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

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 Nitol 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.

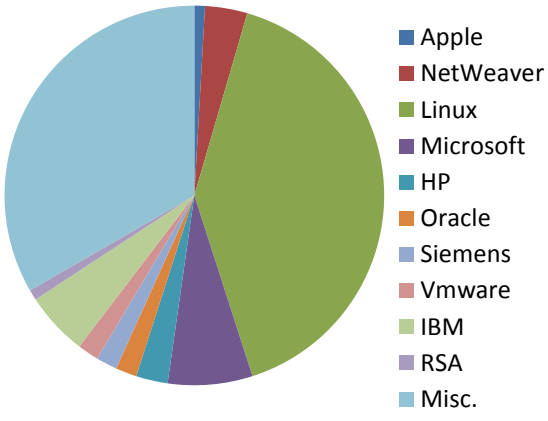
In 2010, 6 out of the top 7 Industrial Espionage cases, costing the United States hundreds of billions of dollars in damages, were found that either the Chinese government or Chinese industry was directly responsible for the loses. This doesn't even include the massive and well known Intellectual Property (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.

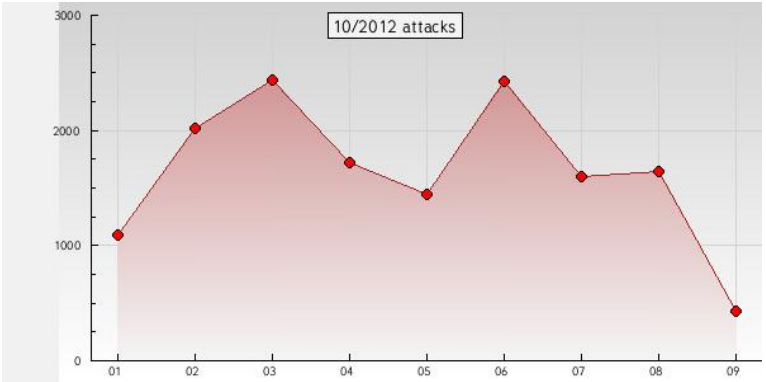
Section	Page	#
In the News	2	77
Papers	5	5
Discussions	NA	NA
Advisories	5	110
Tools released	16	8
Exploits published	17	54
Vulnerable websites	NA	NA
Websites defaced	18	342

Country	Gov't Defaced sites
United States	5
Australia	2
China	60
Mexico	3
Turkey	22
India	25
Brazil	16
Indonesia	3

OS defaced	#
Unix	NA
Linux	202
Unknown	NA
Windows	140

Alerts





In the news

China Focus

- Chinese Nitol 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 ramsomware 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

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

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.

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 Tunning 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 (icclib). 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 and 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

Hostapd versions 0.6 through 1.0 fail to validation 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

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:

- Conntrack 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

- 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

Websites Defaced:

Notifier		Domain	OS	View
@UGBrazil		setur.camacari.ba.gov.br	Linux	mirror
@UGBrazil		www.sefaz.camacari.ba.gov.br	Linux	mirror
@UGBrazil		www.seduc.camacari.ba.gov.br	Linux	mirror
@UGBrazil		sistemas.camacari.ba.gov.br	Linux	mirror
@UGBrazil		www.camacari.ba.gov.br	Linux	mirror
@UGBrazil		turismo.camacari.ba.gov.br	Linux	mirror
@UGBrazil		servidor.camacari.ba.gov.br	Linux	mirror
_Trish	Brazilian Cyber Army	www.skae.in	Linux	Mirror
3xp1r3_stAr	3xp1r3 Cyber Army	stemcellsbanking.in	Linux	Mirror
a.M.e		muftipahang.gov.my/v2/	Linux	mirror
Ablaze Ever	BD GREY HAT HACKERS	www.anjaneya.in/index.php	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	brightcastings.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	www.dfabs.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	www.htl.net.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	www.polyspin.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	www.precitron.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	sreebabafabrics.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	www.tnjb.net.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	www.ubpl.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	scrbbihar.gov.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	asipatnacircle.gov.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	www.cimpl.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	marina.gov.ph	Win 2008	Mirror
Ablaze Ever	BD GREY HAT HACKERS	www.maragondon.gov.ph	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	www.mpmat.unsyiah.ac.id	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	lms.rmutsb.ac.th	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	sttmandalabdg.ac.id	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	y3kimaginations.co.in	Linux	Mirror
Ablaze Ever	BD GREY HAT HACKERS	coolmobiles.co.in	Linux	Mirror
AL.MaX HaCkEr		nutrition.moh.gov.my/index.php	Linux	mirror
AL.MaX HaCkEr		hcameron.moh.gov.my/index.php	Linux	mirror
AL.MaX HaCkEr		www.ucrrhh.mendoza.gov.ar/	Linux	mirror
AL.MaX HaCkEr		www.comip.mendoza.gov.ar	Linux	mirror
ArTiN		jgdw.zjdx.gov.cn	Win 2003	mirror
ArTiN		skxxxh.zjdx.gov.cn/images/inde...	Win 2003	mirror
ArTiN		ltx.zjdx.gov.cn/images/index.htm	Win 2003	mirror
ArTiN		zzc.zjdx.gov.cn/themes/	Win 2003	mirror
ArTiN		pxb.zjdx.gov.cn/images/index.htm	Win 2003	mirror
ArTiN		dxcwc.zjdx.gov.cn/images/index...	Win 2003	mirror
ArTiN		fwzx.zjdx.gov.cn/images	Win 2003	mirror
ArTiN		jdzj.zjdx.gov.cn/images/index.htm	Win 2003	mirror
Ashiyane Digital Security Team		www.blogambiente.sp.gov.br/ind...	Win 2003	mirror
Ashiyane Digital Security Team		www.fflorestal.sp.gov.br/index...	Win 2003	mirror
bagsfreakz	Surabayahacker	www.pinlabs.unair.ac.id	Linux	Mirror
Bangladesh Cyber Army		agendaculturalsj.sc.gov.br/age...	Linux	mirror
Bangladesh Cyber Army		saogoncalodosapucai.mg.gov.br/..	Linux	mirror
Bangladesh Cyber Army		culturaeturismosj.sc.gov.br/Ji...	Linux	mirror
Bangladesh Cyber Army		teatro.ctpmsj.sc.gov.br/JingoB...	Linux	mirror
Bangladesh Cyber Army		cc.ctpmsj.sc.gov.br/JingoBD.html	Linux	mirror
Bangladesh Cyber Army		museu.ctpmsj.sc.gov.br/JingoBD..	Linux	mirror
Bangladesh Cyber Army		funesj.sc.gov.br/JingoBD.html	Linux	mirror
Barbaros-DZ		www.fcrk.gov.cn	Win 2003	mirror
Barbaros-DZ		ft.lzszs.gov.cn	Win 2003	mirror
Barbaros-DZ		jinyan.gdd.gov.cn/dz.htm	Win 2003	mirror
Barbaros-DZ		wh.yuanjiang.gov.cn	Win 2003	mirror
Barbaros-DZ		www.tszs.gov.cn/dz.htm	Win 2003	mirror
Barbaros-DZ		jsw.bynr.gov.cn/dz.htm	Win 2003	mirror
Barbaros-DZ		ls.yasgtzy.gov.cn	Win 2003	mirror
Barbaros-DZ		www.lywsjd.gov.cn/dz.htm	Win 2003	mirror
Barbaros-DZ		bbs.bzqts.gov.cn	Win 2008	mirror

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

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

IR-security		sipf.salud.gob.mx/l0rd.txt	Win 2000	mirror
Jack Riderr	Jack Riderr	ggfw.leiyang.gov.cn/	Win 2003	Mirror
Jean Frey	Wolf Enforced	www.narino.gov.co/media/	Linux	Mirror
k4L0ng666		centroaudiovisual.gob.ar/yenni...	Linux	mirror
k4L0ng666		centroaudiovisual.gov.ar/yenni...	Linux	mirror
l33tb0mb3r	Myanmar Hackers Unite4m	executivecoaching.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	olivecapital.in/readme.html	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	tafnet.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	www.poiema.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	onepoint.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	oliveconsulting.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	indiafacts.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	infovore.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	infobytes.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	lifequest.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	www.kindlebook.in/sk.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	www.christianlife.in/s.php	Linux	Mirror
l33tb0mb3r	Myanmar Hackers Unite4m	www.christianbook.in/s.php	Linux	Mirror
Logic		www.duzceshcek.gov.tr	Win 2003	mirror
Mahesh Haxor	k9 Network Cyber Army	alumni.cttc.gov.in	Linux	Mirror
Mihawkeye Lhc	Lanunhitam Crews	tnvkpmis.gov.in/mihawk.html	Win 2003	Mirror
Mihawkeye Lhc	Lanunhitam Crews	dns.zjwst.gov.cn/mihawk.html	Win 2003	Mirror
Mihawkeye Lhc	Lanunhitam Crews	tks.ylgt.gov.cn/mihawk.html	Win 2003	Mirror
MindCracker		scrbbihar.gov.in	Linux	mirror
MindCracker	PakCyberArmy	askswapnil.co.in	Linux	Mirror
mOk	Myanmar Hackers Unite4m	nbrri.gov.ng	Linux	Mirror
mr.hard		www.issq.gov.co	Linux	mirror
NeoHaxor	Pakistan Cyber Army	www.a2k.co.in	Linux	Mirror
NinjaVirus	NinjaVirus	www.westexpress.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	tanwarpackersandmovers.in	Win 2008	Mirror
NinjaVirus	NinjaVirus	ssigroup.co.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	softnic.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	sipackers.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	sikarkhandal.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	shadesbeauty.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	rkinternationalschool.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	richwebtechnology.co.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	paramhiteshi.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	organicvillage.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	netcomcollege.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	multirc.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	metropipes.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	krishnainfosolution.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	jdbcollege.ac.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	jainprakashanmandir.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	ipsbapora.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	indiano1.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	indianlifescience.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	hotelchandralokk.co.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	hitechitsolutions.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	goyalpackers.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	dharmsena.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	jbengg.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	cdacatcrajasthan.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	agarwalvaishsamaj.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	vlart.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	royalweddingcard.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	sara.org.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	incredibletechnosoft.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	sahityadarshan.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	holidayadventure.in/Nilux.htm	Win 2008	Mirror
NinjaVirus	NinjaVirus	careworldwidebd.in/Nilux.htm	Win 2008	Mirror

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

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

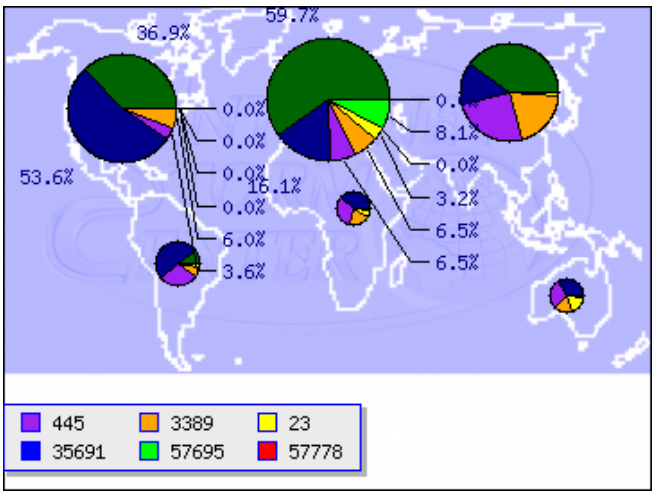
Top Attackers of all time: Zone-H

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

Internet Storm Center

Top 10 Ports

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



Top 10 Source IPs

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

Resources:

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