INFORMATION WARFARE CENTER V3.0 CYBER INTELLIGENCE REPORT

MAY 25, 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.

WEEK IN REVIEW

The past week has been very interesting… Planes hacked… As Always… Yes, many of them have very poor security and the airlines have been told for years. Starbucks in the news. They Patriot Act is about to sunset. The OIL industry is still a target. And Last but not least, if you like ***anonymous sex*** and have an ***ADULT FRIEND FINDER*** account, you may have been a victim of customer data loss.

GOTCHAS:

Date	Notifier	L	★	Domain	View
5/23/2015	DskTeam	🇺🇸	★	www.cambridgema.gov	mirror
5/23/2015	DskTeam	🇺🇸	★	www.congress.gov	mirror
5/23/2015	DskTeam	🇺🇸	★	www.glendaleaz.gov	mirror
5/23/2015	DskTeam	🇺🇸	★	www.bja.gov	mirror
5/22/2015	kj-fido	🇺🇸	★	tap.bja.gov/SitePages/Topic.as...	mirror
5/20/2015	d3b~X	🇺🇸	★	www.cha.wa.gov/images/ganteng.gif	mirror
5/18/2015	Cloudx	🇺🇸	★	www.statelibrary.sc.gov/docume...	mirror
5/17/2015	Hacker Khan	🇺🇸	★	lymansc.gov	mirror
5/12/2015	H3R1-1D	🇺🇸	★	stephenvilletx.gov/bxc.htm	mirror
5/7/2015	NeT-DeViL	🇺🇸	★	www.lakecountyca.gov/x.txt	mirror
5/7/2015	totässer	🇺🇸	★	www.usa.gov	mirror
5/7/2015	Ashiyane Digital Security	🇺🇸	★	pittsburghpa.gov/rss/print.htm...	mirror
5/6/2015	NeT-DeViL	🇨🇦	★	apps.stanley.id.gov/robots.txt	mirror
5/6/2015	-AnonJohor	🇺🇸	★	studentloans.gov	mirror
5/3/2015	Mamad Ershad	🇺🇸	★	idlastro.gsfc.nasa.gov/ftp/	mirror
5/2/2015	TiGER-R00T	🇺🇸	★	www.sheriff.co.wayne.in.us	mirror
5/8/2015	3r3b0s	🇺🇸	★	www.employees.co.brown.wi.us//...	mirror
5/5/2015	Kuroi'SH	🇨🇦	★	town.south-thomaston.me.us/ksh...	mirror

NEWS: INFORMATION WARFARE

- Tropico 5 Expansion 'Espionage' - Gamespresso.
- Chinese University Denies Any Involvement in 'Economic Espionage' - WSJ.
- Bits | Members of Congress Ask for Review of Dropped Espionage Case - NYT.
- Economic Espionage Charges Could Further Dent China-US Ties - Wall Street Journal.
- Community Review: "Modern Espionage" - Paste Magazine.
- Corporate acquisitions carry a new cyber-threat - CIO Australia.
- Government crafting new plan to fend off cyberthreats - The Japan Times.
- Cyber Threat Analysis: A Call for Clarity - Dark Reading.
- US Navy secretary says paying attention to cyber threats - Reuters UK.
- Info sharing best defence against cyber threat - gulfnews.com.
- Starbucks Says Gift Card Hack Was 'Fraudulent Activity'.
- Android Flaw Leaves 500 Million Users Open To Attack.
- Senate Adjourns, Rejects Surveillance Bill.
- Adult Friend Finder Hack Exposes Millions Of Members.
- Obscene Image Shown On Hacked US Billboard.
- Senator Rand Paul Stages Filibuster To Protest Patriot Act.
- NetUSB Flaw Puts Millions Of IoT Devices At Risk.
- Millions Exposed By Latest Health Insurer Hack.
- Federal Prosecutors Charge Chinese Nationals With Trade Secret Theft.
- Bettys Tea Rooms Admit To Massive Data Breach.
- Logjam Attack Consistent With NSA VPN Cracking Efforts.
- Anti-NSA Pranksters Capture Conversations.
- 150 Companies Urge Obama For Strong Encryption.
- St. Louis Federal Reserve Suffers DNS Breach.
- Phantom Menace Hack Strikes Oil Industry.
- Sandbox Leaks In Google App Engine.
- Starbucks Says App Not Hacked.
- Unwilling DNA Samples Used In Advertising.
- Who Really Invented Bitcoin?.
- FBI Says Hacker Hacked Plane.
- The Overhyping of Iran's Cyberarmy.
- National Identity Theft Ring Busted.
- Pass The Polygraph, Go Straight To Jail.
- United Airlines Bug Bounty Pays With Miles.

NEWS: HIPPA

- Science Hill graduate comes full circle to be ETSU's HIPAA compliance officer - Johnson City Press (subscription).
- House Committee OK's Bill Altering HIPAA - GovInfoSecurity.com.
- OCR Enforcement Of HIPAA Affects Entities Of All Sizes: Small Pharmacy Enters ... - Mondaq News Alerts (registration).
- HIPAA breach survival guide - Government Health IT.
- Office for Civil Rights Launches Phase 2 HIPAA Audit Program with Pre-Audit ... - The National Law Review.

NEWS: SCADA

- VMC to restore SCADA to plug leakage - The Hindu.
- Darktrace secures Scada as cyberattacks on industry rise - CBR.
- B-Scada Joins Control System Integrators Association (CSIA) - IT Business Net.
- SCADA Security: How Britain can reinforce its nuclear and weapons control ... - Yahoo.
- SCADA gets better, faster, stronger - Plant Services.

NEWS: CYBER LAWS & LEGISLATION

- Federal law for cyber risk possible in 2015 - Business Insurance.
- Report Highlights Fears of Impending Cyber-Law in Cambodia - Voice of America.
- UK government rewrites surveillance law to get away with hacking and allow ... - Belfast Telegraph.
- House Passes Cybersecurity Information Sharing Bills - JD Supra (press release).
- Report Highlights Fears of Impending Cyber-Law - VOA Khmer.

NEWS: COMPUTER FORENSICS

- Prosecuting predators: Behind-the-scenes look at AG's Forensic Computer Lab - WRIC.
- Computer Forensics Investigations: Body of Evidence - CSO Australia.
- Workshop focus: Girls in science - Northwest Arkansas News.
- New Dubai Police forensics lab stays one step ahead - gulfnews.com.

EXPLOITS

- Fuse Local Privilege Escalation.
- Lenovo System Update Privilege Escalation.
- TCPDF Library 5.9 Arbitrary File Deletion.
- WordPress Video Gallery 2.8 Unprotected Mail Page.
- Sendio ESP Information Disclosure.
- WordPress WP Membership 1.2.3 Privilege Escalation.
- WordPress WP Membership 1.2.3 Cross Site Scripting.
- Webgrind 1.1 Cross Site Scripting.
- SolarWinds Network Performance Monitor Open Redirect.
- Pluck CMS 4.7.2 Directory Traversal.
- Jackrabbit WebDAV XXE Injection.
- Coppermine Gallery 1.5.34 XSS / Open Redirection.
- Newsletter 4.3 SQL Injection.
- WordPress WP Photo Album Plus 6.1.2 Cross Site Scripting.
- Windows 8.0 / 8.1 x64 TrackPopupMenu Privilege Escalation.
- Hikvision DS-7108HWI-SH XML Injection / Abuse Issues.
- HiDisk 2.4 Cross Site Scripting.
- Comodo GeekBuddy Local Privilege Escalation.
- ZOC SSH Client 7.03.0 Buffer Overflow.
- Simple Invoice 2011.1 Cross Site Request Forgery.
- Eisbar SCADA Script Insertion.
- Simple Invoice 2011 Cross Site Scripting.
- DirectAdmin 1.48 Cross Site Request Forgery.
- Clickheat 1.13 Remote Command Execution.
- IPsec-Tools 0.8.2 Denial Of Service.

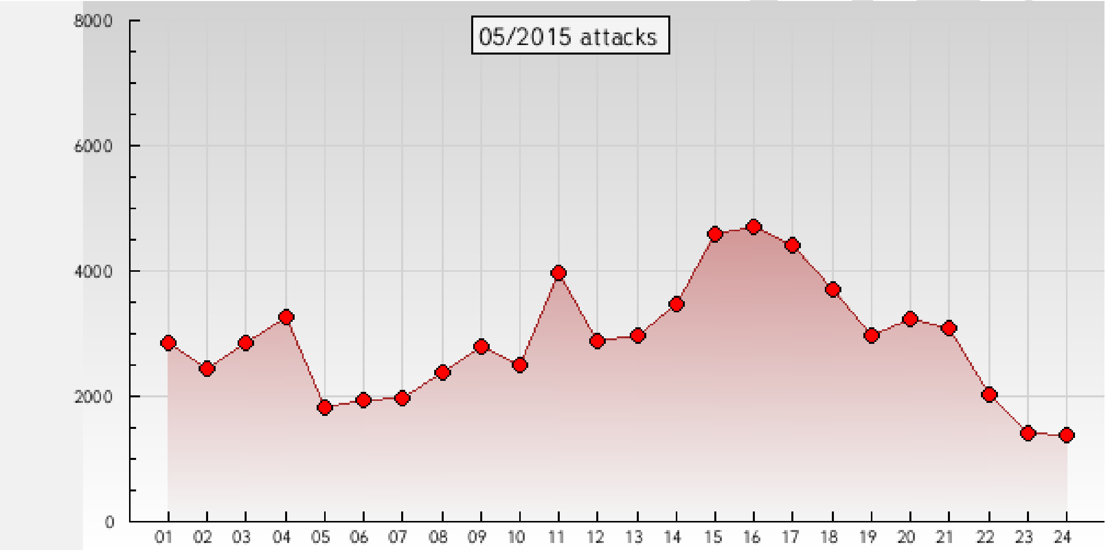
ADVISORIES

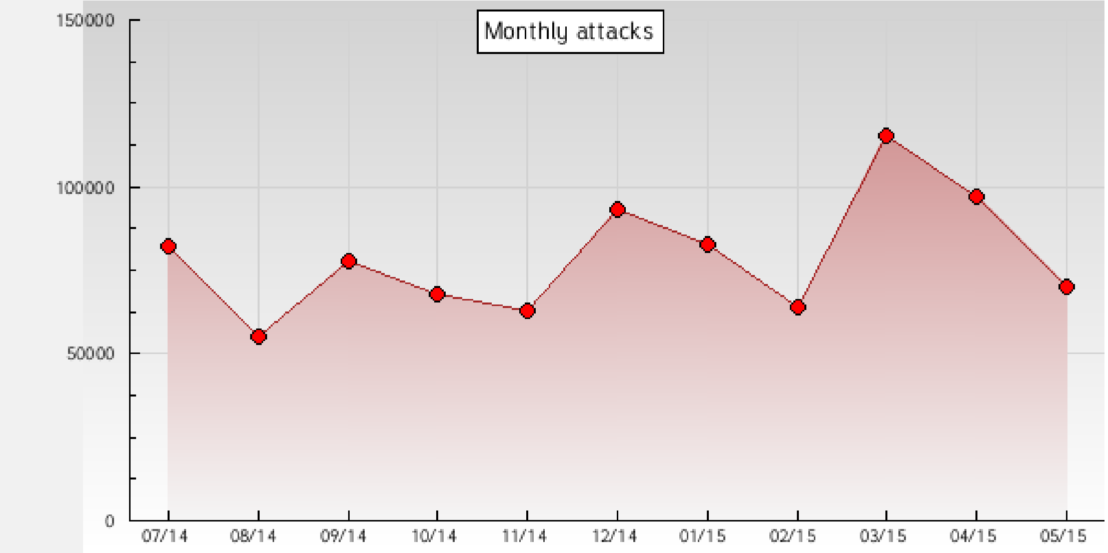
- Ubuntu Security Notice USN-2620-1.
  Sat, 23 May 2015 13:22:42 GMT
  Ubuntu Security Notice 2620-1 - A flaw was discovered in the Linux kernel's IPv4 networking when using TCP fast open to initiate a connection. An unprivileged local user could exploit this flaw to cause a denial of service (system crash).
- Ubuntu Security Notice USN-2619-1.
  Sat, 23 May 2015 13:22:30 GMT
  Ubuntu Security Notice 2619-1 - A flaw was discovered in the Linux kernel's IPv4 networking when using TCP fast open to initiate a connection. An unprivileged local user could exploit this flaw to cause a denial of service (system crash).
- Debian Security Advisory 3270-1.
  Fri, 22 May 2015 22:22:00 GMT
  Debian Linux Security Advisory 3270-1 - Several vulnerabilities have been found in PostgreSQL-9.4, a SQL database system.
- Ubuntu Security Notice USN-2617-2.
  Fri, 22 May 2015 19:32:00 GMT
  Ubuntu Security Notice 2617-2 - USN-2617-1 fixed a vulnerability in FUSE. This update provides the corresponding fix for the embedded FUSE copy in NTFS-3G. Tavis Ormandy discovered that FUSE incorrectly filtered environment variables. A local attacker could use this issue to gain administrative privileges. Various other issues were also addressed.
- Debian Security Advisory 3267-1.
  Fri, 22 May 2015 17:44:00 GMT
  Debian Linux Security Advisory 3267-1 - Several vulnerabilities were discovered in the chromium web browser.
- Debian Security Advisory 3268-1.
  Fri, 22 May 2015 17:02:00 GMT
  Debian Linux Security Advisory 3268-1 - Tavis Ormandy discovered that NTFS-3G, a read-write NTFS driver for FUSE, does not scrub the environment before executing mount or umount with elevated privileges. A local user can take advantage of this flaw to overwrite arbitrary files and gain elevated privileges by accessing debugging features via the environment that would not normally be safe for unprivileged users.
- HP Security Bulletin HPSBMU03336.
  Fri, 22 May 2015 13:33:33 GMT
  HP Security Bulletin HPSBMU03336 - A potential security vulnerability has identified with HP Helion OpenStack. The vulnerability could be exploited resulting in Denial of Service (DoS) or execution of arbitrary code. Revision 1 of this advisory.
- Debian Security Advisory 3261-2.
  Thu, 21 May 2015 22:22:00 GMT
  Debian Linux Security Advisory 3261-2 - The update for libmodule-signature-perl issued as DSA-3261-1 introduced a regression in the handling of the --skip option of cpansign. Updated packages are now available to address this regression.

- Ubuntu Security Notice USN-2610-1.
  Thu, 21 May 2015 22:11:00 GMT
  Ubuntu Security Notice 2610-1 - Several security issues were discovered in the DOM implementation in Blink. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to bypass Same Origin Policy restrictions. A use-after-free was discovered in the WebAudio implementation in Chromium. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via renderer crash, or execute arbitrary code with the privileges of the sandboxed render process. Various other issues were also addressed.
- Ubuntu Security Notice USN-2618-1.
  Thu, 21 May 2015 19:55:00 GMT
  Ubuntu Security Notice 2618-1 - It was discovered that python-dbusmock incorrectly handled template loading from shared directories. A local attacker could possibly use this issue to execute arbitrary code.
- Debian Security Advisory 3266-1.
  Thu, 21 May 2015 19:44:00 GMT
  Debian Linux Security Advisory 3266-1 - Tavis Ormandy discovered that FUSE, a Filesystem in Userspace, does not scrub the environment before executing mount or umount with elevated privileges. A local user can take advantage of this flaw to overwrite arbitrary files and gain elevated privileges by accessing debugging features via the environment that would not normally be safe for unprivileged users.
- Ubuntu Security Notice USN-2609-1.
  Thu, 21 May 2015 19:22:00 GMT
  Ubuntu Security Notice 2609-1 - Sander Bos discovered that Apport incorrectly handled permissions when the system was configured to generate core dumps for setuid binaries. A local attacker could use this issue to gain elevated privileges. Philip Pettersson discovered that Apport contained race conditions resulting core dumps to be generated with incorrect permissions in arbitrary locations. A local attacker could use this issue to gain elevated privileges. Various other issues were also addressed.
- Microsoft Security Bulletin Summary For May, 2015.
  Thu, 21 May 2015 18:32:22 GMT
  This bulletin summary lists one released Microsoft security bulletin for May, 2015.
- KCodes NetUSB Buffer Overflow.
  Thu, 21 May 2015 14:44:44 GMT
  KCodes NetUSB suffers from a kernel stack buffer overflow vulnerability.
- Ubuntu Security Notice USN-2617-1.
  Thu, 21 May 2015 14:44:00 GMT
  Ubuntu Security Notice 2617-1 - Tavis Ormandy discovered that FUSE incorrectly filtered environment variables. A local attacker could use this issue to gain administrative privileges.

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.	Ashiyane Digital Security Team	2921	4120	7041	1322	5719
3.	Hmei7	2853	1511	4364	775	3589
4.	LatinHackTeam	1438	1266	2704	2254	450
5.	iskorpitx	1324	955	2279	786	1493
6.	Fatal Error	1124	1729	2853	2473	380
7.	HighTech	965	3836	4801	3853	948
8.	chinahacker	889	1344	2233	4	2229
9.	MCA-CRB	854	626	1480	374	1106
10.	By_aGReSiF	758	1428	2186	802	1384





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