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 3, 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

October is **National Cyber Security Awareness Month 2012**

The defacements have settled down with the anti-American rhetoric in the messages, but the activity has remained steady in numbers with China again being the focus of the hacking community.

Cisco was a target for advisories this week with over 18 security warnings released. These vulnerabilities range from Denial of Service (DoS) to authentication bypass. Already a Cisco DoS has been released in the wild.

***Gotcha** .gov/.mil/.us – Domains have been notified…*

US Federal/State/Local government sites defaced/compromised this week (details later in this document).

- www.glenwillow-oh.gov, www.ypt-nsn.gov, esg.gsfc.nasa.gov, swag.sunnyvale.ca.gov
- access.co.johnson.in.us, ci.lumberton.nc.us, ci.sherwood.ar.us, co.johnson.in.us, jcpo.co.johnson.in.us

***Gotcha** .edu – Domains have been notified…*

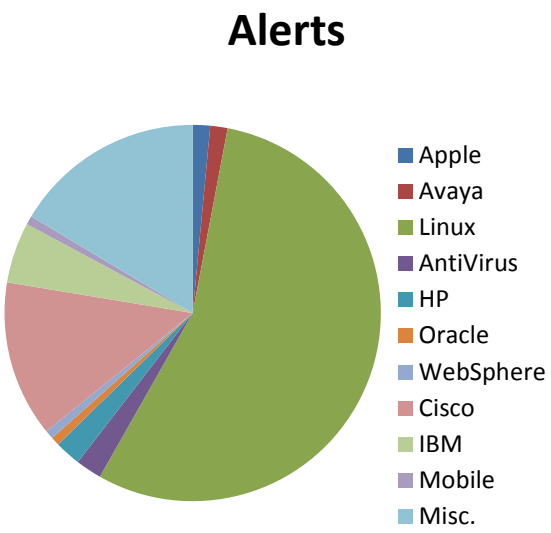
Higher educational sites defaced/compromised this week (details later in this document).

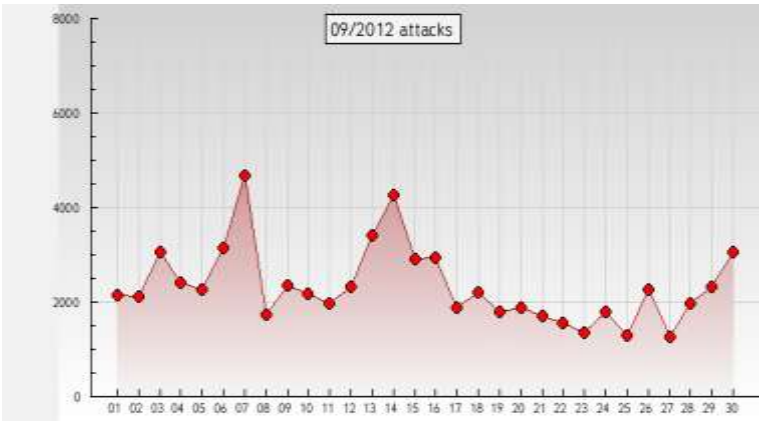
- alcpc1.psfc.mit.edu, reprobio.stanford.edu.

Section	Page	#
In the News	2	77
Papers	4	5
Discussions	0	NA
Advisories	4	136
Tools released	16	8
Exploits published	16	54
Vulnerable websites	NA	NA
Websites defaced	18	786

Country	Gov't Defaced sites
United States	5
Australia	19
China	118
Mexico	3
Turkey	26
India	42
South Korea	4
Indonesia	81

OS defaced	#
Unix	16
Linux	536
Unknown	11
Windows	205





In the news

Government

- Google Warning Targets Of State Sponsored Cyber Attacks
- Justice Department To Defend Warrantless Cell Phone Tracking
- Hackers Infiltrate US Government Nuclear Network
- Privacy Bill Requires Search Warrants for Email, Cell Tracking
- Researchers: Zombies Are Attacking America
- White House Confirms Cyber-Attack On Unclassified System
- White House Confirms Network Breach, Thwarted Attack
- White House Hack Attack
- US Cyber Warrior Accuses China of Targeting Pentagon
- Government Contractors Seeking Commercial Cyber Opportunities
- Government of Canada Launches Cyber Security Awareness Month
- Mikulski joins chorus calling for cybersecurity executive order
- European Security Agency Kicks Off Web Safety Campaign
- Australian Police Want Telco Customer Data Retained Forever
- The growing concern of cyber crime in Austria
- UN: More Should Be Done To Prevent Bio-Terrorism
- Megaupload Spying Case Brings New Zealand Apology
- California Passes Law To Stop Firm Social Networking Snooping
- Wells Fargo Hit By Cyber Attack Despite Industry Warnings
- FTC Stops Firms From Spying On Rented Computers
- Maker Of Smart-Grid Software Discloses Hack – SCADA
- Iran Pursues Stronger, More Restrictive Cyber Strategies
- APWG Hosts Unprecedented Global Coalition in Puerto Rico to Fight Cybercrime
- Government Agencies, Utilities Among Targets in 'VOHO' Cyber-Spy Attack

Security alerts

- DDoS attacks reach new level of sophistication
- DDoS Attacks: 150Gb Per Second And Rising
- Zombie-Animating Malnets Increase 300% In Just 6 Months
- Malware Distributor Handed $163m Fine For Scareware Operation
- Attackers Engage In False Flag Attack Manipulation
- White House Network Attack Highlights Need for Stronger Defenses
- Adobe Code Signing Infrastructure Hacked
- ElcomSoft Breaks Microsoft Office 2013 Passwords
- Hackers Breached Adobe Server in Order to Sign Their Malware
- Televents network security breached, customers warned - Times of India

Mobile

- Android Phone Wipeout Security Flaw Exposed
- Researcher Offers Quick Fix For Samsung Remote Wipe Vuln
- 5 Security Apps For Android Use
- Local Companys Mobile Forensics Help Investigations

News, Technologies and Techniques

- Hackers Leak 120,000 Student Records In Raid On World's Top Universities
- Microsoft Hits Agreement With Site Linked To Counterfeit Windows Botnet
- Cyber Security Awareness Month
- NIST Crowns Next-Gen Hash Algorithm Keccak As Official SHA-3
- Adobe Scrambles To Revoke Stolen Cert
- DotNet Project's Flawed Sample Code Has Crippling Auth Exploit
- Adobe unveils Acrobat XI with cloud services

News, Technologies and Techniques continued…

- IEEE Admits Password Leak, Says Problem Fixed
- New Java Flaw Could Hit 1 Billion Users
- Symantec Source Code Leak Becomes Torrent
- Researchers Claim Yet Another Vulnerability Exists In Java
- In Cyberattacks, Hacking Humans is Highly Effective
- SourceForge Mirror Cracked: phpMyAdmin Backdoored
- Facebook and Gates Foundation host education hackathon
- Security Hole Exposes Twitter Accounts To Hacking, Victim Claims
- Internet Explorer Shines in NSS Labs Browser Security Test
- Mozilla launches first beta version of Persona website authentication system
- Top Spear Phishing Email Phrases Revealed
- US and Russian experts turn up volume on cybersecurity alarms
- Simon Cowell And Will.i.am Plan A Technology X-Factor
- Replace Crypto-Couple Alice And Bob With Sita And Rama
- Bitcoin Foundation Vows To Clean Up Currency's Bad Rep
- Got A Data Security Policy? Chances Are Your IT Bods Don't Know It
- Contrast security plugin invisibly monitors applications during testing
- Free USSD exploit blocker app
- Tool prevents hackers from obtaining Android app source code
- Cyberspace presents significant challenges, UK FS Hague says ahead of Budapest Conference
- General: Nation needs DHS involved in cybersecurity
- KoolSpan, intiGrow Partner on Mobile Security
- Students will be doing vulnerability tests on security products at Iowa State Universitys new lab
- The case of the virtual detective and the missing Facebook chat
- The cyber debate goes public
- Coverity releases development testing platform
- As demand rises for cybersecurity professionals, so does their pay
- Companies seeking to train employees on cybersecurity
- Florida robotics lab working on real-life Robocop
- Pirate Bay founders detention extended amid tax hack probe
- Think tanks website rejects browser do-not-track requests
- Exploring cybercriminal minds, safeguarding privacy among $50M worth of new NSF projects

*** FBI news**

- Identity Theft that Lasted Decades
- Maryland Man Found Guilty in Manhattan Federal Court of Sex Trafficking and Transporting a Minor Interstate for the Purpose of Prostitution
- Judge Sentences Brentwood Man to 20 Years in Prison for Sextortion
- Batavia Man Arrested, Charged with Transporting a Minor to Engage in Sexual Activity
- Cleveland Woman Sentenced to 11 Years in Prison for Sex Trafficking of a Child
- Buffalo Man Pleads Guilty to Distribution of Child Pornography
- Schuylkill County Man Sentenced to 11 Years in Prison for Child Pornography Offense
- St. Francis Man Sentenced for Sexual Abuse of a Minor
- Colorado Man Sentenced for Coercion and Enticement of a Minor in Iowa to Engage in Unlawful Sexual Contact
- Oakland Pimp Pleads Guilty to Exploiting 14-Year-Old Girl in Sacramento and Stockton
- Claycomo Man Indicted for Receiving Child Pornography Over the Internet
- Youngwood Man Charged with Illegal Possession of Child Pornography
- North Versailles Man Admits Possessing Thousands of Pornographic Images of Children
- East Lansing Man Receives 20-Year Sentence for Trading Child Pornography

Papers:

- A Pentester's Guide To Hacking OData
- SinFP3 EuSecWest / Ekoparty Presentation
- CarolinaCon 2013 Call For Papers
- [Hebrew] Digital Whisper Security Magazine #36

Advisories for the week of October 3, 2012

Mobile

Secunia Security Advisory 50780

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

Apple

Apple Mac OS X Lion Arbitrary Code Execution

Andy Davis of NCC Group has discovered an arbitrary code execution vulnerability in Apple OS X Lion versions 10.7 to 10.7.4 and OS X Lion Server versions 10.7 to 10.7.4.

Secunia Security Advisory 50728

Secunia Security Advisory - Apple has acknowledged multiple vulnerabilities in Apple TV, which can be exploited by malicious people to disclose certain information, cause a DoS (Denial of Service), and compromise a user's device.

Avaya

Secunia Security Advisory 50827

Secunia Security Advisory - Avaya has acknowledged some vulnerabilities in Avaya Communication Server 1000, which can be exploited by malicious, local users to bypass certain security restrictions or cause a DoS (Denial of Service).

Secunia Security Advisory 50782

Secunia Security Advisory - Avaya has acknowledged multiple vulnerabilities in Avaya Communication Manager, which can be exploited by malicious users to disclose certain information and by malicious people to disclose potentially sensitive information, hijack a user's session, conduct DNS cache poisoning attacks, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

CA

Security Notice For CA License

CA Technologies Support is alerting customers to two potential risks in CA License (also known as CA Licensing). Vulnerabilities exist that can allow a local attacker to execute arbitrary commands or gain elevated access. CA Technologies has issued patches to address the vulnerabilities.

Cisco

Secunia Security Advisory 50775

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

Secunia Security Advisory 50776

Secunia Security Advisory - A vulnerability has been reported in Catalyst 4500E Series Switch, which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50777

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

Secunia Security Advisory 50779

Secunia Security Advisory - Two vulnerabilities have been reported in Cisco IOS, which can be exploited by malicious people to cause a DoS (Denial of Service).

Secunia Security Advisory 50778

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

Secunia Security Advisory 50774

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

Secunia Security Advisory 50771

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

Secunia Security Advisory 50773

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

Secunia Security Advisory 50772

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

Cisco Security Advisory 20120926-ecc

Cisco Security Advisory - The Catalyst 4500E series switch with Supervisor Engine 7L-E contains a denial of service (DoS) vulnerability when processing specially crafted packets that can cause a reload of the device. Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

Cisco Security Advisory 20120926-dhcp

Cisco Security Advisory - Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload. Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

Cisco Security Advisory 20120926-dhcpv6

Cisco Security Advisory - Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload. Cisco has released free software updates that address this vulnerability.

Cisco Security Advisory 20120926-c10k-tunnels

Cisco Security Advisory - Cisco IOS Software contains a queue wedge vulnerability that can be triggered when processing IP tunneled packets. Only Cisco IOS Software running on the Cisco 10000 Series router has been demonstrated to be affected. Successful exploitation of this vulnerability may prevent traffic from transiting the affected interfaces. Cisco has released free software updates that addresses this vulnerability. There are no workarounds for this vulnerability.

Cisco Security Advisory 20120926-nat

Cisco Security Advisory - The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets. The vulnerabilities are caused when packets in transit on the vulnerable device require translation. Cisco has released free software updates that address these vulnerabilities.

Cisco Security Advisory 20120926-bgp

Cisco Security Advisory - Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature. The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session. Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability.

Cisco Security Advisory 20120926-ios-ips

Cisco Security Advisory - Cisco IOS Software contains a vulnerability in the Intrusion Prevention System (IPS) feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if specific Cisco IOS IPS configurations exist. Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

Cisco Security Advisory 20120926-sip

Cisco Security Advisory - A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable. Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

Cisco Security Advisory 20120926-cucm

Cisco Security Advisory - Cisco Unified Communications Manager contains a vulnerability in its Session Initiation Protocol (SIP) implementation that could allow an unauthenticated, remote attacker to cause a critical service to fail, which could interrupt voice services. Affected devices must be configured to process SIP messages for this vulnerability to be exploitable. Cisco has released free software updates that address this vulnerability. A workaround exists for customers who do not require SIP in their environment.

Debian

Secunia Security Advisory 50763

Secunia Security Advisory - Debian has issued an update for iceape. 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 50761

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

Debian Security Advisory 2552-1

Debian Linux Security Advisory 2552-1 - Several vulnerabilities were discovered in Tiff, a library set and tools to support the Tag Image File Format (TIFF), allowing denial of service and potential privilege escalation.

Debian Security Advisory 2554-1

Debian Linux Security Advisory 2554-1 - Several vulnerabilities have been discovered in Iceape, an internet suite based on Seamonkey.

Debian Security Advisory 2550-2

Debian Linux Security Advisory 2550-2 - A regression in the SIP handling code was found in DSA-2550-1.

Secunia Security Advisory 50623

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

Gentoo

Gentoo Linux Security Advisory 201209-25

Gentoo Linux Security Advisory 201209-25 - Multiple vulnerabilities have been found in VMware Player, Server, and Workstation, allowing remote and local attackers to conduct several attacks, including privilege escalation, remote execution of arbitrary code, and a Denial of Service.

Gentoo Linux Security Advisory 201209-24

Gentoo Linux Security Advisory 201209-24 - Multiple vulnerabilities have been found in PostgreSQL which may allow a remote attacker to conduct several attacks. Versions less than 9.1.5 are affected.

Gentoo Linux Security Advisory 201209-23

Gentoo Linux Security Advisory 201209-23 - Multiple vulnerabilities have been found in GIMP, the worst of which allow execution of arbitrary code or Denial of Service. Versions less than 2.6.12-r2 are affected.

Gentoo Linux Security Advisory 201209-22

Gentoo Linux Security Advisory 201209-22 - A vulnerability in libgssglue may allow a local attacker to gain escalated privileges. Versions less than 0.4 are affected.

Gentoo Linux Security Advisory 201209-21

Gentoo Linux Security Advisory 201209-21 - Two directory traversal vulnerabilities have been found in fastjar, allowing remote attackers to create or overwrite arbitrary files. Versions less than 0.98-r1 are affected.

Secunia Security Advisory 50787

Secunia Security Advisory - Gentoo has issued an update for mod_rpaf. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service) in an application using the module.

Secunia Security Advisory 50700

Secunia Security Advisory - Gentoo has issued an update for postgresql-server. This fixes a weakness and multiple vulnerabilities, which can be exploited by malicious users to bypass certain security restrictions and by malicious people to conduct brute force and spoofing attacks, manipulate certain data, disclose certain sensitive information, and compromise a user's system.

Secunia Security Advisory 50785

Secunia Security Advisory - Gentoo has issued an update for libgssglue. This fixes a vulnerability, which can be exploited by malicious, local users to gain escalated privileges.

Secunia Security Advisory 50788

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

Secunia Security Advisory 50737

Secunia Security Advisory - Gentoo has issued an update for gimp. This fixes some vulnerabilities, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a user's system.

Secunia Security Advisory 50756

Secunia Security Advisory - Gentoo has issued an update for asterisk. This fixes multiple vulnerabilities, which can be exploited by malicious users to bypass certain security restrictions, cause a DoS (Denial of Service), and compromise a vulnerable system.

Gentoo Linux Security Advisory 201209-20

Gentoo Linux Security Advisory 201209-20 - A vulnerability in mod_rpaf may result in Denial of Service. Versions less than 0.6 are affected.

Gentoo Linux Security Advisory 201209-19

Gentoo Linux Security Advisory 201209-19 - A buffer overflow in NUT might allow remote attackers to execute arbitrary code. Versions less than 2.6.3 are affected.

Gentoo Linux Security Advisory 201209-18

Gentoo Linux Security Advisory 201209-18 - Multiple vulnerabilities have been found in Postfixadmin which may lead to SQL injection or cross-site scripting attacks. Versions less than 2.3.5 are affected.

Gentoo Linux Security Advisory 201209-17

Gentoo Linux Security Advisory 201209-17 - A buffer overflow in Pidgin might allow remote attackers to execute arbitrary code or cause Denial of Service. Versions less than 2.10.6 are affected.

Secunia Security Advisory 50757

Secunia Security Advisory - Gentoo has issued an update for sqlalchemy. This fixes two vulnerabilities, which can be exploited by malicious people to conduct SQL injection attacks.

Secunia Security Advisory 50731

Secunia Security Advisory - Gentoo has issued an update for postfixadmin. This fixes multiple vulnerabilities, which can be exploited by malicious users to conduct script insertion and SQL injection attacks and by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50781

Secunia Security Advisory - Gentoo has issued an update for pidgin. This fixes a vulnerability, which can be exploited by malicious people to compromise a user's system.

Gentoo Linux Security Advisory 201209-16

Gentoo Linux Security Advisory 201209-16 - An input sanitation flaw in SQLAlchemy allows remote attacker to conduct SQL injection. Versions less than 0.7.4 are affected.

Gentoo Linux Security Advisory 201209-15

Gentoo Linux Security Advisory 201209-15 - Multiple vulnerabilities have been found in Asterisk, the worst of which may allow execution of arbitrary code. Versions less than 1.8.15.1 are affected.

Gentoo Linux Security Advisory 201209-14

Gentoo Linux Security Advisory 201209-14 - A vulnerability in file could result in Denial of Service. Versions less than 5.11 are affected.

Gentoo Linux Security Advisory 201209-13

Gentoo Linux Security Advisory 201209-13 - A vulnerability in libjpeg-turbo could result in execution of arbitrary code or Denial of Service. Versions prior to 1.2.1 are affected.

Secunia Security Advisory 50733

Secunia Security Advisory - Oracle has acknowledged multiple vulnerabilities in OpenSSL included in Oracle SPARC Enterprise M Series, where one has unknown impacts and the others can be exploited by malicious people to conduct spoofing attacks, bypass certain security restrictions, or cause a DoS (Denial of Service).

Secunia Security Advisory 50739

Secunia Security Advisory - Gentoo has issued an update for libtasn1. This fixes a vulnerability, which can be exploited by malicious people to potentially compromise an application using the library.

Secunia Security Advisory 50740

Secunia Security Advisory - Gentoo has issued an update for opera. This fixes multiple vulnerabilities, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a user's system.

Gentoo Linux Security Advisory 201209-12

Gentoo Linux Security Advisory 201209-12 - A vulnerability in Libtasn1 might cause a Denial of Service condition. Versions less than 2.12 are affected.

Gentoo Linux Security Advisory 201209-11

Gentoo Linux Security Advisory 201209-11 - Multiple vulnerabilities have been found in Opera, the worst of which may allow remote execution of arbitrary code. Versions less than 12.01.1532 are affected.

Secunia Security Advisory 50753

Secunia Security Advisory - Gentoo has issued an update for libjpeg-turbo. This fixes a vulnerability, which can be exploited by malicious people to compromise an application using the library.

Secunia Security Advisory 50706

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

Secunia Security Advisory 50707

Secunia Security Advisory - Gentoo has issued an update for icu. This fixes a vulnerability, which potentially can be exploited by malicious people to compromise an application using the library.

Google Chrome

Secunia Security Advisory 50759

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

HP

HP Security Bulletin HPSBUX02814 SSRT100930

HP Security Bulletin HPSBUX02814 SSRT100930 - A potential security vulnerability has been identified with HP-UX OpenSSL. This vulnerability could be exploited remotely to create a Denial of Service (DoS). Revision 1 of this advisory.

HP Security Bulletin HPSBST02818 SSRT100960

HP Security Bulletin HPSBST02818 SSRT100960 - A potential security vulnerability has been identified with HP IBRIX X9000 Storage. The vulnerability could be remotely exploited to allow disclosure of information. Revision 1 of this advisory.

Secunia Security Advisory 50768

Secunia Security Advisory - HP has issued an update for OpenSSL in HP-UX. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service) of the application using the library.

IBM

Secunia Security Advisory 50708

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

Secunia Security Advisory 50806

Secunia Security Advisory - IBM has acknowledged some vulnerabilities in IBM Rational Synergy, which can be exploited by malicious people to conduct spoofing and cross-site scripting attacks, disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Secunia Security Advisory 50784

Secunia Security Advisory - IBM has acknowledged a weakness and a vulnerability in IBM Rational Change, which can be exploited by malicious people to conduct spoofing and cross-site scripting attacks.

Secunia Security Advisory 50764

Secunia Security Advisory - A security issue has been reported in IBM Rational ClearQuest, which can be exploited by malicious people to conduct spoofing attacks.

Secunia Security Advisory 50783

Secunia Security Advisory - IBM has acknowledged a security issue and a vulnerability in IBM Rational RequisitePro, which can be exploited by malicious people to conduct spoofing attacks and cause a DoS (Denial of Service).

Secunia Security Advisory 50767

Secunia Security Advisory - Some vulnerabilities have been reported in IBM WebSphere Commerce Enterprise, which can be exploited by malicious people to bypass certain security restrictions and cause a DoS (Denial of service).

Secunia Security Advisory 50738

Secunia Security Advisory - IBM has acknowledged a vulnerability in IBM Sterling Secure Proxy, which can be exploited by malicious people to cause a DoS (Denial of Service).

Mandriva

andriva Linux Security Advisory 2012-153-1

Mandriva Linux Security Advisory 2012-153 - ISC DHCP 4.1.x before 4.1-ESV-R7 and 4.2.x before 4.2.4-P2 allows remote attackers to cause a denial of service in opportunistic circumstances by establishing an IPv6 lease in an environment where the lease expiration time is later reduced. The updated packages have been patched to correct this issue.

Mandriva Linux Security Advisory 2012-155-1

Mandriva Linux Security Advisory 2012-155 - builtins.c in Xinetd before 2.3.15 does not check the service type when the tcpmux-server service is enabled, which exposes all enabled services and allows remote attackers to bypass intended access restrictions via a request to tcpmux port 1. The updated packages have been patched to correct this issue.

Mandriva Linux Security Advisory 2012-156

Mandriva Linux Security Advisory 2012-156 - The STARTTLS implementation in INN's NNTP server for readers, nnrpd, before 2.5.3 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted sessions by sending a cleartext command that is processed after TLS is in place, related to a plaintext command injection attack, a similar issue to CVE-2011-0411. The updated packages have been upgraded to inn 2.5.3 which is not vulnerable to this issue.

Mandriva Linux Security Advisory 2012-152-1

Mandriva Linux Security Advisory 2012-152 - A nameserver can be caused to exit with a REQUIRE exception if it can be induced to load a specially crafted resource record. The updated packages have been upgraded to bind 9.7.6-P3 which is not vulnerable to this issue.

Mandriva Linux Security Advisory 2012-154-1

Mandriva Linux Security Advisory 2012-154 - Multiple vulnerabilities has been found and corrected in apache. Insecure handling of LD_LIBRARY_PATH was found that could lead to the current working directory to be searched for DSOs. This could allow a local user to execute code as root if an administrator runs apachectl from an untrusted directory. Possible XSS for sites which use mod_negotiation and allow untrusted uploads to locations which have MultiViews enabled. The updated packages have been upgraded to the latest 2.2.23 version which is not vulnerable to these issues.

Mandriva Linux Security Advisory 2012-155

Mandriva Linux Security Advisory 2012-155 - builtins.c in Xinetd before 2.3.15 does not check the service type when the tcpmux-server service is enabled, which exposes all enabled services and allows remote attackers to bypass intended access restrictions via a request to tcpmux port 1. The updated packages have been patched to correct this issue.

Mandriva Linux Security Advisory 2012-154

Mandriva Linux Security Advisory 2012-154 - Multiple vulnerabilities has been found and corrected in apache. Insecure handling of LD_LIBRARY_PATH was found that could lead to the current working directory to be searched for DSOs. This could allow a local user to execute code as root if an administrator runs apachectl from an untrusted directory. Possible XSS for sites which use mod_negotiation and allow untrusted uploads to locations which have MultiViews enabled. The updated packages have been upgraded to the latest 2.2.23 version which is not vulnerable to these issues.

Oracle

Secunia Security Advisory 50746

Secunia Security Advisory - Oracle has acknowledged some vulnerabilities in Pidgin included in Solaris, which can be exploited by malicious, local users to disclose potentially sensitive information and by malicious people to cause a DoS (Denial of Service) and compromise a user's system.

Red Hat

Red Hat Security Advisory 2012-1325-01

Red Hat Security Advisory 2012-1325-01 - The rhev-hypervisor6 package provides a Red Hat Enterprise Virtualization Hypervisor ISO disk image. The Red Hat Enterprise Virtualization Hypervisor is a dedicated Kernel-based Virtual Machine hypervisor. A flaw was found in the way QEMU handled VT100 terminal escape sequences when emulating certain character devices. A guest user with privileges to write to a character device that is emulated on the host using a virtual console back-end could use this flaw to crash the qemu-kvm process on the host or, possibly, escalate their privileges on the host.

Red Hat Security Advisory 2012-1326-01

Red Hat Security Advisory 2012-1326-01 - FreeRADIUS is a high-performance and highly configurable free Remote Authentication Dial In User Service server, designed to allow centralized authentication and authorization for a network. A buffer overflow flaw was discovered in the way radiusd handled the expiration date field in X.509 client certificates. A remote attacker could possibly use this flaw to crash radiusd if it were configured to use the certificate or TLS tunnelled authentication methods.

Red Hat Security Advisory 2012-1323-01

Red Hat Security Advisory 2012-1323-01 - 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.

Red Hat Security Advisory 2012-1327-01

Red Hat Security Advisory 2012-1327-01 - FreeRADIUS is a high-performance and highly configurable free Remote Authentication Dial In User Service server, designed to allow centralized authentication and authorization for a network. A buffer overflow flaw was discovered in the way radiusd handled the expiration date field in X.509 client certificates. A remote attacker could possibly use this flaw to crash radiusd if it were configured to use the certificate or TLS tunnelled authentication methods.

Red Hat Security Advisory 2012-1324-01

Red Hat Security Advisory 2012-1324-01 - The rhev-hypervisor5 package provides a Red Hat Enterprise Virtualization Hypervisor ISO disk image. The Red Hat Enterprise Virtualization Hypervisor is a dedicated Kernel-based Virtual Machine hypervisor. 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 50765

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

Red Hat Security Advisory 2012-1304-01

Red Hat Security Advisory 2012-1304-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. An integer overflow flaw was found in the i915_gem_do_execbuffer() function in the Intel i915 driver in the Linux kernel. A local, unprivileged user could use this flaw to cause a denial of service. This issue only affected 32-bit systems. A memory leak flaw was found in the way the Linux kernel's memory subsystem handled resource clean up in the mmap() failure path when the MAP_HUGETLB flag was set. A local, unprivileged user could use this flaw to cause a denial of service.

Suse

Secunia Security Advisory 50828

Secunia Security Advisory - SUSE has issued an update for java-1_6_0-ibm. This fixes multiple vulnerabilities, which can be exploited by malicious, local users to disclose potentially sensitive data and by malicious people to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Secunia Security Advisory 50718

Secunia Security Advisory - SUSE has issued an update for postgresql and postgresql-libs. This fixes a weakness and two vulnerabilities, which can be exploited by malicious people to conduct brute force attacks, disclose certain sensitive information, and compromise a user's system.

Secunia Security Advisory 50754

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

Secunia Security Advisory 50723

Secunia Security Advisory - SUSE has issued an update for java-1_7_0-ibm. This fixes multiple vulnerabilities, which can be exploited by malicious, local users to disclose potentially sensitive data and by malicious people to disclose potentially sensitive information, manipulate certain data, cause a DoS (Denial of Service), and compromise a vulnerable system.

Symantec

Secunia Security Advisory 50824

Secunia Security Advisory - Symantec has acknowledged multiple vulnerabilities in Symantec Enterprise Vault, which can be exploited to malicious people to cause a DoS (Denial of Service) and compromise a vulnerable system.

Trend Micro

Secunia Security Advisory 50760

Secunia Security Advisory - A vulnerability has been reported in Trend Micro Control Manager, which can be exploited by malicious users to conduct SQL injection attacks.

Small-CMS 1.0 SQL Injection

Small-CMS version 1.0 suffers from authentication bypass and remote SQL injection vulnerabilities.

Ubuntu

Ubuntu Security Notice USN-1593-1

Ubuntu Security Notice 1593-1 - Raphael Geissert discovered that the debdiff.pl tool incorrectly handled shell metacharacters. If a user or automated system were tricked into processing a specially crafted filename, a remote attacher could possibly execute arbitrary code. Raphael Geissert discovered that the dscverify tool incorrectly escaped arguments to external commands. If a user or automated system were tricked into processing specially crafted files, a remote attacher could possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-1592-1

Ubuntu Security Notice 1592-1 - Niels Heinen discovered that the urllib and urllib2 modules would process Location headers that specify a redirection to file: URLs. A remote attacker could exploit this to obtain sensitive information or cause a denial of service. This issue only affected Ubuntu 11.04. It was discovered that SimpleHTTPServer did not use a charset parameter in the Content-Type HTTP header. An attacker could potentially exploit this to conduct cross-site scripting (XSS) attacks against Internet Explorer 7 users. This issue only affected Ubuntu 11.04. Various other issues were also addressed.

Ubuntu Security Notice USN-1591-1

Ubuntu Security Notice 1591-1 - Alec Warner discovered that xdiagnose improperly handled temporary files in welcome.py when creating user-initiated archive files. While failsafeX does not use the vulnerable code, this update removes this functionality to protect any 3rd party applications which import the vulnerable code. In the default Ubuntu installation, this should be prevented by the Yama link restrictions.

Ubuntu Security Notice USN-1589-1

Ubuntu Security Notice 1589-1 - It was discovered that positional arguments to the printf() family of functions were not handled properly in the GNU C Library. An attacker could possibly use this to cause a stack-based buffer overflow, creating a denial of service or possibly execute arbitrary code. It was discovered that multiple integer overflows existed in the strtod(), strtof() and strtold() functions in the GNU C Library. An attacker could possibly use this to trigger a stack-based buffer overflow, creating a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-1590-1

Ubuntu Security Notice 1590-1 - It was discovered that QEMU incorrectly handled certain VT100 escape sequences. A guest user with access to an emulated character device could use this flaw to cause QEMU to crash, or possibly execute arbitrary code on the host.

Ubuntu Security Notice USN-1588-1

Ubuntu Security Notice 1588-1 - It was discovered that the apt-add-repository tool incorrectly validated PPA GPG keys when importing from a keyserver. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to install altered package repository GPG keys.

Ubuntu Security Notice USN-1551-2

Ubuntu Security Notice 1551-2 - USN-1551-1 fixed vulnerabilities in Thunderbird. The new package caused a regression in the message editor and certain performance regressions as well. This update fixes the problems.

Secunia Security Advisory 50769

Secunia Security Advisory - Ubuntu has issued an update for transmission. This fixes two vulnerabilities, which can be exploited by malicious people to conduct script insertion attacks.

Secunia Security Advisory 50801

Secunia Security Advisory - Ubuntu has issued an update for emacs23. This fixes two vulnerabilities, which can be exploited by malicious people to compromise a user's system.

Secunia Security Advisory 50800

Secunia Security Advisory - Ubuntu has issued an update for libxml2. This fixes some vulnerabilities, 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 50786

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

Ubuntu Security Notice USN-1586-1

Ubuntu Security Notice 1586-1 - Hiroshi Oota discovered that Emacs incorrectly handled search paths. If a user were tricked into opening a file with Emacs, a local attacker could execute arbitrary Lisp code with the privileges of the user invoking the program. Paul Ling discovered that Emacs incorrectly handled certain eval forms in local-variable sections. If a user were tricked into opening a specially crafted file with Emacs, a remote attacker could execute arbitrary Lisp code with the privileges of the user invoking the program. Various other issues were also addressed.

Ubuntu Security Notice USN-1587-1

Ubuntu Security Notice 1587-1 - Juri Aedla discovered that libxml2 incorrectly handled certain memory operations. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause the application to crash or possibly execute arbitrary code with the privileges of the user invoking the program.

Secunia Security Advisory 50770

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

Ubuntu Security Notice USN-1585-1

Ubuntu Security Notice 1585-1 - Timo Warns discovered that FreeRADIUS incorrectly handled certain long timestamps in client certificates. A remote attacker could exploit this flaw and cause the FreeRADIUS server to crash, resulting in a denial of service, or possibly execute arbitrary code. The default compiler options for affected releases should reduce the vulnerability to a denial of service.

Ubuntu Security Notice USN-1584-1

Ubuntu Security Notice 1584-1 - Justin C. Klein Keane discovered that the Transmission web client incorrectly escaped certain strings. If a user were tricked into opening a specially crafted torrent file, an attacker could possibly exploit this to conduct cross-site scripting (XSS) attacks.

Secunia Security Advisory 50721

Secunia Security Advisory - Ubuntu has issued an update for rubygems. This fixes a security issue, which can be exploited by malicious people to conduct spoofing attacks.

Ubuntu Security Notice USN-1582-1

Ubuntu Security Notice 1582-1 - John Firebaugh discovered that the RubyGems remote gem fetcher did not properly verify SSL certificates. A remote attacker could exploit this to perform a man in the middle attack to alter gem files being downloaded for installation. John Firebaugh discovered that the RubyGems remote gem fetcher allowed redirection from HTTPS to HTTP. A remote attacker could exploit this to perform a man in the middle attack to alter gem files being downloaded for installation. Various other issues were also addressed.

Ubuntu Security Notice USN-1583-1

Ubuntu Security Notice 1583-1 - It was discovered that Ruby incorrectly allowed untainted strings to be modified in protective safe levels. An attacker could use this flaw to bypass intended access restrictions. John Firebaugh discovered that the RubyGems remote gem fetcher did not properly verify SSL certificates. A remote attacker could exploit this to perform a man in the middle attack to alter gem files being downloaded for installation. Various other issues were also addressed.

Secunia Security Advisory 50730

Secunia Security Advisory - Ubuntu has issued an update for ruby. This fixes a security issue and a vulnerability, which can be exploited by malicious people to conduct spoofing attacks and bypass certain security restrictions.

WebSphere

Secunia Security Advisory 50821

Secunia Security Advisory - A vulnerability has been reported in WebSphere Commerce, which can be exploited by malicious people to gain knowledge of sensitive information.

Misc

Secunia Security Advisory 50823

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

Secunia Security Advisory 50734

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

Secunia Security Advisory 50758

Secunia Security Advisory - A vulnerability has been reported in Tivoli Federated Identity Manager, which can be exploited by malicious people to bypass certain security restrictions.

Secunia Security Advisory 50755

Secunia Security Advisory - Some vulnerabilities have been reported in Rational Business Developer, which can be exploited by malicious people to conduct spoofing and cross-site scripting attacks and gain knowledge of potentially sensitive information.

Secunia Security Advisory 50830

Secunia Security Advisory - Oracle has acknowledged a security issue in IMPItool included in Solaris, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

Secunia Security Advisory 50789

Secunia Security Advisory - A vulnerability has been reported in Rational Team Concert, which can be exploited by malicious people to conduct cross-site request forgery attacks.

Secunia Security Advisory 50720

Secunia Security Advisory - Two security issues have been reported in the Organic groups module for Drupal, which can be exploited by malicious users to bypass certain security restrictions.

Secunia Security Advisory 50665

Secunia Security Advisory - Two vulnerabilities have been reported in OpenStack Keystone, which can be exploited by malicious people to bypass certain security restrictions.

Secunia Security Advisory 50702

Secunia Security Advisory - A security issue has been reported in openCryptoki, which can be exploited by malicious, local users to perform certain actions with escalated privileges.

Secunia Security Advisory 50762

Secunia Security Advisory - Two vulnerabilities have been discovered in the Multisite Plugin Manager plugin for WordPress, which can be exploited by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50647

Secunia Security Advisory - A security issue has been reported in Thomson TWG850 Cable Modem, which can be exploited by malicious people to bypass certain security restrictions.

Secunia Security Advisory 50510

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

Secunia Security Advisory 50766

Secunia Security Advisory - A security issue has been discovered in Smartfren Connex EC1261, which can be exploited by malicious, local users to gain escalated privileges.

Drupal Organic Groups 7.x Access Bypass

Drupal Organic Groups third party module version 7.x suffers from an access bypass vulnerability.

Secunia Security Advisory 50741

Secunia Security Advisory - A vulnerability has been reported in Cerberus FTP Server, which can be exploited by malicious people to conduct cross-site request forgery attacks.

Secunia Security Advisory 50714

Secunia Security Advisory - A vulnerability has been reported in JAMF Casper Suite, which can be exploited by malicious people to conduct cross-site request forgery attacks.

Secunia Security Advisory 50526

Secunia Security Advisory - Parvez Anwar has discovered a vulnerability in Foxit Reader, which can be exploited by malicious people to compromise a user's system.

Secunia Security Advisory 50711

Secunia Security Advisory - DigiP has reported a vulnerability in the Archin theme for WordPress, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a vulnerable system.

Secunia Security Advisory 50701

Secunia Security Advisory - Gjoko Krstic has discovered a vulnerability in ViArt Shop, which can be exploited by malicious people to compromise a vulnerable system.

Secunia Security Advisory 50608

Secunia Security Advisory - Scott Herbert has discovered a vulnerability in the ABC Test plugin for WordPress, which can be exploited by malicious people to conduct cross-site scripting attacks.

Secunia Security Advisory 50716

Secunia Security Advisory - Gjoko Krstic has discovered multiple vulnerabilities in ViArt Shop, which can be exploited by malicious users to conduct script insertion attacks.

Secunia Security Advisory 50713

Secunia Security Advisory - A vulnerability has been reported in 389 Directory Server, which can be exploited by malicious users to bypass certain security restrictions.

Tools released this week:

- Web Malware Collection
- Usernamer Login Information Generator
- 360-FAAR Firewall Analysis Audit And Repair 0.3.1
- AdSuck DNS Server 2.4.3
- Hashkill 0.3.0
- SinFP3 Fingerprinting Tool 1.00
- 360-FAAR Firewall Analysis Audit And Repair 0.3.0
- LFI Exploiter

Exploits released this week (9):

AlamFifa CMS 1.0 Beta SQL Injection

APlite Technologies Local File Inclusion

Archin WordPress Theme 3.2 Unauthenticated Configuration Access

Cisco DPC2100 Denial Of Service

CMS Balitbang Depdiknas 3.4 HTML Injection

Deadcow Design Local File Inclusion

DM FileManager Remote File Inclusion

Dream Ecommerce SQL Injection

Etoro.it Cross Site Scripting

Foxit Reader 5.4.3.0920 Division By Zero

FvS Groupmp3 CMS SQL Injection

GTA UTM Firewall GB 6.0.3 Cross Site Scripting

IBM Lotus Notes Traveler 8.5.3 XSS / CSRF / Brute Force

JAMF Casper Suite MDM Cross Site Request Forgery

JAMF Casper Suite MDM CSRF Vulnerability

Joomla FreiChat Shell Upload

LG NAS Used / Password Hash Disclosure

Mambo 4.6.4 Remote File Inclusion

MaxForum 2.0.0 Local File Inclusion

MediaRocket Local File Inclusion

Midori Browser 0.3.2 Denial Of Service

MS11-080 AfdJoinLeaf Privilege Escalation

OPlayer 2.0.05 iOS Cross Site Scripting

OSSEC WUI 0.3 Cross Site Scripting

PayPal Cross Site Scripting

phpFreeChat 1.4 Cross Site Scripting

phpMyAdmin 3.5.2.2 server_sync.php Backdoor

phptax 0.8 <= Remote Code Execution Vulnerability

ProjectPier 0.8.8 Shell Upload

QNX QCONN Remote Command Execution

Reaver Pro Livedisc Code Execution

Samba SetInformationPolicy AuditEventsInfo Heap Overflow

Smartfren Connex EC 1261-2 UI OUC Local Privilege Escalation

Smartfren Connex EC 1261-2 UI OUC Local Privilege Escalation Vulnerability

soapbox <= 0.3.1 Local Root Exploit

Soapbox 0.3.1 Local Root

Switchvox Asterisk 5.1.2 Cross Site Scripting

Symantec Messaging Gateway 9.5/9.5.1 SSH Default Password Security Bypass Vulnerability

Trend Micro Control Manager 5.5 / 6.0 Blind SQL Injection

Trend Micro Control Manager 5.5/6.0 AdHocQuery BlindSQL Injection (post-auth)

ViArt Shop Enterprise 4.1 Arbitrary Command Executio

ViArt Shop Enterprise 4.1 Arbitrary Command Execution Vulnerability

ViArt Shop Enterprise 4.1 Cross Site Scripting

ViArt Shop Evaluation 4.1 Remote File Inclusion

ViArt Shop Evaluation v4.1 Multiple Remote File Inclusion Vulnerabilities

Whereincity Cross Site Scripting

WordPress ABC-Test 0.1 Cross Site Scripting

WordPress Archin Theme Unauthenticated Configuration Access

WordPress Themes Book Cross Site Scripting

Xoops 2.3.2 Remote Code Execution

YingZhi Python 1.9 Arbitrary Traversal / Write

Zabbix 1.6.2 Remote Code Execution

DoS attacks (1):

Cisco DPC2100 Denial of Service

Foxit Reader 5.4.3.0920 Crash PoC

Websites Defaced:

Notifier - Hacker	Group Name	Domain	OS
$p!r!t~$33k3r	3xp1r3 Cyber Army	mhcbsl.in	Windows 2008
[Nyu]		cemeca.gob.ar	Linux
[Nyu]		www.ensenada.gov.ar	Linux
[Nyu]		www1.ensenada.gov.ar	Linux
3n_byt3		gclyxx.lncredit.gov.cn/hackye.txt	Win 2003
3thicalnoob		www.ctourism.oy.gov.ng/n00b.html	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	ekrishta.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	jextensions.co.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	nicinteriors.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	padmakumar.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	rosindia.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	seothiru.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	sevencolours.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	thegreenpearl.co.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	webrisers.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	www.pitchblack.in	Linux
3xp1r3_stAr	3xp1r3 Cyber Army	www.simhasolutions.in	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	agcss.edu.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	airpollutionsystem.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	ajayglass.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	amazingmakeovers.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	apex-properties.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	astralsoft.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	astroremedy.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	berry24x7.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	bestinterestrates.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	bigbits.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	bimalmehta.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	bollywoodcard.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	buildyourhome.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	care4animals.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	cashgiftcard.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	colorsnjewels.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	decorp.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	deltacorporation.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	demolab.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	distance-edu.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	dwh.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	eatzz.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	fbindustries.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	fedoriental.in/3ca.html	Linux

3xp1r3-b1gb0s$	3xp1r3 Cyber Army	flighttravel.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	fossacademy.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	fresio.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	globsol.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	googleconsultant.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	hatchcom.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	helpngo.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	holyheart.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	homaa.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	hopechildrenshome.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	iidc.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	indusarc.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	internetmark.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	internetprepaidcard.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	jeevansaralplan.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	kapishdiamonds.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	kiranawala.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	mackfall.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	mahavirimpex.net.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	marutijewelers.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	mbits.edu.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	mettletech.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	mettletechnologies.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	minestar.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	mrfoods.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	msecs.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	neilskitchen.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	oldisgold.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	orangecaterers.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	osavendita.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	pandeysworld.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	planetcomputers.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	plazahotels.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	pmexports.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	pressandmedia.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	presswell.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	rcadvertising.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	rdgemsjewellers.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	reachtones.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	redzebra.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	rmco.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	scotsecurity.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	search4cars.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	shatpathbrahmin.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	shreeramenterprise.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	shwe.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	smngroup.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	ssinteriors.in/3ca.html	Linux

3xp1r3-b1gb0s$	3xp1r3 Cyber Army	styleuhairparlour.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	sunabedapublicschool.edu.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	theblue.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	topbschools.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	treeshaktifilms.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	upcomingsales.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	vakpatitradecenter.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	valgrind.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	vgimpex.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	visaprepaidcard.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	vishwaexports.co.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	vmilan.in/3ca.html	Linux
3xp1r3-b1gb0s$	3xp1r3 Cyber Army	words4today.in/3ca.html	Linux
3xp1r3-v1Ru$	3xp1r3 Cyber Army	anoopweb.in	Linux
3xp1r3-v1Ru$	3xp1r3 Cyber Army	chattivenkateswarlu.co.in	Linux
3xp1r3-v1Ru$	3xp1r3 Cyber Army	creative-career.co.in	Linux
3xp1r3-v1Ru$	3xp1r3 Cyber Army	datakuteer.in	Linux
3xp1r3-v1Ru$	3xp1r3 Cyber Army	mcctindia.co.in	Linux
3xp1r3-v1Ru$	3xp1r3 Cyber Army	www.bluewaves.co.in	Linux
a.M.e		www.pa-sragen.go.id	Linux
Ablaze Ever	BD GREY HAT HACKERS	adi-harel.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	agadot.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	gowithyourheart.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	ohyeah.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	onelifeacademy.net.in	Linux
Ablaze Ever	BD GREY HAT HACKERS	orlaguf.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	parkinglots.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	picturethat.in	Linux
Ablaze Ever	BD GREY HAT HACKERS	raven.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	rhagolan.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	samim.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	smackmotion.in	Linux
Ablaze Ever	BD GREY HAT HACKERS	talital.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	windsurfingisrael.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.braingain.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.brandad.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.cardsdiary.in	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.depstroyzko.gov.kz	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.lemontree.org.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.parkingisrael.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.personeriavalledupar.gov.co	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.superfoodcooking.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.the3i.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.themepress.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.tzipilivni.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.wearelondoners.in	Linux
Ablaze Ever	BD GREY HAT HACKERS	www.webness.co.il	Linux
Ablaze Ever	BD GREY HAT HACKERS	zahava.co.il	Linux

AL.MaX HaCkEr		www.nationalregistration.gov.z...	Linux
AL.MaX HaCkEr		www.zambiaarmy.gov.zm//images/...	Linux
AL.MaX HaCkEr		www.zambiadscsc.gov.zm/images/...	Linux
Anon.India		bstdc.gov.in	Linux
Anonymous	INDISHELL	sdc.gov.pk/dfet.html	Windows 2008
ArTiN		ckm.kerala.gov.in/templates/in...	Unknown
ArTiN		dxcwc.zjdx.gov.cn/images/index...	Win 2003
ArTiN		fwzx.zjdx.gov.cn/images/index.htm	Win 2003
ArTiN		gok-delhi.kerala.gov.in/config...	FreeBSD
ArTiN		hed.kerala.gov.in/configuratio...	FreeBSD
ArTiN		ildm.kerala.gov.in/docs/index.htm	Unknown
ArTiN		jdzj.zjdx.gov.cn/images/index.htm	Win 2003
ArTiN		jgdw.zjdx.gov.cn	Win 2003
ArTiN		keri.kerala.gov.in/templates/i...	Unknown
ArTiN		ltx.zjdx.gov.cn/images/index.htm	Win 2003
ArTiN		minister-publicworks.kerala.go...	Unknown
ArTiN		patentcentre.kerala.gov.in/tem...	Unknown
ArTiN		peppara.kerala.gov.in/template...	Unknown
ArTiN		pxb.zjdx.gov.cn/images/index.htm	Win 2003
ArTiN		rdd-crd.kerala.gov.in/template...	Unknown
ArTiN		skxxxh.zjdx.gov.cn/images/inde...	Win 2003
ArTiN		texfed.kerala.gov.in/templates...	Unknown
ArTiN		tvmyouthhostel.kerala.gov.in/d...	Unknown
ArTiN		www.arari.gov.et	Linux
ArTiN		www.kscbc.kerala.gov.in/templa...	Unknown
ArTiN		zzc.zjdx.gov.cn/themes/	Win 2003
ArYaNZ_KhaN	VOBHH	cliniconline.in	Linux
ArYaNZ_KhaN	VOBHH	fileshub.in	Linux
Ashiyane Digital Security Team		admindev.cad.go.th/angola.html	Win 2003
Ashiyane Digital Security Team		amnatcharoen.cad.go.th/angola....	Win 2003
Ashiyane Digital Security Team		ccs.cad.go.th/templates/angola...	Win 2003
Ashiyane Digital Security Team		z.njxfy.gov.cn/hoss.htm	Win 2003
b4ckd00rMaaN	SIN	akugalau.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	aqad.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	bouncing.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	bouncing1.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	bouncing2.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	bouncing3.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	bouncing4.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	bouncing5.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	bouncing6.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	bouncing7.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	bouncing8.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	fpzi.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	fzyv.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	nua.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	owyz.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	qdi.ycfcglj.gov.cn/js/	Windows 2003

b4ckd00rMaaN	SIN	qvy.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	vboo.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	wrm.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	b4ckd00rMaaN	www.ts.lskjd.gov.cn/rebots.htm	Windows 2003
b4ckd00rMaaN	SIN	www.ycfcglj.gov.cn/js/	Windows 2003
b4ckd00rMaaN	SIN	zhll.ycfcglj.gov.cn/js/	Windows 2003
bagsfreakz	Surabayahacker	indomedis.com	Linux
Bangladesh Cyber Army	Bangladesh Cyber Army	alegria.gob.sv/rexo.html	Linux
Bangladesh Cyber Army		www.uphollandpc.gov.uk	Linux
Barbaros-DZ		basc.luzhou.gov.cn	Win 2003
Barbaros-DZ		bbs.hbjs.gov.cn	Win 2003
Barbaros-DZ		bj.yandu.gov.cn/article/dz.htm	Win 2003
Barbaros-DZ		bmjc.sysbmj.gov.cn	Win 2003
Barbaros-DZ		fl.tq.gov.cn	Win 2003
Barbaros-DZ		fzny.fangzi.gov.cn	Win 2003
Barbaros-DZ		gyyq.yongxin.gov.cn/dz.htm	Win 2003
Barbaros-DZ		hdws.hengdong.gov.cn	Win 2003
Barbaros-DZ		hld.lnzxw.gov.cn	Win 2003
Barbaros-DZ		kx.xzjw.gov.cn	Win 2003
Barbaros-DZ		msxxh.smeqd.gov.cn/dz.htm	Win 2003
Barbaros-DZ		rfb.xzjw.gov.cn	Win 2003
Barbaros-DZ		skl.huaihua.gov.cn	Win 2003
Barbaros-DZ		tks.ylgt.gov.cn	Win 2003
Barbaros-DZ		wsj.lhyc.gov.cn	Win 2003
Barbaros-DZ		www.bbstyj.gov.cn	Win 2003
Barbaros-DZ		www.bjmwr.gov.cn	Win 2003
Barbaros-DZ		www.ctlyj.gov.cn	Win 2003
Barbaros-DZ		www.czei.gov.cn	Win 2003
Barbaros-DZ		www.gdcz.gov.cn/dz.htm	Win 2003
Barbaros-DZ		www.jcgaj.gov.cn	Win 2003
Barbaros-DZ		www.jdylx.gov.cn	Win 2003
Barbaros-DZ		www.jrhealth.gov.cn/dz.htm	Win 2003
Barbaros-DZ		www.luyi.gov.cn	Win 2003
Barbaros-DZ		www.neixiang.gov.cn	Win 2003
Barbaros-DZ		www.pukouqswj.gov.cn	Win 2003
Barbaros-DZ		www.qyfzb.gov.cn	Win 2003
Barbaros-DZ		www.syip.gov.cn	Win 2003
Barbaros-DZ		www.tydj.gov.cn	Win 2003
Barbaros-DZ		www.ycsajj.gov.cn	Win 2003
Barbaros-DZ		www.ytws.gov.cn	Win 2003
Barbaros-DZ		www.yxhb.gov.cn	Win 2003
Barbaros-DZ		ycwjmw.yichun.gov.cn/dz.htm	Win 2003
Barbaros-DZ		ycxx.jmpj.gov.cn	Win 2003
Barbaros-DZ		zhuanti.zgts.gov.cn/dz.htm	Win 2003
Barbaros-DZ		zprd.zhp.gov.cn	Win 2003
Barbaros-DZ		zsj.ybja.gov.cn/dz.htm	Win 2003
BD GREY HAT HACKERS		bhoomi.kerala.gov.in/docs/cb.html	FreeBSD
BD GREY HAT HACKERS		medicalcouncil.kerala.gov.in/m...	FreeBSD

BD GREY HAT HACKERS		nedumbassery.kerala.gov.in	FreeBSD
BD GREY HAT HACKERS		www.ocagz.go.tz	Linux
BL4ckc0d1n6	BL4ckc0d1n6	ace8118.com	Linux
BL4ckc0d1n6	BL4ckc0d1n6	aceallianz.com	Linux
BL4ckc0d1n6	BL4ckc0d1n6	afari.info	Linux
BL4ckc0d1n6	BL4ckc0d1n6	bigbizproperties.info	Linux
BL4ckc0d1n6	BL4ckc0d1n6	donrnr.info	Linux
BL4ckc0d1n6	BL4ckc0d1n6	drsukida.info	Linux
BL4ckc0d1n6	BL4ckc0d1n6	euphrosyne.info	Linux
BL4ckc0d1n6	BL4ckc0d1n6	internetfundmachine.com	Linux
BL4ckc0d1n6	BL4ckc0d1n6	jasontan.info	Linux
BL4ckc0d1n6	BL4ckc0d1n6	killtech.info	Linux
BL4ckc0d1n6	BL4ckc0d1n6	leow.info	Linux
Black Angels		bpmpt.kuburayakab.go.id/IDN.html	Linux
Black Angels		kpmpt.pontianakkab.go.id/IDN.html	Linux
Black Angels		panwaslu.jabarprov.go.id/index...	FreeBSD
BlackHacker		www.museowixarika.mezquitic.go...	Linux
Blackshadow	Sund4nyM0uz Corporation	qx.xiangtan.gov.cn/ganteng.txt	Windows 2003
Blackshadow	Sund4nyM0uz Corporation	www.zzly.gov.cn/ganteng.txt	Windows 2003
Blackshadow	Sund4nyM0uz Corporation	z.njxfy.gov.cn/ganteng.txt	Windows 2003
brwsk007		www.dogansehir.gov.tr/gelendos...	Win 2008
brwsk007		www.trakyagumruk.gov.tr/fckdos...	Win 2003
Cr4ck-Br4iN	BD GREY HAT HACKERS	bhoomi.kerala.gov.in/docs/cb.html	Linux
Cr4ck-Br4iN	BD GREY HAT HACKERS	dslr.kerala.gov.in/ml/cb.html	Linux
Cr4ck-Br4iN	BD GREY HAT HACKERS	medicalcouncil.kerala.gov.in/modules/cb.html	Linux
Cr4ck-Br4iN	BD GREY HAT HACKERS	nedumbassery.kerala.gov.in	Linux
cyb3r snip3r	Anonymous Bangladesh	www.inversioneshjp.com.ve	Linux
Cyb3r.Bl@d3r	BD BLACK HAT	yogahouse.in	Linux
Cyb3rSec		ndc.gov.ng/robots.txt	Linux
Cyb3rSec		www.ns.gov.my/s.txt	Linux
Cybertaziex	-	atulk.in/x.html	Linux
Cybertaziex	-	beetalfinancial.in/x.html	Linux
Cybertaziex	-	bhagiratha.in/x.html	Linux
Cybertaziex	-	bhagiratha.org.in/x.html	Linux
Cybertaziex	-	codencoder.in/x.html	Linux
Cybertaziex	-	firstlook.co.in/x.html	Linux
Cybertaziex	-	ilookfirst.in/x.html	Linux
Cybertaziex	-	infratimes.in/x.html	Linux
Cybertaziex	-	iroot.in/x.html	Linux
Cybertaziex	-	medhini.co.in/x.html	Linux
Cybertaziex	-	mydoc.co.in/x.html	Linux
Cybertaziex	-	nst.net.in/x.html	Linux
Cybertaziex	-	onecare.in/x.html	Linux
Cybertaziex	-	onecare.org.in/x.html	Linux
Cybertaziex	-	onlinebuzz.in/x.html	Linux
Cybertaziex	-	raneja.in/x.html	Linux
Cybertaziex	-	sgps.in/x.html	Linux

Cybertaziex	-	shieldindiasecurity.in/x.html	Linux
Cybertaziex	-	shopbazaar.in/x.html	Linux
Cybertaziex	-	shopbazar.in/x.html	Linux
Cybertaziex	-	spectrumtech.in/x.html	Linux
Cybertaziex	-	ultraindia.co.in/x.html	Linux
Cybertaziex	-	ultraindia.in/x.html	Linux
Cybertaziex	-	vasanthosh.in/x.html	Linux
d3str0yers		honducor.gob.hn	Linux
d3str0yers		www.scad.gob.hn	Linux
DaiLexX		www.komunakallmet.gov.al	Linux
DaiLexX		www.vaudejes.gov.al	Linux
Dangerous		www.ncema.gov.ng	Linux
Dark Knight	AnonymousPakistan	abakus.co.in	Windows 2008
Dark Knight	AnonymousPakistan	firebolt.bitmesra.ac.in	Windows 2008
Dark Knight	AnonymousPakistan	tserv.in/r00t@3x3r00t.htm	Linux
Dbuzz		bkpm.nttprov.go.id/id.htm	Linux
Dbuzz		kupang2010.kab-kupang.go.id/db...	Linux
Dbuzz		kupangkab.go.id/id.htm	Linux
Dbuzz		www.englishweb.kab-kupang.go.i...	Linux
Dbuzz		www.kpde.kab-kupang.go.id	Linux
Dbuzz		www.newkab.kab-kupang.go.id/db...	Linux
Dbuzz		www.newreal.kab-kupang.go.id	Linux
DevilScreaM	ScreaM-Crew	nur-elghazy.ac.id/administrator/	Linux
DexteR		www.yokohama.com.tr	Win 2008
Dr.SHA6H		corcumvi.gov.co	Linux
Dr.SHA6H		cpgapuertosdelariari.gov.co	Linux
Dr.SHA6H		www.hospitalvillavicencio.gov.co	Linux
Dr.SHA6H		www.turismovillavicencio.gov.c...	Linux
Dr.SHA6H		www.villavicencio.gov.co	Linux
Dr.TaiGeR		micde.moai.gov.mm	Win 2008
Dr.TaiGeR		wrud.moai.gov.mm	Win 2008
Dr.Zir0	3xp1r3 Cyber Army	www.csds.in/index.php	Linux
Dr3@m3r~1986	3xp1r3 Cyber Army	4be.co.in/3ca.html	Linux
EpoolRoy	Wolf Enforced	www.elpis.co.in	Linux
Force Ex	Haxorsistz	inocar.mil.ec	Linux
Gabby	The Crows Crew	kytay.in.ua	Linux
gilang		kalianda.imigrasi.go.id	Linux
Golam Kibria	BD GREY HAT HACKERS	littlesewandsew.info	Linux
h311 c0d3		dns.com.eg	Linux
h311 c0d3		dns.eg	Linux
h311 c0d3		dns.net.eg	Linux
h311 c0d3		dns.org.eg	Linux
h311 c0d3		domain.com.eg	Linux
h311 c0d3		domain.eg	Linux
h311 c0d3		domain.net.eg	Linux
h311 c0d3		domain.org.eg	Linux
h311 c0d3		domains.com.eg	Linux
h311 c0d3		domains.eg	Linux

h311 c0d3	domains.net.eg	Linux
h311 c0d3	domains.org.eg	Linux
h311 c0d3	egdns.com.eg	Linux
h311 c0d3	eg-dns.com.eg	Linux
h311 c0d3	egdns.eg	Linux
h311 c0d3	eg-dns.eg	Linux
h311 c0d3	egdns.net.eg	Linux
h311 c0d3	eg-dns.net.eg	Linux
h311 c0d3	egdns.org.eg	Linux
h311 c0d3	eg-dns.org.eg	Linux
h311 c0d3	egdomain.com.eg	Linux
h311 c0d3	eg-domain.com.eg	Linux
h311 c0d3	egdomain.eg	Linux
h311 c0d3	eg-domain.eg	Linux
h311 c0d3	egdomain.net.eg	Linux
h311 c0d3	eg-domain.net.eg	Linux
h311 c0d3	egdomain.org.eg	Linux
h311 c0d3	eg-domain.org.eg	Linux
h311 c0d3	egdomains.com.eg	Linux
h311 c0d3	eg-domains.com.eg	Linux
h311 c0d3	egdomains.eg	Linux
h311 c0d3	eg-domains.eg	Linux
h311 c0d3	egdomains.net.eg	Linux
h311 c0d3	eg-domains.net.eg	Linux
h311 c0d3	egdomains.org.eg	Linux
h311 c0d3	eg-domains.org.eg	Linux
h311 c0d3	egtld.com.eg	Linux
h311 c0d3	eg-tld.com.eg	Linux
h311 c0d3	egtld.eg	Linux
h311 c0d3	eg-tld.eg	Linux
h311 c0d3	egtld.net.eg	Linux
h311 c0d3	eg-tld.net.eg	Linux
h311 c0d3	egtld.org.eg	Linux
h311 c0d3	eg-tld.org.eg	Linux
h311 c0d3	nic.com.eg	Linux
h311 c0d3	nic.eg	Linux
h311 c0d3	nic.net.eg	Linux
h311 c0d3	nic.org.eg	Linux
h311 c0d3	tld.com.eg	Linux
h311 c0d3	tld.eg	Linux
h311 c0d3	tld.net.eg	Linux
h311 c0d3	tld.org.eg	Linux
h4x0r HuSsY	clr.kerala.gov.in/docs/	FreeBSD
h4x0r HuSsY	envt.kerala.gov.in	FreeBSD
h4x0r HuSsY	kerams.kerala.gov.in	FreeBSD
h4x0r HuSsY	ksrrda.kerala.gov.in	FreeBSD
h4x0r HuSsY	neyyar.kerala.gov.in/templates/	FreeBSD
h4x0r HuSsY	slb.kerala.gov.in	FreeBSD

h4x0r HuSsY		www.biotechcommission.kerala.g...	FreeBSD
h4x0r HuSsY		www.spd.kerala.gov.in/docs/	FreeBSD
HacKed By LaMiN3 DK		analyse_srm.med.univ-tours.fr	Linux
HacKed By LaMiN3 DK		biostat.med.univ-tours.fr/inde...	Linux
HacKed By LaMiN3 DK		cic.med.univ-tours.fr/old/SITE...	Linux
HacKed By LaMiN3 DK		egsss.med.univ-tours.fr	Linux
HacKed By LaMiN3 DK		genomique.med.univ-tours.fr	Linux
HacKed By LaMiN3 DK		imagerie-pancreas.med.univ-tou...	Linux
HacKed By LaMiN3 DK		limesurvey.med.univ-tours.fr/i...	Linux
HacKed By LaMiN3 DK		microscopies.med.univ-tours.fr...	Linux
HacKed By LaMiN3 DK		mut2012.med.univ-tours.fr/logs...	Linux
HacKed By LaMiN3 DK		neuropediatrie.med.univ-tours.fr	Linux
HacKed By LaMiN3 DK		orl.med.univ-tours.fr	Linux
HacKed By LaMiN3 DK		ppf.med.univ-tours.fr	Linux
HacKed By LaMiN3 DK		psychetu.med.univ-tours.fr/these/	Linux
hacked by mo.bkafek hacker	hacked by mo.bkafek hacker	amd.moai.gov.mm	Linux
hacked by mo.bkafek hacker	hacked by mo.bkafek hacker	sd.moai.gov.mm	Linux
hacked by mo.bkafek hacker	hacked by mo.bkafek hacker	slrd.moai.gov.mm	Linux
hacked by mo.bkafek hacker	hacked by mo.bkafek hacker	wrud.moai.gov.mm	Linux
hacked by mo.bkafek hacker	hacked by mo.bkafek hacker	www.moai.gov.mm	Linux
hacked by mo.bkafek hacker	hacked by mo.bkafek hacker	yau.moai.gov.mm	Linux
Hacker Indonesia		sunda.garutkab.go.id/download_...	Linux
HackerMalaya	MALAYSIAN	www.nahrim.gov.my	Linux
hatrk		www.aacc.gov.et	Linux
hatrk		www.aacitymanager.gov.et/index...	Linux
hatrk		www.aafepra.gov.et/index.php	Linux
hatrk		www.aahdpo.gov.et	Linux
hatrk		www.aajs.gov.et	Linux
hatrk		www.aasc.gov.et	Linux
hatrk		www.aata.gov.et	Linux
hatrk		www.aictda.gov.et	Linux
hatrk		www.amharareg.gov.et	Linux
hatrk		www.amharasecurity.gov.et	Linux
hatrk		www.amra.gov.et	Linux
hatrk		www.anrsbolsa.gov.et	Linux
hatrk		www.arra.gov.et	Linux
hatrk		www.bowrd.gov.et	Linux
hatrk		www.dcadb.gov.et	Linux
hatrk		www.eiar.gov.et	Linux
hatrk		www.erta.gov.et	Linux
hatrk		www.fmhaca.gov.et/index.php	Linux
hatrk		www.gse.gov.et	Linux
hatrk		www.kahtamuftulugu.gov.tr	Linux
hatrk		www.modhd.gov.et	Linux
hatrk		www.ocacc.gov.et	Linux

hatrk		www.ococ.gov.et	Linux
hatrk		www.oromiaforest.gov.et	Linux
hatrk		www.pcdp.gov.et	Linux
hatrk		www.sictda.gov.et	Linux
HaXor Black	Bangladesh Altered Hackers Team (BAHT)	www.ssmce.ac.in	Linux
HaYaL-ET-06		izmirozelidare.gov.tr	Linux
HighTech		alcpc1.psfc.mit.edu	Win XP
HighTech		diperta.pamekasankab.go.id	Linux
HighTech		wokeyw.hnbys.gov.cn/index.html	Win 2003
HighTech		www.nacli.pa.gov.sg/tmp/index.php	Linux
HighTech		www.nyc.pa.gov.sg/tmp/index.php	Linux
HighTech		www.obs.pa.gov.sg/video/index.php	Linux
HighTech		zzdxxxw.hnbys.gov.cn/index.html	Win 2003
HighTech		zzdxyw.hnbys.gov.cn/index.html	Win 2003
Hmei7	Hmei7	access.co.johnson.in.us/x.htm	Win 2000
Hmei7	Hmei7	access.co.johnson.in.us/x.htm	Win 2000
Hmei7		aris.sc.gov.br	Linux
Hmei7		bmwhk.com/lifestyle/	Win 2008
Hmei7		camarafranciscomorato.sp.gov.b...	Linux
Hmei7		ciga.sc.gov.br/tmp/x.htm	Linux
Hmei7		intranet.salvadoratende.ba.gov...	Win 2003
Hmei7		labangan.gov.ph/x.htm	Linux
Hmei7		novaluzitania.sp.gov.br/x.htm	Linux
Hmei7		rfq.foxconn.com/x.htm	Win 2003
Hmei7		sdma.kerala.gov.in	Linux
Hmei7		shilpakala.gov.bd	Linux
Hmei7		site.tce.ma.gov.br/x.htm	Linux
Hmei7		sras.gov-madeira.pt/x.htm	Linux
Hmei7		telecom.unog.ch/x.htm	Linux
Hmei7		tnvkpmis.gov.in/x.htm	Win 2003
Hmei7		www.ans.gov.br/x.htm	Linux
Hmei7		www.bahia.salvador.ba.gov.br/x...	Win 2003
Hmei7		www.boletim.salvador.ba.gov.br...	Win 2003
Hmei7		www.ci.lumberton.nc.us/x.htm	Linux
Hmei7		www.ci.lumberton.nc.us/x.htm	Linux
Hmei7		www.ci.sherwood.ar.us/tmp/x.htm	Win 2003
Hmei7		www.ci.sherwood.ar.us/tmp/x.htm	Win 2003
Hmei7		www.cidadao.salvador.ba.gov.br...	Win 2003
Hmei7		www.cidadao2.salvador.ba.gov.b...	Win 2003
Hmei7		www.cidadessedes.salvador.ba.g...	Win 2003
Hmei7		www.co.johnson.in.us/x.htm	Win 2000
Hmei7		www.co.johnson.in.us/x.htm	Win 2000
Hmei7		www.conferenciamunicipal.salva...	Win 2003
Hmei7		www.copa.salvador.ba.gov.br/x.htm	Win 2003
Hmei7		www.coraldascriancas.salvador....	Win 2003
Hmei7		www.cra.salvador.ba.gov.br/x.htm	Win 2003
Hmei7		www.culturafgm.salvador.ba.gov...	Win 2003

Hmei7		www.demandas.educacao.salvador...	Win 2003
Hmei7		www.desal.salvador.ba.gov.br/x...	Win 2003
Hmei7		www.eventofinanciamento.salvad...	Win 2003
Hmei7		www.festivaldefogos.salvador.b...	Win 2003
Hmei7		www.financasetributos.salvador...	Win 2003
Hmei7		www.gestaopublica.salvador.ba....	Win 2003
Hmei7		www.guardamunicipal.salvador.b...	Win 2003
Hmei7		www.infraestrutura.salvador.ba...	Win 2003
Hmei7		www.intrasusprev.salvador.ba.g...	Win 2003
Hmei7		www.jcpo.co.johnson.in.us/x.htm	Win 2000
Hmei7		www.jcpo.co.johnson.in.us/x.htm	Win 2000
Hmei7		www.jovemaprendiz.salvador.ba....	Win 2003
Hmei7		www.ocomon.salvador.ba.gov.br/...	Win 2003
Hmei7		www.ondeestaseublocowap.salvad...	Win 2003
Hmei7		www.pc.es.gov.br/site/x.htm	Linux
Hmei7		www.previs.salvador.ba.gov.br/...	Win 2003
Hmei7		www.prodasal.salvador.ba.gov.b...	Win 2003
Hmei7		www.relacoesinternacionais.sal...	Win 2003
Hmei7		www.salvadoratende.ba.gov.br/x...	Win 2003
Hmei7		www.salvadorbarcelona.salvador...	Win 2003
Hmei7		www.secom.salvador.ba.gov.br/x...	Win 2003
Hmei7		www.secri.salvador.ba.gov.br/x...	Win 2003
Hmei7		www.sedam.ro.gov.br/x.htm	Linux
Hmei7		www.segurancaurbana.salvador.b...	Win 2003
Hmei7		www.servicospublicos.salvador....	Win 2003
Hmei7		www.sgdc.salvador.ba.gov.br/x.htm	Win 2003
Hmei7		www.sgo.salvador.ba.gov.br/x.htm	Win 2003
Hmei7		www.sigest.salvador.ba.gov.br/...	Win 2003
Hmei7		www.soe.salvador.ba.gov.br/x.htm	Win 2003
Indishell		www.dae.gov.bd	Linux
IR-Security		www.xinzhousafety.gov.cn/l0rd.htm	Win 2003
ISCN		educal.gob.mx	Linux
ISCN		pa-jakartatimur.go.id	Linux
ISCN		www.ccen.ufpb.br/biblioteca/in...	Linux
ISCN		www.hospitalclinicosanborjaarr...	Linux
islamic ghosts team		ilic.gov.tr/tmp/x.html	Linux
islamic ghosts team		kemahmuftulugu.gov.tr/tmp/x.html	Linux
Jack Riderr	Jack Riderr	gcly.lncredit.gov.cn/JohorHackingCrew.html	Windows 2003
Jas0nz666		childprotection.gov.gh	Linux
k4L0ng666		eaplikasi.keda.gov.my/esharing...	Linux
k4L0ng666		maydolong-esamar.gov.ph/robots...	Linux
kab[u]ss		daj.zhuzhou.gov.cn/imt.html	Win 2003
kab[u]ss		ymj.zhuzhou.gov.cn/imt.html	Win 2003
kingkill		rdhy.tlrd.gov.cn/king.html	Win 2003
kingkill		www.lntl.lm.gov.cn/king.html	Win 2003
kingkill		www.tielingws.gov.cn/king.html	Win 2003
kingkill		www.tlda.gov.cn/king.html	Win 2003
kingkill		www.tlfzb.gov.cn/king.html	Win 2003

kingkill		www.tljs.gov.cn/king.html	Win 2003
kingkill		www.tlnj.gov.cn/king.html	Win 2003
kingkill		www.tlsafety.gov.cn/king.html	Win 2003
kingkill		www.tlsghj.gov.cn/king.html	Win 2003
kingkill		www.tltyj.gov.cn/king.html	Win 2003
kingkill		www.tlxm.gov.cn/king.html	Win 2003
kingkill		www.tlzwgk.gov.cn/king.html	Win 2003
kingkill		www.tlzys.gov.cn/king.html	Win 2003
KmL!		saplee.go.th/index2.php	Linux
KurdHackTeaM		tesislerimiz.ibb.gov.tr/index....	Win 2003
LeTh_HaCkEr		www.shaqraedu.gov.sa/index1.php	Linux
LoSt.HaCkEr		depstroyzko.gov.kz	Linux
MagelangCyber		larkjsw.gov.cn/jundab.txt	Win 2003
MagelangCyber		www.tongcheng.jcy.gov.cn/junda...	Win 2003
MaX-HaCker	AnonymousPakistan	asominfo.in	Linux
MaX-HaCker	AnonymousPakistan	www.amtecindia.in	Linux
MaX-HaCker	AnonymousPakistan	www.fenzgard.co.in	Linux
MaX-HaCker	AnonymousPakistan	www.learningpoint.co.in	Linux
MaX-HaCker	AnonymousPakistan	www.royalweb.co.in	Linux
Mihawkeye Lhc	Lanunhitam Crews	daj.zhuzhou.gov.cn/mihawk.html	Windows 2003
Mihawkeye Lhc	Lanunhitam Crews	www.zcny.gov.cn/mihawk.html	Windows 2003
milanisti	Hacker Newbie Comunity	aceeranvankate.org	Linux
milanisti	Hacker Newbie Comunity	andix.info	Linux
milanisti	Hacker Newbie Comunity	intermediansk.ru	Linux
milanisti	Hacker Newbie Comunity	www.insomnestudi.com	FreeBSD
milanisti	Hacker Newbie Comunity	www.internews.kz	Linux
MindCracker	PakCyberArmy	ansalroyal-heritage.in/index.php	Linux
MindCracker	PakCyberArmy	bbscet.ac.in/index.php	Linux
MindCracker	PakCyberArmy	bbscet.in/index.php	Linux
MindCracker	PakCyberArmy	bbsimt.ac.in/index.php	Linux
MindCracker	PakCyberArmy	cosmicparkindia.in/index.php	Linux
MindCracker		en.pa-tangerangkota.go.id	Linux
MindCracker	PakCyberArmy	globelindustries.in/index.php	Linux
MindCracker	PakCyberArmy	indianaviationservices.com/index.php	Linux
MindCracker	PakCyberArmy	interadservices.com/index.php	Linux
MindCracker	PakCyberArmy	landmarkeon.in/index.php	Linux
MindCracker		m.pa-tangerangkota.go.id/index...	Linux
MindCracker	PakCyberArmy	nirala-estate.in/index.php	Linux
MindCracker	PakCyberArmy	nrrinstitute.co.in/index.php	Linux
MindCracker		pdg-sibusuk.sijunjung.go.id	Linux
MindCracker	PakCyberArmy	proximityswitches.in/index.php	Linux
MindCracker	PakCyberArmy	sairailwaysociety.in/index.php	Linux
MindCracker	PakCyberArmy	shaadighar.in/index.php	Linux
MindCracker	PakCyberArmy	sigmainternational.in/index.php	Linux
MindCracker	PakCyberArmy	star-management.in/index.php	Linux
MindCracker	PakCyberArmy	sunlust.in/index.php	Linux
MindCracker	PakCyberArmy	www.sigalbcoaching.co.il	Linux
MindCracker		www.sijunjung.go.id	Linux

misafir		caecom.ufam.edu.br	Linux
misafir		fes.ufam.edu.br	Linux
misafir		petdesign.ufam.edu.br	Linux
misafir		posfes.ufam.edu.br	Linux
MoJrIm HaCkErS		www.nfdin.gov.np	Linux
mOk	Myanmar Hackers Unite4m	onstageindia.in/mok.html	Linux
Mr.Simple	Myanmar Hackers Unite4m	www.shewratan.in/rocket.php	Windows 2003
MrFawkesYou		almaobledu-gov.kz	Linux
NeT-DeViL		amd.moai.gov.mm	Win 2008
NeT-DeViL		id.moai.gov.mm	Win 2008
NeT-DeViL		www.comune.galbiate.lc.it	Linux
NeT-DeViL		www.comune.portofino.genova.it...	Linux
NeT-DeViL		www.espcex.ensino.eb.br	Linux
NeT-DeViL		www.telecom.go.cr	Linux
NeT-DeViL		www.ypt-nsn.gov	Linux
NinjaVirus		0745.hhly.gov.cn/NV.htm	Win 2003
NinjaVirus	NinjaVirus	bcwtest.in/nick/admin/orignal/orignal.jpg	Linux
NinjaVirus	NinjaVirus	copyrightoffice.gov.bd/Nilux.htm	Linux
NinjaVirus		idpcenter.gov.ge/Nilux.htm	Linux
NinjaVirus	NinjaVirus	idpcenter.gov.ge/Nilux.htm	Linux
NinjaVirus		www.laguna.gov.ph/brandon/Nilu...	Linux
NinjaVirus	NinjaVirus	www.laguna.gov.ph/brandon/Nilux.htm	Linux
Nob0dy		e-lib.ddc.moph.go.th	Linux
Nob0dy		kuesioner-online.mahkamahagung...	Win 2003
Nob0dy		p4tkipa.kemdikbud.go.id	Unknown
Nob0dy		pusdiklat.pu.go.id	Win 2003
Nob0dy		ranong.nfe.go.th	Win 2008
Nob0dy		www.mubakab.go.id	Win 2003
Nob0dy		www.rizalkalinga.gov.ph/wp-con...	Linux
NoEntry Phc		ditu.zhuzhou.gov.cn/bb.html	Win 2003
NoEntry Phc		live.zhuzhou.gov.cn/bb.html	Win 2003
NoEntry Phc		sgzw.zhuzhou.gov.cn/bb.html	Win 2003
NoEntry Phc		www.zcny.gov.cn/bb.html	Win 2003
orioshunter	BD BLACK HAT	www.everestassociates.in	Linux
P4K-CoMManDeR	Team Cyber Switch	dailygrindcafe.in	Linux
P4K-CoMManDeR	Team Cyber Switch	dialatest.in	Linux
P4K-CoMManDeR	Team Cyber Switch	ekdantam.in	Linux
P4K-CoMManDeR	Team Cyber Switch	managementtreasures.in	Linux
P4K-CoMManDeR	Team Cyber Switch	uditraj.in	Linux
P4K-CoMManDeR	Team Cyber Switch	www.ssmarketingservices.in	Linux
Pencegah Maksiat	Wolf Enforced	cjzp.hnbys.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	clfcglj.zjjcl.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	clkx.zjjcl.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	dbegs.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	hbj.zjjcl.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	indiagallery.net/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	jxyhfda.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	nyp.aqny.gov.cn/x.html	Windows 2003

Pencegah Maksiat	Wolf Enforced	sdfco.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	wokeyw.hnbys.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	www.cc.lskjd.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	www.df.lskjd.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	www.ds.lskjd.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	www.qznyxx.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	www.sdw.lskjd.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	www.sjp.lskjd.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	www.wgjsj.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	www.yhdw.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	ycj.jc.gansu.gov.cn/x.html	Linux
Pencegah Maksiat	Wolf Enforced	zzdxxxw.hnbys.gov.cn/x.html	Windows 2003
Pencegah Maksiat	Wolf Enforced	zzdxyw.hnbys.gov.cn/x.html	Windows 2003
Phoenix64	Bengal Cyber Warrior	spmadaripur.gov.bd	Linux
Pr0grammer		www.pjzhzf.gov.cn/22.html	Win 2003
R3DD3V1L	Hacker Newbie Comunity	aloft.co.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	aquazonesystems.co.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	bmsservices.co.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	classicprints.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	deltacomindia.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	energycreators.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	epspl.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	hmsapp.co.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	iimindia.co.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	insuranceadvisory.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	naturalherbs.org.in	Windows 2008
R3DD3V1L		ppesumatera.menlh.go.id/index....	Linux
R3DD3V1L	Hacker Newbie Comunity	premierlifestyle.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	rena.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	shubhsandesh.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	speedymail.co.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	suvidhalawfirm.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	vickysports.in	Windows 2008
R3DD3V1L	Hacker Newbie Comunity	yungminds.in	Windows 2008
randomdude		www.lafederalonline.gov.ar	Win 2008
rEd X	3xp1r3 Cyber Army	chaiturokzzz.co.in	Linux
rEd X	3xp1r3 Cyber Army	chitwan.info	Linux
rEd X	3xp1r3 Cyber Army	gangabag.in	Linux
rEd X	3xp1r3 Cyber Army	mbmc.co.in	Linux
rEd X	3xp1r3 Cyber Army	mohib.in	Linux
rEd X	3xp1r3 Cyber Army	onedayweb.in	Linux
rEd X	3xp1r3 Cyber Army	simhasolutions.co.in	Linux
rEd X	3xp1r3 Cyber Army	www.mtenitseo.in	Linux
rooterror		www.tsd.gov.ly	Linux
s0ul inj3ct0r	IT DOSTI	oakhill.co.in	Windows 2008
SaccaFrazi		cjzp.hnbys.gov.cn/l.txt	Win 2003
SaccaFrazi		gcly.lncredit.gov.cn/l.txt	Win 2003
SanFour25		revistas.roche.es/Dz.htm	Linux

Saudi - Hack		econ.ncape.gov.za/2.txt	Win 2003
Saudi - Hack		economic.ncape.gov.za//images/...	Win 2008
Saudi - Hack		gra.gov.gy/2.txt	Linux
Saudi - Hack		www.identity.go.ke/2.txt	Win 2003
SeCuR!TY ** DR@G0N		karapurcek.gov.tr/site/	Linux
serseridelikan		aza.geumcheon.go.kr	Linux
serseridelikan		edu.gen.go.kr	Linux
serseridelikan		lens.sens.go.kr	Linux
serseridelikan		medu.gen.go.kr	Linux
Silent Hacker	INDISHELL	financebatagram.gov.pk/Sil3nT_H4x0r.html	Linux
SIMAVLI		kutahyahemaso.gov.tr	Linux
SLYHACKER		armidale-dumaresq.ses.nsw.gov....	Linux
SLYHACKER		corindi.ses.nsw.gov.au/albums	Linux
SLYHACKER		gosford.ses.nsw.gov.au/albums	Linux
SLYHACKER		guyra.ses.nsw.gov.au/nphp.old/	Linux
SLYHACKER		hurstville.ses.nsw.gov.au/albums	Linux
SLYHACKER		inverell.ses.nsw.gov.au/forum1	Linux
SLYHACKER		kogarah.ses.nsw.gov.au/cache	Linux
SLYHACKER		lismore.ses.nsw.gov.au/albums	Linux
SLYHACKER		lithgow.ses.nsw.gov.au/albums	Linux
SLYHACKER		manly.ses.nsw.gov.au/albums	Linux
SLYHACKER		orange.ses.nsw.gov.au/albums/	Linux
SLYHACKER		randwick.ses.nsw.gov.au/albums/	Linux
SLYHACKER		ryde.ses.nsw.gov.au/albums/	Linux
SLYHACKER		shoalhaven.ses.nsw.gov.au	Linux
SLYHACKER		sydneysouthern.ses.nsw.gov.au/...	Linux
SLYHACKER		tamworth.ses.nsw.gov.au/albums/	Linux
SLYHACKER		wollongong.ses.nsw.gov.au/albums/	Linux
striker	pak mad hunter	6767.in	Linux
T0MS1N	sund4nyM0uz Corporation	studioxl.in	Linux
T0r3x		bhczj.gov.cn/x.txt	Win 2003
T0r3x		gzzw.gov.cn/x.txt	Win 2003
T0r3x		www.alata.gov.tr	Linux
T0r3x		www.bpkg.gov.ba	Linux
T0r3x		www.cqbbszj.gov.cn/x.txt	Unknown
T0r3x		www.rzeic.gov.cn/x.txt	Win 2003
The_BeKiR		www.crossriverrail.qld.gov.au	Linux
The_BeKiR		www.glenwillow-oh.gov	Linux
Tomcat Security Team		www.rusoagri.go.th/index.php	Linux
ToP-TeaM		tinhdoanyenbai.gov.vn	Linux
TR4CK3R	Pak Cyber Army	www.demredevlethst.gov.tr	Linux
Turkish Energy Team		www.cdp.mil.do	Linux
Turkish Energy Team		www.egfr.roche.es	Linux
Turkish Energy Team		www.ntl.gov.bd	Linux
ulow	ulow	a.bzqfy.gov.cn/indonesia.htm	Win 2003
ulow		bagianap.sidoarjokab.go.id/uls...	Linux
ulow		balongbendo.sidoarjokab.go.id/...	Linux
ulow		bappeda.sidoarjokab.go.id/uls.txt	Linux

ulow		bkd.sidoarjokab.go.id/uls.txt	Linux
ulow		blh.sidoarjokab.go.id/uls.txt	Linux
ulow		buduran.sidoarjokab.go.id/uls.txt	Linux
ulow		candi.sidoarjokab.go.id/uls.txt	Linux
ulow		dinkop.sidoarjokab.go.id/uls.txt	Linux
ulow		dispendik.sidoarjokab.go.id/ul...	Linux
ulow		dns.zjwst.gov.cn/a.txt	Win 2003
ulow		dtpp.sijunjung.go.id/uls.txt	Linux
ulow		gedangan.sidoarjokab.go.id/uls...	Linux
ulow		gloria.gov.ph/tmp/uls.txt	Linux
ulow		jabon.sidoarjokab.go.id/uls.txt	Linux
ulow		jdih.sidoarjokab.go.id/uls.txt	Linux
ulow		koperindag.sijunjung.go.id/uls...	Linux
ulow		kota.sidoarjokab.go.id/uls.txt	Linux
ulow		kpud.sidoarjokab.go.id/uls.txt	Linux
ulow		krembung.sidoarjokab.go.id/uls...	Linux
ulow		lelang.sijunjung.go.id/uls.txt	Linux
ulow		pariwisata.sidoarjokab.go.id/u...	Linux
ulow		pasar.sidoarjokab.go.id/uls.txt	Linux
ulow		pdam.sidoarjokab.go.id/uls.txt	Linux
ulow		perijinan.sidoarjokab.go.id/ul...	Linux
ulow		perikanan.sidoarjokab.go.id/ul...	Linux
ulow		perpus-arsip.sidoarjokab.go.id...	Linux
ulow		perpusda.sidoarjokab.go.id/uls...	Linux
ulow		peta.sijunjung.go.id/uls.txt	Linux
ulow		porong.sidoarjokab.go.id/uls.txt	Linux
ulow		porprov.sijunjung.go.id/uls.txt	Linux
ulow		prambon.sidoarjokab.go.id/uls.txt	Linux
ulow		rsd.sidoarjokab.go.id/uls.txt	Linux
ulow		sedati.sidoarjokab.go.id/uls.txt	Linux
ulow		sipjaki.sidoarjokab.go.id/uls.txt	Linux
ulow		sipkd.sijunjung.go.id/uls.txt	Linux
ulow		sukodono.sidoarjokab.go.id/uls...	Linux
ulow		taman.sidoarjokab.go.id/uls.txt	Linux
ulow		tanggulangin.sidoarjokab.go.id...	Linux
ulow		tarik.sidoarjokab.go.id/uls.txt	Linux
ulow		tulangan.sidoarjokab.go.id/uls...	Linux
ulow		wonoayu.sidoarjokab.go.id/uls.txt	Linux
ulow		www.cqzm.gov.cn/a.txt	Win 2003
ulow		www.jnsafety.gov.cn	Win 2003
ulow		www.zagori.gov.gr/uls.txt	Linux
ulow		z.bzfy.gov.cn/a.htm	Win 2003
ulow		z.tjfy.gov.cn/a.htm	Win 2003
Xc0t3z	Xc0t3z	andoshops.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	a-n-shilo.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	ashtar.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	bar-optic.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	bioback.co.il/~kablu/images/rooz/x.php	Linux

Xc0t3z	Xc0t3z	cars-mall.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	clalcar.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	classicyael-store.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	computers-mall.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	electronics-mall.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	gayaflowers.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	hakolbezol.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	harel-systems-shop.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	house-mall.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	ilholiday.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	island-sound.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	kids-mall.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	kolav.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	mashoaher.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	mrihut.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	niceshop.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	omega3health.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	phone-team.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	pomodent.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	rihut-mall.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	shani-packs-shop.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	shay-lagan.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	shragay.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	sport-mall.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	yd-misim.co.il/~kablu/images/rooz/x.php	Linux
Xc0t3z	Xc0t3z	zlilei-oranim.co.il/~kablu/images/rooz/x.php	Linux
x-hayben21		www.zsorangpur.gov.bd	Linux
xr00tx	sund4nyM0uz Corporation	www.tigerarmy.in.th	Linux
ynR !	ynR !	mohfw.gov.bd	Linux
Z4R4THUSTR4		biroadmrek.jabarprov.go.id	FreeBSD
Z4R4THUSTR4		www.pdmo.go.th/zara.txt	Win 2008
ZiyaretCi		ppp.gov.tr	Linux
ZiyaretCi		www.kamuozel.gov.tr	Linux
ZoRRoKiN		www.kawasakichile.com/noticias...	Linux

Top Attackers of all time: Zone-H

Rank	Notifier	Single def.	Mass def.	Total def.	Homepage def.	Subdir def.
1	Barbaros-DZ	3126	156	3282	955	2327
2	Ashiyane Digital Security Team	2485	3219	5704	1045	4659
3	Hmei7	2053	1168	3221	700	2521
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	382	197	579	104	475
25	Triad	375	315	690	397	293

Top 10 Ports

by Reports

Port	Reports
445	336286
3389	116036
23	68045
22	65981
80	64643
139	62145
1433	50954
53	32281
4899	21526
587	13070

by Targets

Port	Targets
23	58648
3389	46059
22	38332
1433	37578
445	21857
4899	20460
1434	9277
8080	9162
80	5685
9090	4708

by Sources

Port	Sources
445	14308
3389	9369
80	6962
53	3517
35691	3269
25	865
23	822
4899	576
30247	391
57631	376

Top 10 Source IPs

IP Address	Reports	Attacks	First Seen	Last Seen
069.175.126.170 (US)	1,408,705	136,279	2012-07-11	2012-09-26
037.009.053.002 (RU)	525,972	106,360	2012-09-12	2012-09-25
117.211.092.122 (IN)	167,150	102,115	2012-08-25	2012-09-26
061.147.068.211 (CN)	530,967	99,872	2012-09-02	2012-09-25
061.147.103.098 (CN)	250,935	99,039	2012-09-25	2012-09-25
074.055.087.138 (US)	171,800	86,623	2012-09-09	2012-09-25
195.242.072.139 (NL)	75,666	74,866	2012-09-25	2012-09-25
222.043.097.006 (CN)	130,437	74,681	2012-06-27	2012-09-26
222.187.220.179 ()	71,600	71,566	2012-09-25	2012-09-26
220.225.004.021 (IN)	177,200	70,995	2012-09-14	2012-09-26

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	www.informationwarfarecenter.com