INFORMATION WARFARE CENTER V3.0

CYBER INTELLIGENCE REPORT

MARCH 3, 2015

The IWC CIR is an 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.

SUMMARY

Symantec ThreatCon Level 2 - Medium: Increased alertness

This condition applies when knowledge or the expectation of attack activity is present, without specific events occurring or when malicious code reaches a moderate risk rating.

THE DIGITAL LANDSCAPE IS CHANGING

Industrial and state sponsored espionage incidents have become daily news recently. Countries are even becoming more brazen about acts of cyber warfare when in the past they at least tried to hide it. The same threats have always been there, thought it seems that the actors are just getting lazier and louder. I hear many people ask "how do you stop it? "… "How do I prevent from becoming a victim?" Truth is, you never could and you can't. Not if you are in the game. It helps to know your enemies. It helps not to put a bulls eye on your back. It also helps if you are not perpetrating in the same attacks you condemn. What helps more is if you practice Operational Security (OPSEC).

To many organizations, across all sectors, fail to do the basic steps in securing their assets. They fail even more to protect your assets. We have seen this increasingly in the healthcare, medical, automotive, national infrastructure and even the government sectors. To quote a saying I grew up with "Common sense isn't that common". It is true, but if you try to follow the prudent person principle, you will most likely fall within Due Diligence. Meaning, what would a reasonable person in a similar situation do. Understand that everyone is at risk… You are at risk. The further we move into the future, the more the digital landscape is changes… "Don't be that guy"… Don't BE the risk…

NEWS: INFORMATION WARFARE

- Corproate espionage case: GMR official quizzed by police - Daily News & Analysis.
- Venezuelan President Claims Americans Detained for 'Espionage' - NBCNews.com.
- Maduro claims Venezuela has detained Americans for 'espionage' - CNN.
- Venezuela tells US embassy in Caracas: Cut staff by 80 percent - Reuters.
- Corporate Espionage: Indian Oil suspends official for leaking information - Daily News & Analysis.
- US spy chief James Clapper highlights cyber threats - BBC News.
- Russia Tops China as Principal Cyber Threat to US - The Diplomat.
- NATO Says Russia Moving Its Weapons Systems In Crimea; Russian Cyber ... - International Business Times
- PM demands solutions against cyber threats from IT sector - Deccan Herald.
- Turkey Seeks National Plan for Cyber Threats - DefenseNews.com.
- Feds Admit Stingrays Can Disrupt Cell Service Of Bystanders.
- ASML Plays Down Mystery Hack.
- Twitter Triples Abuse Team, Knocks Dox.
- Russian Cyber Menace Threatens Industrial Systems.
- Joomla Botnet Furthers DDoS-For-Hire Scheme.
- Report: Majority Of Health Websites Leak Data To Third Parties.
- Iran Hacks America Where It Hurts: Las Vegas Casinos.
- TalkTalk Admits To Massive Data Breach.
- Net Neutrality Prevails In Historic FCC Vote.
- Lizard Squad Hackers Attack Lenovo After Superfish Scandal.
- China Drops US Tech Giants From Approved List.
- Google Cancels Annual Pwnium Competition To Accept Bugs Year-Round.
- Target Breach Costs Company $191M, Financials Show.
- FBI Lobbying To Keep Phone Metadata Spying Powers.
- Secret Service To Test Its Own Drones To Avoid Future Crashes.
- Video: Brain-Controlled Drone Shown Off By Tekever In Lisbon.
- Chicago Police Disappearing Americans At Their Own Black Site.
- Despite FCC Vote, Republicans In Congress Not Conceding On Net Neutrality.
- U.S. Offers Its Largest Bounty For Zeus Hacker Borgachev.
- Europol Shuts Down Darn RAMNIT Botnet.
- Gemalto Claims NSA/GCHQ Did Not Get Their SIM Database.
- 8 Burning Questions About Net Neutrality.
- WordPress Plugin Imperils More Than 1 Million Sites.
- Lenovo Hit By Lawsuit Over Superfish Adware.
- Florida Law Enforcement Docs Show Widespread Stingray Use.

NEWS: HIPPA

- 10 Critical Facts About HIPAA & Claims - PropertyCasualty360.
- HIPAA crackdown extends beyond health care providers - The Tennessean.
- Despite OCR 'crackdown,' few organizations fined for HIPAA violations - FierceHealthIT.
- Potential HIPAA Violations After Wisc. and Texas Thefts - HealthITSecurity.com.

NEWS: SCADA

- Siemens sighs: SCADA bugs abound - The Register.
- The Impact of Piracy on SCADA - Automation World.
- SMA extends collaboration with GreenPowerMonitor with SCADA solutions for ... - solarserver.com.
- SMA and GreenPowerMonitor to Bring SCADA Solutions to PV Power Plants - Solar Novus Today.

NEWS: CYBER LAWS & LEGISLATION

- Legislation Would Criminalize Revenge Porn; Allow Search Warrants for Cyber ... - SCVNEWS.com.
- Nova Scotia's cyber bullying law is a disaster - Canadian Lawyer Magazine.
- Senate advances cyber stalking bill - DesMoinesRegister.com.
- Draft of Senate Cyber Bill Tackles Retaliation Rules - Wall Street Journal.
- Federal law on cyber security is crucial - Seacoastonline.com.

NEWS: COMPUTER FORENSICS

- Companies turn to forensic investigators to detect cyber crime - Channel News
- 'CSI: Cyber' review: Patricia Arquette fine, idea old - New York Daily News.
- Man and woman arrested over missing Becky Watts - Daily Mail.
- Two held in becky 'murder' probe - Daily Mail.
- CSI Reboots Its Franchise With Cybercrime Show - Newsweek.

EXPLOITS

- Symantec Web Gateway 5 restore.php Command Injection.
- Seagate Business NAS Unauthenticated Remote Command Execution.
- D-Link DIR636L Remote Command Injection.
- WordPress Calculated Fields Form 1.0.10 SQL Injection.
- ECCMS 1.0 Cross Site Scripting / SQL Injection.
- ATutor LCMS 2.2 Cross Site Request Forgery.
- BEdita CMS 3.5.0 Cross Site Request Forgery / Cross Site Scripting.
- Linux CVE-2014-9322 Proof Of Concept.
- Linux CVE-2014-4943 Proof Of Concept.
- Linux CVE-2014-3631 Proof Of Concept.
- Fortimail 5.2.1 Cross Site Scripting.
- NetCat CMS 3.12 Remote File Inclusion.
- Packet Storm New Exploits For February, 2015.
- Swiss File Knife 1.7.4 Buffer Overflow.
- WordPress WP All 3.2.3 Shell Upload.
- WordPress Photocrati Theme 4.x.x SQL Injection.
- Ubuntu Vivid Upstart Privilege Escalation.
- Seagate Business NAS 2014.00319 Remote Code Execution.
- NetCat CMS 5.01 Open Redirect.
- NetCat CMS 5.01 / 3.12 Full Path Disclosure.
- Comsenz SupeSite CMS 7.0 Code Execution.
- vBulletin 4.2.2 Remote Code Injection.
- Comsenz SupeSite CMS 7.0 Cross Site Scripting.
- Loxone Smart Home CSRF / XSS / DoS / Credential Leakage.
- HelpDezk 1.0.1 Shell Upload / Code Execution / Disclosure.vBulletin vBSEO 4.x.x 'visitormessage.php' Remote Code Injection Vulnerability.
- Persistent Systems Client Automation Command Injection RCE.
- Seagate Business NAS <= 2014.00319 - Pre-Authentication Remote Code Execution (0day).
- Ubisoft Uplay 5.0 - Insecure File Permissions Local Privilege Escalation.
- Electronic Arts Origin Client 9.5.5 - Multiple Privilege Escalation Vulnerabilities.
- Beehive Forum 1.4.4 - Stored XSS Vulnerability.
- HP Client Automation Command Injection.
- WonderPlugin Audio Player 2.0 - Blind SQL Injection and XSS.
- PCMan FTP Server 2.0.7 - Buffer Overflow - MKD Command.
- Realtek 11n Wireless LAN utility - Privilege Escalation.

CVE ADVISORIES

- CVE-2015-2102.
  - 2015-02-27
    SQL injection vulnerability in view_item.php in ClipBucket 2.7 RC3 (2.7.0.4.v2929-rc3) allows remote attackers to execute arbitrary SQL commands via the item parameter. (CVSS:0.0) (Last Update:2015-02-27)
- CVE-2015-2090.
  - 2015-02-26
    SQL injection vulnerability in the ajax_survey function in settings.php in the WordPress Survey and Poll plugin 1.1.7 for Wordpress allows remote attackers to execute arbitrary SQL commands via the

survey_id parameter in an ajax_survey action to wp-admin/admin-ajax.php. (CVSS:7.5) (Last Update:2015-02-26)

- CVE-2015-2084.
  - 2015-02-25
    Cross-site request forgery (CSRF) vulnerability in the Easy Social Icons plugin before 1.2.3 for WordPress allows remote attackers to hijack the authentication of administrators for requests that conduct cross-site scripting (XSS) attacks via the image_file parameter in an edit action in the cnss_social_icon_add page to wp-admin/admin.php. (CVSS:6.8) (Last Update:2015-02-26)
- CVE-2015-2071.
  - 2015-02-24
    Directory traversal vulnerability in cm/newui/blog/export.jsp in eTouch SamePage Enterprise Edition 4.4.0.0.239 allows remote authenticated users to read arbitrary files via a .. (dot dot) in the filepath parameter. (CVSS:4.0) (Last Update:2015-02-25)
- CVE-2015-2070.
  - 2015-02-24
    SQL injection vulnerability in eTouch SamePage Enterprise Edition 4.4.0.0.239 allows remote attackers to execute arbitrary SQL commands via the catId parameter to cm/blogrss/feed. (CVSS:7.5) (Last Update:2015-02-25)
- CVE-2015-2068.
  - 2015-02-24
    Multiple cross-site scripting (XSS) vulnerabilities in the MAGMI (aka Magento Mass Importer) plugin for Magento Server allow remote attackers to inject arbitrary web script or HTML via the (1) profile parameter to web/magmi.php or (2) QUERY_STRING to web/magmi_import_run.php. (CVSS:4.3) (Last Update:2015-02-25)

ADVISORIES

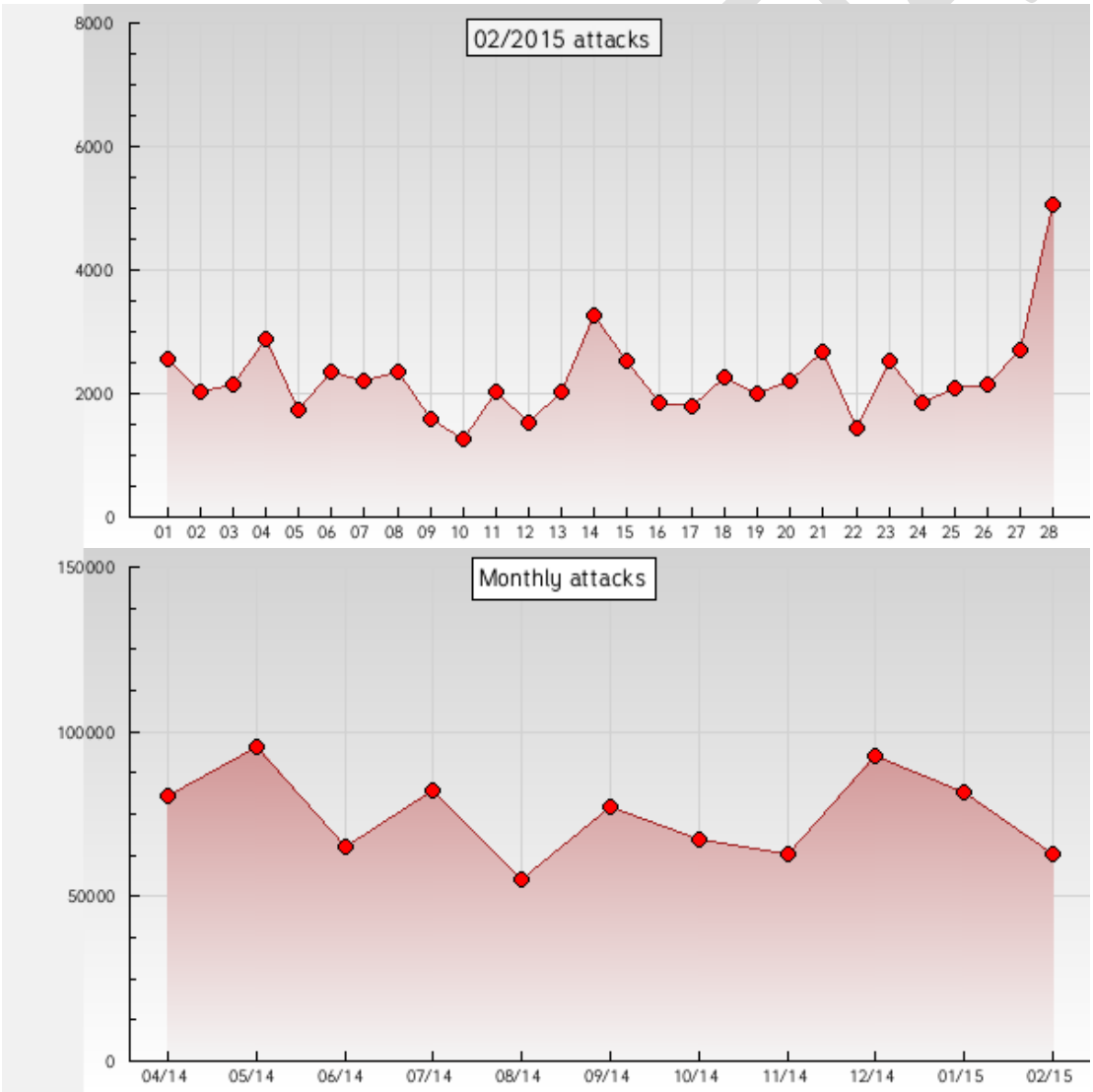
- Mandriva Linux Security Advisory 2015-050.
  - Mon, 02 Mar 2015 22:57:18 GMT
    Mandriva Linux Security Advisory 2015-050 - It was reported that a crafted diff file can make patch eat memory and later segfault. It was reported that the versions of the patch utility that support Git-style patches are vulnerable to a directory traversal flaw. This could allow an attacker to overwrite arbitrary files by applying a specially crafted patch, with the privileges of the user running patch. GNU patch before 2.7.4 allows remote attackers to write to arbitrary files via a symlink attack in a patch file.
- HP Security Bulletin HPSBST03274 1.
  - Mon, 02 Mar 2015 17:44:18 GMT
    HP Security Bulletin HPSBST03274 1 - Potential security vulnerabilities have been identified with HP XP P9000 Command View Advanced Edition Software Online Help for Windows and Linux. The vulnerabilities could be exploited resulting in remote Cross-site scripting (XSS). Revision 1 of this advisory.
- Slim PHP Framework 2.5.0 Weak Cryptography.
  - Mon, 02 Mar 2015 17:34:07 GMT
    Slim PHP Framework versions 2.5.0 and below suffer weak cryptographic implementations.
- Mandriva Linux Security Advisory 2015-049.
  - Mon, 02 Mar 2015 17:24:01 GMT
    Mandriva Linux Security Advisory 2015-049 - A malformed file with an invalid page header and compressed raster data can trigger a buffer overflow in cupsRasterReadPixels.
- Ubuntu Security Notice USN-2516-2.
  - Mon, 02 Mar 2015 17:23:25 GMT
    Ubuntu Security Notice 2516-2 - USN-2516-1 fixed vulnerabilities in the Linux kernel. There was an unrelated regression in the use of the virtual counter (CNTVCT) on arm64 architectures. This update fixes the problem. A flaw was discovered in the Kernel Virtual Machine's (KVM) emulation of the SYSTENTER instruction when the guest OS does not initialize the SYSENTER MSRs. A guest OS user

could exploit this flaw to cause a denial of service of the guest OS (crash) or potentially gain privileges on the guest OS. Various other issues were also addressed.

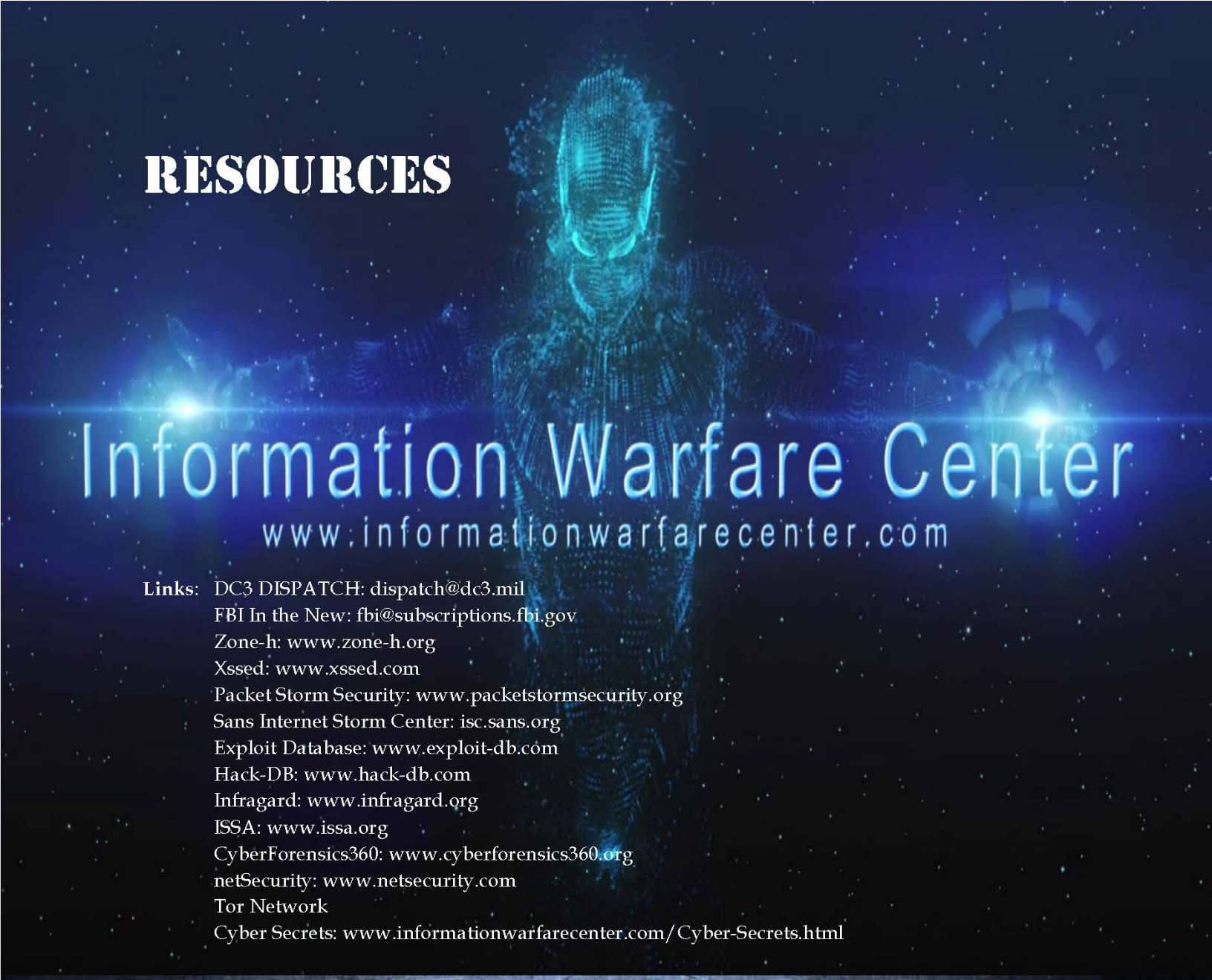
- Piwik Signature Validation.
  - Mon, 02 Mar 2015 03:44:44 GMT
    Piwik fails to perform signature validation when running updates.
- Hikvision DS-7204HWI-SH Brute Force.
  - Sun, 01 Mar 2015 10:11:11 GMT
    Hikvision DS-7204HWI-SH suffers from abuse of functionality and brute force vulnerabilities.
- Apache Standard Taglibs 1.2.1 XXE / Remote Command Execution.
  - Fri, 27 Feb 2015 20:22:22 GMT
    Apache Standard Taglibs version 1.2.1 suffers from XXE and remote command execution vulnerabilities via the XSL extension in JSTL XML tags.
- Debian Security Advisory 3176-1.
  - Fri, 27 Feb 2015 01:58:40 GMT
    Debian Linux Security Advisory 3176-1 - Multiple vulnerabilities have been discovered in Request Tracker, an extensible trouble-ticket tracking system.
- FreeBSD Security Advisory - BIND Denial Of Service.
  - Thu, 26 Feb 2015 17:25:28 GMT
    FreeBSD Security Advisory - BIND servers which are configured to perform DNSSEC validation and which are using managed keys (which occurs implicitly when using "dnssec-validation auto;" or "dnssec-lookaside auto;") may exhibit unpredictable behavior due to the use of an improperly initialized variable. A remote attacker can trigger a crash of a name server that is configured to use managed keys under specific and limited circumstances. However, the complexity of the attack is very high unless the attacker has a specific network relationship to the BIND server which is targeted.
- FreeBSD Security Advisory - IGMP Integer Overflow.
  - Thu, 26 Feb 2015 17:20:51 GMT
    FreeBSD Security Advisory - An integer overflow in computing the size of IGMPv3 data buffer can result in a buffer which is too small for the requested operation. An attacker who can send specifically crafted IGMP packets could cause a denial of service situation by causing the kernel to crash.
- Ubuntu Security Notice USN-2512-1.
  - Thu, 26 Feb 2015 17:15:00 GMT
    Ubuntu Security Notice 2512-1 - A race condition was discovered in the Linux kernel's key ring. A local user could cause a denial of service (memory corruption or panic) or possibly have unspecified impact via the keyctl commands. A memory leak was discovered in the ISO 9660 CDROM file system when parsing rock ridge ER records. A local user could exploit this flaw to obtain sensitive information from kernel memory via a crafted iso9660 image. Various other issues were also addressed.
- Ubuntu Security Notice USN-2519-1.
  - Thu, 26 Feb 2015 17:14:43 GMT
    Ubuntu Security Notice 2519-1 - Arnaud Le Blanc discovered that the GNU C Library incorrectly handled file descriptors when resolving DNS queries under high load. This may cause a denial of service in other applications, or an information leak. This issue only affected Ubuntu 10.04 LTS, Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. It was discovered that the GNU C Library incorrectly handled receiving a positive answer while processing the network name when performing DNS resolution. A remote attacker could use this issue to cause the GNU C Library to hang, resulting in a denial of service. Various other issues were also addressed.
- Ubuntu Security Notice USN-2520-1.
  - Thu, 26 Feb 2015 17:14:29 GMT
    Ubuntu Security Notice 2520-1 - Peter De Wachter discovered that CUPS incorrectly handled certain malformed compressed raster files. A remote attacker could use this issue to cause CUPS to crash, resulting in a denial of service, or possibly execute arbitrary code.
- Slackware Security Advisory - mozilla-firefox Updates.
  - Thu, 26 Feb 2015 17:14:18 GMT
    Slackware Security Advisory - New mozilla-firefox packages are available for Slackware 14.1 and -current to fix security issues.

ZONE-H ATTACK STATISTICS:

N°	Notifier	Single def.	Mass def.	Total def.	Homepage def.	Subdir def.
1.	Barbaros-DZ	3449	157	3606	1223	2383
2.	Hmei7	2843	1510	4353	774	3579
3.	Ashiyane Digital Security Team	2838	4101	6939	1314	5625
4.	LatinHackTeam	1438	1266	2704	2254	450
5.	iskorpitx	1324	955	2279	786	1493
6.	Fatal Error	1110	1723	2833	2453	380
7.	HighTech	926	3218	4144	3255	889
8.	chinahacker	889	1344	2233	4	2229
9.	MCA-CRB	854	626	1480	374	1106
10.	By_aGReSiF	757	1427	2184	802	1382



RESOURCES



Links: 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
Hack-DB: www.hack-db.com
Infragard: www.infragard.org
ISSA: www.issa.org
CyberForensics360: www.cyberforensics360.org
netSecurity: www.netsecurity.com
Tor Network
Cyber Secrets: www.informationwarfarecenter.com/Cyber-Secrets.html