

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

September, 26 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

Many of the cyber-attacks the last two weeks have been related to the Muslim unrest, blaming America for the anti-Islamic film released prior to 9/11/2012. The attacks haven't increased in number really, but the messages to the victims have been more focused on "defending" the name of the Prophet Muhammad. Messages such as "You open the doors of hell on yourselves when you insulted Prophet Muhammad, peace be upon him, by producing a dirty film hurts the position of prophecy. And by scorn every Islamic sacred!" and "The Muslim's soul's thirst or revenge from the accursed insulter impugning the Chief if the First and Last is only quenched by killing and crucifying him after torturing and beating him, for that is what he deserves and what deters others." Messages like this have replaced the traditional "You've been hacked" type banners normally posted. There are several dozen active (Muslim affiliated) hacker groups that will likely focus their activities solely on America and it's allies in the event of an Iranian conflict. Most of these attackers are not that advanced, but can still cause a nuisance.

Gotcha .gov/.mil – Domains have been notified...

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

- identix.state.gov, (multi).usda.gov, istanbul.usconsulate.gov, sbcounty.gov, brighamcity.utah.gov, ltdhd.ky.gov, westbendwi.gov, wmatc.gov, and 41 other .gov websites

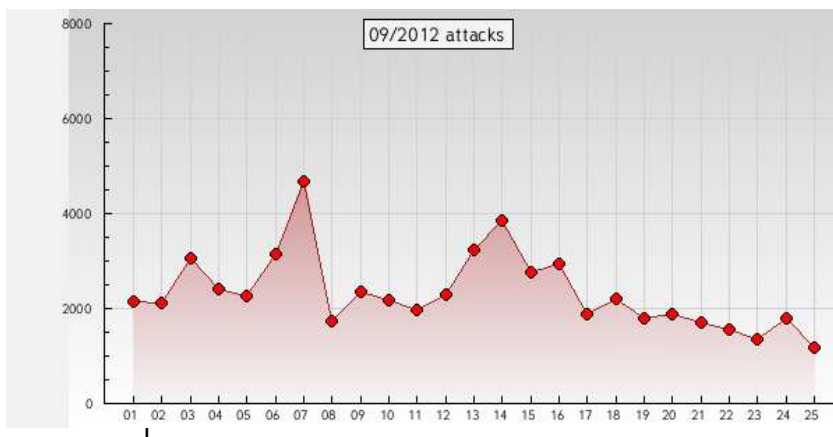
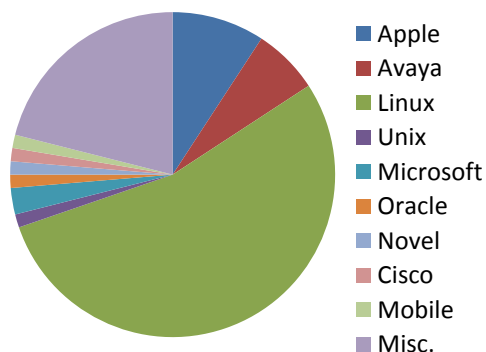
Gotcha .edu – Domains have been notified...

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

- Northwestern University was defaced an astonishing **34+** times since last Wednesday.
- Duke, Harvard, Stanford, Berkley, Caltech, Columbia, Cornell, and MIT each have been defaced.

Section	Page	Instances
In the News	2	44
Papers	3	1
Discussions	3	3
Advisories	4	82
Tools released	12	5
Exploits published	12	10
Vulnerable websites	13	35
Websites defaced	14	469

Alerts



CIR

In the news:

- Iran's Top Brass Deny Nuking US Bank Websites
- Japan Confirms Cyberattacks Over Island Dispute
- More Malware Targeting Iran Could Yet Be Discovered
- Mexican Hackers Hit Official Websites In Cyber Protest
- Foreign Hacks In China Hit With Malicious Emails
- Huawei And ZTE Deny Backdoor Allegations
- GCHQ In New Challenge For Cybersecurity Wannabes
- Kim Dotcom: Inquiry Ordered Into Unlawful Spying
- Firms At Risk From APTs And State Sponsored Attacks
- IEEE Admits Password Leak, Says Problem Fixed
- Researchers Claim Yet Another Vulnerability Exists In Java
- Google Go Language Gets Used: For File-Scrambling Trojan, Though
- Skyper Freed After Accidentally Hacking Bank
- Chase Joins Bank Of America In Possible Islamic Attack Outage
- Microsoft Issues Emergency IE Bug Patch
- Oracle Flaw Puts Users Passwords At Risk To Brute Force Assault
- Facebook To Remove Facial Recognition Tool In Europe
- Facebook Suspends Photo Tag Tool In Europe
- iPhone 4S Hacked By Dutch Team
- Samsung Galaxy Phones Are Vulnerable To A Remote Wipe Attack
- Exploit Beamed Via NFC To Hack Samsung Galaxy S3
- Some Android phones can be reset to factory default by clicking on links
- Researchers Reveal NFC Subway Permanent Bypass

* FBI news

- Albany Man Sentenced for Distributing Child Pornography – Albany
- Man Sentenced to 34 Years for Pandering and Pimping of a Child - Denver
- Buffalo Man Indicted for Advertising, Receiving, and Distributing Child Pornography - Buffalo
- Hancock County Man Charged with Distribution of Child Pornography - Indianapolis
- Bethlehem Man Sentenced for Making Threats on His Facebook Page - Philadelphia

* DC3.mil content:

- **Cyber Crime**
 - [Fraudsters put new twists on cyber scams, says FBI](#)
 - There's less malware being created, but whats left is much smarter
- **Government**
 - Federal workers skeptical when it comes to government cybersecurity programs
 - Napolitano Says Cybersecurity Executive Order Almost Ready
- **News, Technologies and Techniques**
 - SUSE Manager update streamlines Linux management
 - Guidance Software Celebrates 50000 EnCase(r) Students
 - Indonesia advances worlds most ambitious biometric-based national ID project
 - LM case: only 1 person involved
 - Tableau TD3 Forensic Imager Introduction
 - New Service Takes the Faux Out of Photos
 - Passware Kit Forensic v.12
 - Software Code Sandboxes a Bright Spot as Security Flaws Trend Higher
 - Taiwan co. fined \$500 million for LCD price fixing
 - Why Fingerprints Aren't the Proof We Thought They Were

CIR

- **Security Alerts:**
- Microsoft: Patch for critical IE zero-day bug coming Friday
- U.S. banks on high alert against cyberattacks

Papers:

- [The Making Of A Full, Undetectable USB Dropper](#)

Discussions

- Operation Trident Tribunal -Targeted by the FBI Cybercrime Investigators and several NATO partners. <http://ow.ly/dMb3s>
- Obama's Draft Cybersecurity Executive Order
- DOD announces new Internet services, capabilities policy

Advisories for the week of September 26, 2012

Apache

[Secunia Security Advisory 50573](#)

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

Apple

[Apple Security Advisory 2012-09-19-3](#)

Apple Security Advisory 2012-09-19-3 - Safari 6.0.1 is now available and addresses multiple vulnerabilities in itself and WebKit.

[Apple Security Advisory 2012-09-19-2](#)

Apple Security Advisory 2012-09-19-2 - OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004 are now available and address Apache, BIND, CoreText, Data Security, and many other vulnerabilities.

[Apple Security Advisory 2012-09-19-1](#)

Apple Security Advisory 2012-09-19-1 - iOS 6 is now available and addresses CFNetwork, CoreGraphics, CoreMedia, DHCP, and many other vulnerabilities.

[Secunia Security Advisory 50586](#)

Secunia Security Advisory - Multiple vulnerabilities have been reported in Apple iOS, which can be exploited by malicious, local users to disclose system information and gain escalated privileges, by malicious people to disclose potentially sensitive information, conducts spoofing attacks, and compromise a user's device, and by malicious people with physical access to disclose potentially sensitive information and bypass certain security restrictions.

[Secunia Security Advisory 50577](#)

Secunia Security Advisory - Multiple vulnerabilities have been reported in Safari, which can be exploited by malicious people to bypass certain security restrictions, gain knowledge of sensitive information, or compromise a user's system.

[Secunia Security Advisory 50628](#)

Secunia Security Advisory - Apple has issued a security update for Mac OS X, which fixes multiple vulnerabilities.

[Apple Security Advisory 2012-09-24-1](#)

Apple Security Advisory 2012-09-24-1 - Apple TV 5.1 is now available and addresses issues relating to malicious media loading, memory corruption, and more.

Avaya

[Secunia Security Advisory 50684](#)

Secunia Security Advisory - Avaya has acknowledged multiple weaknesses and vulnerabilities in Avaya Aura Communication Manager, which can be exploited by malicious, local users to disclose certain system information, bypass certain security restrictions, cause a DoS (Denial of Service), and to potentially gain escalated privileges, by malicious, local users in a guest virtual machine to cause a DoS, and by malicious people to cause a DoS.

[Secunia Security Advisory 50614](#)

Secunia Security Advisory - Avaya has acknowledged a weakness and multiple vulnerabilities in Avaya Voice Portal, which can be exploited by malicious, local users to disclose system and sensitive information and by malicious people to bypass certain security restrictions and cause a DoS (Denial of Service).

[Secunia Security Advisory 50712](#)

Secunia Security Advisory - Avaya has acknowledged two vulnerabilities in Avaya Application Enablement Services, which can be exploited by malicious people to cause a DoS (Denial of Service).

[Secunia Security Advisory 50678](#)

Secunia Security Advisory - Avaya has acknowledged two vulnerabilities in Avaya Aura Session Manager, which can be exploited by malicious people to bypass certain security restrictions and cause a DoS (Denial of Service) in an application using the library.

[Secunia Security Advisory 50675](#)

Secunia Security Advisory - Avaya has acknowledged a weakness in Avaya Aura System Manager, which can be exploited by malicious, local users to disclose system and sensitive information.

Cisco

[Secunia Security Advisory 50669](#)

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

Debian

[Debian Security Advisory 2553-1](#)

Debian Linux Security Advisory 2553-1 - Several vulnerabilities have been discovered in Iceweasel, a web browser based on Firefox. The included XULRunner library provides rendering services for several other applications included in Debian.

[Debian Security Advisory 2551-1](#)

Debian Linux Security Advisory 2551-1 - Glen Eustace discovered that the ISC DHCP server, a server for automatic IP address assignment, is not properly handling changes in the expiration times of a lease. An attacker may use this flaw to crash the service and cause denial of service conditions, by reducing the expiration time of an active IPv6 lease.

[Secunia Security Advisory 50727](#)

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

Dell

[Dell Data Protection | Access \(DDPA\) Vulnerable Components](#)

The current version of Dell's Data Protection | Access (DDPA) software for Windows (Build 2.2.00003.008 from 2012-06-14, released August 2012) contains and installs several outdated, superfluous and vulnerable Windows system components as well as outdated and vulnerable 3rd party components and drivers.

Fortinet

[Secunia Security Advisory 50638](#)

Secunia Security Advisory - Benjamin Kunz Mejri has reported two vulnerabilities in Fortinet FortiOS (FortiGate), which can be exploited by malicious people to conduct cross-site scripting attacks.

Gentoo

[Gentoo Linux Security Advisory 201209-04](#)

Gentoo Linux Security Advisory 201209-4 - Multiple vulnerabilities have been found in BIND, the worst of which may allow remote Denial of Service. Versions less than 9.9.1_p3 are affected.

[Gentoo Linux Security Advisory 201209-03](#)

Gentoo Linux Security Advisory 201209-3 - Multiple vulnerabilities were found in PHP, the worst of which lead to remote execution of arbitrary code. Versions less than 5.3.15 are affected.

[Gentoo Linux Security Advisory 201209-02](#)

Gentoo Linux Security Advisory 201209-2 - Multiple vulnerabilities in libTIFF could result in execution of arbitrary code or Denial of Service. Versions less than 4.0.2-r1 are affected.

[Gentoo Linux Security Advisory 201209-10](#)

Gentoo Linux Security Advisory 201209-10 - A buffer overflow vulnerability in Calligra could result in the execution of arbitrary code. Versions less than 2.4.3-r1 are affected.

[Gentoo Linux Security Advisory 201209-09](#)

Gentoo Linux Security Advisory 201209-9 - A vulnerability has been found in Atheme which may lead to Denial of Service or a bypass of security restrictions. Versions less than 6.0.10 are affected.

[Gentoo Linux Security Advisory 201209-08](#)

Gentoo Linux Security Advisory 201209-8 - A vulnerability in SquidClamav may result in Denial of Service. Versions less than 6.8 are affected.

[Gentoo Linux Security Advisory 201209-07](#)

Gentoo Linux Security Advisory 201209-7 - A buffer overflow in International Components for Unicode could result in execution of arbitrary code or Denial of Service. Versions less than 49.1.1-r1 are affected.

[Gentoo Linux Security Advisory 201209-06](#)

Gentoo Linux Security Advisory 201209-6 - Multiple vulnerabilities have been found in Expat, possibly resulting in Denial of Service. Versions less than 2.1.0_beta3 are affected.

[Gentoo Linux Security Advisory 201209-05](#)

Gentoo Linux Security Advisory 201209-5 - Multiple vulnerabilities have been found in LibreOffice, allowing remote attackers to execute arbitrary code or cause a Denial of Service. Versions less than 3.5.5.3 are affected.

[Gentoo Linux Security Advisory 201209-04](#)

Gentoo Linux Security Advisory 201209-4 - Multiple vulnerabilities have been found in BIND, the worst of which may allow remote Denial of Service. Versions less than 9.9.1_p3 are affected.

[Gentoo Linux Security Advisory 201209-03](#)

Gentoo Linux Security Advisory 201209-3 - Multiple vulnerabilities were found in PHP, the worst of which lead to remote execution of arbitrary code. Versions less than 5.3.15 are affected.

[Gentoo Linux Security Advisory 201209-02](#)

Gentoo Linux Security Advisory 201209-2 - Multiple vulnerabilities in libTIFF could result in execution of arbitrary code or Denial of Service. Versions less than 4.0.2-r1 are affected.

[Secunia Security Advisory 50725](#)

Secunia Security Advisory - Gentoo has issued an update for php. This fixes a weakness, a security issue, and multiple vulnerabilities, which can be exploited by malicious people to conduct brute force attacks, disclose certain sensitive information, bypass certain security restrictions, cause a DoS (Denial of Service), and compromise a vulnerable system.

[Secunia Security Advisory 50726](#)

Secunia Security Advisory - Gentoo 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 compromise an application using the library.

[Secunia Security Advisory 50692](#)

Secunia Security Advisory - Gentoo has issued an update for libreoffice. This fixes multiple vulnerabilities, which can be exploited by malicious people to disclose potentially sensitive information and compromise a user's system

[Secunia Security Advisory 50695](#)

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

[Secunia Security Advisory 50724](#)

Secunia Security Advisory - Gentoo has issued an update for bind. This fixes multiple vulnerabilities, which can be exploited by malicious people to conduct spoofing attacks, disclose potentially sensitive information, and cause a DoS (Denial of Service).

[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.

HP

[HP Security Bulletin HPSBMU02815 SSRT100715 2](#)

HP Security Bulletin HPSBMU02815 SSRT100715 2 - Potential security vulnerabilities have been identified with HP SiteScope. The vulnerabilities in SiteScope SOAP features could be remotely exploited to allow disclosure of information or code execution. Revision 2 of this advisory.

[HP Security Bulletin HPSBMU02815 SSRT100715 3](#)

HP Security Bulletin HPSBMU02815 SSRT100715 3 - Potential security vulnerabilities have been identified with HP SiteScope. The vulnerabilities in SiteScope SOAP features could be remotely exploited to allow disclosure of information or code execution. Revision 3 of this advisory.

IBM

[Secunia Security Advisory 50729](#)

Secunia Security Advisory - A weakness and a vulnerability have been reported in IBM Installation Manager, which can be exploited by malicious people to conduct spoofing and cross-site scripting attacks.

Microsoft

[Technical Cyber Security Alert 2012-265A](#)

Technical Cyber Security Alert 2012-265A - Microsoft has released Security Bulletin MS12-063 to address the use-after-free vulnerability that has been actively exploited this past week.

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

This bulletin summary lists 3 released Microsoft security bulletins for September, 2012.

Oracle

[Yet Another Oracle Java Vulnerability](#)

Security Explorations has announced that they have discovered yet another sandbox bypass of Oracle Java and have reported little in the way of details until the vendor fixes the issue. It currently affects all versions of Java. It's probably best to just keep Java off in your browser for now.

Novell

[Novell GroupWise Agents Arbitrary File Retrieval](#)

The HTTP interfaces for Novell GroupWise 8.0.2 Post Office Agent, Message Transfer Agent, and GroupWise Internet Agent are vulnerable to an arbitrary file retrieval condition due to a failure to properly filter certain crafted directory traversal sequences. An unauthenticated remote attacker can leverage this flaw to retrieve files with the privileges of the vulnerable agent. Novell has provided solutions for this issue in the form of GroupWise 8.0 SP3 as well as in the latest GroupWise 2012 SP1 release.

Red Hat

[Secunia Security Advisory 50697](#)

Secunia Security Advisory - Red Hat has issued an update for Red Hat Enterprise MRG. This fixes multiple vulnerabilities, which can be exploited by malicious, local users to gain escalated privileges, malicious users to bypass certain security restrictions, conduct SQL injection attacks, and cause a DoS (Denial of Service), and by malicious people to disclose potentially sensitive information, conduct brute force, cross-site scripting, and cross-site request forgery attacks, and potentially compromise a vulnerable system.

CIR

[Secunia Security Advisory 50602](#)

Secunia Security Advisory - Red Hat has issued an update for Red Hat Enterprise MRG. This fixes a vulnerability, which can be exploited by malicious people to bypass certain security restrictions.

[Secunia Security Advisory 50699](#)

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

[Red Hat Security Advisory 2012-1308-01](#)

Red Hat Security Advisory 2012-1308-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength, general purpose cryptography library. Multiple numeric conversion errors, leading to a buffer overflow, were found in the way OpenSSL parsed ASN.1 data from BIO inputs. Specially-crafted DER encoded data read from a file or other BIO input could cause an application using the OpenSSL library to crash or, potentially, execute arbitrary code.

[Red Hat Security Advisory 2012-1306-01](#)

Red Hat Security Advisory 2012-1306-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength, general purpose cryptography library. Multiple numeric conversion errors, leading to a buffer overflow, were found in the way OpenSSL parsed ASN.1 data from BIO inputs. Specially-crafted DER encoded data read from a file or other BIO input could cause an application using the OpenSSL library to crash or, potentially, execute arbitrary code.

[Red Hat Security Advisory 2012-1307-01](#)

Red Hat Security Advisory 2012-1307-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength, general purpose cryptography library. Multiple numeric conversion errors, leading to a buffer overflow, were found in the way OpenSSL parsed ASN.1 data from BIO inputs. Specially-crafted DER encoded data read from a file or other BIO input could cause an application using the OpenSSL library to crash or, potentially, execute arbitrary code.

RSA

[RSA Authentication Agent 7.1 / Client 3.5 Access Control](#)

Under some configuration conditions, a user of RSA Authentication Agent 7.1 for Windows or RSA Authentication Client who has privilege to access a desktop or a server is incorrectly able to do so with only Windows credentials.

SonicWall

[Secunia Security Advisory 50686](#)

Secunia Security Advisory - Benjamin Kunz Mejri has reported some vulnerabilities in SonicWALL Anti-Spam & Email Security, which can be exploited by malicious people to conduct cross-site scripting attacks.

Suse

[Secunia Security Advisory 50662](#)

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

[Secunia Security Advisory 50694](#)

Secunia Security Advisory - SUSE has issue an update for rubygem-actionpack and rubygem-activesupport. This fixes two vulnerabilities, which can be exploited by malicious people to conduct cross-site scripting attacks.

Toshiba

[Toshiba ConfigFree CF7 File Remote Command Execution](#)

There is a command execution vulnerability in the Toshiba ConfigFree CF7 file format used on Toshiba laptops to import and export network configurations. An attacker could execute arbitrary commands with the privileges of the current logged-in user by enticing a Toshiba laptop user to download and execute a crafted CF7 file.

[Toshiba ConfigFree CF7 ProfileName Overflow](#)

There is a stack buffer overflow vulnerability in the Toshiba ConfigFree CF7 file format used on Toshiba laptops. An attacker could execute arbitrary code by enticing a Toshiba laptop user to download and execute a malicious CF7 file if they manipulate the ProfileName.

[Toshiba ConfigFree CF7 Comment Field Overflow](#)

There is a stack buffer overflow vulnerability in the Toshiba ConfigFree CF7 file format used on Toshiba laptops. An attacker could execute arbitrary code by enticing a Toshiba laptop user to download and execute a malicious CF7 file.

Ubuntu

[Secunia Security Advisory 50710](#)

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

[Ubuntu Security Notice USN-1580-1](#)

Ubuntu Security Notice 1580-1 - Ben Hutchings reported a flaw in the Linux kernel with some network drivers that support TSO (TCP segment offload). A local or peer user could exploit this flaw to to cause a denial of service. Jay Fenlason and Doug Ledford discovered a bug in the Linux kernel implementation of RDS sockets. A local unprivileged user could potentially use this flaw to read privileged information from the kernel. Various other issues were also addressed.

[Ubuntu Security Notice USN-1579-1](#)

Ubuntu Security Notice 1579-1 - Ben Hutchings reported a flaw in the Linux kernel with some network drivers that support TSO (TCP segment offload). A local or peer user could exploit this flaw to to cause a denial of service. Jay Fenlason and Doug Ledford discovered a bug in the Linux kernel implementation of RDS sockets. A local unprivileged user could potentially use this flaw to read privileged information from the kernel. Various other issues were also addressed.

[Ubuntu Security Notice USN-1578-1](#)

Ubuntu Security Notice 1578-1 - Ben Hutchings reported a flaw in the Linux kernel with some network drivers that support TSO (TCP segment offload). A local or peer user could exploit this flaw to to cause a denial of service. Jay Fenlason and Doug Ledford discovered a bug in the Linux kernel implementation of RDS sockets. A local unprivileged user could potentially use this flaw to read privileged information from the kernel. Various other issues were also addressed.

CIR

[Ubuntu Security Notice USN-1577-1](#)

Ubuntu Security Notice 1577-1 - A flaw was discovered in the Linux kernel's KVM (kernel virtual machine). An administrative user in the guest OS could leverage this flaw to cause a denial of service in the host OS. Ben Hutchings reported a flaw in the Linux kernel with some network drivers that support TSO (TCP segment offload). A local or peer user could exploit this flaw to to cause a denial of service. Jay Fenlason and Doug Ledford discovered a bug in the Linux kernel implementation of RDS sockets. A local unprivileged user could potentially use this flaw to read privileged information from the kernel. Various other issues were also addressed.

[Secunia Security Advisory 50633](#)

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

[Secunia Security Advisory 50652](#)

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

[Ubuntu Security Notice USN-1581-1](#)

Ubuntu Security Notice 1581-1 - Marc Schoenefeld discovered that Ghostscript did not correctly handle certain image files. If a user or automated system were tricked into opening a specially crafted file, an attacker could cause a denial of service and possibly execute arbitrary code with user privileges.

[Secunia Security Advisory 50732](#)

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

[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

Misc:

[Secunia Security Advisory 50660](#)

Secunia Security Advisory - Multiple vulnerabilities have been reported in Cumin, which can be exploited by malicious users to bypass certain security restrictions, conduct SQL injection attacks, and cause a DoS (Denial of Service) and by malicious people to disclose potentially sensitive information, conduct brute force, cross-site scripting, and cross-site request forgery attacks.

[Secunia Security Advisory 50570](#)

Secunia Security Advisory - A vulnerability has been discovered in Manhali, which can be exploited by malicious people to disclose sensitive information.

[Secunia Security Advisory 50682](#)

Secunia Security Advisory - Multiple vulnerabilities have been reported in Zend Framework, which can be exploited by malicious people to conduct cross-site scripting attacks.

[Secunia Security Advisory 50603](#)

Secunia Security Advisory - Eugene Dokukin has reported multiple vulnerabilities in iFOBS, which can be exploited by malicious people to conduct cross-site scripting attacks.

[Secunia Security Advisory 50690](#)

Secunia Security Advisory - Brendan Coles has discovered two security issues in Zen Load Balancer, which can be exploited by malicious people to disclose system and potentially sensitive information.

[Secunia Security Advisory 50524](#)

Secunia Security Advisory - A vulnerability has been reported in multiple Webify products, which can be exploited by malicious people to manipulate certain data.

[Secunia Security Advisory 50693](#)

Secunia Security Advisory - Blake Entrekin has discovered a vulnerability in the WP-TopBar plugin for WordPress, which can be exploited by malicious people to conduct cross-site request forgery attacks.

[Secunia Security Advisory 50688](#)

Secunia Security Advisory - Justin C. Klein Keane has reported a vulnerability in the FileField Sources module for Drupal, which can be exploited by malicious users to conduct script insertion attacks.

[Secunia Security Advisory 50571](#)

Secunia Security Advisory - Reaction Information Security has discovered a vulnerability in the MF Gig Calendar plugin for WordPress, which can be exploited by malicious people to conduct cross-site scripting attacks.

[Secunia Security Advisory 50666](#)

Secunia Security Advisory - Multiple vulnerabilities have been reported in Condor, which can be exploited by malicious, local users to gain escalated privileges, by malicious users to bypass certain security restrictions, and by malicious people to disclose sensitive information and potentially compromise a vulnerable system.

[Secunia Security Advisory 50683](#)

Secunia Security Advisory - A vulnerability has been reported in the Imagemenu module for Drupal, which can be exploited by malicious users to conduct script insertion attacks.

[Thomson SpeedTouch ST780 Insecure SSL Connection](#)

Thomson SpeedTouch ST780, by design, has mixed content in the DOM during an SSL encapsulated session.

CIR

[Secunia Security Advisory 50727](#)

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

[Secunia Security Advisory 50691](#)

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

[Secunia Security Advisory 50715](#)

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

[Secunia Security Advisory 50685](#)

Secunia Security Advisory - A vulnerability has been discovered in SafeNet Sentinel Protection Installer, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

Tools released this week:

- [Tor-ramdisk i686 UClIBC-based Linux Distribution x86_64 20120923](#)
- [Tor-ramdisk i686 UClIBC-based Linux Distribution x86 20120923](#)
- [Tor-ramdisk i686 UClIBC-based Linux Distribution MIPS 20120923](#)
- [I2P 0.9.2](#)
- [ipset 6.14](#)

Exploits released this week (9):

[Guacamole 0.6.0 Buffer Overflow](#)

[HP ALM Remote Code Execution](#)

[NTR ActiveX Control Check\(\) Method Buffer Overflow](#)

[NTR ActiveX Control StopModule\(\) Remote Code Execution](#)

[QNX QCONN Remote Command Execution Vulnerability](#)

[Samba 3.x Remote Root](#)

[Thomson Wireless VoIP Cable Modem Auth Bypass](#)

[Thomson Wireless VoIP Cable Modem Authentication Bypass](#)

[ZEN Load Balancer Filelog Command Execution](#)

DoS attacks (1):

- [SafeNet Sentinel Keys Server Crash PoC](#)

Website attacks (35):

Joomla 2.5.6 Cross Site Scripting
2xI Cross Site Scripting / SQL Injection
AM4Design SQL Injection
AShop 5.3.4 Cross Site Scripting
Atlassian Confluence 3.0 Cross Site Request Forgery
Auxilium RateMyPet Arbitrary File Upload
Brother Bear SQL Injection
cgCraft LLC SQL Injection
Custom Designed Sites SQL Injection / XSS / LFI
Drupal 7.15 Path Disclosure
Gazine2 Cross Site Scripting
IFOBS Cross Site Request Forgery / Cross Site Scripting
Jessica Rhaye Design Cross Site Scripting
Manhali 1.8 Local File Inclusion
Manhali v1.8 Local File Inclusion Vulnerability
Microcart 1.0 Checkout Cross Site Scripting
Microcart 1.0 Cross Site Scripting
NW7Design SQL Injection
Olojin SQL Injection
Rocket Web Consulting SQL Injection
Sino Solutions Cross Site Scripting
Spiceworks 6.0.00993 Multiple Script Injection Vulnerabilities
Tariq Rauf SQL Injection
Tariq Rauf SQL Injection
WEBBISH SQL Injection
WordPress 3.4.2 Cross Site Request Forgery
WordPress Add Multiple Users Cross Site Request Forgery
WordPress MF Gig Calendar 0.9.2 Cross Site Scripting
WordPress Notices CSRF / XSS
Wordpress Plugin Token Manager Cross Site Scripting
WordPress Sexy Add Template CSRF Shell Upload
WordPress Sociable Cross Site Scripting
WordPress Wp-TopBar 4.02 CSRF / XSS
Wordpress Wp-TopBar 4.02 Multiple Vulnerabilities
YCommerce Pro / Reseller SQL Injection

CIR

Websites Defaced:











































.GOV (30)

Date	L	★ Domain	OS	View
Black Angels		★ aplus-schools.ncdcr.gov/indexx...	Win 2008	mirror
Black Angels		★ blogs.usembassy.gov/test2/2012...	Linux	mirror
Th3 K!LL3r Dz		★ brighamcity.utah.gov/images/te...	Linux	mirror
4n0wG2		★ bsee.detroitmi.gov/PLCWebOnlin...	Linux	mirror
NeT-DeViL		★ fdtraining.plymouthmn.gov	Win 2003	mirror
NeT-DeViL		★ fire.plymouthmn.gov	Win 2003	mirror
asad hemati		★ greenbaywi.gov	Linux	mirror
b0ogle		★ identix.state.gov/qotw/Dynamic...		mirror
SsBlack		★ istanbul.usconsulate.gov	Linux	mirror
lol		★ justice.gov	F5 Big-IP	mirror
HaCkeD By Dr.D1G		★ ltdhd.ky.gov	Win 2003	mirror
NeT-DeViL		★ mswg.cap.gov	Linux	mirror
m0y		★ saltoncsd.ca.gov	Win 2008	mirror
Black Angels		★ tsacareercoaching.tsa.dhs.gov/...	Linux	mirror
syhmfz		★ vcapride.virginia.gov	Win 2003	mirror
NeT-DeViL		★ visit.nebraska.gov	Linux	mirror
ALG-LOVE MOHAMED		★ www.cia.gov/cia/publications/f...	Shared	mirror
Red Hat Security Team		★ www.driveclean.ca.gov/Learn_Mo...	Linux	mirror
Turkish Energy Team		★ www.forum.daughertytownship-pa...	Linux	mirror
NeT-DeViL		★ www.lawrenceburgtn.gov	Linux	mirror
BANGLADESH CYBER ARMY		★ www.morris.ars.usda.gov	Win 2003	mirror
BANGLADESH CYBER ARMY		★ www.mrsars.usda.gov	Win 2003	mirror
BANGLADESH CYBER ARMY		★ www.mwa.ars.usda.gov	Win 2003	mirror
Ashiyane Digital Security Team		★ www.nmvb.ca.gov	Win 2008	mirror
BROTHERS TEAM		★ www.photos.opc-dc.gov	Linux	mirror
Gaza HaCkeR Team		★ www.sbcounty.gov/workforce/ind...	F5 Big-IP	mirror
Black Angels		★ www.tupeloms.gov/parkandrec/20...	Linux	mirror
NeT-DeViL		★ www.visitnebraska.gov	Linux	mirror
M0sted		★ www.westbendwi.gov	Linux	mirror
NeT-DeViL		★ www.wmatc.gov	Win 2003	mirror

.EDU (61)

Date	L	★ Domain	OS	View
HighTech		★ alpc1.psfc.mit.edu	Win 2000	mirror
M0sted		★ ameerlab.northwestern.edu	Linux	mirror
M0sted		★ bagheri.northwestern.edu	Linux	mirror
M0sted		★ ber-reu.northwestern.edu	Linux	mirror
M0sted		★ cepm.northwestern.edu	Linux	mirror
NeT-DeViL		★ cs.stanford.edu/pldi10/	Linux	mirror
M0sted		★ csml.northwestern.edu	Linux	mirror
NeT-DeViL		★ dcmrc.duhs.duke.edu/index.php	MacOSX	mirror
NeT-DeViL		★ dcmrc.mc.duke.edu/index.php	MacOSX	mirror
M0sted		★ ddays2010.northwestern.edu	Linux	mirror

CIR

M0sted	 ★ dendrites.northwestern.edu	Linux	mirror
M0sted	 ★ dysa.northwestern.edu	Linux	mirror
TeslaTeam	 ehouse.rit.edu	Linux	mirror
M0sted	 ★ entrepreneur.northwestern.edu	Linux	mirror
9-gate	 faculty.quinnipiac.edu	Win 2003	mirror
M0sted	 ★ foil.northwestern.edu	Linux	mirror
NeT-DeViL	 ★ forum.stanford.edu/images/cont...	Linux	mirror
NeT-DeViL	 ★ frechet.cchem.berkeley.edu	Win 2003	mirror
Team Posion	 ★ harvard.edu	Win 2008	mirror
M0sted	 ★ hl.mccormick.northwestern.edu	Linux	mirror
M0sted	 ★ i2m2.northwestern.edu	Linux	mirror
M0sted	 ★ icomm.northwestern.edu	Linux	mirror
M0sted	 ★ icomm2012.northwestern.edu	Linux	mirror
M0sted	 ★ kung.northwestern.edu	Linux	mirror
M0sted	 ★ leonard.northwestern.edu	Linux	mirror
M0sted	 ★ manufacturing.northwestern.edu	Linux	mirror
M0sted	 ★ mason.northwestern.edu	Linux	mirror
M0sted	 ★ mbp.northwestern.edu	Linux	mirror
ks	 ★ missouriwestern.edu	Win 2003	mirror
M0sted	 ★ mpd.northwestern.edu	Linux	mirror
M0sted	 ★ msec2008.northwestern.edu	Linux	mirror
M0sted	 ★ mtl.northwestern.edu	Linux	mirror
M0sted	 ★ netfrontier2011.northwestern.edu	Linux	mirror
9-gate	 online.subr.edu	Win 2008	mirror
9-gate	 online.sus.edu	Win 2008	mirror
BOLIVIAN - HACKING	 privalsky.mic.ucdavis.edu/joom...	MacOSX	mirror
NeT-DeViL	 ★ qp.ee.columbia.edu/qp/	MacOSX	mirror
M0sted	 ★ rocs.northwestern.edu	Linux	mirror
Swan	 ★ scienceclub.northwestern.edu/c...	Linux	mirror
M0sted	 ★ shahlab.northwestern.edu	Linux	mirror
Dr.SHA6H	 supertiger.wustl.edu/tmp/	MacOSX	mirror
313	 uanews.ua.edu	Linux	mirror
Dr.SHA6H	 ub.iit.edu	Linux	mirror
M4ST£R 1T4L14N H@CK£RS T£4M	 vinecon.ucdavis.edu	Linux	mirror
HighTech	 ★ www.bc.edu/economics/		mirror
M0sted	 ★ www.bcics.northwestern.edu	Linux	mirror
M0sted	 ★ www.cics.northwestern.edu	Linux	mirror
M0sted	 ★ www.cqe.northwestern.edu	Linux	mirror
jo & tu team	 ★ www.cs.sunysb.edu	Linux	mirror
M0sted	 ★ www.dunand.northwestern.edu	Linux	mirror
M0sted	 ★ www.etopia.northwestern.edu	Linux	mirror
M0sted	 ★ www.infotech.northwestern.edu	Linux	mirror

CIR

M0sted	★ www.isense.northwestern.edu	Linux	mirror
M0sted	★ www.lead.northwestern.edu	Linux	mirror
M0sted	★ www.lps.cornell.edu	Linux	mirror
M0sted	★ www.nuim.northwestern.edu	Linux	mirror
M0sted	★ www.ppcr.hms.harvard.edu	Linux	mirror
Dr.SHA6H	★ www.rso.cornell.edu/consulting/	Linux	mirror
SaccaFrazi	★ www3.law.harvard.edu/orgs/memb...	Linux	mirror
NeT-DeViL	★ www-cs.stanford.edu/pldi10/	Linux	mirror
NeT-DeViL	★ www-forum.stanford.edu/images/...	Linux	mirror














































.Other (378)

Notifier	L ★ Domain	OS	View
9-gate	★ 1cebuexpo.cebuph.gov.ph/_ssi/	Win 2008	mirror
Ashiyane Digital Security Team	a2zsell.com	Linux	mirror
1923Turk	acpm.netii.net	Linux	mirror
TNCA	adidasioriunde.net	Linux	mirror
TNCA	adidasisport.net	Linux	mirror
Maxney	★ admin.mercedes-benz.hu/hacked...	Linux	mirror
Dr BiLLi	adriana-serban.com	Linux	mirror
مستتر هزام	★ afdc-mdu53.rtarf.mi.th/home/lo...	Linux	mirror
مستتر هزام	★ afdc-sdo.rtarf.mi.th/new/media...	Linux	mirror
Maxney	★ ajanlatok.mercedes-benz.hu/ind...	Linux	mirror
Ashiyane Digital Security Team	albrekords.com	Linux	mirror
Dr BiLLi	aliantawebdesign.ro	Linux	mirror
HighTech	★ ananiev-rada.odessa.gov.ua	Linux	mirror
HighTech	★ arciz-rada.odessa.gov.ua	Linux	mirror
Ashiyane Digital Security Team	arsenbeatz.com	Linux	mirror
Maxney	★ artbank.mercedes-benz.hu/index...	Linux	mirror
Hacked by Dr. Cruz	★ aspirasi.kulonprogokab.go.id/.php	Linux	mirror
مستتر هزام	★ aukkrit.rtarf.mi.th/phpbb_old/	Linux	mirror
HighTech	★ balta-rada-t.odessa.gov.ua	Linux	mirror
Dbuzz	★ bappeda.gorontaloikota.go.id/id...	Linux	mirror
TNCA	basketone.ro/index.php?route=i...	Linux	mirror
Hacked by Dr. Cruz	★ batik.kulonprogokab.go.id/.php	Linux	mirror
MagelangCyber	★ bbs.zhuzhou.gov.cn/jundab.txt	Win 2003	mirror
HighTech	★ bd-rada.odessa.gov.ua	Linux	mirror
HighTech	★ berezivka-rada.odessa.gov.ua	Linux	mirror
HighTech	★ bilyaivka-rada.odessa.gov.ua	Linux	mirror
Hacked by Dr. Cruz	★ bkd.kulonprogokab.go.id/.php	Linux	mirror
hatrk001	bkkgt.com/wp-content/themes/tw...	Linux	mirror
hatrk	★ boleta.ugelleoncioprado.gob.pe	Linux	mirror
HighTech	★ bolgrad-rada.odessa.gov.ua	Linux	mirror
ExE.Ps	boschcordless-pt.com	Linux	mirror
ExE.Ps	boschpowertools-pt.com	Linux	mirror














































CIR

Black Angels	★ bss.preview.extreme.co.tz/inde...	Linux	mirror
Hacked by Dr. Cruzz	★ budparpora.kulonprogokab.go.id...	Linux	mirror
Black Angels	bulwark.preview.extreme.co.tz/...	Linux	mirror
Black Angels	campaign.preview.extreme.co.tz...	Linux	mirror
3xp1r3	carnztraining.co.nz/3ca.html	Linux	mirror
Black Angels	casl.preview.extreme.co.tz/ind...	Linux	mirror
Black Angels	cc.preview.extreme.co.tz/index...	Linux	mirror
Hmei7	★ cema.vitis.uspnet.usp.br/x.htm	Linux	mirror
Dr-TaiGaR	★ cepavi.jalisco.gob.mx	Win 2008	mirror
Tmide Hacker	cfimmo.fr	HP-UX	mirror
Ashiyane Digital Security Team	chatfriends.me	Linux	mirror
hitcher	★ chicago.mfa.gov.il/hitcher-own...	Win 2008	mirror
KSG-CREW	chinatravel.kz/index.htm	Linux	mirror
Hmei7	★ cnc.benq.com.cn/x.htm	Win 2003	mirror
3xp1r3	colouredwarmbloods.co.nz/3ca.html	Linux	mirror
3xp1r3	corpmassage.co.nz/3ca.html	Linux	mirror
1923Turk	★ cr.regioncusco.gob.pe	Linux	mirror
Turkish Energy Team	★ criesprojetos.unesco.org.br/b...	Win 2003	mirror
Hmei7	★ ct4.ct.ufrj.br/x.htm	Linux	mirror
HighTech	★ customs.odessa.gov.ua	Linux	mirror
مستتر هزام	★ dcjs3.rtarf.mi.th/Dep1/languag...	Linux	mirror
Hacked by Dr. Cruzz	★ dinkes.kulonprogokab.go.id/.php	Linux	mirror
Hacked by Dr. Cruzz	★ dipertahut.kulonprogokab.go.id...	Linux	mirror
Hacked by Dr. Cruzz	★ disperindagesdm.kulonprogokab....	Linux	mirror
SaccaFrazi	★ doea.klcc.gov.tw/l.txt	Unknown	mirror
Hacked by Dr. Cruzz	★ dppka.kulonprogokab.go.id/.php	Linux	mirror
Hacked by Dr. Cruzz	★ dpu.kulonprogokab.go.id/.php	Linux	mirror
3xp1r3	dreamweaver.co.nz/3ca.html	Linux	mirror
1923Turk	★ drem.regioncusco.gob.pe	Linux	mirror
Hmei7	★ eagle.lamcso.coppe.ufrj.br/x.htm	Linux	mirror
TNCA	e-anastore.com	Linux	mirror
Turkish Energy Team	★ ece.unesco.org.br/byrcp.html	Win 2003	mirror
hatrk001	ecolcars.com/wp-content/themes...	Linux	mirror
KSG-CREW	economtour.kz/index.htm	Linux	mirror
Mugair	ecopaint.co.za/backup/	Linux	mirror
مستتر هزام	★ e-learningagd.rtarf.mi.th/mood...	Linux	mirror
Black Angels	elegant.preview.extreme.co.tz/...	Linux	mirror
3body	enazah1.com	Linux	mirror
a.M.e	★ energiabc.gob.mx/index.php	Linux	mirror
Black Angels	energy.preview.extreme.co.tz/i...	Linux	mirror
Black Angels	energysecurity.preview.extreme...	Linux	mirror
Maxney	★ e-osztaly.mercedes-benz.hu	Linux	mirror
Black Angels	equip.preview.extreme.co.tz/in...	Linux	mirror
Black Angels	equipgrc.preview.extreme.co.tz...	Linux	mirror
Ashiyane Digital Security Team	eroticcamslive.com	Linux	mirror












































CIR

KSG-CREW		familyresort.kz/index.htm	Linux	mirror
Black Angels		fatema.preview.extreme.co.tz/i...	Linux	mirror
Ashiyane Digital Security Team	 ★	ffmpegservers.info	Linux	mirror
Cu do MRC	 ★	finance-mansehra.gov.pk	Linux	mirror
Bangladesh cyber army	 ★	fincom.gov.lk/bca.html	F5 Big-IP	mirror
Black Angels	 ★	flights.preview.extreme.co.tz/...	Linux	mirror
StRoNiX	 ★	foxnews2go.mobi	Unknown	mirror
3xp1r3		freeholdexpress.co.nz/3ca.html	Linux	mirror
Ashiyane Digital Security Team		free-nude-pics-hardcore-teen-s...	Linux	mirror
Ashiyane Digital Security Team		freeonlinechatforum.com	Linux	mirror
HighTech	 ★	frunzivka-rada.odessa.gov.ua	Linux	mirror
Black Angels		gallow.preview.extreme.co.tz/i...	Linux	mirror
Black Angels		gallow.preview.extreme.co.tz/i...	Linux	mirror
Black Angels		genesis.preview.extreme.co.tz/...	Linux	mirror
3xp1r3		georgludwig.co.nz/3ca.html	Linux	mirror
ExE.Ps		germes.com	Linux	mirror
Black Angels		gifts.preview.extreme.co.tz/in...	Linux	mirror
Black Angels		giftsandvarieties.preview.extr...	Linux	mirror
Maxney	 ★	glkroadshow.mercedes-benz.hu/i...	Linux	mirror
xc0d3	 ★	gobierno.mdsanluis.gob.pe	Linux	mirror
Black Angels		golden.preview.extreme.co.tz/i...	Linux	mirror
T0r3x	 ★	gomel.customs.gov.by	Win 2003	mirror
TUBE		google.com.tr	Linux	mirror
1923Turk	 ★	grde.regioncusco.gob.pe	Linux	mirror
1923Turk	 ★	grppat.regioncusco.gob.pe	Linux	mirror
1923Turk	 ★	grrngma.regioncusco.gob.pe	Linux	mirror
Black Angels		gumblowcabxi.com/index.php	Linux	mirror
Bangladesh cyber army	 ★	heritagemin.gov.lk/bca.html	F5 Big-IP	mirror
Damane-Dz	 ★	highereducation.gov.ly	Linux	mirror
McStone	 ★	hospitaldepacora.gov.co	Linux	mirror
ExE.Ps		hostingprestashop.com/capturas/	Linux	mirror
KSG-CREW		hotelemirates.kz/index.htm	Linux	mirror
sTeel	 ★	http.www.maitum.gov.ph/mon/	Win 2003	mirror
SA3D HaCk3D	 ★	hy.tlrd.gov.cn/x.txt	Win 2003	mirror
Black Angels		hyundai.preview.extreme.co.tz/...	Linux	mirror
HighTech	 ★	iac.odessa.gov.ua	Linux	mirror
Black Angels	 ★	ict.preview.extreme.co.tz/inde...	Linux	mirror
b0ogle	 ★	identix.state.gov/qotw/Dynamic...		mirror
ExE.Ps		iesdaran.com	Linux	mirror
ExE.Ps		iesprimerodemayo.com	Linux	mirror
hatrk	 ★	incidencias.ugelleoncioprado.g...	Linux	mirror
Black Angels		indian.preview.extreme.co.tz/i...	Linux	mirror
ArTiN		indiancommodities.com/ar.txt	Win 2003	mirror
KHG		infoshqperia.org	Linux	mirror
Dbuzz	 ★	inspektorat.gorontaloikota.go.i...	Linux	mirror














































CIR

Hacked by Dr. Cruzz	 ★ inspektorat.kulonprogokab.go.i...	Linux	mirror
Black Angels	 instyle.preview.extreme.co.tz/...	Linux	mirror
Ashiyane Digital Security Team	 ★ intranet.comune.specchia.lecce...	Win 2003	mirror
hatrk	 ★ intranet.ugelleoncioprado.gob.pe	Linux	mirror
hatrk	 ★ intranet2.ugelleoncioprado.gob.pe	Linux	mirror
HighTech	 ★ invest.odessa.gov.ua	Linux	mirror
Black Angels	 issa.preview.extreme.co.tz/ind...	Linux	mirror
Black Angels	 ist.preview.extreme.co.tz/inde...	Linux	mirror
ExE.Ps	 ★ itvadomicilio.com	Linux	mirror
HighTech	 ★ ivanivka-rada-t.odessa.gov.ua	Linux	mirror
HighTech	 ★ izmail-rada.odessa.gov.ua	Linux	mirror
مستر هزام	 ★ j1.rtarf.mi.th/new/images/ozio...	Linux	mirror
Black Angels	 jamana.preview.extreme.co.tz/i...	Linux	mirror
Hacked by Dr. Cruzz	 ★ jdih.kulonprogokab.go.id/.php	Linux	mirror
ExE.Ps	 jesuitinasmedina.com	Linux	mirror
ExE.Ps	 josemiguelduran.com	Linux	mirror
ExE.Ps	 juegogratis.es	Linux	mirror
Dr.SHA6H	 ★ kamparkab.go.id	Linux	mirror
Dbuzz	 ★ kamus.gorontalokota.go.id/id.htm	Linux	mirror
Black Angels	 karibuholidays.preview.extreme...	Linux	mirror
HighTech	 ★ kiliya-rada.odessa.gov.ua	Linux	mirror
Black Angels	 kisima.preview.extreme.co.tz/i...	Linux	mirror
HighTech	 ★ kodima-rada.odessa.gov.ua	Linux	mirror
ynR !	 ★ kogap.gov.tr/ynr.php	Linux	mirror
HighTech	 ★ komintern-rada.odessa.gov.ua	Linux	mirror
Dbuzz	 ★ kotautara.gorontalokota.go.id/...	Linux	mirror
HighTech	 ★ kotovsk-rada.odessa.gov.ua	Linux	mirror
Dbuzz	 ★ kpde.gorontalokota.go.id/id.htm	Linux	mirror
Hacked by Dr. Cruzz	 ★ kpm.kulonprogokab.go.id/.php	Linux	mirror
Hacked by Dr. Cruzz	 ★ kpt.kulonprogokab.go.id/.php	Linux	mirror
Dbuzz	 ★ kpud-tangselkota.go.id/id.htm	Linux	mirror
HighTech	 ★ krasnookn-rada.odessa.gov.ua	Linux	mirror
Hacked by Dr. Cruzz	 ★ kulonprogokab.go.id/.php	Linux	mirror
Black Angels	 kunduchi.preview.extreme.co.tz...	Linux	mirror
داعس هكر	 ★ loei.nfe.go.th/portal/	Win 2008	mirror
Hacked by Dr. Cruzz	 ★ lppd.kulonprogokab.go.id/.php	Linux	mirror
HighTech	 ★ lybashivka-rada.odessa.gov.ua	Linux	mirror
Hacked by Dr. Cruzz	 ★ mail.kulonprogokab.go.id/.php	Linux	mirror
Black Angels	 makepovertyhistory.preview.ext...	Linux	mirror
3xp1r3	 ★ mariedisomma.co.nz/3ca.html	Linux	mirror
مستر هزام	 ★ mdo.rtarf.mi.th/magazine/magaz...	Linux	mirror
hatrk	 ★ mdyuracyacu.gob.pe/index.html	Linux	mirror
Turkish Ajan Hack Team	 ★ media.daimler.hu/hacked.html	Linux	mirror
ExE.Ps	 mgmfloresycomplementos.es	Linux	mirror
HighTech	 ★ mikolaivka-rada.odessa.gov.ua	Linux	mirror

CIR

Black Angels		mind-health.preview.extreme.co...	Linux	mirror
The Viper 404	 ★	mkhambathini.gov.za	Linux	mirror
Antonio		mmenterprisebd.com	ThePlanet/ Shared	mirror
3xp1r3		mobilesandblasting.co.nz/3ca.html	Linux	mirror
Black Angels		montblanc.preview.extreme.co.t...	Linux	mirror
HighTech	 ★	morroreuter.rs.gov.br	Linux	mirror
Ashiyane Digital Security Team		motivateinspire.net	Linux	mirror
sLaSh HaCkEr	 ★	mri.gov.lk	Linux	mirror
Saudi Terrorist		mrwhippy.net	Linux	mirror
Bangladesh Cyber Army	 ★	municanchis.gob.pe/rexo.html	Linux	mirror
hatrk	 ★	muniesv.gob.pe/index.html	Linux	mirror
Bangladesh Cyber Army	 ★	muniquiruvilca.gob.pe/rexo.html	Linux	mirror
Bangladesh Cyber Army	 ★	muni-salcahuasi.gob.pe/rexo.html	Linux	mirror
Saudi Terrorist		my-ipod-nano.com	Linux	mirror
Saudi Terrorist		myownpharmacy.com	Linux	mirror
Black Angels		ndege.preview.extreme.co.tz/in...	Linux	mirror
Saudi Terrorist	 ★	newartistreview.com	Linux	mirror
Maxney	 ★	newsletter.mercedes-benz.hu/in...	Linux	mirror
Saudi Terrorist		newsnow247.com	Linux	mirror
NeT-DeViL	 ★	nigeriaembassysyria.org	Linux	mirror
Z4R4THUSTR4	 ★	nongphi.go.th/htaccess.txt	Linux	mirror
Turkish Energy Team	 ★	ns2.iaem.gob.ve/x.txt	Linux	mirror
Ashiyane Digital Security Team		nsfwweblog.com	Linux	mirror
HighTech	 ★	oblrada.odessa.gov.ua	Linux	mirror
HighTech	 ★	oda.odessa.gov.ua	Linux	mirror
Black Angels		offer.preview.extreme.co.tz/in...	Linux	mirror
Saudi Terrorist		olive-groove.com	FreeBSD	mirror
Saudi Terrorist		oliveonline.com	Linux	mirror
Black Angels		olympic.preview.extreme.co.tz/...	Linux	mirror
ExE.Ps		onlydosmaletas.com	Linux	mirror
HighTech	 ★	orsf.odessa.gov.ua	Linux	mirror
HighTech	 ★	ovidopol-rada.odessa.gov.ua	Linux	mirror
Dbuzz	 ★	pa-barru.go.id	Linux	mirror
siberian_husky	 ★	pa-bengkayang.go.id/images/hus...	Linux	mirror
3xp1r3		palletimprovements.co.nz/3ca.html	Linux	mirror
ZiyaretCi	 ★	pappasbp.mercedes-benz.hu/alol...	Linux	mirror
ZiyaretCi	 ★	pappaspecs.mercedes-benz.hu/al...	Linux	mirror
siberian_husky	 ★	pa-tilamuta.go.id/tmp/huskydow...	Linux	mirror
3xp1r3		pauabay.com/3ca.html	MacOSX	mirror
Dr.SHA6H	 ★	pdkjateng.go.id	Linux	mirror
hatrk	 ★	pedagogica.ugelleoncioprado.go...	Linux	mirror
Dbuzz	 ★	pendidikan.gorontaloikota.go.id...	Linux	mirror
Hacked by Dr. Cruzz	 ★	perpustakaan.kulonprogokab.go...	Linux	mirror
Black Angels		picoage.preview.extreme.co.tz/...	Linux	mirror

CIR

3xp1r3	 pilgrims.co.nz/3ca.html	Linux	mirror
gilang	 ★ pn-lahat.go.id/tmp/index.php	Linux	mirror
alex_owners	 ★ policebloodbank.gov.bd	Linux	mirror
ExE.Ps	 posicionamientoengoogleplaces.com	Linux	mirror
war0k	 ★ pramuka.baubaukota.go.id/index...	Linux	mirror
Black Angels	 preview.extreme.co.tz/indexx.html	Linux	mirror
Black Angels	 proactive.preview.extreme.co.t...	Linux	mirror
ExE.Ps	 programadefidelizacion.com	Linux	mirror
hatrk001	 prowing.org/wp-content/themes/...	Linux	mirror
Black Angels	 radelicious.preview.extreme.co...	Linux	mirror
1923Turk	 ★ regioncusco.gob.pe/index.php	Linux	mirror
HighTech	 ★ reni-rada.odessa.gov.ua	Linux	mirror
M0sted	 ★ rocs.northwestern.edu	Linux	mirror
Xc0t3z	 ★ rosariodalimeira.mg.gov.br	Linux	mirror
HighTech	 ★ rozdilna-rada.odessa.gov.ua	Linux	mirror
Hacked by Dr. Cruz	 ★ rsud.kulonprogokab.go.id/.php	Linux	mirror
Black Angels	 rujeva.preview.extreme.co.tz/i...	Linux	mirror
3bady	 s666k.org	Linux	mirror
The Viper 404	 ★ sals.gov.za	Linux	mirror
HighTech	 ★ sarata-rada.odessa.gov.ua	Linux	mirror
Black Angels	 sarawany.preview.extreme.co.tz...	Linux	mirror
HighTech	 ★ savran-rada.odessa.gov.ua	Linux	mirror
Black Angels	 secure7.preview.extreme.co.tz/...	Linux	mirror
Hacked by Dr. Cruz	 ★ setda.kulonprogokab.go.id/.php	Linux	mirror
HighTech	 ★ shiryaivo-rada.odessa.gov.ua	Linux	mirror
ArTiN	 shiyan.foredu.com.cn/ar.txt	Linux	mirror
ExE.Ps	 shop.icarpio.com	Linux	mirror
HighTech	 ★ siaz.odessa.gov.ua	Linux	mirror
ExE.Ps	 simemimas.com	Linux	mirror
Dr-TaiGaR	 ★ sistemadif.jalisco.gob.mx	Win 2008	mirror
NeT-DeViL	 ★ sistemas01.ufscar.br/relea/con...	Linux	mirror
X-Line	 ★ sivasilozelidaresi.gov.tr	Win 2003	mirror
X-Line	 ★ sivasozelidare.gov.tr	Win 2003	mirror
Black Angels	 skylink.preview.extreme.co.tz/...	Linux	mirror
DR-MTMRD	 ★ sokhcn.cantho.gov.vn/index.htm	Win 2008	mirror
Black Angels	 sophiahouse.preview.extreme.co...	Linux	mirror
Black Angels	 spear.preview.extreme.co.tz/in...	Linux	mirror
Black Angels	 speed.preview.extreme.co.tz/in...	Linux	mirror
h4x0r HuSsY	 ★ sra.gov.in	Win 2003	mirror
ExE.Ps	 suministroemergencias.biz	Linux	mirror
ExE.Ps	 suministroemergencias.com	Linux	mirror
ExE.Ps	 suministroemergencias.es	Linux	mirror
ExE.Ps	 suministroemergencias.net	Linux	mirror
ExE.Ps	 suministroemergencias.org	Linux	mirror
9-gate	 ★ suroysuroy.cebu.gov.ph/htmlfile/	Win 2008	mirror








CIR

NeT-DeViL	★ swissconsulate.mn	Linux	mirror
Black Angels	tanzanair.preview.extreme.co.t...	Linux	mirror
HighTech	★ tarutino-rada.odessa.gov.ua	Linux	mirror
Dbuzz	★ tatakota.gorontaloikota.go.id/i...	Linux	mirror
HighTech	★ tatarbunar-rada.odessa.gov.ua	Linux	mirror
hatrk	★ terceros.ugelleoncioprado.gob.pe	Linux	mirror
CaRaBaSaN	★ thanhtratinh.kontum.gov.vn/pag...	Win 2008	mirror
ExE.Ps	tiendapiscinasonline.es	Linux	mirror
YaCiNe t-h-e***h-e-l-l	★ tlalpujahu.gob.mx/thehEIL.php	Linux	mirror
3xp1r3	tongancommunity.org.nz/3ca.html	Linux	mirror
Black Angels	toplis.preview.extreme.co.tz/i...	Linux	mirror
Black Angels	tppl.preview.extreme.co.tz/ind...	Linux	mirror
Black Angels	transcargo.preview.extreme.co....	Linux	mirror
hatrk	★ transparencia.munibellavistasm...	Linux	mirror
hatrk	★ transparencia.ugelleoncioprado...	Linux	mirror
Black Angels	travellink.preview.extreme.co....	Linux	mirror
Black Angels	★ tsacareercoaching.tsa.dhs.gov/...	Linux	mirror
Black Angels	★ tsacareercoaching.tsa.dhs.gov/...	Linux	mirror
Hmei7	★ tunisianembassyjakarta.com/a.txt	Linux	mirror
Black Angels	tupohapa.preview.extreme.co.tz...	Linux	mirror
ExE.Ps	turiweb.es	Linux	mirror
ExE.Ps	tutorial-wordpress.com	Linux	mirror
Black Angels	tznic.preview.extreme.co.tz/in...	Linux	mirror
hatrk	★ ugelleoncioprado.gob.pe/index....	Linux	mirror
ZiyaretCi	★ ujhelyi.mercedes-benz.hu/alold...	Linux	mirror
3xp1r3	underfloorheating.org.nz/3ca.html	Linux	mirror
Ashiyane Digital Security Team	unitedconstructioninc.com	Linux	mirror
Core Team	★ uto2.moph.go.th/ict/templates/	Linux	mirror
ExE.Ps	valentiaautores.com	Linux	mirror
Bangladesh cyber army	★ valuationdept.gov.lk/bca.html	F5 Big-IP	mirror
ExE.Ps	vdb-racing.com	Linux	mirror
HighTech	★ ved.odessa.gov.ua	Linux	mirror
3xp1r3	vervecatering.co.nz/3ca.html	Linux	mirror
Ashiyane Digital Security Team	videocopilot.co.nz/article_det...	Linux	mirror
3xp1r3	vintagetractorparts.co.nz/3ca....	Linux	mirror
HighTech	★ v-mihailivka-rada.odessa.gov.ua	Linux	mirror
3xp1r3	volexstyle.com/3ca.html	Linux	mirror
Black Angels	wambi.preview.extreme.co.tz/in...	Linux	mirror
Turkish Energy Team	★ web.cmr.ensino.eb.br/byrcp.htm	Linux	mirror
CyberBellona	★ winbig.microsoftstore.com/elma...	Win 2008	mirror
3xp1r3	woodendlandscape.co.nz/3ca.html	Linux	mirror
T0r3x	★ www.5.circolopozzuoli.gov.it	Linux	mirror
TNCA	www.adidasioferta.net	Linux	mirror
x-hayben21	★ www.ahcollege.gov.bd/root.txt	Linux	mirror
Antonio	www.alas7ar.com/hsh.php	Linux	mirror

CIR

Turkish Ajan Hack Team	 ★	www.alkatresz.daimlerchrysler...	Linux	mirror
Antonio		www.angkanas.com/hsh.php	Linux	mirror
Antonio		www.aotkc.com/hsh.php	Linux	mirror
TeAm Dr.Hacker		www.ardalmahaba.com/vb	Linux	mirror
Ashiyane Digital Security Team		www.bikontakt.net	Linux	mirror
Baader Meinhof	 ★	www.cb.sc.gov.br/ditisoftlivre...	Linux	mirror
Baader Meinhof	 ★	www.cbm.sc.gov.br/ditisoftlivr...	Linux	mirror
NeT-DeViL	 ★	www.ccco.danang.gov.vn/asset/	Win 2008	mirror
Hmei7	 ★	www.chevrolet.com.np/news_and_...	Linux	mirror
ALG-LOVE MOHAMED	 ★	www.cia.gov/cia/publications/f...	ThePlanet/ Shared	mirror
rooterror	 ★	www.copyrightlabs.in	Linux	mirror
Hmei7	 ★	www.ct.ufrj.br/x.htm	Linux	mirror
Turkish Ajan Hack Team	 ★	www.daimlerchrysler.hu	Linux	mirror
HighTech	 ★	www.erzincankontrollab.gov.tr	Linux	mirror
TNCA	 ★	www.evaluare.mercantil-online.ro	Linux	mirror
CrAzY HaCkEr		www.fastfitnessstation.com	Linux	mirror
Turkish Energy Team	 ★	www.forum.daughertytownship-pa...	Linux	mirror
ZxX		www.goldensun.busko.com.pl/pag...	Linux	mirror
anwaraze	 ★	www.gorgas.gob.pa	Linux	mirror
Digital Boys Underground Team	 ★	www.gowerplacepractice.nhs.uk	Win 2003	mirror
m1I05		www.grad-zadar.hr/vijest/opce-...	Linux	mirror
Ashiyane Digital Security Team	 ★	www.gysq.gov.cn/zcfg/ShowArtic...	Win 2003	mirror
1923Turk		www.hadhhogayi.com/tmp/ToRoSBe...	Linux	mirror
br4v37		www.harmony.org.uk	Linux	mirror
syhmfz	 ★	www.hy96345.gov.cn	Win 2003	mirror
syhmfz	 ★	www.jepb.gov.cn	Win 2003	mirror
HighTech	 ★	www.juntadesalto.gub.uy	Linux	mirror
m1I05		www.kkzadar.net/vijest/2012-09...	Linux	mirror
EviLHaCk		www.kuwaitystock.com/vb	Linux	mirror
TeslaTeam		www.latina.hr	Linux	mirror
Saudi - Hack	 ★	www.lesgargouilles.fr	Linux	mirror
Saudi - Hack		www.madifor.fr/index2.php	Linux	mirror
TeaM MosTa	 ★	www.mairie-la-talaudiere.fr/up...	Linux	mirror
Turkish Ajan Hack Team	 ★	www.media.daimlerchrysler.hu/h...	Linux	mirror
liderpirata	 ★	www.mhc15.go.th	Linux	mirror
liderpirata	 ★	www.mhc15.go.th	Linux	mirror
ExE.Ps		www.milenciaerotica.es	Linux	mirror
Hmei7	 ★	www.mozbusiness.gov.mz	Win 2008	mirror
The Viper 404	 ★	www.mpuleg.gov.za	Linux	mirror
KmLI	 ★	www.muniancolamar.gob.pe/sites/	Linux	mirror
Vidson	 ★	www.munisanmiguel.gob.pe	Win 2003	mirror
Audisoft Hacker Team	 ★	www.munisansebastian.gob.pe	Linux	mirror
Bangladesh Cyber Army	 ★	www.munitalavera.gob.pe/rexo.html	Linux	mirror
br4v37	 ★	www.nsgproject.com	Linux	mirror

CIR

HighTech	 ★	www.odessa.gov.ua	Win 2003	mirror
br4v37		www.peopleforwork.com	Linux	mirror
HaYaL-ET-06		www.pmjumu.oni.cc	Linux	mirror
Dbuzz	 ★	www.pn-karanganyar.go.id	Linux	mirror
منظمة الإرهاب السعودي	 ★	www.qkadmin.gov.sa//index.htm	Unknown	mirror
ExE.Ps		www.regaloydetalle.com	Linux	mirror
T0r3x	 ★	www.rela.gov.my	Unknown	mirror
Gaza HaCKeR Team	 ★	www.sbcounty.gov/workforce/ind...	F5 Big-IP	mirror
Ashiyane Digital Security Team		www.sexchatvideotube.com	Linux	mirror
LeTh_HaCkEr	 ★	www.shaqraedu.gov.sa/index1.php	Linux	mirror
RedHack	 ★	www.siverek.gov.tr	Win 2003	mirror
MagelangCyber	 ★	www.sxsrc.gov.cn/jundab.txt	Win 2003	mirror
TheWayEnd	 ★	www.syftec.gov.cn/Art_Single_e...	Win 2003	mirror
ExE.Ps		www.tiendanostradamus.com	Linux	mirror
MINDCRACKER	 ★	www.tuncelidh.gov.tr	Linux	mirror
Black Angels	 ★	www.tupeloms.gov/parkandrec/20...	Linux	mirror
Black Angels	 ★	www.tupeloms.gov/parkandrec/20...	Linux	mirror
a.M.e	 ★	www.ugelsihuas.gob.pe	Linux	mirror
Hmei7	 ★	www.un.org.ph	Win 2003	mirror
virtual hacker	 ★	www.unece.net	Linux	mirror
ZoRRoKiN	 ★	www.unesco.org/cu/lacult/pais/...	Win 2003	mirror
CrAzY HaCkEr	 ★	www.vbspervijze.be	Linux	mirror
Antonio		www.viageraes.com.br/noticias/	Linux	mirror
ExE.Ps		www.videojuegosbilbao.com	Linux	mirror
Hmei7	 ★	www.xerem.ufrj.br/tmp/x.htm	Linux	mirror
MagelangCyber	 ★	www.zzkj.gov.cn/jundab.txt	Win 2003	mirror
RainsevenDotMy	 ★	www1.mada.gov.my/Rain.php	Linux	mirror
Black Angels	 ★	xcar.preview.extreme.co.tz/ind...	Linux	mirror
ArTiN		xinshilu.foredu.com.cn/ar.txt	Linux	mirror
MagelangCyber	 ★	xmsc.zhuzhou.gov.cn/jundab.txt	Win 2003	mirror
Black Angels		zamzam.preview.extreme.co.tz/i...	Linux	mirror
Black Angels		zantravel.preview.extreme.co.t...	Linux	mirror
ExE.Ps		zpatos.com	Linux	mirror

CIR

Top 10 Ports

by Reports		by Targets		by Sources	
Port	Reports	Port	Targets	Port	Sources
445	336286	23	58648	445	14308
3389	116036	3389	46059	3389	9369
23	68045	22	38332	80	6962
22	65981	1433	37578	53	3517
80	64643	445	21857	35691	3269
139	62145	4899	20460	25	865
1433	50954	1434	9277	23	822
53	32281	8080	9162	4899	576
4899	21526	80	5685	30247	391
587	13070	9090	4708	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

If you do not want to receive future emails from us, contact remove@informationwarfarecenter.com