Bonnes pratiques pour les Utilisateurs

CERT OSIRIS

UNIVERSITÉ DE STRASBOURG

Sensibilisation aux menaces Internet
&
Formation aux bonnes pratiques pour les utilisateurs (BPU) de systèmes informatiques

Goodies
Les Botnets

Septembre 2013

Les botnets : naissance et usages

1- utilisation d'un crimeware pack
2- ciblage des vulnérabilités à exploiter
3- implémentation de la charge virale
4- campagne d'infection de postes
5- pilotage des ordinateurs infectés

Naissance d'un botnet (1/5) : Utilisation d'un crimeware pack

(blackhole)

Annual license: $ 1500
Half-year license: $ 1000
3-month license: $ 700

Update cryptor $ 50
Changing domain $ 20 multidomain $ 200 to license.
During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): $ 200
2 weeks (14 full days): $ 300
3 weeks (21 full day): $ 400
4 weeks (31 full day): $ 500
24-hour test: $ 50

- There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

Providing our proper domain included. The subsequent change of the domain: $ 35
No longer any hidden fees, rental includes full support for the duration of the contract.

Extrait du *readme.txt* illustrant le modèle de tarification pour Blackhole v1.0.0

Naissance d'un botnet (2/5) : Ciblage de vulnérabilités publiées

Avis en 2013

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir.

CERTA-2013-AVI-421	Multiples vulnérabilités dans Oracle Database Server (17 juillet 2013)
CERTA-2013-AVI-420	Vulnérabilité dans Oracle Industry Applications (17 juillet 2013)
CERTA-2013-AVI-419	Multiples vulnérabilités dans Oracle MySQL (17 juillet 2013)
CERTA-2013-AVI-418	Vulnérabilité dans Oracle iLearning (17 juillet 2013)
CERTA-2013-AVI-417	Multiples vulnérabilités dans Oracle Virtualization (17 juillet 2013)
CERTA-2013-AVI-416	Multiples vulnérabilités dans Oracle Solaris (17 juillet 2013)
CERTA-2013-AVI-415	Multiples vulnérabilités dans Moodle (17 juillet 2013)
CERTA-2013-AVI-414	Vulnérabilité dans PHP (16 juillet 2013)
CERTA-2013-AVI-413	Multiples vulnérabilités dans Juniper Junos (15 juillet 2013)
CERTA-2013-AVI-412	Multiples vulnérabilités dans le noyau Linux de Mandriva (15 juillet 2013)
CERTA-2013-AVI-411	Multiples vulnérabilités dans le noyau Linux de SUSE (15 juillet 2013)
CERTA-2013-AVI-408	Multiples vulnérabilités dans Google Chrome (10 juillet 2013)
CERTA-2013-AVI-407	Multiples vulnérabilités dans Adobe ColdFusion (10 juillet 2013)
CERTA-2013-AVI-406	Vulnérabilité dans Adobe Shockwave Player (10 juillet 2013)
CERTA-2013-AVI-405	Multiples vulnérabilités dans Adobe Flash Player (10 juillet 2013)
CERTA-2013-AVI-404	Vulnérabilité dans Microsoft Windows Defender (10 juillet 2013)
CERTA-2013-AVI-403	Vulnérabilité dans Microsoft Windows Media Format Runtime (10 juillet 2013)
CERTA-2013-AVI-402	Vulnérabilité dans Microsoft DirectShow (10 juillet 2013)
CERTA-2013-AVI-401	Multiples vulnérabilités dans Microsoft Internet Explorer (10 juillet 2013)
CERTA-2013-AVI-400	Vulnérabilité dans Microsoft GDI+ (10 juillet 2013)
CERTA-2013-AVI-399	Multiples vulnérabilités dans le noyau Microsoft Windows (10 juillet 2013)
CERTA-2013-AVI-398	Multiples vulnérabilités dans Microsoft Framework .net et Silverlight (10 juillet 2013)
CERTA-2013-AVI-394	Vulnérabilité dans Citrix XenServer (08 juillet 2013)
CERTA-2013-AVI-393	Multiples vulnérabilités dans Apple OS X (08 juillet 2013)
CERTA-2013-AVI-392	Vulnérabilité dans Siemens COMOS (05 juillet 2013)
CERTA-2013-AVI-391	Multiples vulnérabilités dans le noyau Linux de Ubuntu (04 juillet 2013)
CERTA-2013-AVI-390	Multiples vulnérabilités dans Barracuda SSL VPN (04 juillet 2013)
CERTA-2013-AVI-389	Vulnérabilité dans Alcatel-Lucent OmniTouch (03 juillet 2013)
CERTA-2013-AVI-388	Multiples vulnérabilités dans Symantec Security Information Manager (03 juillet 2013)

AVIS EN 2013

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir.

- CERTA-2013-AVI-421 Multiples vulnérabilités dans Oracle Database Server (17 juillet 2013)
- CERTA-2013-AVI-420 Vulnérabilité dans Oracle Industry Applications (17 juillet 2013)
- CERTA-2013-AVI-419 Multiples vulnérabilités dans Oracle MySQL (17 juillet 2013)
- CERTA-2013-AVI-418 Vulnérabilité dans Oracle iLearning (17 juillet 2013)
- CERTA-2013-AVI-417 Multiples vulnérabilités dans Oracle Virtualization (17 juillet 2013)
- CERTA-2013-AVI-416 Multiples vulnérabilités dans Oracle Solaris (17 juillet 2013)
- CERTA-2013-AVI-415 Multiples vulnérabilités dans Moodle (17 juillet 2013)
- CERTA-2013-AVI-414 Vulnérabilité dans PHP (16 juillet 2013)
- CERTA-2013-AVI-413 Multiples vulnérabilités dans Juniper Junos (15 juillet 2013)
- CERTA-2013-AVI-412 Multiples vulnérabilités dans le noyau Linux de Mandriva (15 juillet 2013)
- CERTA-2013-AVI-411 Multiples vulnérabilités dans le noyau Linux de SUSE (15 juillet 2013)

- CERTA-2013-AVI-408 Multiples vulnérabilités dans Google Chrome (10 juillet 2013)
- CERTA-2013-AVI-407 Multiples vulnérabilités dans Adobe ColdFusion (10 juillet 2013)
- CERTA-2013-AVI-406 Vulnérabilité dans Adobe Shockwave Player (10 juillet 2013)
- CERTA-2013-AVI-405 Multiples vulnérabilités dans Adobe Flash Player (10 juillet 2013)
- CERTA-2013-AVI-404 Vulnérabilité dans Microsoft Windows Defender (10 juillet 2013)
- CERTA-2013-AVI-403 Vulnérabilité dans Microsoft Windows Media Format Runtime (10 juillet 2013)
- CERTA-2013-AVI-402 Vulnérabilité dans Microsoft DirectShow (10 juillet 2013)
- CERTA-2013-AVI-401 Multiples vulnérabilités dans Microsoft Internet Explorer (10 juillet 2013)
- CERTA-2013-AVI-400 Vulnérabilité dans Microsoft GDI+ (10 juillet 2013)
- CERTA-2013-AVI-399 Multiples vulnérabilités dans le noyau Microsoft Windows (10 juillet 2013)
- CERTA-2013-AVI-398 Multiples vulnérabilités dans Microsoft Framework .net et Silverlight (10 juillet 2013)

- CERTA-2013-AVI-394 Vulnérabilité dans Citrix XenServer (08 juillet 2013)
- CERTA-2013-AVI-393 Multiples vulnérabilités dans Apple OS X (08 juillet 2013)
- CERTA-2013-AVI-392 Vulnérabilité dans Siemens COMOS (05 juillet 2013)
- CERTA-2013-AVI-391 Multiples vulnérabilités dans le noyau Linux de Ubuntu (04 juillet 2013)
- CERTA-2013-AVI-390 Multiples vulnérabilités dans Barracuda SSL VPN (04 juillet 2013)
- CERTA-2013-AVI-389 Vulnérabilité dans Alcatel-Lucent OmniTouch (03 juillet 2013)
- CERTA-2013-AVI-388 Multiples vulnérabilités dans Symantec Security Information Manager (03 juillet 2013)

CERTA-2013-AVI-418 Vulnérabilité dans Oracle iLearning (17 juillet 2013)
CERTA-2013-AVI-417 Multiples vulnérabilités dans Oracle Virtualization (17 juillet 2013)
CERTA-2013-AVI-416 Multiples vulnérabilités dans Oracle Solaris (17 juillet 2013)
CERTA-2013-AVI-415 Multiples vulnérabilités dans Moodle (17 juillet 2013)
CERTA-2013-AVI-414 Vulnérabilité dans PHP (16 juillet 2013)
CERTA-2013-AVI-413 Multiples vulnérabilités dans Juniper Junos (15 juillet 2013)
CERTA-2013-AVI-412 Multiples vulnérabilités dans le noyau Linux de Mandriva (15 juillet 2013)
CERTA-2013-AVI-411 Multiples vulnérabilités dans le noyau Linux de SUSE (15 juillet 2013)

CERTA-2013-AVI-408 Multiples vulnérabilités dans Google Chrome (10 juillet 2013)
CERTA-2013-AVI-407 Multiples vulnérabilités dans Adobe ColdFusion (10 juillet 2013)
CERTA-2013-AVI-406 Vulnérabilité dans Adobe Shockwave Player (10 juillet 2013)
CERTA-2013-AVI-405 Multiples vulnérabilités dans Adobe Flash Player (10 juillet 2013)
CERTA-2013-AVI-404 Vulnérabilité dans Microsoft Windows Defender (10 juillet 2013)
CERTA-2013-AVI-403 Vulnérabilité dans Microsoft Windows Media Format Runtime (10 juillet 2013)
CERTA-2013-AVI-402 Vulnérabilité dans Microsoft DirectShow (10 juillet 2013)

CERTA-2013-AVI-401 Multiples vulnérabilités dans Microsoft Internet Explorer (10 juillet 2013)
CERTA-2013-AVI-400 Vulnérabilité dans Microsoft GDI+ (10 juillet 2013)
CERTA-2013-AVI-399 Multiples vulnérabilités dans le noyau Microsoft Windows (10 juillet 2013)
CERTA-2013-AVI-398 Multiples vulnérabilités dans Microsoft Framework .net et Silverlight (10 juillet 2013)

CERTA-2013-AVI-394 Vulnérabilité dans Citrix XenServer (08 juillet 2013)
CERTA-2013-AVI-393 Multiples vulnérabilités dans Apple OS X (08 juillet 2013)
CERTA-2013-AVI-392 Vulnérabilité dans Siemens COMOS (05 juillet 2013)
CERTA-2013-AVI-391 Multiples vulnérabilités dans le noyau Linux de Ubuntu (04 juillet 2013)
CERTA-2013-AVI-390 Multiples vulnérabilités dans Barracuda SSL VPN (04 juillet 2013)
CERTA-2013-AVI-389 Vulnérabilité dans Alcatel-Lucent OmniTouch (03 juillet 2013)
CERTA-2013-AVI-388 Multiples vulnérabilités dans Symantec Security Information Manager (03 juillet 2013)

CERTA-2013-AVI-341 Multiples vulnérabilités dans Apple Safari (05 juin 2013)

CERTA-2013-AVI-144 Multiples vulnérabilités dans Mozilla Firefox (21 février 2013)

CERTA-2013-AVI-418 Vulnérabilité dans Oracle iLearning (17 juillet 2013)
CERTA-2013-AVI-417 Multiples vulnérabilités dans Oracle Virtualization (17 juillet 2013)
CERTA-2013-AVI-416 Multiples vulnérabilités dans Oracle Solaris (17 juillet 2013)
CERTA-2013-AVI-415 Multiples vulnérabilités dans Moodle (17 juillet 2013)
CERTA-2013-AVI-414 Vulnérabilité dans PHP (16 juillet 2013)
CERTA-2013-AVI-413 Multiples vulnérabilités dans Juniper Junos (15 juillet 2013)

CERTA-2013-ALE-002 Vulnérabilités dans Adobe Reader et Acrobat (Corrigée le 21 février 2013)

CERTA-2013-AVI-408 Multiples vulnérabilités dans Google Chrome (10 juillet 2013)
CERTA-2013-AVI-407 Multiples vulnérabilités dans Adobe ColdFusion (10 juillet 2013)
CERTA-2013-AVI-406 Vulnérabilité dans Adobe Shockwave Player (10 juillet 2013)
CERTA-2013-AVI-405 Multiples vulnérabilités dans Adobe Flash Player (10 juillet 2013)
CERTA-2013-AVI-404 Vulnérabilité dans Microsoft Windows Defender (10 juillet 2013)
CERTA-2013-AVI-403 Vulnérabilité dans Microsoft Windows Media Format Runtime (10 juillet 2013)
CERTA-2013-AVI-402 Vulnérabilité dans Microsoft DirectShow (10 juillet 2013)
CERTA-2013-AVI-401 Multiples vulnérabilités dans Microsoft Internet Explorer (10 juillet 2013)
CERTA-2013-AVI-400 Vulnérabilité dans Microsoft GDI+ (10 juillet 2013)
CERTA-2013-AVI-399 Multiples vulnérabilités dans le noyau Microsoft Windows (10 juillet 2013)
CERTA-2013-AVI-398 Multiples vulnérabilités dans Microsoft Framework .net et Silverlight (10 juillet 2013)

CERTA-2013-AVI-394 Vulnérabilité dans Citrix XenServer (08 juillet 2013)
CERTA-2013-AVI-393 Multiples vulnérabilités dans Apple OS X (08 juillet 2013)
CERTA-2013-AVI-392 Vulnérabilité dans Siemens COMOS (05 juillet 2013)
CERTA-2013-AVI-391 Multiples vulnérabilités dans le noyau Linux de Ubuntu (04 juillet 2013)
CERTA-2013-AVI-390 Multiples vulnérabilités dans Barracuda SSL VPN (04 juillet 2013)
CERTA-2013-AVI-389 Vulnérabilité dans Alcatel-Lucent OmniTouch (03 juillet 2013)
CERTA-2013-AVI-388 Multiples vulnérabilités dans Symantec Security Information Manager (03 juillet 2013)

CERTA-2013-AVI-361 Multiples vulnérabilités dans Oracle Java (19 juin 2013)

CERTA-2013-AVI-354 Vulnérabilité dans Microsoft Office (12 juin 2013)

Juin 2013 : Java 7 Update 25 corrige 40 failles de sécurité

CVE#	Component	Protocol	composant	CVSS VERSION 2.0 RISK (see Risk Matrix Definitions)						
				sévérité /10	vecteur d'infection	complexité d'utilisation	Authen-tification	Confiden-tialité	Intégrité	disponibilité
CVE-2013-2470	Java Runtime Environment	Multiple	2D	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2471	Java Runtime Environment	Multiple	2D	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2472	Java Runtime Environment	Multiple	2D	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2473	Java Runtime Environment	Multiple	2D	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2463	Java Runtime Environment	Multiple	2D	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2464	Java Runtime Environment	Multiple	2D	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2465	Java Runtime Environment	Multiple	2D	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2469	Java Runtime Environment	Multiple	2D	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2459	Java Runtime Environment	Multiple	AWT	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2468	Java Runtime Environment	Multiple	Deployment	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-2466	Java Runtime Environment	Multiple	Deployment	10.0	Network	Low	None	Complete	Complete	Complete
CVE-2013-3743	Java Runtime Environment	Multiple	AWT	9.3	Network	Medium	None	Complete	Complete	Complete
CVE-2013-2462	Java Runtime Environment	Multiple	Deployment	9.3	Network	Medium	None	Complete	Complete	Complete
CVE-2013-2460	Java Runtime Environment	Multiple	Serviceability	9.3	Network	Medium	None	Complete	Complete	Complete
CVE-2013-2445	Java Runtime Environment	Multiple	Hotspot	7.8	Network	Low	None	None	None	Complete
CVE-2013-2448	Java Runtime Environment	Multiple	Sound	7.6	Network	High	None	Complete	Complete	Complete
CVE-2013-2442	Java Runtime Environment	Multiple	Deployment	7.5	Network	Low	None	Partial	Partial	Partial
CVE-2013-2461	Java Runtime Environment	Multiple	Libraries	7.5	Network	Low	None	Partial	Partial	Partial
CVE-2013-2467	Java Runtime Environment	None	Install	6.9	Local	Medium	None	Complete	Complete	Complete
CVE-2013-2407	Java Runtime Environment	Multiple	Libraries	6.4	Network	Low	None	Partial	None	Partial
CVE-2013-2454	Java Runtime Environment	Multiple	JDBC	5.8	Network	Medium	None	Partial	Partial	None
CVE-2013-2458	Java Runtime Environment	Multiple	Libraries	5.8	Network	Medium	None	Partial	Partial	None
CVE-2013-2444	Java Runtime Environment	Multiple	AWT	5.0	Network	Low	None	None	None	Partial
CVE-2013-2446	Java Runtime Environment	Multiple	CORBA	5.0	Network	Low	None	Partial	None	None
CVE-2013-2437	Java Runtime Environment	Multiple	Deployment	5.0	Network	Low	None	Partial	None	None
CVE-2013-2400	Java Runtime Environment	Multiple	Deployment	5.0	Network	Low	None	None	Partial	None
CVE-2013-3744	Java Runtime Environment	Multiple	Deployment	5.0	Network	Low	None	None	Partial	None
CVE-2013-2457	Java Runtime Environment	Multiple	JMX	5.0	Network	Low	None	None	Partial	None
CVE-2013-2453	Java Runtime Environment	Multiple	JMX	5.0	Network	Low	None	None	Partial	None
CVE-2013-2443	Java Runtime Environment	Multiple	Libraries	5.0	Network	Low	None	Partial	None	None
CVE-2013-2452	Java Runtime Environment	Multiple	Libraries	5.0	Network	Low	None	Partial	None	None
CVE-2013-2455	Java Runtime Environment	Multiple	Libraries	5.0	Network	Low	None	Partial	None	None
CVE-2013-2447	Java Runtime Environment	Multiple	Networking	5.0	Network	Low	None	Partial	None	None
CVE-2013-2450	Java Runtime Environment	Multiple	Serialization	5.0	Network	Low	None	None	None	Partial
CVE-2013-2456	Java Runtime Environment	Multiple	Serialization	5.0	Network	Low	None	Partial	None	None
CVE-2013-2412	Java Runtime Environment	Multiple	Serviceability	5.0	Network	Low	None	Partial	None	None
CVE-2013-2449	Java Runtime Environment	Multiple	Libraries	4.3	Network	Medium	None	Partial	None	None
CVE-2013-1571	Javadoc	HTTP	-	4.3	Network	Medium	None	None	Partial	None
CVE-2013-2451	Java Runtime Environment	None	Networking	3.7	Local	High	None	Partial	Partial	Partial
CVE-2013-1500	Java Runtime Environment	None	2D	3.6	Local	Low	None	Partial	Partial	None

AVIS EN 2013

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir.

CERTA-2013-AVI-421	Multiples vulnérabilités dans Oracle Database Server (17 juillet 2013)
CERTA-2013-AVI-420	Vulnérabilité dans Oracle Industry Applications (17 juillet 2013)
CERTA-2013-AVI-419	Multiples vulnérabilités dans Oracle MySQL (17 juillet 2013)
CERTA-2013-AVI-418	Vulnérabilité dans Oracle iLearning (17 juillet 2013)
CERTA-2013-AVI-417	Multiples vulnérabilités dans Oracle Virtualization (17 juillet 2013)
CERTA-2013-AVI-416	Multiples vulnérabilités dans Oracle Solaris (17 juillet 2013)
CERTA-2013-AVI-415	Multiples vulnérabilités dans Moodle (17 juillet 2013)
CERTA-2013-AVI-414	Vulnérabilité dans PHP (16 juillet 2013)
CERTA-2013-AVI-413	Multiples vulnérabilités dans Juniper Junos (15 juillet 2013)
CERTA-2013-AVI-412	Multiples vulnérabilités dans le noyau Linux de Mandriva (15 juillet 2013)
CERTA-2013-AVI-411	Multiples vulnérabilités dans le noyau Linux de SUSE (15 juillet 2013)
CERTA-2013-AVI-274	Multiples vulnérabilités dans Cisco Device Manager (25 avril 2013)
CERTA-2013-AVI-408	Multiples vulnérabilités dans Google Chrome (10 juillet 2013)
CERTA-2013-AVI-407	Multiples vulnérabilités dans Adobe ColdFusion (10 juillet 2013)
CERTA-2013-AVI-406	Vulnérabilité dans Adobe Shockwave Player (10 juillet 2013)
CERTA-2013-AVI-405	Multiples vulnérabilités dans Adobe Flash Player (10 juillet 2013)
CERTA-2013-AVI-404	Vulnérabilité dans Microsoft Windows Defender (10 juillet 2013)
CERTA-2013-AVI-403	Vulnérabilité dans Microsoft Windows Media Format Runtime (10 juillet 2013)
CERTA-2013-AVI-402	Vulnérabilité dans Microsoft DirectShow (10 juillet 2013)
CERTA-2013-AVI-401	Multiples vulnérabilités dans Microsoft Internet Explorer (10 juillet 2013)
CERTA-2013-AVI-400	Vulnérabilité dans Microsoft GDI+ (10 juillet 2013)
CERTA-2013-AVI-399	Multiples vulnérabilités dans le noyau Microsoft Windows (10 juillet 2013)
CERTA-2013-AVI-398	Multiples vulnérabilités dans Microsoft Framework .net et Silverlight (10 juillet 2013)
CERTA-2013-AVI-394	Vulnérabilité dans Citrix XenServer (08 juillet 2013)
CERTA-2013-AVI-393	Multiples vulnérabilités dans Apple OS X (08 juillet 2013)
CERTA-2013-AVI-392	Vulnérabilité dans Siemens COMOS (05 juillet 2013)
CERTA-2013-AVI-391	Multiples vulnérabilités dans le noyau Linux de Ubuntu (04 juillet 2013)
CERTA-2013-AVI-390	Multiples vulnérabilités dans Barracuda SSL VPN (04 juillet 2013)
CERTA-2013-AVI-244	Multiples vulnérabilités dans les systèmes SCADA Schneider (12 avril 2013)

AVIS EN 2013

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir.

CERTA-2013-AVI-421	Multiples vulnérabilités dans Oracle Database Server (17 juillet 2013)
CERTA-2013-AVI-420	Vulnérabilité dans Oracle Industry Applications (17 juillet 2013)
CERTA-2013-AVI-419	Multiples vulnérabilités dans Oracle MySQL (17 juillet 2013)
CERTA-2013-AVI-418	Vulnérabilité dans Oracle iLearning (17 juillet 2013)
CERTA-2013-AVI-417	Multiples vulnérabilités dans Oracle Virtualization (17 juillet 2013)
CERTA-2013-AVI-416	Multiples vulnérabilités dans Oracle Solaris (17 juillet 2013)
CERTA-2013-AVI-415	Multiples vulnérabilités dans Moodle (17 juillet 2013)
CERTA-2013-AVI-414	Vulnérabilité dans PHP (16 juillet 2013)
CERTA-2013-AVI-413	Multiples vulnérabilités dans Juniper Junos (15 juillet 2013)
CERTA-2013-AVI-412	Multiples vulnérabilités dans le noyau Linux de Mandriva (15 juillet 2013)
CERTA-2013-AVI-411	Multiples vulnérabilités dans le noyau Linux de SUSE (15 juillet 2013)
CERTA-2013-AVI-408	Multiples vulnérabilités dans Google Chrome (10 juillet 2013)
CERTA-2013-AVI-407	Multiples vulnérabilités dans Adobe ColdFusion (10 juillet 2013)
CERTA-2013-AVI-406	Vulnérabilité dans Adobe Shockwave Player (10 juillet 2013)
CERTA-2013-AVI-405	Multiples vulnérabilités dans Adobe Flash Player (10 juillet 2013)
CERTA-2013-AVI-404	Vulnérabilité dans Microsoft Windows Defender (10 juillet 2013)
CERTA-2013-AVI-403	Vulnérabilité dans Microsoft Windows Media Format Runtime (10 juillet 2013)
CERTA-2013-AVI-402	Vulnérabilité dans Microsoft DirectShow (10 juillet 2013)
CERTA-2013-AVI-401	Multiples vulnérabilités dans Microsoft Internet Explorer (10 juillet 2013)
CERTA-2013-AVI-400	Vulnérabilité dans Microsoft GDI+ (10 juillet 2013)
CERTA-2013-AVI-399	Multiples vulnérabilités dans le noyau Microsoft Windows (10 juillet 2013)
CERTA-2013-AVI-398	Multiples vulnérabilités dans Microsoft Framework .net et Silverlight (10 juillet 2013)
CERTA-2013-AVI-394	Vulnérabilité dans Citrix XenServer (08 juillet 2013)
CERTA-2013-AVI-393	Multiples vulnérabilités dans Apple OS X (08 juillet 2013)
CERTA-2013-AVI-392	Vulnérabilité dans Siemens COMOS (05 juillet 2013)
CERTA-2013-AVI-391	Multiples vulnérabilités dans le noyau Linux de Ubuntu (04 juillet 2013)
CERTA-2013-AVI-390	Multiples vulnérabilités dans Barracuda SSL VPN (04 juillet 2013)
CERTA-2013-AVI-388	Multiples vulnérabilités dans Symantec Security Information Manager (03 juillet 2013)

Naissance d'un botnet (3/5) : implémentation de la charge virale

metasploit community

Project - test ▼ Account - georges... ▼ Administr

Overview Analysis Sessions Campaigns Web Apps Modules Tags Reports Tasks

Home test Modules

Search Modules java

metasploit®

Module Statistics show Search Keywords show

Found 81 matching modules

Module Type	OS	Module	Disclosure Date	Module Ranking	CVE	BID	OSVDB
Client Exploit		Java CMM Remote Code Execution	March 1, 2013	★★	2013-1493	58238	90737
Auxiliary		Apple Safari .webarchive File Format UXSS	February 22, 2013	★★			
Client Exploit		Java Applet JMX Remote Code Execution	January 19, 2013	★★★★★	2013-0431	57726	89613
Server Exploit		Jenkins Script-Console Java Execution	January 18, 2013	★★★			
Client Exploit		Java Applet JMX Remote Code Execution	January 10, 2013	★★★★★	2013-0422		
Client Exploit		Java Applet Reflection Type Confusion Remote Code Execution	January 10, 2013	★★★★★	2013-2423	59162	92348
Client Exploit		Java Applet AverageRangeStatisticImpl Remote Code Execution	October 16, 2012	★★★★★	2012-5076	56054	86363
Client Exploit		Java Applet Method Handle Remote Code Execution	October 16, 2012	★★★★★	2012-5088	56057	86352
Client Exploit		Java Applet JAX-WS Remote Code Execution	October 16, 2012	★★★★★	2012-5076	56054	86363
Client Exploit		Microsoft Internet Explorer Option Element Use-After-Free	October 11, 2012	★★	2011-1996		

Naissance d’un botnet (4/5) : campagne d’infection de postes

Dissémination des charges virales sur internet

Infection de sites web légitimes
Redirection de sites légitimes vers des sites infectés
iframe, Attaque de point d'eau (Water holing)

Propagation de liens frauduleux sur internet (messagerie, blogs, forum, commentaires…)

Naissance d'un botnet (5/5) : pilotage des ordinateurs infectés

STATISTIC

TOTAL INFO

600327 HITED **461163** HOSTS **67742** LOADS **14.69%**

TODAY INFO

2568 HITED **2531** HOSTS **285** LOADS **11.26%**

OS	HITS	HOSTS	LOADS ↑	%
Windows 7	290890	219291	28879	13.17
Windows XP	163899	128063	23110	18.05
Windows Vista	107408	81266	15648	19.26
Windows 2003	700	529	158	29.87
Windows 2000	342	290	27	9.34
Windows NT	173	145	6	4.14
Windows 98	79	75	4	5.41
Mac OS	32982	30799	1	0.00
Linux	3803	3672	1	0.03
Windows 95	8	8	0	0.00

THREADS ↓	HITS	HOSTS	LOADS	%
10k US	1775	1729	135	7.81
2k loads AU	18956	17345	1493	8.61
2k uk loads	29509	26810	3506	13.08
3k UK loads mattew	22449	20091	3010	14.98
50k AU	14244	12949	1920	14.83
50k CA i EU	9159	8547	1807	21.14

EXPLOITS	LOADS	% ↑
Java Rhino	54430	79.89
PDF LIBTIFF	8771	12.87
PDF ALL	1983	2.91
Java OBE	1396	2.05
FLASH	571	0.84
HCP	503	0.74
MDAC	475	0.70

BROWSERS ↓	HITS	HOSTS	LOADS	%
Aol	4	4	0	0.00
Chrome	27574	23726	576	2.43
Firefox	174630	142879	25778	18.05
MSIE	348070	256067	40008	15.63
Mozilla	3889	3594	11	0.31
Opera	7900	5429	882	16.25
Safari	38213	35387	681	1.92

COUNTRIES	HITS ↑	HOSTS	LOADS	%
France	306438	209039	30779	14.72
United Kingdom	103352	89037	11190	12.57
United States	98661	86664	14679	16.95
Australia	53145	46296	5925	12.80
Germany	10476	9874	1468	14.88
Russian Federation	9871	4149	532	12.83
Canada	6994	5958	1041	17.47
Spain	4636	4367	1200	27.48
Italy	3471	3190	409	12.83

« Dans la peau d'un hacker black hat »
par Korben
http://korben.info/interview-black-hat.html

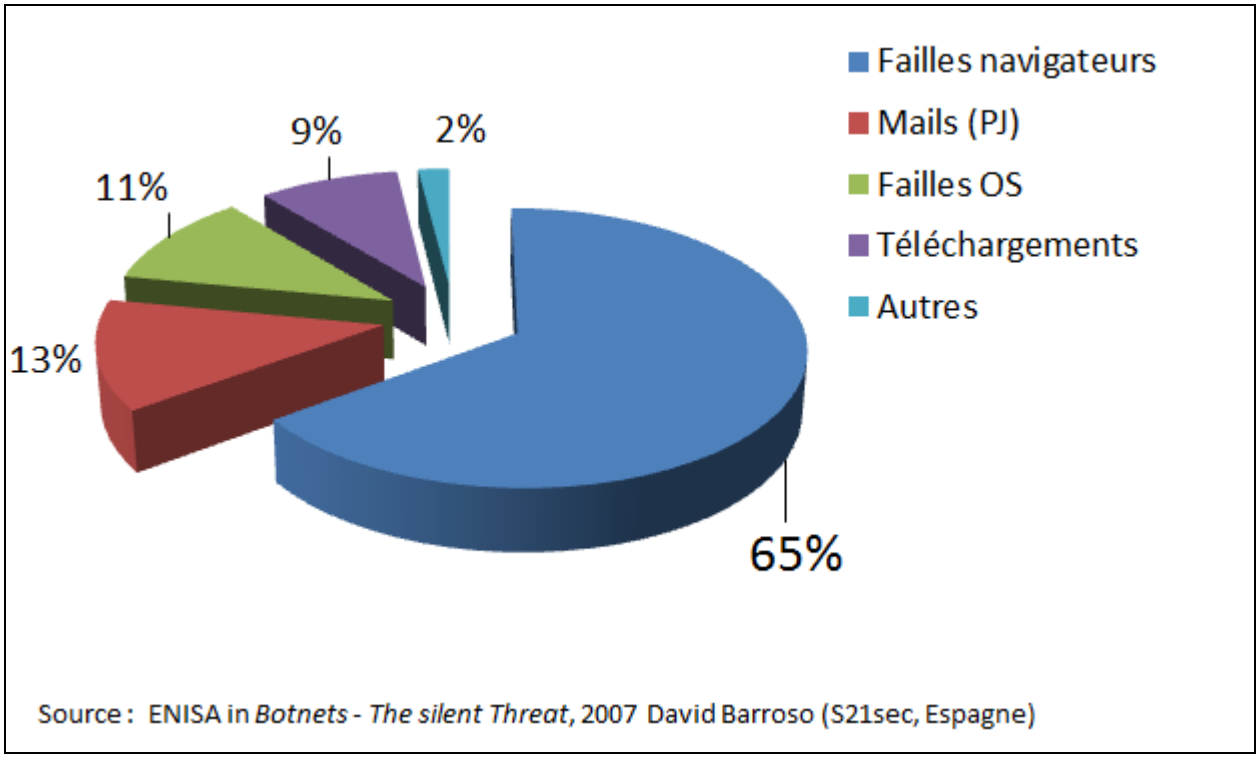
« de nombreux sites sont ciblés par le biais de méthodes très simples et banales »

Spécialité : ingénierie sociale
Domaines : Piratage de cartes de crédit, construction de botnets, abattage de serveurs

Techniques : injections SQL (SQLi), le XSS basique et avancé, le CSRF et l'empoisonnement de cache DNS

« en une journée, on peut gagner plusieurs centaines de milliers de dollars. Le milieu black hat a évolué, pour passer d'actions manuelles à une automatisation générale des logiciels. »

BOTNETS : MÉTHODES D'INFECTION



Source : ENISA in *Botnets - The silent Threat*, 2007 David Barroso (S21sec, Espagne)

Un simple CLIC sur un lien frauduleux peut suffire, navigation sur un site web compromis, téléchargement d'un programme infecté, ouverture d'une pièce jointe piégée…

EXEMPLE D'INFECTION : « DRIVE BY DOWNLOAD »

De : Facebook [notification+zrdozoee1ohe@facebookmail.com]
À : xxx yyy
Cc :
Objet : Amy Fibro commented on your photo.
Date : ven. 26/11/2010 02:59

Amy Fibro commented on your photo.

To see the comment thread, follow the link below:
http://www.facebook.com/n/?photo.php&fbid=155175754523620&set=a.145049682202894.23363.100000035890817&mid=33283faG5af34842cf81G...7f9cbG9
Thanks,
The Facebook Team

http://188.120.225.116/config/iqywjmypgzknisaugpkv.php
Cliquez pour suivre le lien

Journaux de gestion des clients - Journal de sécurité

Fichier Edition Afficher Filtrer Opération ?

Date et heure	Type d'événement	Gravité	Direction	Protocole	Hôte distant
26/11/2010 09:02:42	Réponse active	Majeure	Entrant	Aucun(e)	188.120.225.116
26/11/2010 09:02:42	Prévention d'intrusion	Critique	Entrant	TCP	188.120.225.116

[SID : 23528] Détection de HTTP Fragus Toolkit Download Activity.
Le trafic a été bloqué à partir de cette application : firefox.exe

adresse ip

188.120.225.116

st35.ru

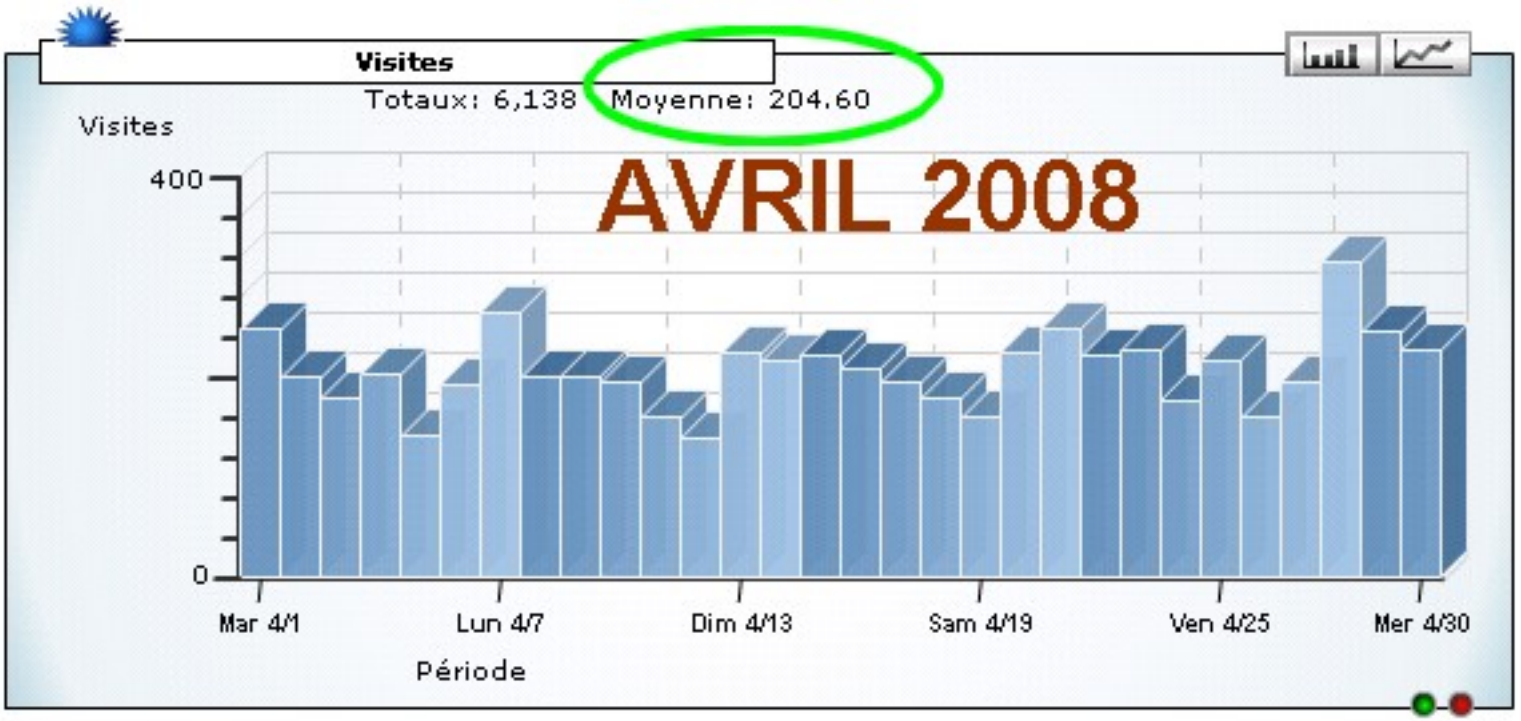
Moscow, RU
Latitude : 55.752201, Longitude : 37.615601
Fournisseur d'accès : ISPsystem, cjsc

BOTNETS : A QUOI ÇA SERT ?

Utilisation de l'ordinateur infecté *(à l'insu de son propriétaire)* pour :

- Envoi massif de mails : spam, phishing
- Attaque groupée d'une cible tierce : déni de service (DDoS)
- Masquer l'origine d'une attaque : serveur proxy
- Vol de données : carte de crédit, mots de passe, messagerie…
- Stockage pour les contenus illicites pour redistribution : films, musique, …

EXEMPLE D'UN SITE WEB ATTAQUÉ PAR UN BOTNET (1/3)



EXEMPLE D'UN SITE WEB ATTAQUÉ PAR UN BOTNET (2/3)

EXEMPLE D'UN SITE WEB ATTAQUÉ PAR UN BOTNET (3/3)

Origines géographiques des connexions

Période: 1/6/2008 - 30/6/2008 — Meilleurs pays

Précédent	Visiteurs	Précédent	Visiteurs	Précédent Nbr. Affiché	Visiteurs
1. net (Network)	6 951	21. br (Brazil)	197	41. ve (Venezuela)	81
2. com (Commercial)	5 287	22. ru (Russian Federation)	188	42. il (Israel)	72
3. fr (France)	1 908	23. ar (Argentina)	187	43. id (Indonesia)	64
4. de (Germany)	1 627	24. lu (Luxembourg)	178	44. ni (Nicaragua)	63
5. jp (Japan)	1 362	25. tw (Taiwan)	162	45. si (Slovenia)	58
6. pl (Poland)	951	26. ae (United Arab Emirates)	151	46. mx (Mexico)	55
7. edu (Educational)	852	27. hu (Hungary)	145	47. kr (South Korea)	49
8. au (Australia)	753	28. gr (Greece)	145	48. ec (Ecuador)	47
9. org (Non-Profit Organizations)	694	29. no (Norway)	142	49. sk (Slovak Republic)	47
10. it (Italy)	576	30. th (Thailand)	139	50. hk (Hong Kong)	31
11. nl (Netherlands)	524	31. at (Austria)	128	51. be (Belgium)	28
12. ch (Switzerland)	448	32. ee (Estonia)	127	52. my (Malaysia)	26
13. es (Spain)	421	33. cz (Czech Republic)	123	53. tr (Turkey)	25
14. dk (Denmark)	391	34. jo (Jordan)	118	54. md (Moldavia)	5
15. ca (Canada)	369	35. za (South Africa)	112	55. ie (Ireland)	3
16. se (Sweden)	282	36. tv (Tuvalu)	107	56. ro (Romania)	3
17. us (United States)	274	37. nz (New Zealand)	104	57. lv (Latvia)	2
18. ua (Ukraine)	268	38. sa (Saudi Arabia)	97	58. bg (Bulgaria)	1
19. other	227	39. fi (Finland)	95	59. gov (USA Government)	1
20. uk (United Kingdom)	225	40. yu (Yugoslavia)	90		