| <a href="#">Deep Sparrow</a>    | <a href="#">Single Attacker Crew</a>    | <a href="#">www.arad-group.co.il</a>              | Linux    | <a href="#">Mirror</a> |
| <a href="#">Dew1Ls</a>          |   | <a href="#">www.balikesiraile.gov.tr</a>          | Linux    | <a href="#">mirror</a> |
| <a href="#">DiL-ZoNe</a>        | <a href="#">Devil-GrouP</a>             | <a href="#">www.indiamines.in/DiL-ZoNe.php</a>    | Linux    | <a href="#">Mirror</a> |
| <a href="#">Dr.SHA6H</a>        |   | <a href="#">munisandia.gob.pe</a>                 | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>        |   | <a href="#">munichurcampa.gob.pe</a>              | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>        |   | <a href="#">www.cumayeri.gov.tr/configurat...</a> | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>        |   | <a href="#">www.yigilcatarim.gov.tr/wp-con...</a> | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>        |   | <a href="#">www.duzceafetacil.gov.tr/tmp/</a>     | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>        |   | <a href="#">www.akcakocamuftulugu.gov.tr/i...</a> | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>        |   | <a href="#">www.visitkaraman.gov.tr/images/</a>   | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>        |   | <a href="#">cilimlitarim.gov.tr/images/</a>       | Linux    | <a href="#">mirror</a> |

CIR

|  |  |  |          |                        |
|--|--|--|----------|------------------------|
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.iyideremuftulugu.gov.tr/tmp/</a>   | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.duzceafad.gov.tr/tmp/</a>          | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.akcakoca.gov.tr/images/hab</a>     | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">cilimli.gov.tr/tmp/</a>                | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.duzdem.gov.tr/images/</a>          | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.canakkalekutup.gov.tr/tmp/</a>     | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.duzce.gov.tr/site/</a>             | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.duzcemuftulugu.gov.tr/tmp/</a>     | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.diforizaba.gob.mx</a>              | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">duzcesaglik.gov.tr</a>                 | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.duzcetarim.gov.tr</a>              | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.duzcehalksagligi.gov.tr</a>        | Linux    | <a href="#">mirror</a> |
| <a href="#">Dr.SHA6H</a>                   |  | <a href="#">www.pdphscoast.go.ke</a>               | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Dr3@m3r~1986</a>               | <a href="#">3xp1r3 Cyber Army</a>          | <a href="#">walkinfo.in/3ca.html</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">Dr3@m3r~1986</a>               | <a href="#">3xp1r3 Cyber Army</a>          | <a href="#">riyo.in/3ca.html</a>                   | Linux    | <a href="#">Mirror</a> |
| <a href="#">Error_hand</a>                 | <a href="#">Silent Error Crew</a>          | <a href="#">cqzm.gov.cn/zZz.html</a>               | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">Gabby</a>                      | <a href="#">The Crows Crew</a>             | <a href="#">panabocity.gov.ph/luv.php</a>          | Linux    | <a href="#">Mirror</a> |
| <a href="#">GHOST-AL-RAFIDAIN</a>          |  | <a href="#">www.bagaces.go.cr</a>                  | Linux    | <a href="#">mirror</a> |
| <a href="#">Golam Kibria</a>               | <a href="#">BD GREY HAT HACKERS</a>        | <a href="#">cce.unsyiah.ac.id/maintenance.ph</a>   | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">www.biotechcommission.kerala.g</a>     | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">ov.in/docs</a>                         |          |                        |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">www.spd.kerala.gov.in/docs</a>         | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">ildm.kerala.gov.in/docs</a>            | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">hed.kerala.gov.in/docs</a>             | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">dme.kerala.gov.in/pdf</a>              | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">minister-publicworks.kerala.gov.in</a> | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">gok-delhi.kerala.gov.in</a>            | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">clr.kerala.gov.in/docs</a>             | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">patentcentre.kerala.gov.in</a>         | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">texfed.kerala.gov.in</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">slb.kerala.gov.in</a>                  | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">rdd-crd.kerala.gov.in</a>              | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">ksrrda.kerala.gov.in</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">kscbc.kerala.gov.in</a>                | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">keri.kerala.gov.in</a>                 | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">kerams.kerala.gov.in</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">envt.kerala.gov.in</a>                 | Linux    | <a href="#">Mirror</a> |
| <a href="#">h4x0r HuSsY</a>                | <a href="#">VOBHH</a>                      | <a href="#">ckm.kerala.gov.in</a>                  | Linux    | <a href="#">Mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">www.carabobo.gob.ve/dz.txt</a>         | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">www.ville-marolles.fr/dz.txt</a>       | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">ville.mairie-plumelin.fr/piwik...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">piwik.mairie-plumelin.fr/piwik...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">www.mairie-plumelin.fr/piwik/d...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">melin.mairie-plumelin.fr/piwik...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">piwik.mairie-locmine.fr/robots...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">plu.mairie-plumelin.fr/piwik/d...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">men.mairie-plumelin.fr/piwik/d...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">info.mairie-locmine.fr/dz.txt</a>      | Linux    | <a href="#">mirror</a> |
| <a href="#">HacKed By LaMiN3 DK</a>        |  | <a href="#">pw.mairie-plumelin.fr/servicep...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">hacked by mo.bkafek hacker</a> | <a href="#">hacked by mo.bkafek hacker</a> | <a href="#">fdtraining.plymouthmn.gov</a>          | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">hasnain haxor</a>              | <a href="#">P4K!\$74N H4X0R\$</a>          | <a href="#">theaum.in/wp/</a>                      | Linux    | <a href="#">Mirror</a> |
| <a href="#">hasnain haxor</a>              | <a href="#">P4K!\$74N H4X0R\$</a>          | <a href="#">freakyfashion.in</a>                   | Linux    | <a href="#">Mirror</a> |
| <a href="#">hasnain haxor</a>              | <a href="#">P4K!\$74N H4X0R\$</a>          | <a href="#">woodsmith.co.in</a>                    | Linux    | <a href="#">Mirror</a> |
| <a href="#">hasnain haxor</a>              | <a href="#">P4K!\$74N H4X0R\$</a>          | <a href="#">fastindia.in</a>                       | Linux    | <a href="#">Mirror</a> |
| <a href="#">hasnain haxor</a>              | <a href="#">P4K!\$74N H4X0R\$</a>          | <a href="#">fish-oil.in</a>                        | Linux    | <a href="#">Mirror</a> |
| <a href="#">hasnain haxor</a>              | <a href="#">Team Cyber Switch</a>          | <a href="#">kjbible.in</a>                         | Linux    | <a href="#">Mirror</a> |
| <a href="#">hatrk</a>                      |  | <a href="#">nitc.gov.np</a>                        | Linux    | <a href="#">mirror</a> |
| <a href="#">HighTech</a>                   |  | <a href="#">xm.daqing.gov.cn/index.htm</a>         | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Hmei7</a>                      |  | <a href="#">tnvkpmis.gov.in/x.htm</a>              | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Indishell</a>                  |  | <a href="#">www.npa.gov.pk</a>                     | Linux    | <a href="#">mirror</a> |
| <a href="#">IR-security</a>                |  | <a href="#">tecu.salud.gob.mx/l0rd.txt</a>         | Win 2000 | <a href="#">mirror</a> |



CIR

|                               |   |  |          |                        |
|-------------------------------|---|--|----------|------------------------|
| <a href="#">IR-security</a>   |   | <a href="#">sipf.salud.gob.mx/l0rd.txt</a>         | Win 2000 | <a href="#">mirror</a> |
| <a href="#">Jack Riderr</a>   | <a href="#">Jack Riderr</a>             | <a href="#">ggfw.leiyang.gov.cn/</a>               | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">Jean Frey</a>     | <a href="#">Wolf Enforced</a>           | <a href="#">www.narino.gov.co/media/</a>           | Linux    | <a href="#">Mirror</a> |
| <a href="#">k4L0ng666</a>     |   | <a href="#">centroaudiovisual.gob.ar/yenni...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">k4L0ng666</a>     | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">centroaudiovisual.gob.ar/yenni...</a>  | Linux    | <a href="#">mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">executivecoaching.in/sk.php</a>        | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">olivecapital.in/readme.html</a>        | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">tafnet.in/sk.php</a>                   | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">www.poiema.in/sk.php</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">onepoint.in/sk.php</a>                 | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">oliveconsulting.in/sk.php</a>          | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">indiafacts.in/sk.php</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">infovore.in/sk.php</a>                 | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">infobytes.in/sk.php</a>                | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">lifequest.in/sk.php</a>                | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">www.kindlebook.in/sk.php</a>           | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">www.christianlife.in/s.php</a>         | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">www.christianbook.in/s.php</a>         | Linux    | <a href="#">Mirror</a> |
| <a href="#">I33tb0mb3r</a>    | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">www.duzceshcek.gov.tr</a>              | Win 2003 | <a href="#">mirror</a> |
| <a href="#">Logic</a>         |   | <a href="#">alumni.cttc.gov.in</a>                 | Linux    | <a href="#">Mirror</a> |
| <a href="#">Mahesh Haxor</a>  | <a href="#">k9 Network Cyber Army</a>   | <a href="#">tnvkpmis.gov.in/mihawk.html</a>        | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">Mihawkeye Lhc</a> | <a href="#">Lanunhitam Crews</a>        | <a href="#">dns.zjwst.gov.cn/mihawk.html</a>       | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">Mihawkeye Lhc</a> | <a href="#">Lanunhitam Crews</a>        | <a href="#">tks.ylgt.gov.cn/mihawk.html</a>        | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">Mihawkeye Lhc</a> | <a href="#">Lanunhitam Crews</a>        | <a href="#">scrbbihar.gov.in</a>                   | Linux    | <a href="#">mirror</a> |
| <a href="#">MindCracker</a>   |   | <a href="#">askswapnil.co.in</a>                   | Linux    | <a href="#">Mirror</a> |
| <a href="#">MindCracker</a>   | <a href="#">PakCyberArmy</a>            | <a href="#">nbrri.gov.ng</a>                       | Linux    | <a href="#">Mirror</a> |
| <a href="#">mOk</a>           | <a href="#">Myanmar Hackers Unite4m</a> | <a href="#">www.issq.gov.co</a>                    | Linux    | <a href="#">mirror</a> |
| <a href="#">mr.hard</a>       |   | <a href="#">www.a2k.co.in</a>                      | Linux    | <a href="#">Mirror</a> |
| <a href="#">NeoHaxor</a>      | <a href="#">Pakistan Cyber Army</a>     | <a href="#">www.westexpress.in/Nilux.htm</a>       | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">tanwarpackersandmovers.in</a>          | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">ssigroup.co.in/Nilux.htm</a>           | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">softnic.in/Nilux.htm</a>               | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">sipackers.in/Nilux.htm</a>             | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">sikarkhandal.in/Nilux.htm</a>          | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">shadesbeauty.in/Nilux.htm</a>          | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">rkinternationalschool.in/Nilux.htm</a> | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">richwebtechnology.co.in/Nilux.htm</a>  | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">paramhiteshi.in/Nilux.htm</a>          | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">organicvillage.in/Nilux.htm</a>        | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">netcomcollege.in/Nilux.htm</a>         | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">multirc.in/Nilux.htm</a>               | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">metropipes.in/Nilux.htm</a>            | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">krishnainfosolution.in/Nilux.htm</a>   | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">jdbcollege.ac.in/Nilux.htm</a>         | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">jainprakashanmandir.in/Nilux.htm</a>   | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">ipsbapora.in/Nilux.htm</a>             | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">indiano1.in/Nilux.htm</a>              | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">indianlifescience.in/Nilux.htm</a>     | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">hotelchandralokk.co.in/Nilux.htm</a>   | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">hitechitsolutions.in/Nilux.htm</a>     | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">goyalpackers.in/Nilux.htm</a>          | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">dharmsena.in/Nilux.htm</a>             | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">jbengg.in/Nilux.htm</a>                | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">cdacatcrajusthan.in/Nilux.htm</a>      | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">agarwalvaishsamaj.in/Nilux.htm</a>     | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">vlart.in/Nilux.htm</a>                 | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">royalweddingcard.in/Nilux.htm</a>      | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">sara.org.in/Nilux.htm</a>              | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">incredibletechnosoft.in/Nilux.htm</a>  | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">sahityadarshan.in/Nilux.htm</a>        | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">holidayadventure.in/Nilux.htm</a>      | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>              | <a href="#">careworldwidebd.in/Nilux.htm</a>       | Win 2008 | <a href="#">Mirror</a> |

CIR

|                               |                                   |   |          |                        |
|-------------------------------|-----------------------------------|---|----------|------------------------|
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">indianhawk.in/Nilux.htm</a>           | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">primepropertiesindia.in/Nilux.htm</a> | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">nify.co.in/Nilux.htm</a>              | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">sktc.ac.in/Nilux.htm</a>              | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">rbid.in/Nilux.htm</a>                 | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">honeymoonparadise.in/Nilux.htm</a>    | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">creativeartdesign.in/Nilux.htm</a>    | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">vhmvision.in/Nilux.htm</a>            | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">orbitnet.co.in/Nilux.htm</a>          | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">mandelahouse.in/Nilux.htm</a>         | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">mandeepmarble.in/Nilux.htm</a>        | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">kyals.in/Nilux.htm</a>                | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">indigame.in/Nilux.htm</a>             | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">hvms.in/Nilux.htm</a>                 | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">emeraldqueen.in/Nilux.htm</a>         | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">earthstoneglobal.co.in/Nilux.htm</a>  | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">bharatvikas.co.in/Nilux.htm</a>       | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">aikf.in/Nilux.htm</a>                 | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">ambidextrous.in/Nilux.htm</a>         | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">rezai.in/Nilux.htm</a>                | Linux    | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">rathilawcollege.ac.in/Nilux.htm</a>   | Linux    | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">rac.ac.in/Nilux.htm</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">pca4u.in/Nilux.htm</a>                | Linux    | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">parees.co.in/Nilux.htm</a>            | Linux    | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">gpwashim.edu.in/Nilux.htm</a>         | Linux    | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">gcindia.co.in/Nilux.htm</a>           | Linux    | <a href="#">Mirror</a> |
| <a href="#">NinjaVirus</a>    | <a href="#">NinjaVirus</a>        | <a href="#">eemidwashim.in/Nilux.htm</a>          | Linux    | <a href="#">Mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">rd.yuehu.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">zx.yuehu.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">gtzy.fangzi.gov.cn/bb.html</a>        | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">aj.ahhs.gov.cn/bb.html</a>            | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">fgw.ahhs.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">ljt.ahhs.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">www.xiongxian.gov.cn/bb.html</a>      | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">xxgk.yizhou.gov.cn/bb.html</a>        | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">gxs.ahhs.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">whj2.ahhs.gov.cn/bb.html</a>          | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">sbt.ahhs.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">tc.ahhs.gov.cn/bb.html</a>            | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">tjj.ahhs.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">xzzx.ahhs.gov.cn/bb.html</a>          | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">sjj.ahhs.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">whj.ahhs.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">yjj.ahhs.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">forum.ahhs.gov.cn/bb.html</a>         | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">hfx.ahhs.gov.cn/bb.html</a>           | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">hm.ahhs.gov.cn/bb.html</a>            | Win 2003 | <a href="#">mirror</a> |
| <a href="#">NoEntry Phc</a>   |                                   | <a href="#">lx.ahhs.gov.cn/bb.html</a>            | Win 2003 | <a href="#">mirror</a> |
| <a href="#">P4K-CoMManDeR</a> | <a href="#">Team Cyber Switch</a> | <a href="#">deliverhome.in</a>                    | Linux    | <a href="#">Mirror</a> |
| <a href="#">P4K-CoMManDeR</a> | <a href="#">Team Cyber Switch</a> | <a href="#">shashidhar.co.in</a>                  | Linux    | <a href="#">Mirror</a> |
| <a href="#">P4K-CoMManDeR</a> | <a href="#">Team Cyber Switch</a> | <a href="#">vaatsalya.co.in</a>                   | Linux    | <a href="#">Mirror</a> |
| <a href="#">P4K-CoMManDeR</a> | <a href="#">Team Cyber Switch</a> | <a href="#">www.propertyindwarka.in</a>           | Linux    | <a href="#">Mirror</a> |
| <a href="#">P4K-CoMManDeR</a> | <a href="#">Team Cyber Switch</a> | <a href="#">flatsindwarka.in</a>                  | Linux    | <a href="#">Mirror</a> |
| <a href="#">P4K-CoMManDeR</a> | <a href="#">Team Cyber Switch</a> | <a href="#">gulel.in</a>                          | Linux    | <a href="#">Mirror</a> |
| <a href="#">P4K-CoMManDeR</a> | <a href="#">Team Cyber Switch</a> | <a href="#">housingtimes.in</a>                   | Linux    | <a href="#">Mirror</a> |
| <a href="#">P4K-CoMManDeR</a> | <a href="#">Team Cyber Switch</a> | <a href="#">kingsmenindia.in</a>                  | Linux    | <a href="#">Mirror</a> |
| <a href="#">P4K-CoMManDeR</a> | <a href="#">Team Cyber Switch</a> | <a href="#">nextnews.in</a>                       | Linux    | <a href="#">Mirror</a> |
| <a href="#">rEd X</a>         | <a href="#">3xp1r3 Cyber Army</a> | <a href="#">www.lakshmishree.in</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">rEd X</a>         | <a href="#">3xp1r3 Cyber Army</a> | <a href="#">www.gsts.co.in</a>                    | Linux    | <a href="#">Mirror</a> |
| <a href="#">rEd X</a>         | <a href="#">3xp1r3 Cyber Army</a> | <a href="#">logodesigning.org.in</a>              | Linux    | <a href="#">Mirror</a> |
| <a href="#">rEd X</a>         | <a href="#">3xp1r3 Cyber Army</a> | <a href="#">logodesigner.org.in</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">rEd X</a>         | <a href="#">3xp1r3 Cyber Army</a> | <a href="#">rnawebsoft.in/blog/</a>               | Linux    | <a href="#">Mirror</a> |

CIR

|                                       |   |  |          |                        |
|---------------------------------------|---|--|----------|------------------------|
| <a href="#">rEd X</a>                 | <a href="#">3xp1r3 Cyber Army</a>       | <a href="#">eventmanagementcompany.co.in</a>     | Linux    | <a href="#">Mirror</a> |
| <a href="#">rEd X</a>                 | <a href="#">3xp1r3 Cyber Army</a>       | <a href="#">dcon.gov.np</a>                      | Linux    | <a href="#">Mirror</a> |
| <a href="#">rEd X</a>                 | <a href="#">3xp1r3 Cyber Army</a>       | <a href="#">www.centralchronicle.in/myfiles/</a> | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">rEd X</a>                 | <a href="#">3xp1r3 Cyber Army</a>       | <a href="#">mbmc.co.in</a>                       | Linux    | <a href="#">Mirror</a> |
| <a href="#">S.O.A T34m</a>            |   | <a href="#">www.quarantinedomestic.gov.au</a>    | Linux    | <a href="#">mirror</a> |
| <a href="#">sahrawihacker</a>         |   | <a href="#">nepalntp.gov.np</a>                  | Linux    | <a href="#">mirror</a> |
| <a href="#">sahrawihacker</a>         |   | <a href="#">opmcm.gov.np/index.htm</a>           | Linux    | <a href="#">mirror</a> |
| <a href="#">Sanji Lhc</a>             | <a href="#">Lanunhitam Crews</a>        | <a href="#">id-production.co.il/z.txt</a>        | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">Sanji Phc</a>             | <a href="#">PhantomCrews</a>            | <a href="#">www.jsw.in/sanji.html</a>            | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">Saudi - Hack</a>          |   | <a href="#">alcaldiadematurin.gob.ve</a>         | Linux    | <a href="#">mirror</a> |
| <a href="#">Sizzling Soul</a>         | <a href="#">Pak Cyber Army</a>          | <a href="#">mtc.gov.ph/joomla/images/SS.php</a>  | Win 2008 | <a href="#">Mirror</a> |
| <a href="#">Striker</a>               | <a href="#">PAK MAD HUNTERS</a>         | <a href="#">shivkripa.co.in</a>                  | Linux    | <a href="#">Mirror</a> |
| <a href="#">Striker</a>               | <a href="#">PAK MAD HUNTERS</a>         | <a href="#">www.freeclassified.net.in</a>        | Linux    | <a href="#">Mirror</a> |
| <a href="#">syrian_dragon</a>         |   | <a href="#">blog.doc-dc.gov.sy/x.txt</a>         | Win 2008 | <a href="#">mirror</a> |
| <a href="#">syrian_dragon</a>         |   | <a href="#">doc-dc.gov.sy/blog/x.txt</a>         | Win 2008 | <a href="#">mirror</a> |
| <a href="#">The UnderTaker</a>        |   | <a href="#">www.dtop.gov.pr/noticias.asp</a>     | Win 2003 | <a href="#">mirror</a> |
| <a href="#">ulow</a>                  |   | <a href="#">fwpt.larkjsw.gov.cn/a.txt</a>        | Win 2003 | <a href="#">mirror</a> |
| <a href="#">VirusDuba</a>             |   | <a href="#">rizeram.gov.tr</a>                   | Linux    | <a href="#">mirror</a> |
| <a href="#">walangkaji</a>            | <a href="#">The Crows Crew</a>          | <a href="#">www.satyamdausa.in</a>               | Linux    | <a href="#">Mirror</a> |
| <a href="#">walangkaji</a>            | <a href="#">The Crows Crew</a>          | <a href="#">www.richaworldtravels.in</a>         | Linux    | <a href="#">Mirror</a> |
| <a href="#">walangkaji</a>            | <a href="#">The Crows Crew</a>          | <a href="#">bizwebsite.in</a>                    | Linux    | <a href="#">Mirror</a> |
| <a href="#">White Hat</a>             | <a href="#">Shabab Hacker</a>           | <a href="#">www.thiqarinvest.gov.iq/news.php</a> | Linux    | <a href="#">Mirror</a> |
| <a href="#">xr00tx</a>                | <a href="#">sund4nyM0uz Corporation</a> | <a href="#">mixus.in</a>                         | Linux    | <a href="#">Mirror</a> |
| <a href="#">Yassine fajraoui</a>      |   | <a href="#">thanhdovanvinh.gov.vn</a>            | Linux    | <a href="#">mirror</a> |
| <a href="#">ynR !</a>                 | <a href="#">ynR !</a>                   | <a href="#">www.etze.co.il</a>                   | Linux    | <a href="#">Mirror</a> |
| <a href="#">ynR !</a>                 | <a href="#">ynR !</a>                   | <a href="#">www.filmind.co.il/index.php</a>      | Linux    | <a href="#">Mirror</a> |
| <a href="#">ynR !</a>                 | <a href="#">ynR !</a>                   | <a href="#">limanskiy.in.ua</a>                  | Linux    | <a href="#">Mirror</a> |
| <a href="#">ynR !</a>                 | <a href="#">ynR !</a>                   | <a href="#">www.seafarers.edu.in</a>             | Linux    | <a href="#">Mirror</a> |
| <a href="#">ynR !</a>                 | <a href="#">ynR !</a>                   | <a href="#">www.dprneuquen.gov.ar</a>            | Linux    | <a href="#">Mirror</a> |
| <a href="#">ynR !</a>                 | <a href="#">ynR !</a>                   | <a href="#">www.denr.gov.ph</a>                  | Linux    | <a href="#">Mirror</a> |
| <a href="#">ynR !</a>                 | <a href="#">ynR !</a>                   | <a href="#">www.dotc.gov.ph/images/ynr.php</a>   | Linux    | <a href="#">Mirror</a> |
| <a href="#">ZARYAB HAXOR</a>          | <a href="#">P4K!\$74N H4X0R\$</a>       | <a href="#">webnimbus.in</a>                     | Linux    | <a href="#">Mirror</a> |
| <a href="#">ZARYAB HAXOR</a>          | <a href="#">P4K!\$74N H4X0R\$</a>       | <a href="#">wrma.in</a>                          | Linux    | <a href="#">Mirror</a> |
| <a href="#">ZCompany Hacking Crew</a> | <a href="#">ZHC</a>                     | <a href="#">sapnet.gov.in/index.htm</a>          | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">ZCompany Hacking Crew</a> | <a href="#">ZHC</a>                     | <a href="#">vrschool.in/home.htm</a>             | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">ZCompany Hacking Crew</a> | <a href="#">ZHC</a>                     | <a href="#">countryoven.in/home.htm</a>          | Win 2003 | <a href="#">Mirror</a> |
| <a href="#">ZCompany Hacking Crew</a> | <a href="#">ZHC</a>                     | <a href="#">biosyn.in/home.htm</a>               | Win 2003 | <a href="#">Mirror</a> |



## CIR

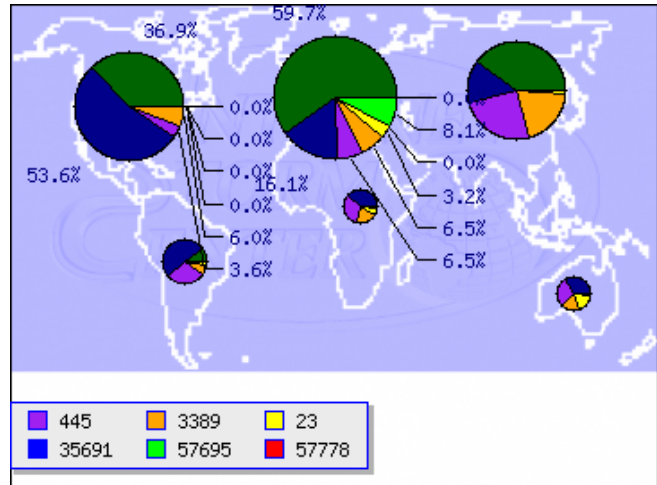
## Top Attackers of all time: Zone-H

| N° | Notifier                                       | Single def. | Mass def. | Total def. | Homepage def. | Subdir def. |
|----|--|-------------|-----------|------------|---------------|-------------|
| 1  | <a href="#">Barbaros-DZ</a>                    | 3167        | 156       | 3323       | 985           | 2338        |
| 2  | <a href="#">Ashiyane Digital Security Team</a> | 2486        | 3220      | 5706       | 1045          | 4661        |
| 3  | <a href="#">Hmei7</a>                          | 2054        | 1168      | 3222       | 700           | 2522        |
| 4  | <a href="#">LatinHackTeam</a>                  | 1428        | 1276      | 2704       | 2254          | 450         |
| 5  | <a href="#">iskorpitx</a>                      | 1322        | 953       | 2275       | 784           | 1491        |
| 6  | <a href="#">Fatal Error</a>                    | 1017        | 1127      | 2144       | 1764          | 380         |
| 7  | <a href="#">chinahacker</a>                    | 878         | 1309      | 2187       | 4             | 2183        |
| 8  | <a href="#">MCA-CRB</a>                        | 851         | 621       | 1472       | 367           | 1105        |
| 9  | <a href="#">By_aGReSiF</a>                     | 747         | 1424      | 2171       | 802           | 1369        |
| 10 | <a href="#">3n_byt3</a>                        | 621         | 1808      | 2429       | 847           | 1582        |
| 11 | <a href="#">HEXB00T3R</a>                      | 603         | 630       | 1233       | 405           | 828         |
| 12 | <a href="#">Red Eye</a>                        | 579         | 1551      | 2130       | 2093          | 37          |
| 13 | <a href="#">uykusuz001</a>                     | 534         | 146       | 680        | 34            | 646         |
| 14 | <a href="#">brwsk007</a>                       | 524         | 177       | 701        | 24            | 677         |
| 15 | <a href="#">Mafia Hacking Team</a>             | 496         | 589       | 1085       | 322           | 763         |
| 16 | <a href="#">Swan</a>                           | 494         | 258       | 752        | 219           | 533         |
| 17 | <a href="#">Digital Boys Underground Team</a>  | 461         | 441       | 902        | 179           | 723         |
| 18 | <a href="#">Iran Black Hats Team</a>           | 458         | 326       | 784        | 417           | 367         |
| 19 | <a href="#">1923Turk</a>                       | 417         | 1482      | 1899       | 415           | 1484        |
| 20 | <a href="#">DeltahackingSecurityTEAM</a>       | 415         | 443       | 858        | 232           | 626         |
| 21 | <a href="#">Over-X</a>                         | 399         | 1397      | 1796       | 1217          | 579         |
| 22 | <a href="#">D.O.M</a>                          | 392         | 645       | 1037       | 824           | 213         |
| 23 | <a href="#">kaMtiEz</a>                        | 391         | 390       | 781        | 238           | 543         |
| 24 | <a href="#">ZoRRoKiN</a>                       | 383         | 197       | 580        | 104           | 476         |
| 25 | <a href="#">Triad</a>                          | 375         | 315       | 690        | 397           | 293         |
| 26 | <a href="#">[#Elite Top Team]</a>              | 362         | 303       | 665        | 570           | 95          |
| 27 | <a href="#">sinaritx</a>                       | 359         | 98        | 457        | 160           | 297         |
| 28 | <a href="#">k4L0ng666</a>                      | 344         | 1203      | 1547       | 222           | 1325        |
| 29 | <a href="#">Ma3sTr0-Dz</a>                     | 313         | 735       | 1048       | 300           | 748         |
| 30 | <a href="#">core-project</a>                   | 313         | 325       | 638        | 629           | 9           |
| 31 | <a href="#">linuXploit_crew</a>                | 311         | 166       | 477        | 477           | 0           |
| 32 | <a href="#">misafir</a>                        | 295         | 297       | 592        | 214           | 378         |
| 33 | <a href="#">Turkish Energy Team</a>            | 275         | 212       | 487        | 292           | 195         |
| 34 | <a href="#">ISCN</a>                           | 272         | 123       | 395        | 96            | 299         |
| 35 | <a href="#">!nf3rN.4iL</a>                     | 262         | 376       | 638        | 176           | 462         |
| 36 | <a href="#">PoizonB0x</a>                      | 251         | 3         | 254        | 254           | 0           |
| 37 | <a href="#">NeT-DeViL</a>                      | 242         | 256       | 498        | 328           | 170         |
| 38 | <a href="#">eMP3R0r TEAM</a>                   | 239         | 306       | 545        | 136           | 409         |
| 39 | <a href="#">PowerDream</a>                     | 237         | 164       | 401        | 174           | 227         |
| 40 | <a href="#">Vezir.04</a>                       | 236         | 112       | 348        | 152           | 196         |
| 41 | <a href="#">KHG</a>                            | 233         | 281       | 514        | 210           | 304         |
| 42 | <a href="#">S4t4n1c_S0uls</a>                  | 230         | 144       | 374        | 311           | 63          |
| 43 | <a href="#">Hi-Tech Hate</a>                   | 223         | 6         | 229        | 229           | 0           |
| 44 | <a href="#">XTech Inc</a>                      | 223         | 328       | 551        | 548           | 3           |
| 45 | <a href="#">BeLa</a>                           | 210         | 123       | 333        | 147           | 186         |
| 46 | <a href="#">spook</a>                          | 209         | 31        | 240        | 40            | 200         |
| 47 | <a href="#">Prime Suspectz</a>                 | 205         | 0         | 205        | 205           | 0           |
| 48 | <a href="#">m0sted</a>                         | 201         | 206       | 407        | 98            | 309         |
| 49 | <a href="#">the freedom</a>                    | 198         | 136       | 334        | 22            | 312         |
| 50 | <a href="#">c4uR</a>                           | 191         | 383       | 574        | 397           | 177         |

## Internet Storm Center

### Top 10 Ports

| by Reports            |         | by Targets           |         | by Sources            |         |
|-----------------------|---------|----------------------|---------|-----------------------|---------|
| Port                  | Reports | Port                 | Targets | Port                  | Sources |
| <a href="#">53</a>    | 467953  | <a href="#">22</a>   | 72225   | <a href="#">445</a>   | 48801   |
| <a href="#">3389</a>  | 431037  | <a href="#">3389</a> | 71522   | <a href="#">3389</a>  | 16605   |
| <a href="#">445</a>   | 390658  | <a href="#">53</a>   | 71515   | <a href="#">23</a>    | 13410   |
| <a href="#">22</a>    | 307065  | <a href="#">80</a>   | 66633   | <a href="#">35691</a> | 10516   |
| <a href="#">23</a>    | 260200  | <a href="#">443</a>  | 65400   | <a href="#">57695</a> | 7384    |
| <a href="#">443</a>   | 210482  | <a href="#">23</a>   | 62508   | <a href="#">57778</a> | 7221    |
| <a href="#">80</a>    | 172267  | <a href="#">1433</a> | 57826   | <a href="#">57662</a> | 7132    |
| <a href="#">1433</a>  | 138791  | <a href="#">445</a>  | 45345   | <a href="#">57694</a> | 4772    |
| <a href="#">57695</a> | 97972   | <a href="#">3306</a> | 41717   | <a href="#">57692</a> | 4720    |
| <a href="#">57778</a> | 89941   | <a href="#">8080</a> | 35251   | <a href="#">47625</a> | 4475    |



### Top 10 Source IPs

| IP Address                           | Reports   | Attacks | First Seen                 | Last Seen                  |
|--------------------------------------|-----------|---------|----------------------------|----------------------------|
| <a href="#">069.175.126.170</a> (US) | 1,111,973 | 136,648 | <a href="#">2012-07-11</a> | <a href="#">2012-10-10</a> |
| <a href="#">037.009.053.002</a> (RU) | 929,050   | 131,926 | <a href="#">2012-09-12</a> | <a href="#">2012-10-10</a> |
| <a href="#">222.043.097.006</a> (CN) | 299,991   | 118,153 | <a href="#">2012-06-27</a> | <a href="#">2012-10-10</a> |
| <a href="#">060.174.198.082</a> (CN) | 264,951   | 93,439  | <a href="#">2012-10-09</a> | <a href="#">2012-10-09</a> |
| <a href="#">061.147.068.211</a> (CN) | 519,986   | 92,188  | <a href="#">2012-09-02</a> | <a href="#">2012-10-10</a> |
| <a href="#">221.195.083.181</a> (CN) | 85,375    | 82,488  | <a href="#">2012-09-14</a> | <a href="#">2012-10-09</a> |
| <a href="#">204.114.051.151</a> (US) | 81,415    | 81,400  | <a href="#">2012-07-07</a> | <a href="#">2012-10-09</a> |
| <a href="#">183.063.031.122</a> (CN) | 157,261   | 81,398  | <a href="#">2012-09-04</a> | <a href="#">2012-10-10</a> |
| <a href="#">220.225.004.021</a> (IN) | 456,814   | 78,952  | <a href="#">2012-09-14</a> | <a href="#">2012-10-10</a> |
| <a href="#">069.175.054.106</a> (US) | 1,340,819 | 78,613  | <a href="#">2012-07-14</a> | <a href="#">2012-10-10</a> |

### Resources:

|  |  |
|--|--|
| DC3 DISPATCH                           | <a href="mailto:dispatch@dc3.mil">dispatch@dc3.mil</a>                         |
| FBI In the New                         | <a href="mailto:fbi@subscriptions.fbi.gov">fbi@subscriptions.fbi.gov</a>       |
| Zone-h                                 | <a href="http://www.zone-h.org">www.zone-h.org</a>                             |
| Xssed                                  | <a href="http://www.xssed.com">www.xssed.com</a>                               |
| Packet Storm Security                  | <a href="http://www.packetstormsecurity.org">www.packetstormsecurity.org</a>   |
| Sans Internet Storm Center             | <a href="http://isc.sans.org">isc.sans.org</a>                                 |
| Exploit Database                       | <a href="http://www.exploit-db.com">www.exploit-db.com</a>                     |
| Exploits Database                      | <a href="http://www.exploitsdownload.com">www.exploitsdownload.com</a>         |
| Islamic Republic of Iran Security Team | <a href="http://irist.ir">irist.ir</a>   |
| Hack-DB                                | <a href="http://www.hack-db.com">www.hack-db.com</a>                           |
| Infragard                              | <a href="http://www.infragard.org">www.infragard.org</a>                       |
| ISSA                                   | <a href="http://www.issa.org">www.issa.org</a>                                 |
| Information Warfare Center             | <a href="http://informationwarfarecenter.com">informationwarfarecenter.com</a> |

If you do not want to receive future emails from us, contact [remove@informationwarfarecenter.com](mailto:remove@informationwarfarecenter.com)