INFORMATION WARFARE CENTER

V3.0

CYBER INTELLIGENCE REPORT

## MARCH 10, 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: WEBSITE DEFACEMENTS

| Time | Notifier | H | M | R | L | | Domain | OS | View |
|---|---|---|---|---|---|---|---|---|---|
| 3/10/2015 | Toxic Dz | H | | R | 🇺🇸 | ★ | calumettwp-in.gov | Win 2012 | mirror |
| 3/7/2015 | Shin0bi H4x0r | | | | 🇺🇸 | ★ | bigdatawg.nist.gov/_uploadfile... | Linux | mirror |
| 3/7/2015 | NeT-DeViL | | | | 🇺🇸 | ★ | watershed.lakecountyca.gov/x.txt | Win 2003 | mirror |
| 015/03/07 | NeT-DeViL | | | | 🇺🇸 | ★ | mouse.ncifcrf.gov/db | Win 2008 | mirror |
| 3/7/2015 | NeT-DeViL | | | | 🇺🇸 | ★ | ncifrederick.cancer.gov/Logs | Win 2008 | mirror |
| 3/7/2015 | NeT-DeViL | | | | 🇺🇸 | ★ | frederick.cancer.gov/Logs | Win 2008 | mirror |
| 3/6/2015 | robots.txt | | | | 🇳🇱 | ★ | www.dot.gov/robots.txt | Linux | mirror |
| 3/5/2015 | NeT-DeViL | | | | 🇺🇸 | ★ | azgeo.az.gov/azgeo/hacked-grou... | Win 2008 | mirror |
| 3/4/2015 | NeT-DeViL | | | | 🇺🇸 | ★ | accessguide.doe.louisiana.gov/... | Win 2003 | mirror |
| 3/4/2015 | NeT-DeViL | | | | 🇺🇸 | ★ | sda.doe.louisiana.gov/_layouts... | Win 2003 | mirror |
| 3/4/2015 | NeT-DeViL | | | | 🇺🇸 | ★ | www.friscotx.gov/_layouts/list... | Win 2008 | mirror |
| 3/4/2015 | NeT-DeViL | | | R | 🇺🇸 | ★ | www.friscotexas.gov/_layouts/l... | Win 2008 | mirror |

## MICROSOFT FREAKING OUT

What is the FREAK technique and why is it an issue? To put it shortly, it is a cryptographic issue where the attacker can man-in-the-middle attack against Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections.

*"Microsoft is aware of a security feature bypass vulnerability in Secure Channel (Schannel) that affects all supported releases of Microsoft Windows. Our investigation has verified that the vulnerability could allow an attacker to force the downgrading of the cipher suites used in an SSL/TLS connection on a Windows client system. The vulnerability facilitates exploitation of the publicly disclosed FREAK technique, which is an industry-wide issue that is not specific to Windows operating systems. When this security advisory was originally released, Microsoft had not received any information to indicate that this issue had been publicly used to attack customers."*

## NEWS: INFORMATION WARFARE

- How Hillary Clinton Could Be Targeted Under The Espionage Act - Huffington Post.
- Coleman: We're not prepared to stop cyber espionage - C4ISR & Networks (blog).
- Revolutionary tale of espionage - The Australian.
- The Switchboard: CIA will shake things up to focus on digital espionage - Washington Post (blog).
- Chile wants to get past espionage controversy w/ Peru, foreign minister says - Fox News Latino.
- Kaspersky Labs prospering from 'Internet of Threats' - Boston Globe (subscription).
- How prepared is Wisconsin to block “cyber attacks” that target state agencies? - fox6now.com.
- Clark Calls For More Prosecution Of Cyber Threats Against Women - CBS Local.
- CIA reorganizing to meet cyber threats - Federal Times.
- Israeli Agata Fights Latest Cyber Threats With Third Generation Forensics Suite - Jewish Business News.
- NY Private Investigator Pleads Guilty To Computer Hacking.
- Banning Tor Unwise And Infeasible, MPs Told.
- Cutting-Edge DRAM Hack Gives Superuser Status.
- The CIA Campaign To Steal Apple's Secrets.
- Wikimedia Foundation Sues NSA Over Surveillance.
- Seagate Admits Zero Day Vuln In NAS, Won't Fix Until May.
- Attackers Targeting Elasticsearch Remote Code Execution Hole.
- NEXTEP POS Provider Investigating Possible Breach.
- Three Charged Over Largest Data Breach In US History.
- Cyberespionage Is A Top Priority For CIA's New Directorate.
- Apache ActiveMQ Flaws Leave Servers Open To DoS Attacks.
- Dozens Arrested In Cybercrime 'Strike Week'.
- Adobe Launches Cashless Bug Bounty.
- Mandarin Oriental Hotel Group Is Investigating A Credit Card Breach.
- Microsoft Admits Freak Affects All Versions Of Windows.
- France Fingered As Source Of Syria-Spying Babar Malware.
- Broadband Routers: SOHOpeless And Vendors Don't Care.
- Uber Is Hardly An Exception. Github Is Awash In Passwords.
- Chrome Splatters 51 Bugs, Mozilla Bumps Cert Checker.
- Civil Liberties Groups Call For UN Privacy Watchdog.
- The C99Shell Is Not Dead.
- D-Link Removes Fingers From Ears, Preps Mass Router Patch.
- Freak SSL/TLS Flaw Puts Android And Apple Users At Risk.
- China And US Clash Over Software Backdoor Proposals.
- US Air Traffic Control Vulnerable To Terrorist Hackers.

## NEWS: HIPPA

- HIPAAtrek Tackles the Beast of HIPAA Healthcare Compliance - Techli.
- HIPAA, Wiretapping Laws Pose Legal Questions for Nursing Home Cameras - CBS Local.
- HIPAA crackdown extends beyond health care providers - The Tennessean.
- Is HIPAA the Biggest Challenge to mHealth Development? - mHealthIntelligence.com.
- When HIPAA Applies To Patient Assistance Programs (And When It Doesn't) - Mondaq News Alerts .

## NEWS: SCADA

- BRS Labs Launches Artificial-Intelligence-Based SCADA Analysis Portal - Business Wire (press release).
- Research and Markets: SCADA Market in the APAC Region 2015-2019 with ... - Business Wire (press release).
- CeBIT Innovation: gateprotect Offers Unique New SCADA Protection for Energy ... - RealWire (press release).
- SMA and GreenPowerMonitor to Bring SCADA Solutions to PV Power Plants - Solar Novus Today.

## NEWS: CYBER LAWS & LEGISLATION

- New York State Charges Ahead on Critical Infrastructure Cybersecurity Legislation - JD Supra (press release).
- Legislation Would Criminalize Revenge Porn; Allow Search Warrants for Cyber ... - SCVNEWS.com.
- Federal law on cyber security is crucial - Seacoastonline.com.
- Draft of Senate Cyber Bill Tackles Retaliation Rules - Wall Street Journal.
- Cyber-Surveillance Bill to Move Forward, Secretly - Center for Democracy and Technology.

## NEWS: COMPUTER FORENSICS

- Companies turn to forensic investigators to detect cyber crime - Channel News
- Review: In 'CSI: Cyber,' CBS Digitizes the Forensics Formula - New York Times.
- Here's What the Senate's Massive Sex-Trafficking Bill Would Actually Do - Reason (blog).
- Real-life look at cyber crime investigations - CBS 8 San Diego.
- Jury working late on Casey Frederiksen's decision - kwwl.com.

## EXPLOITS

- Kguard SHA104 / SHA108 Bypass / Command Injection.
- Codoforum 2.5.1 Arbitrary File Download.
- WordPress Fraction Theme 1.1.1 Privilege Escalation.
- Manage Engine AD Audit Manager Plus Cross Site Scripting.
- Varnish Cache 4.03 Buffer Overflow.
- NaCl Sandbox Escape For Rowhammer.
- Rowhammer Linux Kernel Privilege Escalation.
- ocPortal 9.0.16 Cross Site Scripting.
- OverCoffee Instant 2.0 SQL Injection.
- Untangle NGFW 9 / 10 / 11 XSS / Code Execution.
- NetCat CMS 5.01 Header Injection.
- MikroTik RouterOS Cross Site Request Forgery.
- OpenKM Stored Cross Site Scripting.
- Yahoo Query Language Cross Site Scripting.
- WordPress Daily Edition 1.6.2 File Upload.
- NetCat CMS 5.01 Cross Site Scripting.
- WordPress Daily Edition 1.6.2 SQL Injection.
- WordPress Yoast Google Analytics 5.3.2 Cross Site Scripting.
- ASUS RT-G32 Cross Site Request Forgery / Cross Site Scripting.
- Elastix 2.5.0 SQL Injection.
- Betster 1.0.4 SQL Injection / Authentication Bypass.
- Nvidia Mental Ray Satellite Service Arbitrary DLL Injection.
- ProjectSend r561 SQL Injection.
- WordPress Download Manager 2.7.2 Privilege Escalation.
- PHPMoAdmin 1.1.2 Remote Code Execution.
- GeniXCMS 0.0.1 - Multiple Vulnerabilities.
- Codoforum 2.5.1 - Arbitrary File Download.
- Rowhammer: NaCl Sandbox Escape PoC.
- Rowhammer: Linux Kernel Privilege Escalation PoC.
- [papers] - [Hebrew] Digital Whisper Security Magazine #59.
- HP Data Protector 8.10 Remote Command Execution.
- ProjectSend r561 - SQL Injection Vulnerability.
- WordPress Download Manager 2.7.2 - Privilege Escalation.
- Sagem F@st 3304-V2 - LFI.
- Calculated Fields Form Wordpress Plugin <= 1.0.10 - Remote SQL Injection Vulnerability.

## ADVISORIES

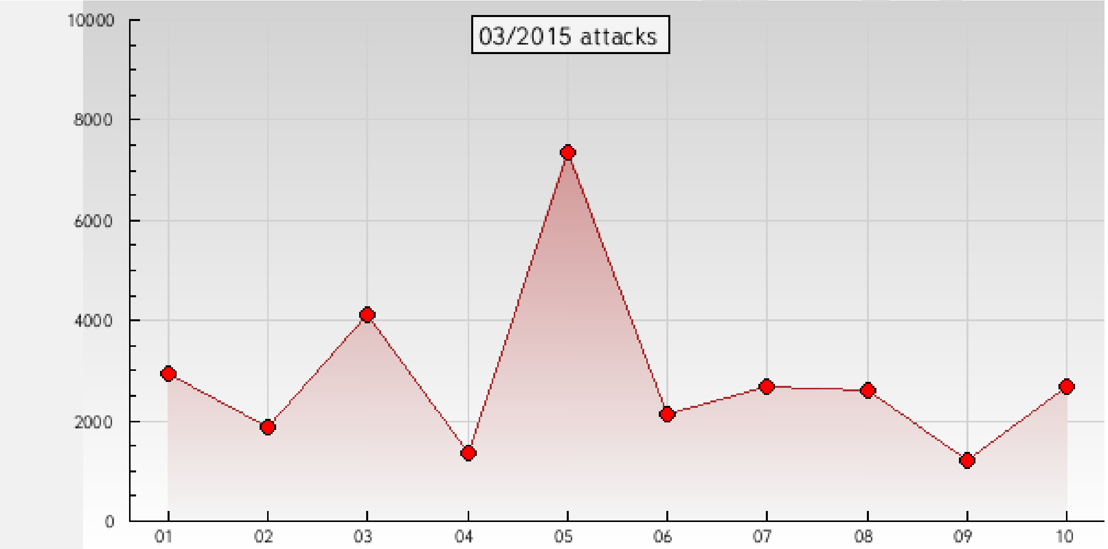
- Apple Security Advisory 2015-03-09-4.
  - Tue, 10 Mar 2015 16:22:37 GMT
    Apple Security Advisory 2015-03-09-4 - Xcode 6.2 is now available and addresses spoofing and validation checking issues.
- Apple Security Advisory 2015-03-09-3.
  - Tue, 10 Mar 2015 16:20:32 GMT
    Apple Security Advisory 2015-03-09-3 - Security Update 2015-002 is now available and addresses buffer overflow, off-by-one, type confusion, and secure transport vulnerabilities.

- Apple Security Advisory 2015-03-09-2.
  - Tue, 10 Mar 2015 16:17:57 GMT
    Apple Security Advisory 2015-03-09-2 - AppleTV 7.1 is now available and addresses folder creation, code execution, and tls-related vulnerabilities.
- Apple Security Advisory 2015-03-09-1.
  - Tue, 10 Mar 2015 16:14:34 GMT
    Apple Security Advisory 2015-03-09-1 - iOS 8.2 is now available and addresses null pointer dereference, code execution, buffer overflows, and various other vulnerabilities.
- Ubuntu Security Notice USN-2521-1.
  - Tue, 10 Mar 2015 16:03:06 GMT
    Ubuntu Security Notice 2521-1 - Several out-of-bounds write bugs were discovered in Skia. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking the program. A use-after-free was discovered in the V8 bindings in Blink. 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-2523-1.
  - Tue, 10 Mar 2015 16:02:55 GMT
    Ubuntu Security Notice 2523-1 - Martin Holst Swende discovered that the mod_headers module allowed HTTP trailers to replace HTTP headers during request processing. A remote attacker could possibly use this issue to bypass RequestHeaders directives. Mark Montague discovered that the mod_cache module incorrectly handled empty HTTP Content-Type headers. A remote attacker could use this issue to cause the server to stop responding, leading to a denial of service. This issue only affected Ubuntu 14.04 LTS and Ubuntu 14.10. Various other issues were also addressed.
- Mandriva Linux Security Advisory 2015-057.
  - Tue, 10 Mar 2015 16:02:11 GMT
    Mandriva Linux Security Advisory 2015-057 - The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bind system call for an AF_ALG socket with a parenthesized module template expression in the salg_name field, as demonstrated by the vfat expression, a different vulnerability than CVE-2013-7421. net/netfilter/nf_conntrack_proto_generic.c in the Linux kernel before 3.18 generates incorrect conntrack entries during handling of certain iptables rule sets for the SCTP, DCCP, GRE, and UDP-Lite protocols, which allows remote attackers to bypass intended access restrictions via packets with disallowed port numbers. The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bind system call for an AF_ALG socket with a module name in the salg_name field, a different vulnerability than CVE-2014-9644. The updated packages provides a solution for these security issues.
- Cisco Security Advisory 20150309-rowhammer.
  - Tue, 10 Mar 2015 16:00:47 GMT
    Cisco Security Advisory - On March 9, 2015, new research was published that takes advantage of a flaw in double data rate type 3 (DDR3) synchronous dynamic random-access memory (SDRAM) to perform privilege escalation attacks on systems that contain the affected hardware. The flaw is known as Row Hammer. To attempt an attack, the attacker must execute a malicious binary on an affected system. In addition, the research focused on consumer hardware that did not have a number of mitigations and memory protections that have been integrated into chipsets and memory modules used in Cisco server-class products. Of note in the paper is that the researchers were unable, in their testing, to exploit devices that use Error-Correcting Code (ECC) memory. Cisco offers a limited number of products that allow an unprivileged user to load and execute binaries.
- tcpdump Denial Of Service / Code Execution.
  - Tue, 10 Mar 2015 15:49:46 GMT
    tcpdump versions prior to 4.7.2 suffer from denial of service and code execution vulnerabilities.

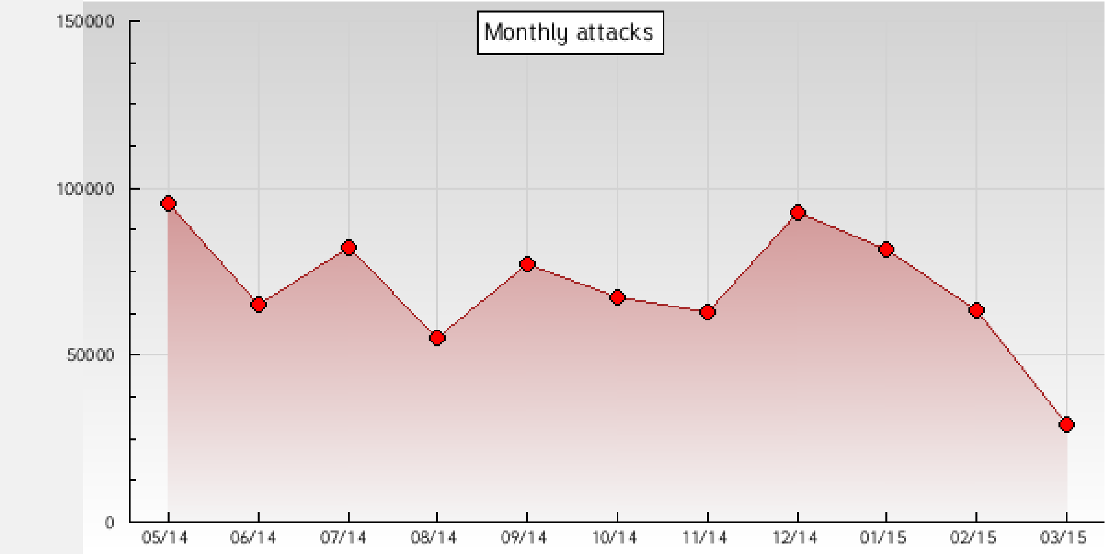
- Ubuntu Security Notice USN-2505-2.
  - Mon, 09 Mar 2015 20:19:37 GMT
    Ubuntu Security Notice 2505-2 - USN-2505-1 fixed vulnerabilities in Firefox. This update removed the deprecated "-remote" command-line switch that some older software still depends on. This update fixes the problem. Matthew Noorenberghe discovered that whitelisted Mozilla domains could make UITour API calls from background tabs. If one of these domains were compromised and open in a background tab, an attacker could potentially exploit this to conduct clickjacking attacks. Jan de Mooij discovered an issue that affects content using the Caja Compiler. If web content loads specially crafted code, this could be used to bypass sandboxing security measures provided by Caja. Armin Razmdjou discovered that opening hyperlinks with specific mouse and key combinations could allow a Chrome privileged URL to be opened without context restrictions being preserved. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to bypass security restrictions. Various other issues were also addressed.
- Red Hat Security Advisory 2015-0660-01.
  - Mon, 09 Mar 2015 20:18:47 GMT
    Red Hat Security Advisory 2015-0660-01 - Red Hat Enterprise MRG is a next-generation IT infrastructure for enterprise computing. MRG offers increased performance, reliability, interoperability, and faster computing for enterprise customers. The Qpid packages provide a message broker daemon that receives, stores and routes messages using the open AMQP messaging protocol along with run-time libraries for AMQP client applications developed using Qpid C++. Clients exchange messages with an AMQP message broker using the AMQP protocol. It was discovered that the Qpid daemon did not restrict access to anonymous users when the ANONYMOUS mechanism was disallowed.
- Red Hat Security Advisory 2015-0661-01.
  - Mon, 09 Mar 2015 20:18:28 GMT
    Red Hat Security Advisory 2015-0661-01 - Red Hat Enterprise MRG is a next-generation IT infrastructure for enterprise computing. MRG offers increased performance, reliability, interoperability, and faster computing for enterprise customers. The Qpid packages provide a message broker daemon that receives, stores and routes messages using the open AMQP messaging protocol along with run-time libraries for AMQP client applications developed using Qpid C++. Clients exchange messages with an AMQP message broker using the AMQP protocol. It was discovered that the Qpid daemon did not restrict access to anonymous users when the ANONYMOUS mechanism was disallowed.
- Mandriva Linux Security Advisory 2015-056.
  - Mon, 09 Mar 2015 20:18:17 GMT
    Mandriva Linux Security Advisory 2015-056 - It was found that RPM wrote file contents to the target installation directory under a temporary name, and verified its cryptographic signature only after the temporary file has been written completely. Under certain conditions, the system interprets the unverified temporary file contents and extracts commands from it. This could allow an attacker to modify signed RPM files in such a way that they would execute code chosen by the attacker during package installation. It was found that RPM could encounter an integer overflow, leading to a stack-based buffer overflow, while parsing a crafted CPIO header in the payload section of an RPM file. This could allow an attacker to modify signed RPM files in such a way that they would execute code chosen by the attacker during package installation.
- HP Security Bulletin HPSBGN03277 1.
  - Mon, 09 Mar 2015 20:18:03 GMT
    HP Security Bulletin HPSBGN03277 1 - Potential security vulnerabilities have been identified with the NTP service that is present on HP Virtualization Performance Viewer (vPV). These could be exploited remotely to execute code, create a Denial of Service (DoS), and other vulnerabilities. Revision 1 of this advisory.

## 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 | 2848 | 4109 | 6957 | 1314 | 5643 |
| 3. | Hmei7 | 2846 | 1510 | 4356 | 775 | 3581 |
| 4. | LatinHackTeam | 1438 | 1266 | 2704 | 2254 | 450 |
| 5. | iskorpitx | 1324 | 955 | 2279 | 786 | 1493 |
| 6. | Fatal Error | 1111 | 1724 | 2835 | 2455 | 380 |
| 7. | HighTech | 934 | 3655 | 4589 | 3684 | 905 |
| 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