INFORMATION WARFARE CENTER V3.0

CYBER INTELLIGENCE REPORT

MARCH APRIL 7, 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.

Gotcha

Date	Notifier	H	M	R	L	Domain	OS	View
2015/04/06	NeT-DeViL					www.wvlegislature.gov/Joint/Po...	Win 2008	mirror
2015/04/05	OPciberBR					www.bullittcounty.ky.gov/old/o...	MacOSX	mirror

NEW EPISODE OF CYBER SECRETS FOR APRIL:

Starting a Metasploit Project: https://youtu.be/ZwK2NReSRFU

EXECUTIVE ORDER 2015-07788 – "BLOCKING THE PROPERTY OF CERTAIN PERSONS ENGAGING IN SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES":

Released April 1, 2015.

…

"I, BARACK OBAMA, President of the United States of America, find that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat."

…

Download the entire order here

2015-07788.pdf

NEWS: INFORMATION WARFARE

- US geologist accused of espionage released from Chinese prison - KHOU.
- The Rosenbergs are sentenced to death for espionage in 1951 - New York Daily News.
- Study abroad students could be espionage targets, FBI says - USA TODAY.
- Corporate espionage: Court seeks MoPNG's report on leaked docs - Business Standard.
- Israeli Military Indicts Soldier on Espionage Charges - ABC News.
- Monday Morning Regulatory Review – 4/6/15: Cyber-Threat Executive Order ... - FRA.
- Obama declares "national emergency" based on alleged cyber threats from ... - World Socialist.
- Our Latest Tool to Combat Cyber Attacks: What You Need to Know - The White House (blog). .
- Turkey Blocks Twitter, YouTube Over Hostage Photos.
- Dyre Wolf Malware Steals More Than $1 Million.
- NewPosThings Malware Evolves, Traced To Airports.
- John Oliver Sits Down With Edward Snowden.
- Mozilla Follows Google, Shows CNNIC's Cert The Door.
- Four Indicted In Federal Reserve Notes Counterfeiting.
- Teen Pleads Guilty In Microsoft And Valve Hacking Case.
- Google Chrome Will Banish Chinese CA For Breach Of Trust.
- This Tool Detects Then Attacks Evil Twin Access Points.
- Sanctions Against Overseas Hackers?.
- Evidence Links China To GitHub Attack.
- Mozilla Offers New Threat Modelling Tool For SysAdmins.
- Flaw Deletes YouTube Videos In Just A Few Clicks.
- Facebook Privacy Policies Breach EU Laws, Claims Researcher.
- Uber Denies It Was Hacked.
- DEA Agent Charged With Acting As A Paid Mole For Silk Road.
- Periscope Smeared By Streaming Security SNAFU.
- Men Disguised As Women Storm NSA HQ.
- The US Has Used Zero-Day Exploits For Quite A While.
- Verizon Tells Congress To Reign In FCC's Powers Over Providers.
- British Airways Admits Frequent Flyer Account Hack.
- DDoS Attack Cripples GitHub Coding Site, China Blamed.
- Silicon Valley Powers Hope Section 215 Of The Patriot Act Dies.
- TLS Hit With 2 New Decryption Attacks.
- RSA Bans Booth Babes.

NEWS: HIPPA

- Ashley Trotto: HIPAA in the social media era - Knoxville News Sentinel.
- How Much Do You Need to Know About HIPAA? - Massage Magazine.
- Current HIPAA Requirements Sufficient, AHA Tells ONC - HealthITSecurity.com.
- HIMSS Workshop Offers HIPAA Refresh, New Ideas - Health Data Management.
- Don't confuse EHR HIPAA compliance with total HIPAA compliance - Healthcare IT News (blog).

NEWS: SCADA

- SCADA Market in the APAC Region 2015-2019 - Virtual-Strategy Magazine (press release).
- The State of SCADA Security - CSO Online..
- BRS Labs Launches Artificial-Intelligence-Based SCADA Analysis Portal - Yahoo Finance UK.

NEWS: CYBER LAWS & LEGISLATION

- CISA Cybersecurity Bill Advances Despite Privacy Concerns - Wired.
- How Big Business Is Helping Expand NSA Surveillance, Snowden Be Damned.
- Lawmakers in cybersecurity rush - The Hill.

NEWS: COMPUTER FORENSICS

- Madigan wants to increase funding for crime labs - The Times.
- Defense Rests in Boston Marathon Bombing Trial After Just 4 Witnesses - New York Times.
- Influencers: Companies should not be allowed to hack back - Christian Science Monitor.
- UA to Launch Interdisciplinary Cyber Crime Minor - UA News.

EXPLOITS

- JBoss Seam 2 File Upload / Execute.
- Kemp Load Master 7.1-16 CSRF / XSS / DoS / Code Execution.
- phpSFP Schedule Facebook Posts 1.5.6 SQL Injection.
- Airties Air5650v3TT Remote Stack Overflow.
- WordPress Simple Ads Manager 2.5.94 / 2.5.96 SQL Injection.
- WordPress Simple Ads Manager 2.5.94 File Upload.
- WordPress PHP Event Calendar 1.5 Arbitrary File Upload.
- WordPress Simple Ads Manager 2.5.94 / 2.5.96 Information Disclosure.
- Synology.com Cross Site Scripting.
- Ceragon FibeAir IP-10 SSH Private Key Exposure.
- Ceragon FibeAir IP-10 SSH Private Key Exposure.
- Samba / OpenLDAP Jitterbug Cross Site Scripting.
- phpList 3.0.10 Insecure Direct Object Reference.
- WordPress VideoWhisper Video Presentation 3.31.17 Shell Upload.
- WordPress VideoWhisper Video Conference Integration 4.91.8 Shell Upload.
- WordPress Revolution Slider File Upload.
- Joomla Simple Photo Gallery Shell Upload.
- WordPress DesignFolio+ Theme File Upload.
- Packet Storm New Exploits For March, 2015.
- Ericsson Drutt MSDP (Instance Monitor) Directory Traversal / File Access.
- Ericsson Drutt MSDP (Report Viewer) Cross Site Scripting.
- Ericsson Drutt MSDP (3PI Manager) Cross Site Scripting.
- Ericsson Drutt MSDP (3PI Manager) Open Redirect.
- Java.com Cross Site Scripting.
- WordPress Business Intelligence Lite 1.6.1 SQL Injection.
- [papers] - [Hebrew] Digital Whisper Security Magazine #60.
- Ericsson Drutt MSDP (Instance Monitor) - Directory Traversal.
- VideoWhisper Video Conference Integration 4.91.8 - Remote File Upload.
- WordPress VideoWhisper Video Presentation 3.31.17 - Remote File Upload.
- phpSFP - Schedule Facebook Posts 1.5.6 SQL Injection.
- Wordpress Simple Ads Manager - Information Disclosure.
- Wordpress Simple Ads Manager 2.5.94 - Arbitrary File Upload.
- Wordpress Simple Ads Manager Plugin - Multiple SQL Injection.
- Wordpress WP Easy Slideshow Plugin 1.0.3 - Multiple Vulnerabilities.
- Wordpress Video Gallery Plugin 2.8 - Multiple CSRF Vulnerabilities.

ADVISORIES

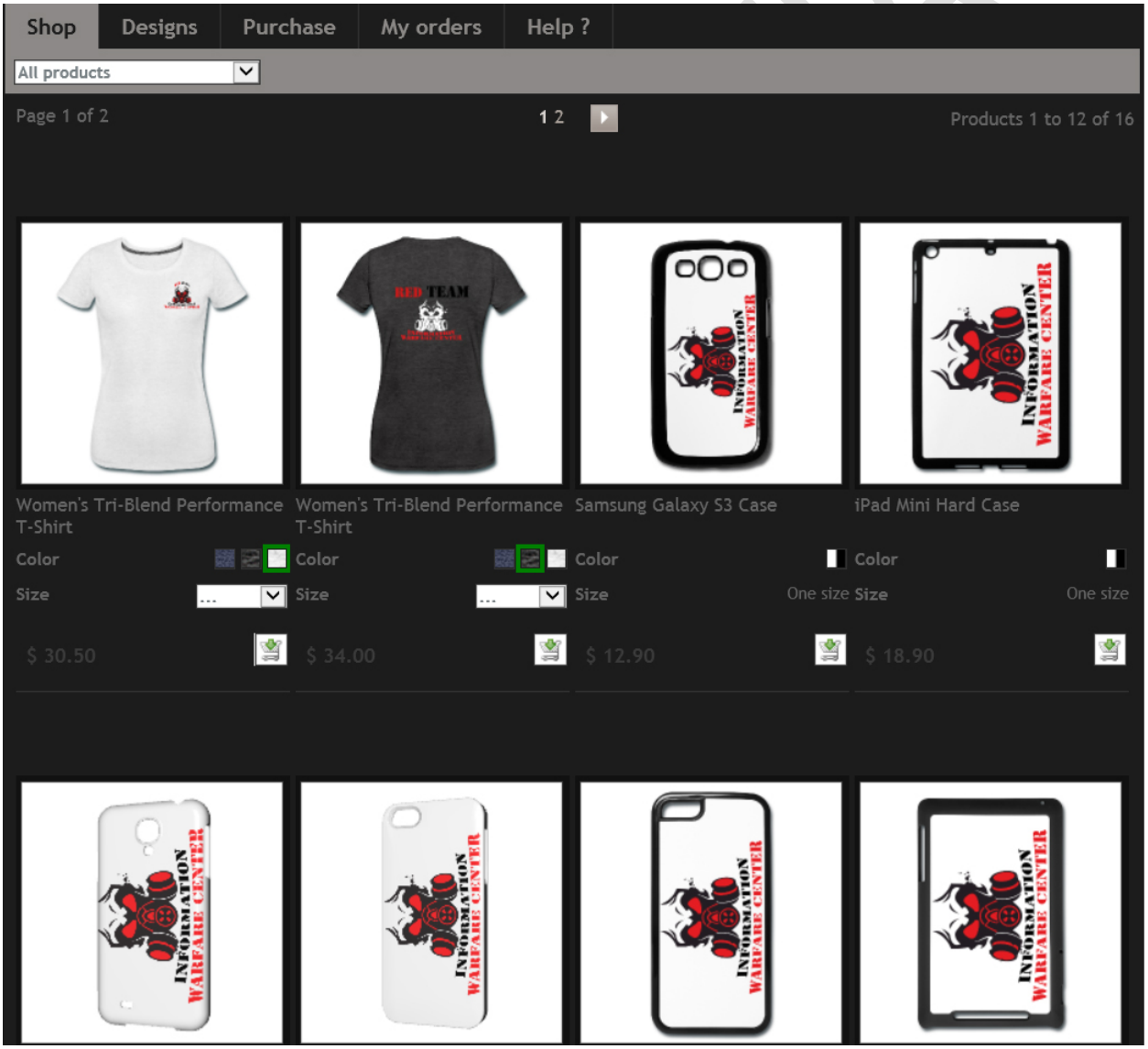
- Mandriva Linux Security Advisory 2015-192.
  - Fri, 03 Apr 2015 15:47:42 GMT
    Mandriva Linux Security Advisory 2015-192 - Multiple vulnerabilities has been discovered and corrected in subversion. Subversion HTTP servers with FSFS repositories are vulnerable to a remotely triggerable excessive memory use with certain REPORT requests. Subversion mod_dav_svn and svnserve are vulnerable to a remotely triggerable assertion DoS vulnerability for certain requests with dynamically evaluated revision numbers. Subversion HTTP servers allow spoofing svn:author property values for new revisions. The updated packages have been upgraded to the 1.7.20 and 1.8.13 versions where these security flaws has been fixed.
- HP Security Bulletin HPSBST03195 1.
  - Fri, 03 Apr 2015 15:46:45 GMT
    HP Security Bulletin HPSBST03195 1 - Potential security vulnerabilities have been identified with HP 3PAR Service Processor (SP) running OpenSSL and Bash. The OpenSSL vulnerability known as "Heartbleed" which could be exploited remotely resulting in disclosure of information. The SSLv3 vulnerability known as "Padding Oracle on Downgraded Legacy Encryption" also known as "Poodle", which could be exploited remotely resulting in disclosure of information. The Bash Shell vulnerability known as "Shellshock" which could be exploited remotely resulting in execution of code. Revision 1 of this advisory.
- Debian Security Advisory 3212-1.
  - Fri, 03 Apr 2015 15:46:37 GMT
    Debian Linux Security Advisory 3212-1 - Multiple security issues have been found in Icedove, Debian's version of use-after-frees and other implementation errors may lead to the execution of arbitrary code, the bypass of security restrictions or denial of service.
- HP Security Bulletin HPSBHF03300 1.
  - Fri, 03 Apr 2015 15:45:16 GMT
    HP Security Bulletin HPSBHF03300 1 - Potential security vulnerabilities have been identified with HP Network Products running OpenSSL. The SSLv3 vulnerability known as "Padding Oracle on Downgraded Legacy Encryption" also known as "POODLE", which could be exploited remotely resulting in disclosure of information. Other vulnerabilities which could be remotely exploited resulting in Denial of Service (DoS) and unauthorized access. Revision 1 of this advisory.
- OpenSSH 6.8 Insecure Functions.
  - Fri, 03 Apr 2015 03:03:03 GMT
    OpenSSH version 6.8 makes use of some insecure functions.
- OpenSSL 1.0.2a Insecure Functions.
  - Fri, 03 Apr 2015 02:22:22 GMT
    OpenSSL version 1.0.2a makes use of some insecure functions.
- VMware Security Advisory 2015-0003.
  - Thu, 02 Apr 2015 23:51:54 GMT
    VMware Security Advisory 2015-0003 - VMware product updates address critical information disclosure issue in JRE.

- Mandriva Linux Security Advisory 2015-188.
  - Thu, 02 Apr 2015 23:50:53 GMT
    Mandriva Linux Security Advisory 2015-188 - Heap-based buffer overflow in stream_decoder.c in libFLAC before 1.3.1 allows remote attackers to execute arbitrary code via a crafted.flac file. Stack-based buffer overflow in stream_decoder.c in libFLAC before 1.3.1 allows remote attackers to execute arbitrary code via a crafted.flac file. The updated packages provides a solution for these security issues.
- Mandriva Linux Security Advisory 2015-187.
  - Thu, 02 Apr 2015 23:50:35 GMT
    Mandriva Linux Security Advisory 2015-187 - Format string vulnerability in the yyerror function in lib/cgraph/scan.l in Graphviz allows remote attackers to have unspecified impact via format string specifiers in unknown vector, which are not properly handled in an error string. Additionally the gtkglarea2 and gtkglext packages were missing and was required for graphviz to build, these packages are also being provided with this advisory.
- Red Hat Security Advisory 2015-0776-01.
  - Thu, 02 Apr 2015 23:50:22 GMT
    Red Hat Security Advisory 2015-0776-01 - Docker is a service providing container management on Linux. It was found that the fix for the CVE-2014-5277 issue was incomplete: the docker client could under certain circumstances erroneously fall back to HTTP when an HTTPS connection to a registry failed. This could allow a man-in-the-middle attacker to obtain authentication and image data from traffic sent from a client to the registry.
- Ubuntu Security Notice USN-2552-1.
  - Thu, 02 Apr 2015 23:50:09 GMT
    Ubuntu Security Notice 2552-1 - Olli Pettay and Boris Zbarsky discovered an issue during anchor navigations in some circumstances. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit this to bypass same-origin policy restrictions. Christoph Kerschbaumer discovered that CORS requests from navigator.sendBeacon() followed 30x redirections after preflight. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit this to conduct cross-site request forgery (XSRF) attacks. Various other issues were also addressed.
- HP Security Bulletin HPSBGN03302 1.
  - Thu, 02 Apr 2015 23:48:52 GMT
    HP Security Bulletin HPSBGN03302 1 - A potential security vulnerability has been identified with HP IceWall Federation Agent. The vulnerability could be exploited remotely resulting in Denial of Service (DoS). Revision 1 of this advisory.
- Mandriva Linux Security Advisory 2015-161-1.
  - Thu, 02 Apr 2015 23:48:12 GMT
    Mandriva Linux Security Advisory 2015-161 - The Regular Expressions package in International Components for Unicode 52 before SVN revision 292944 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to a zero-length quantifier or look-behind expression. The collator implementation in i18n/ucol.cpp in International Components for Unicode 52 through SVN revision 293126 does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted character sequence. It was discovered that ICU incorrectly handled memory operations when processing fonts. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program.

- Mandriva Linux Security Advisory 2015-191.
  - Thu, 02 Apr 2015 23:47:09 GMT
    Mandriva Linux Security Advisory 2015-191 - Multiple vulnerabilities has been discovered and corrected in owncloud. The updated packages have been upgraded to the 7.0.5 version where these security flaws has been fixed.
- Mandriva Linux Security Advisory 2015-190.
  - Thu, 02 Apr 2015 23:46:25 GMT
    Mandriva Linux Security Advisory 2015-190 - Multiple vulnerabilities have been discovered and corrected in owncloud. The updated packages have been upgraded to the 5.0.19 version where these security flaws has been fixed.

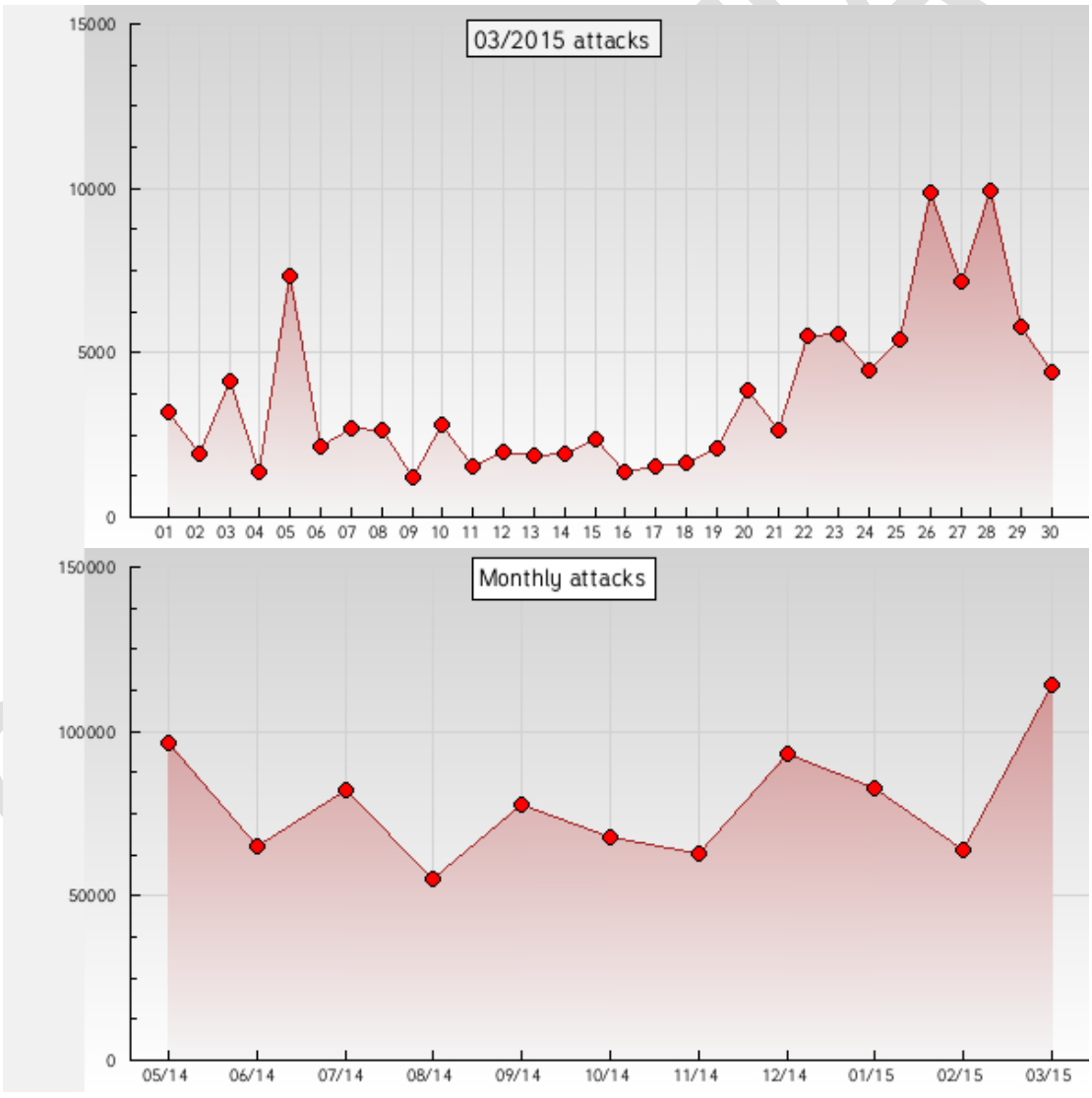
SWAG SALES

If interested, you can now get IWC swag from http://iwccybersec.spreadshirt.com/

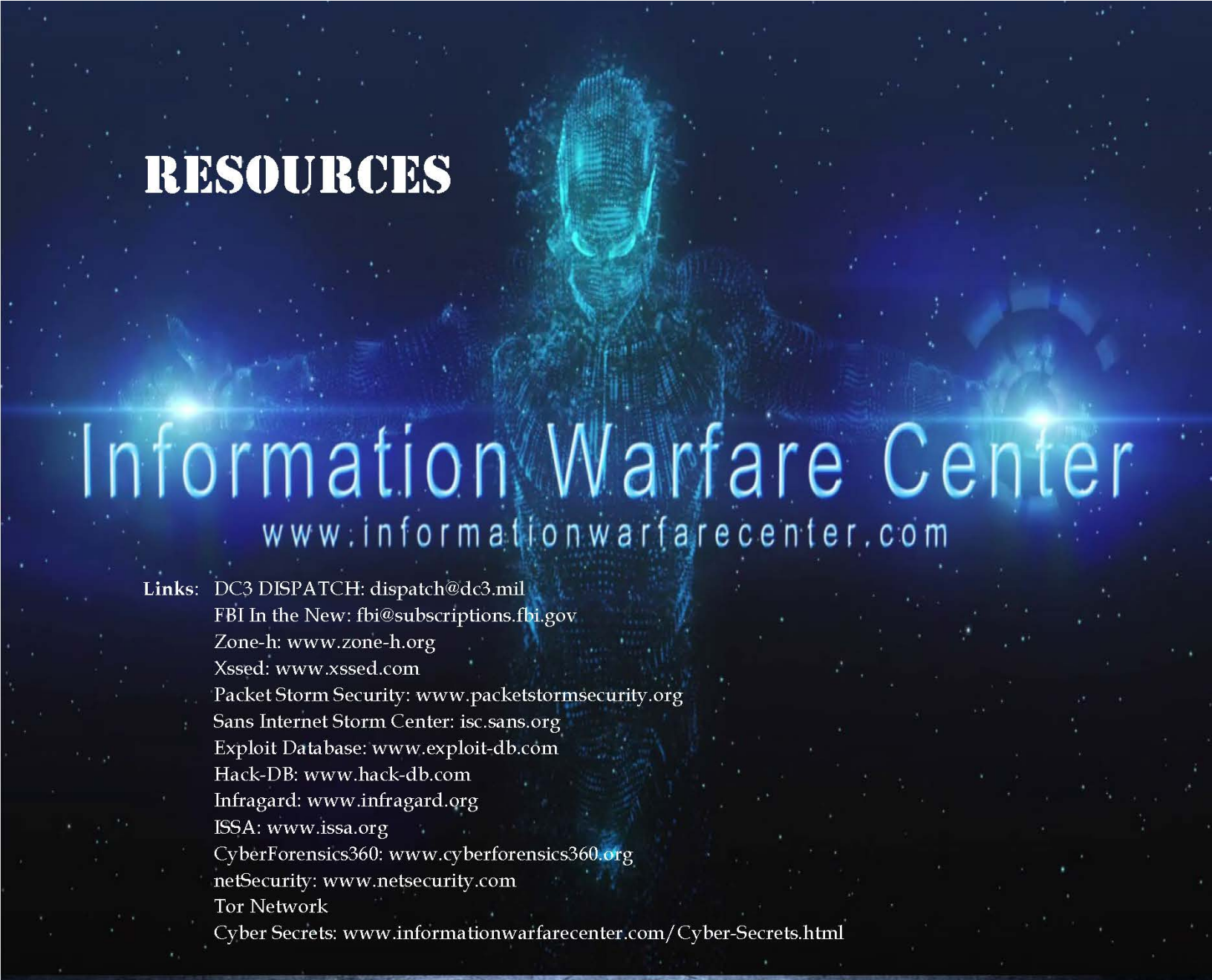


ZONE-H ATTACK STATISTICS:

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	2871	4113	6984	1319	5665
3.	Hmei7	2852	1511	4363	775	3588
4.	LatinHackTeam	1438	1266	2704	2254	450
5.	iskorpitx	1324	955	2279	786	1493
6.	Fatal Error	1113	1726	2839	2459	380
7.	HighTech	948	3779	4727	3788	939
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