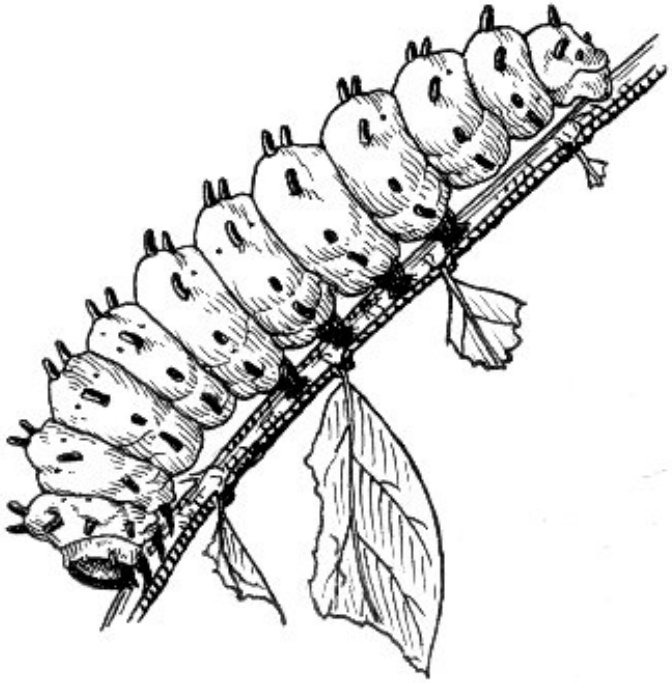
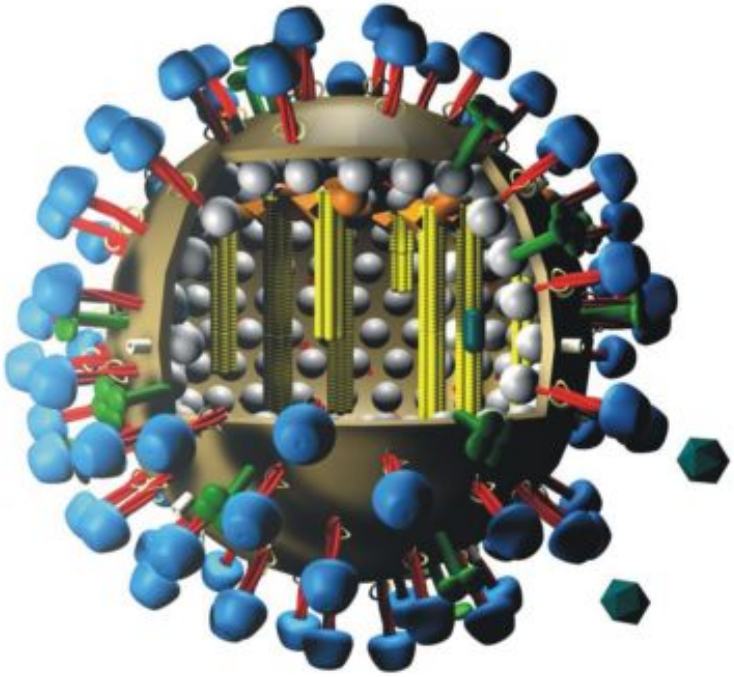
Apadrina un Gusano

Conficker

Marcos Sanz
sanz@denic.de





Win32/Conficker

Worm.Downadup

Downup

W32.Downadup

Win32.Worm.Downadup.Gen

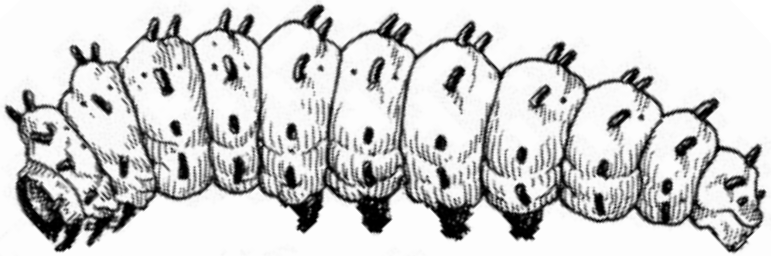
Win32:Confi

Net-Worm.Win32.Kido.bt

W32/Conficker.worm

Kido

WORM_DOWNAD



#1
Vulnerabilidad RPC Windows

Microsoft Security Bulletin MS08-067 – Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

Version: 1.0

General Information

Executive Summary

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, and rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None

Top of section

Affected and Non-Affected Software

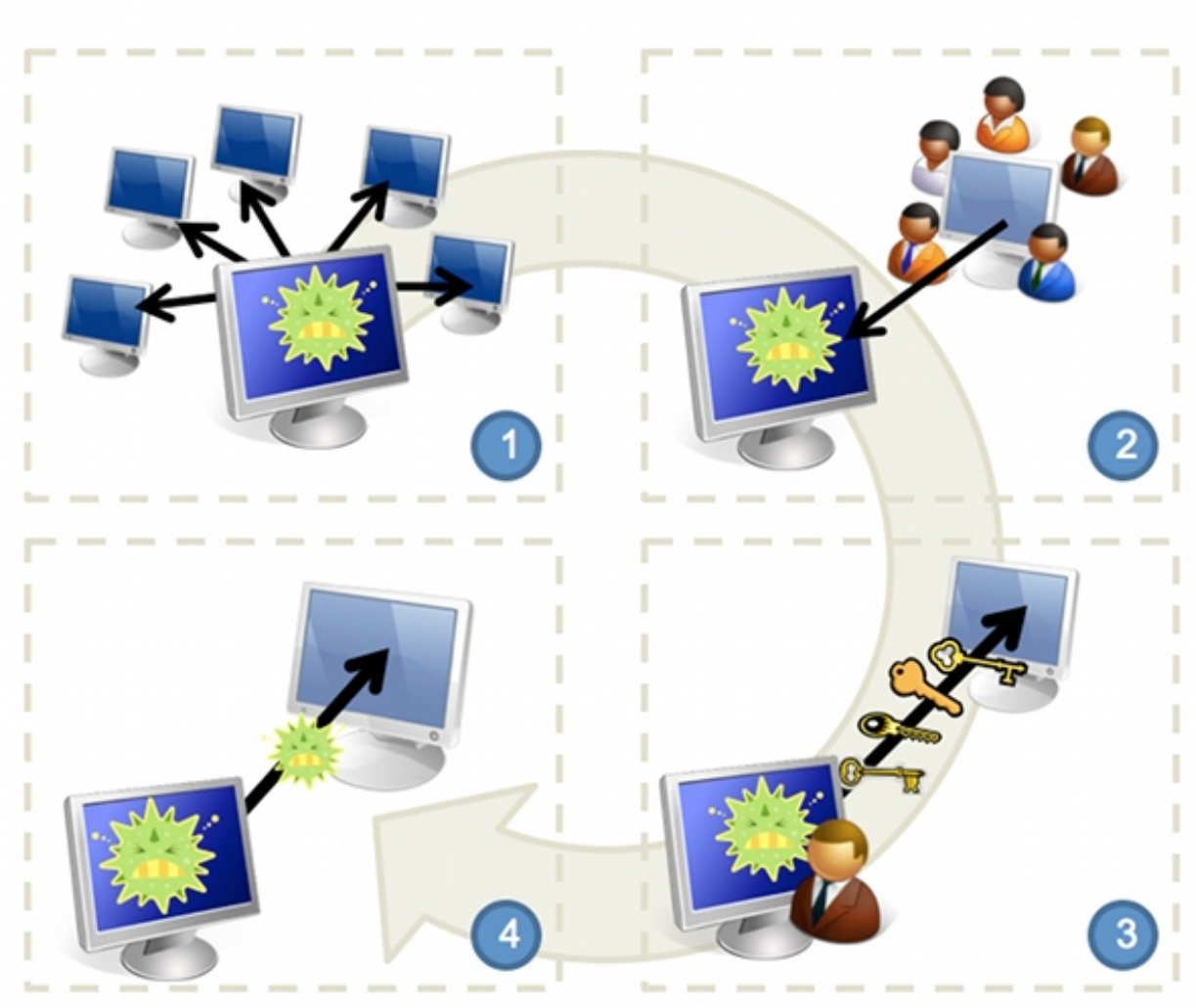
The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

Affected Software

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Windows 2000 Service Pack 4	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 2	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 3	Remote Code Execution	Critical	None
Windows XP Professional x64 Edition	Remote Code Execution	Critical	MS06-040
Windows XP Professional x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 Service Pack 1	Remote Code Execution	Critical	MS06-040
Windows Server 2003 Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 x64 Edition	Remote Code Execution	Critical	MS06-040
Windows Server 2003 x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 with SP1 for Itanium-based Systems	Remote Code Execution	Critical	MS06-040
Windows Server 2003 with SP2 for Itanium-based Systems	Remote Code Execution	Critical	None
Windows Vista and Windows Vista Service Pack 1	Remote Code Execution	Important	None
Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1	Remote Code Execution	Important	None
Windows Server 2008 for 32-bit Systems*	Remote Code Execution	Important	None
Windows Server 2008 for x64-based Systems*	Remote Code Execution	Important	None
Windows Server 2008 for Itanium-based Systems	Remote Code Execution	Important	None

#2

Admin Netshare


1
2
3
4

00000, 0000000, 00000000, 0987654321, 11111, 111111, 1111111, 11111111, 123123, 12321, 123321, 12345, 123456, 1234567, 12345678, 123456789, 1234567890, 1234abcd, 1234qwer, 123abc, 123asd, 123qwe, 1q2w3e, 22222, 222222, 2222222, 22222222, 33333, 333333, 3333333, 33333333, 44444, 444444, 4444444, 44444444, 54321, 55555, 555555, 5555555, 55555555, 654321, 66666, 666666, 6666666, 66666666, 7654321, 77777, 777777, 7777777, 77777777, 87654321, 88888, 888888, 8888888, 88888888, 987654321, 99999, 999999, 9999999, 99999999

a1b2c3, aaaaa, abc123, academia, access, account, Admin, admin, admin1, admin12, admin123, adminadmin, administrator, anything, asddsa, asdfgh, asdsa, asdzxc

backup, boss123, business

campus, changeme, cluster, codename, codeword, coffee, computer, controller, cookie, customer

database, default, desktop, domain

example, exchange, explorer

files, foobar, foofoo, forever, freedom

games

home123

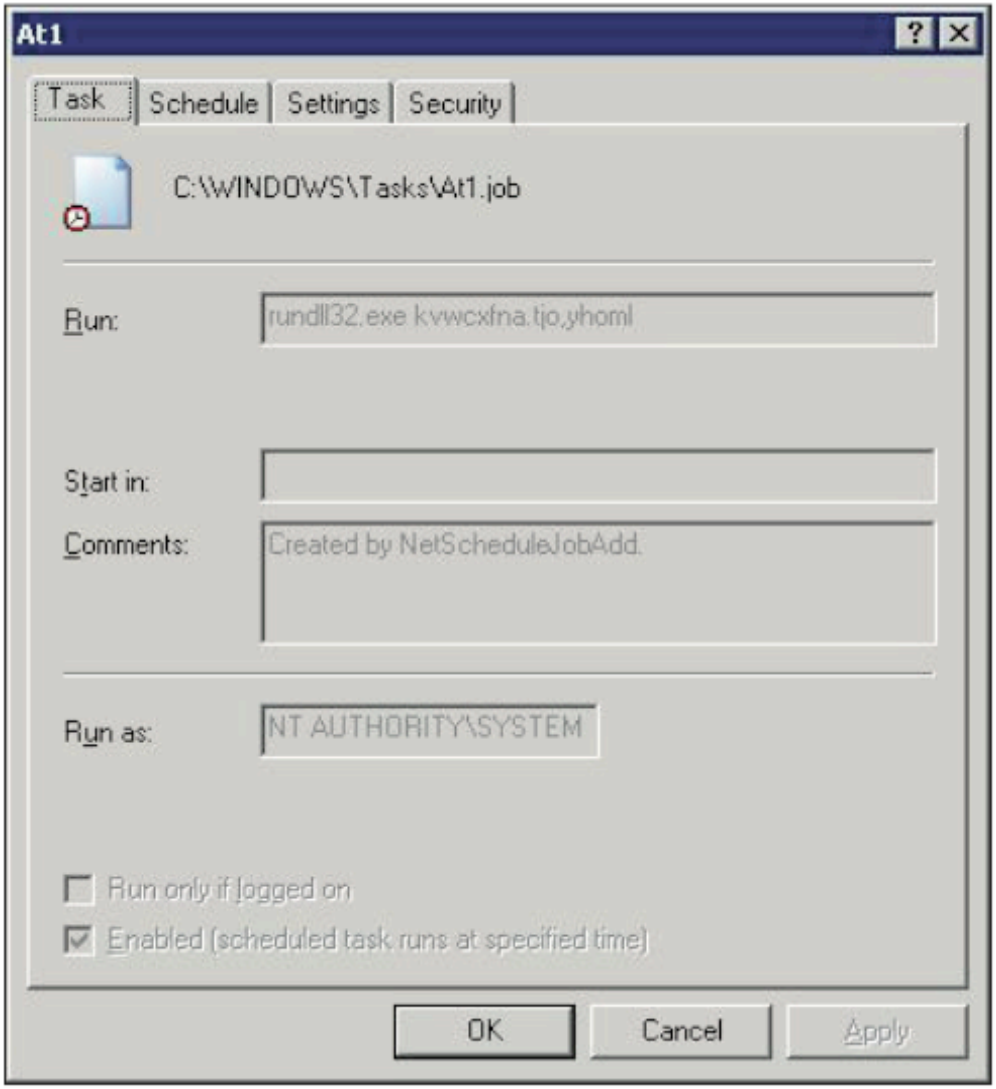
ihavenopass, Internet, internet, intranet

killer

letitbe, letmein, Login, login, lotus, love123

manager, market, money, monitor, mypass, mypassword, mypc123

nimda, nobody, nopass, nopassword, nothing

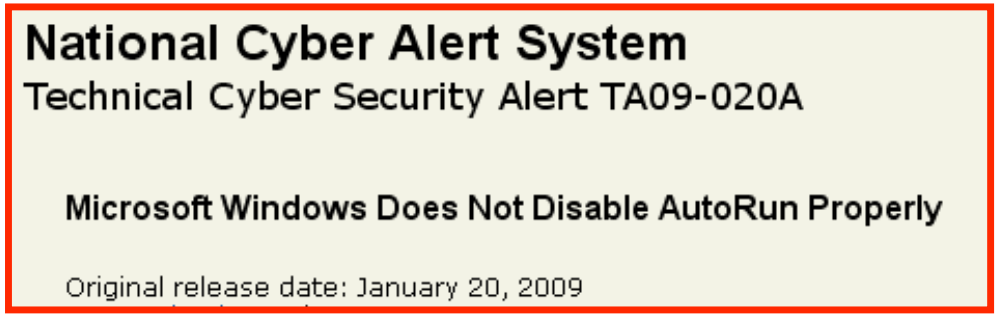

At1
Task
Schedule
Settings
Security
C:\WINDOWS\Tasks\At1.job
Run:
rundll32.exe kvwcxfna.tjo,yhoml
Start in:
Comments:
Created by NetScheduleJobAdd.
Run as:
NT AUTHORITY\SYSTEM
Run only if logged on
Enabled (scheduled task runs at specified time)
OK
Cancel
Apply

#3

Pendrive


AutoPlay
Removable Disk (E:)
Always do this for software and games:
Install or run program
Open folder to view files
Publisher not specified
General options
Open folder to view files
using Windows Explorer
Speed up my system
using Windows ReadyBoost
Set AutoPlay defaults in Control Panel

Cómo desactivar Autorun:
http://support.microsoft.com/kb/953252



Cómo desactivar Autorun (II)

http://www.us-cert.gov/cas/techalerts/TA09-020A.html

Cómo desactivar Autorun (*ahora sí*)
http://support.microsoft.com/kb/967715


Remote Desktop Connection
Remote Desktop
Connection
Local devices and resources
Choose the devices and resources on this computer that you want to use in your remote session.
Smart cards
Serial ports
Drives
C:
D:
E:
F:
Drives that I connect to later
Supported Plug and Play devices
Devices that I plug in later
Which Plug and Play devices can I use in my remote session?
OK
Cancel

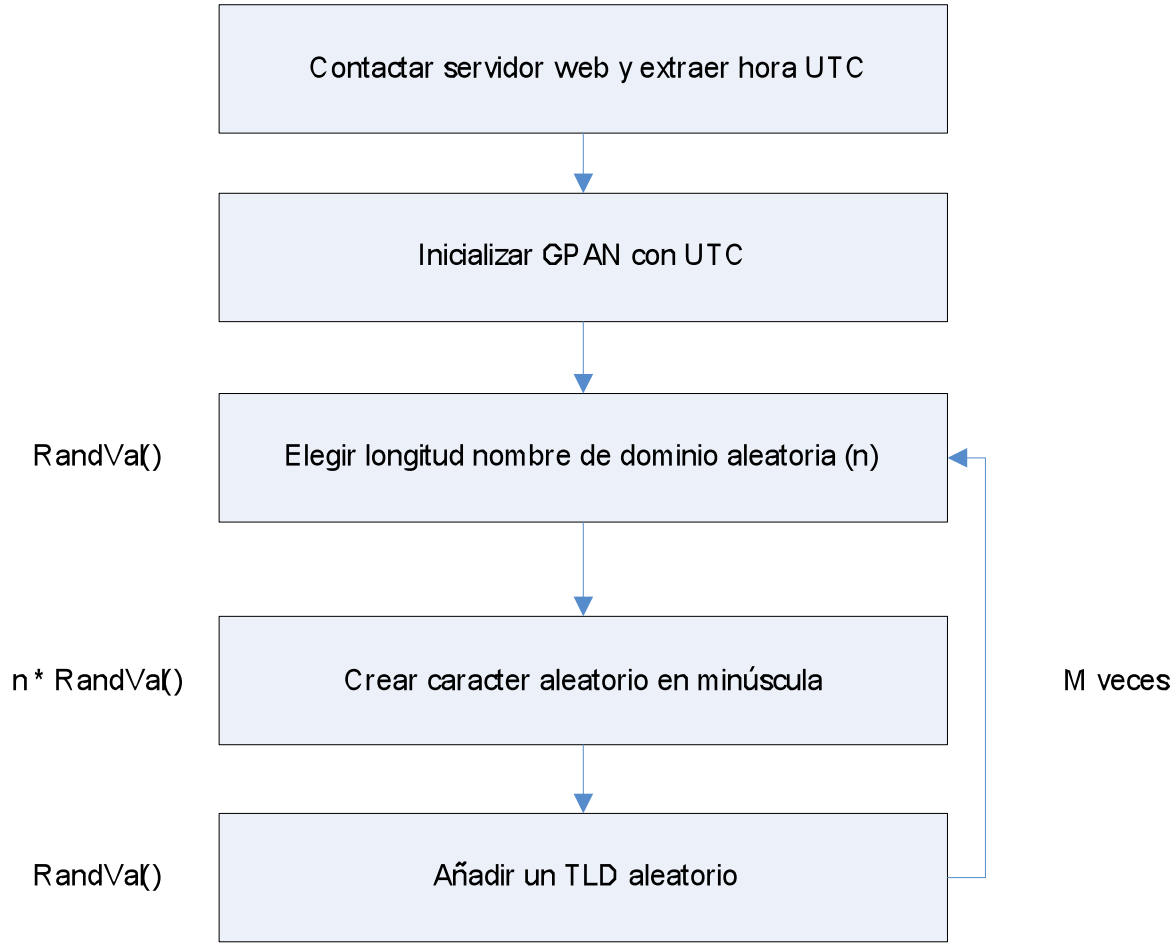
¿Eso es todo?

- Se antepone al resolver de DNS: bloquea páginas web que contengan ‘avg.*’, ‘bit9.*’, ‘ca.*’,‘nai.*’, ‘sans*’, ...
- Se inyecta en services.exe / dnsrslvr.dll (Win2000).
- Parchea DNSQuery_A(), DNSQuery_UTF8(), DNSQuery_W(), Query_Main() en dnsapi.dll via svchost -k NetworkServices (Non Win2000)
- Devuelve ERROR_TIMEOUT a consultas de DNS a: avast, avira, clamav, esafe, ikarus, gdata, fsecure, microsoft, etc...
- Detiene Windows Defender + Autorun
- Detiene Windows Security Center Service (wscsvc)
- Detiene Windows Autoupdate
- Detiene Windows Error Reporting Service (ersvc)
- Detiene Wireshark y otras utilidades de debug

¿Pero eso sí es todo, no?

#4

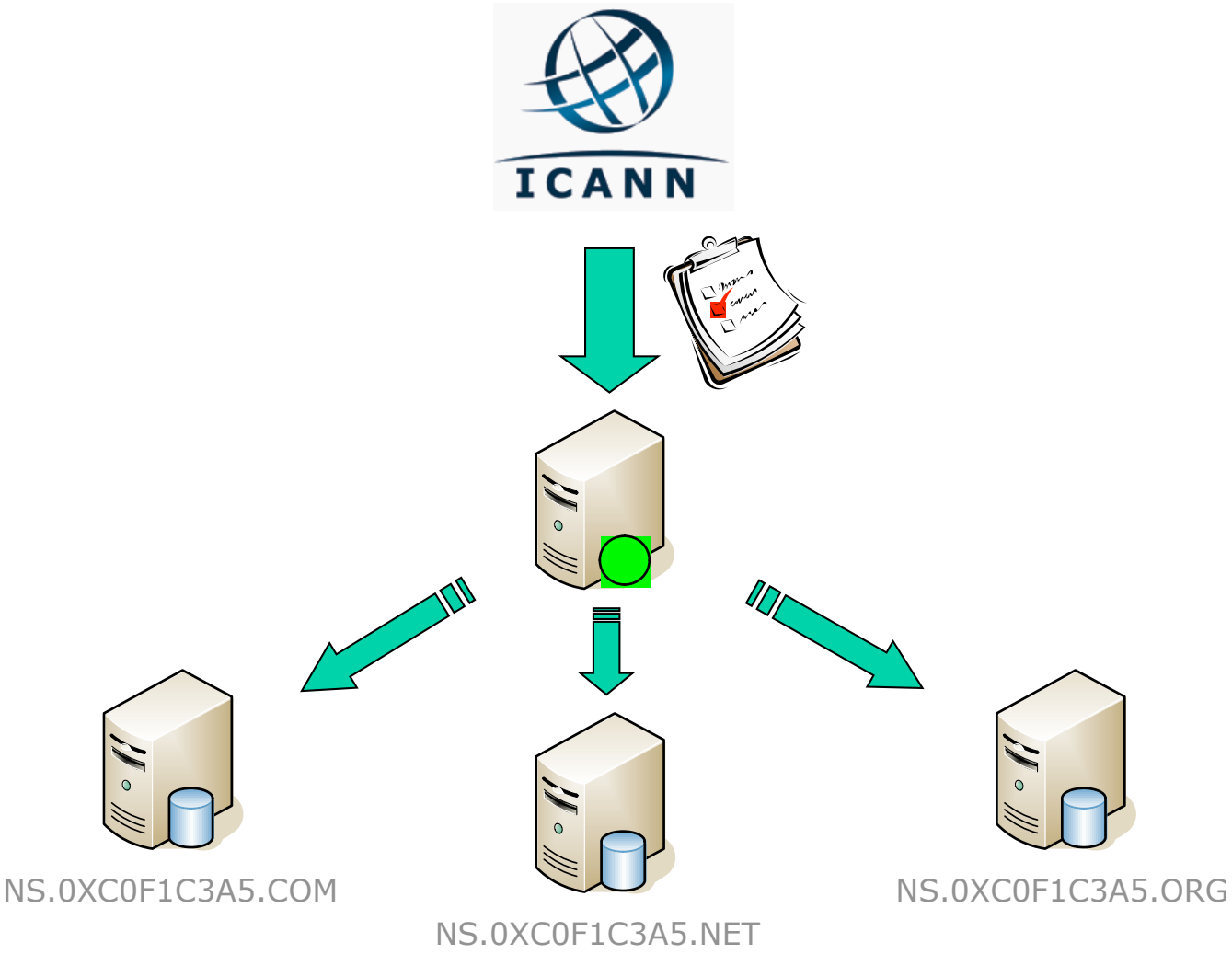
Nombres de dominio aleatorios


Contactar servidor web y extraer hora UTC
Inicializar GPAN con UTC
RandVal()
Elegir longitud nombre de dominio aleatoria (n)
n * RandVal()
Crear caracter aleatorio en minúscula
M veces
RandVal()
Añadir un TLD aleatorio

HTTP://$IP_DEL_DOMINIO/SEARCH?Q=$CONTADOR

	Conficker A	Conficker B/ C	Conficker D
Dominios por día	250	250	50000
Longitud nombre	8-11	8-11	4-9
TLDs afectados	5	8	110

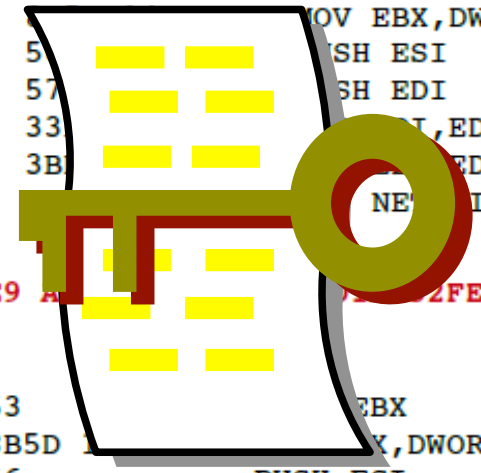
ac, ae, ag, ai, am, ar, as, at, be, bo, br,
bs, bz, ca, cd, ch, cl, cn, co, cr, cx, cz,
dj, dk, dm, do, ec, es, fj, fm, fr, gd, gh,
gl, gr, gs, gt, gy, hk, hn, ht, hu, id, ie, il,
im, in, ir, is, jm, ke, ki, kn, kr, kz, la, lc,
li, lu, lv, ly, md, me, mn, ms, mt, mu,
mw, mx, my, nf, ng, ni, nl, no, nz, pa,
pe, pk, pl, pr, ps, pt, py, ro, ru, sc, sg,
sh, sk, su, sv, tc, tj, tl, tn, to, tr, tt, tw,
ua, ug, uk, us, uy, vc, ve, vi, vn, za


ICANN
NS.0XC0F1C3A5.COM
NS.0XC0F1C3A5.NET
NS.0XC0F1C3A5.ORG

```
5B86A259   8BFF          MOV EDI,EDI
5B86A25B   55            PUSH EBP
5B86A25C   8BEC          MOV EBP,ESP
5B86A25E   53            PUSH EBX
5B86A25F                 OV EBX,DWORD PTR SS:[EBP+14]
5B86A262   5             SH ESI
5B86A263   57            SH EDI
5B86A264   33              ,EDI
5B86A266   3B              DI
5B86A268                   I32.5B8780FC

5B86A259 E9 A              2FE


5B86A25E 53                BX
5B86A25F 8B5D              ,DWORD PTR SS:[EBP+14]
5B86A262 56              PUSH ESI
5B86A263 57              PUSH EDI
5B86A264 33FF            XOR EDI,EDI
5B86A266 3BDF            CMP EBX,EDI
5B86A268 0F85 8EDE0000   JNZ NETAPI32.5B8780FC
```



Conficker Cabal

Microsoft

shadowserver

symantec

Support Intelligence

AOL

ISC

F-SECURE

.org

VeriSign

ICANN

NEUSTAR

CNNIC
中国互联网络信息中心
China Internet Network Information Center

WebSite.ws
your internet address for life.

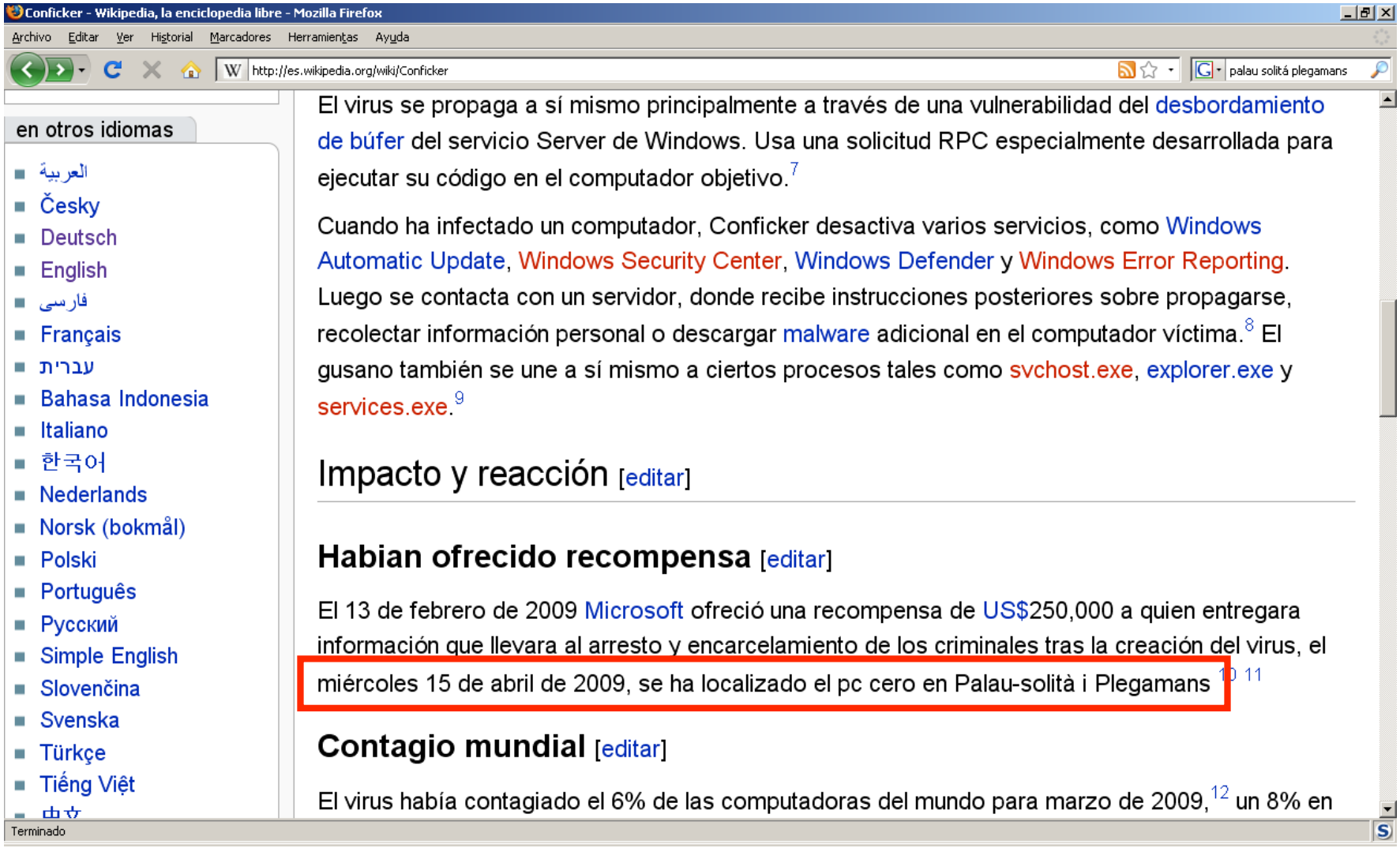
Afilias

M1D Global

ARBOR NETWORKS

```
Domain ID:  D155329089-LROR
Domain Name:  PWULRROG.ORG
Created On:  10-Feb-2009 23:  47:  07 UTC
Last Updated On:  12-Apr-2009 03:  56:  15 UTC
Expiration Date:  10-Feb-2010 23:  47:  07 UTC
Sponsoring Registrar:  PIR Special Projects (R1776-LROR)
Status:  OK
Registrant ID:  Special-001
Registrant Name:  Conficker Cabal
Registrant Organization:  Microsoft
Registrant Street1:  One Microsoft Way
Registrant Street2:
Registrant Street3:
Registrant City:  Redmond
Registrant State/Province:  WA
Registrant Postal Code:  98052
Registrant Country:  US
Registrant Phone:  +1.2023243000
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:  cflicker@live.com
```


REWARD
250.000 $$$



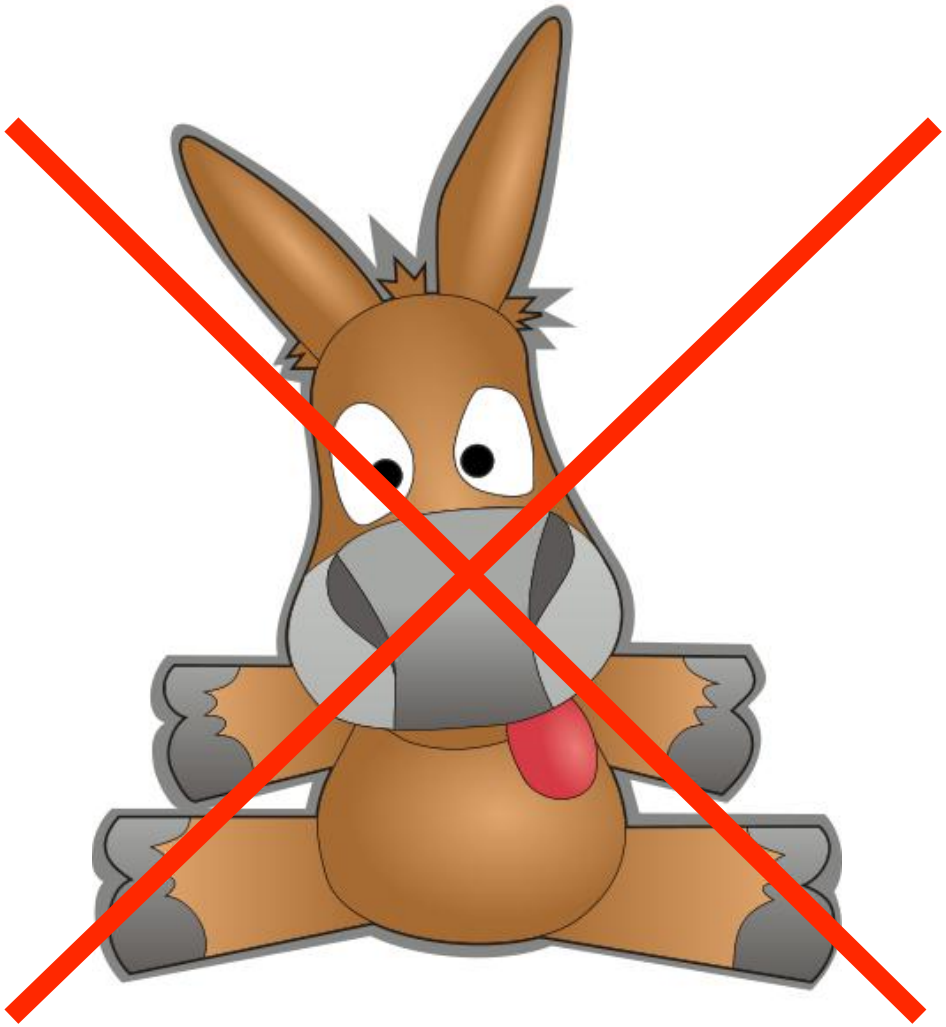
http://es.wikipedia.org/w/index.php?title=Conficker&oldid=25738704

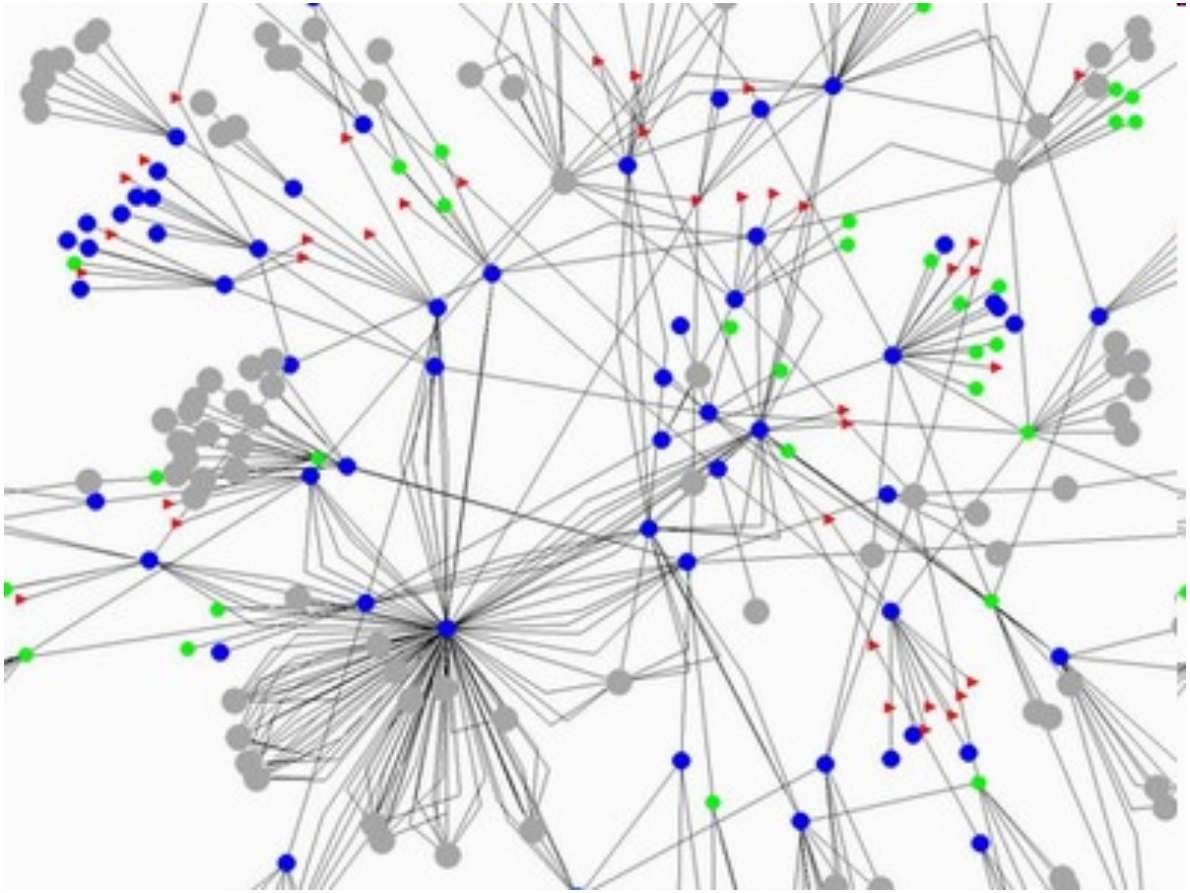
"[…] *probably the Downadup G will affect all TLDs, instead of only 116, and will generate a list of 500,000 random domains a day, instead of only 50,000*."

Marcos Sanz a la lista de correo "CENTR Technical WG", 15/3/2009

#5

Peer to peer

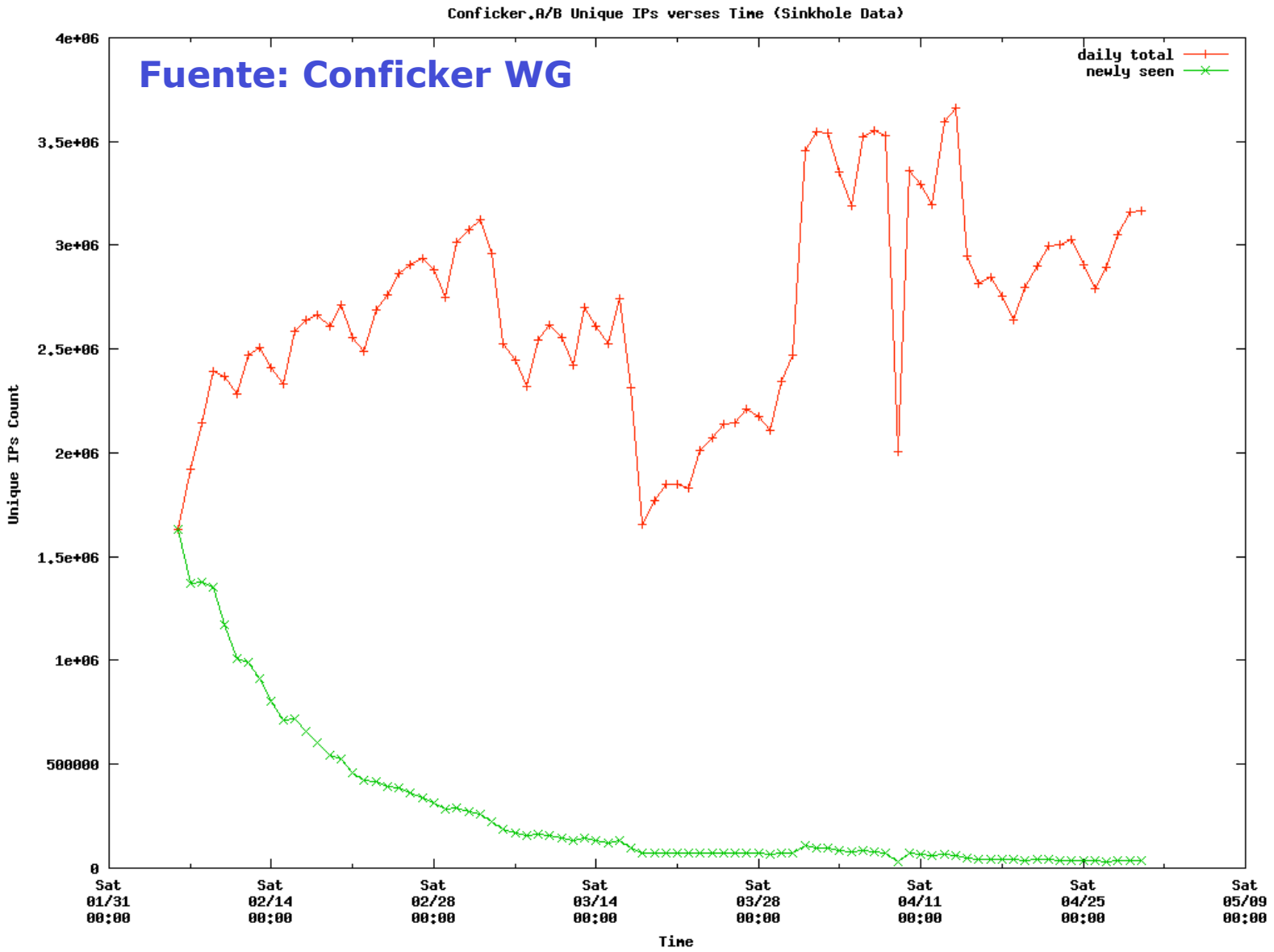


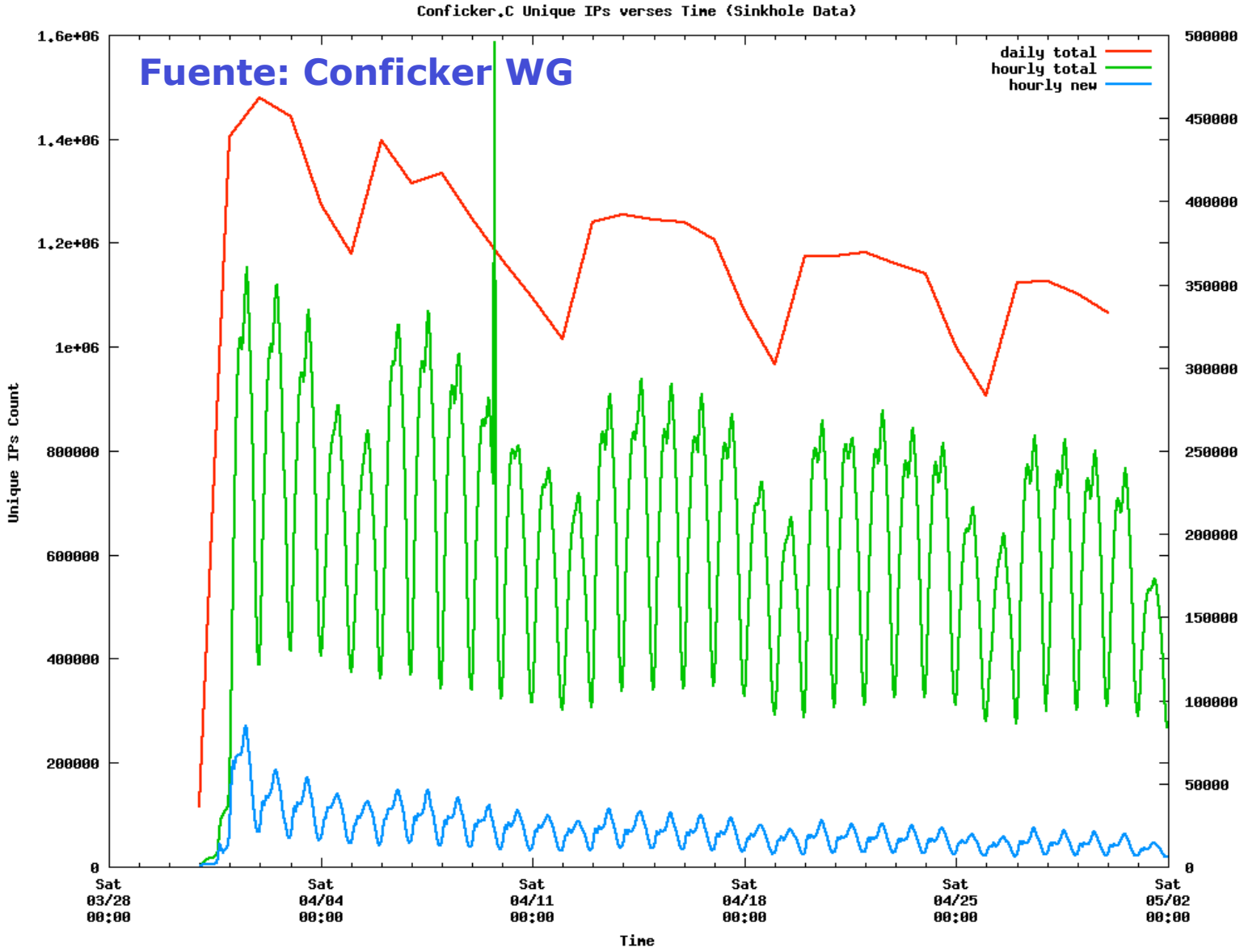


¿Cuántos son?

Fuente: F-Secure

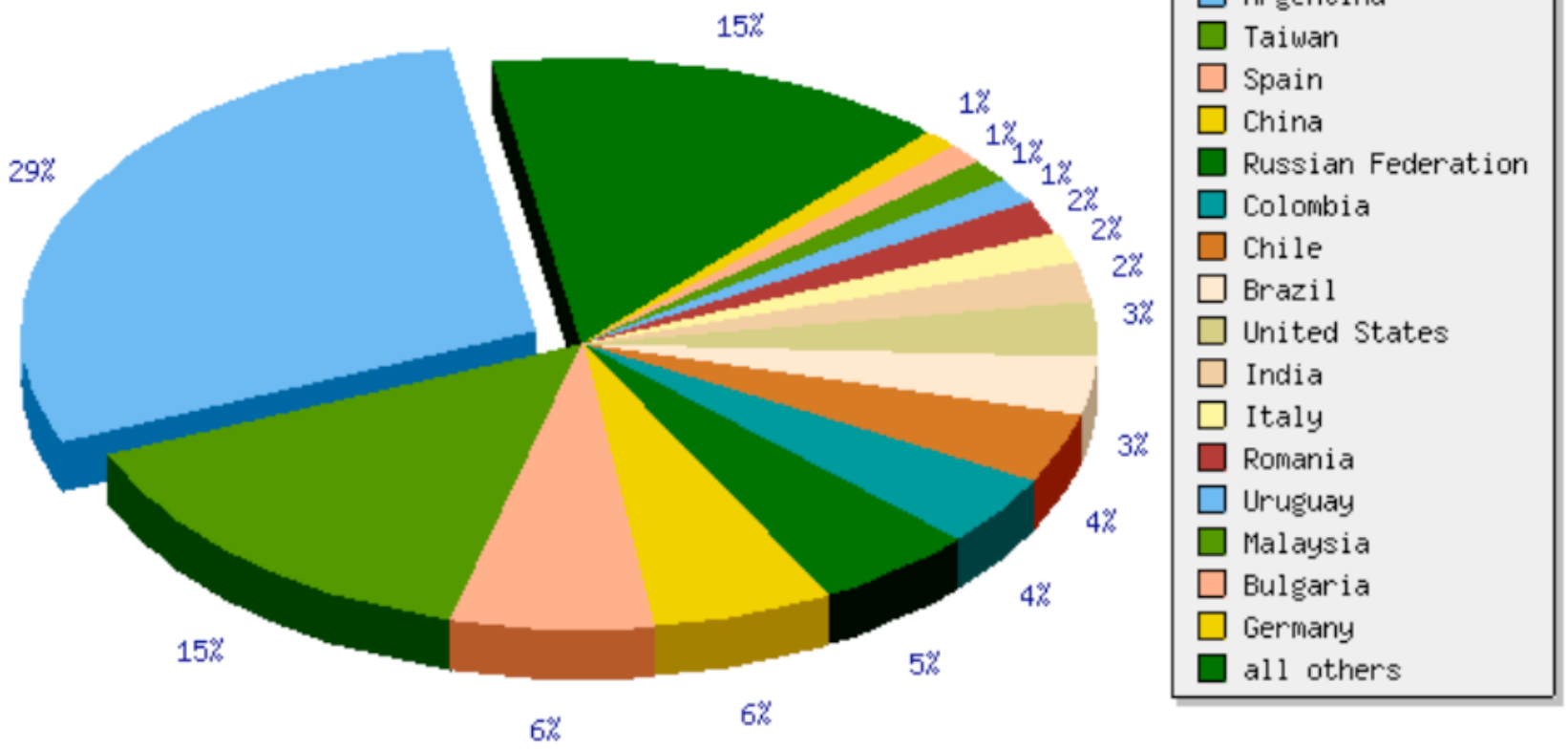

```
188.223.102  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=0 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)"
5.77.236  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=8 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; .NET CLR
23.52.82  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=12 HTTP/1.1" "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.
5.194.11  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=29 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)"
87.190.140  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=0 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
236.5.231  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=116 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)"
22.209.247  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=1 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)"
42.135.216  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=0 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1)"
18.189.245  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=0 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; FunWebProducts)"
7.89.146  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=3 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
176.105.47  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=0 HTTP/1.1" "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)"
46.131.10  - [15/Jan/2009:18:16:05 +0000] "GET /search?q=25 HTTP/1.0" "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
```


Conficker.A/B Unique IPs verses Time (Sinkhole Data)
Fuente: Conficker WG
daily total
newly seen
Unique IPs Count
4e+06
3.5e+06
3e+06
2.5e+06
2e+06
1.5e+06
1e+06
500000
0
Sat 01/31 00:00
Sat 02/14 00:00
Sat 02/28 00:00
Sat 03/14 00:00
Sat 03/28 00:00
Sat 04/11 00:00
Sat 04/25 00:00
Sat 05/09 00:00
Time


Conficker.C Unique IPs verses Time (Sinkhole Data)
Fuente: Conficker WG
daily total
hourly total
hourly new
Unique IPs Count
1.6e+06
1.4e+06
1.2e+06
1e+06
800000
600000
400000
200000
0
500000
450000
400000
350000
300000
250000
200000
150000
100000
50000
0
Sat 03/28 00:00
Sat 04/04 00:00
Sat 04/11 00:00
Sat 04/18 00:00
Sat 04/25 00:00
Sat 05/02 00:00
Time

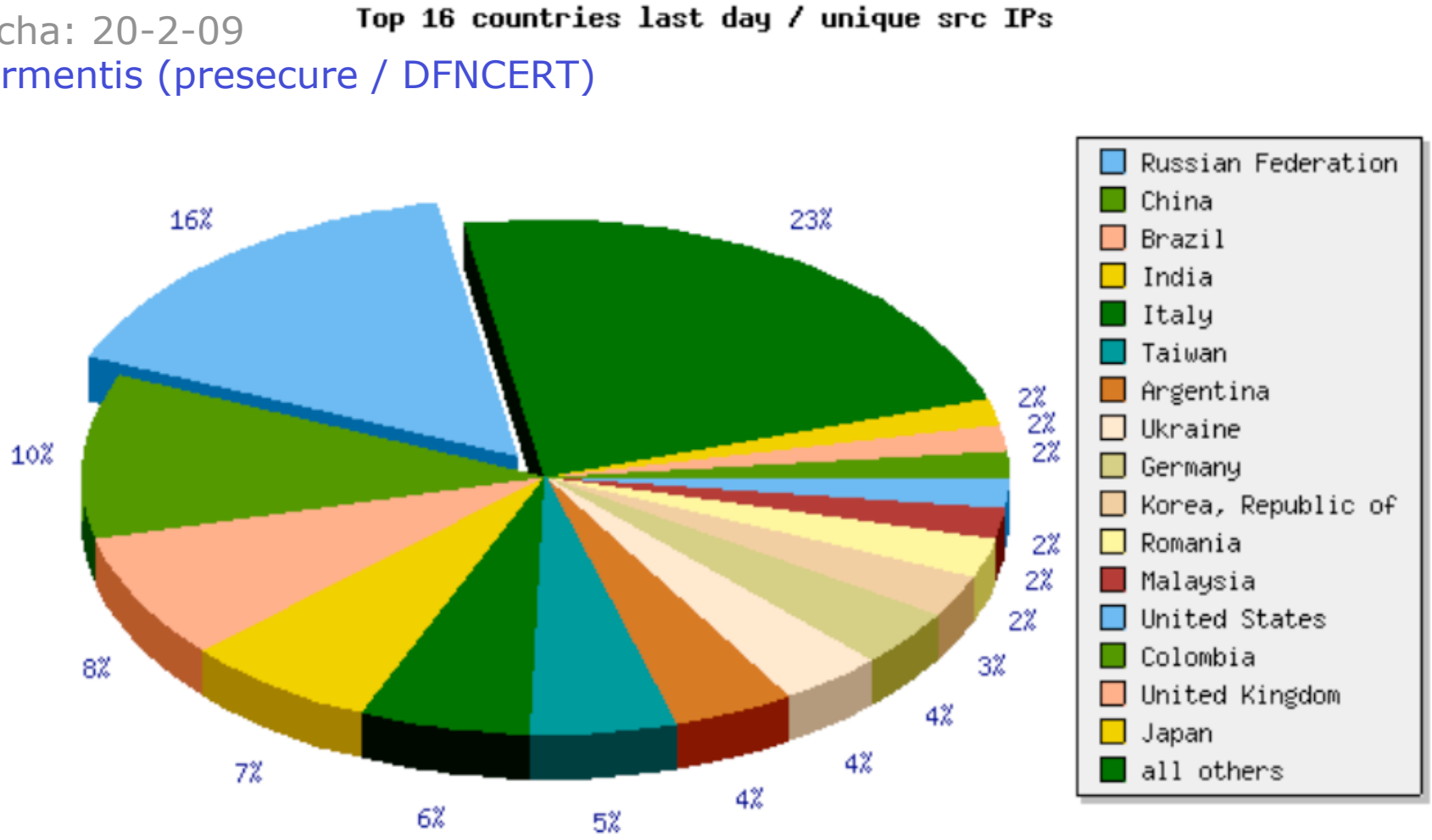
Fecha: 21-11-08

Carmentis (presecure / DFNCERT)



Fecha: 20-2-09

Carmentis (presecure / DFNCERT)



Conficker Research Project
CERT.AT/ZID Universidad Viena

Contar

Geolocalizar

Autonotificar

¿Para qué?


Spyware Protect 2009
Protecting every second...
Perform scan
Adjust settings
Get updates
Activate now
Help & support
Performing scan
Start scan
Current state: Scan complete
Warning
There are serious threats detected on your computer. Your privacy and personal data may not be safe. Do you want to Clean and Protect your PC?
Yes, remove threats
No, continue unprotected
LdPinch V
Critical
A variant of the Key Logger that captures passwords as t
Advanced Stealth Email
Critical
Advanced Stealth Email Redirector (Advanced SER) is a pr
VMalum AWS
High
Trojan: Any program with a hidden intent. Trojans are one
CNNIC Update U
Very high
A program that downloads and may execute or install soft
Bancos DMD
Critical
A variant of the Key Logger that captures passwords as t
Scan progress
100% completed
Your PC is currently unprotected and may be exposed to spyware adware, trojans and viruses
Get full real-time protection

100% Satisfaction Guarantee !

We guarantee that Spyware Protect 2009 (c) subscriptions will make your computer more secure or your money back. If for any reason you are not 100% satisfied, just let us know within 30 days of purchase and get a full refund. Just send an email to us. That's risk-free protection. Never get caught without the latest defense

Why Choose Spyware Protect 2009 ?

Proactive security for what you value most Unparalleled protection by blending the most sophisticated security technologies available Spyware Protect 2009 (c) service automatically and continually upgrades software and updates threat protection.

Maximum Support Guarantee !

Fast support will help you with any troubles and will answer your questions within 24h. We work 24/7 for You.

Qty.	Item	Delivery	Support and Updates	Price
1	Spyware Protect	Online download	Lifetime	USD 49.95

☑ Yes, I have read and agreed to the following Terms and Conditions

NOTE: **Download and install full version after purchase.**

CONTINUE TO SECURE ORDER PAGE

VISA MasterCard We accept Visa and MasterCard credit or debit cards. Your order will be entered using a secure server witch SSL certificate and data encryption.

¿Y ahora?

Propuesta CERT.AT

"I say we take off and nuke the entire site from orbit. It's the only way to be sure."

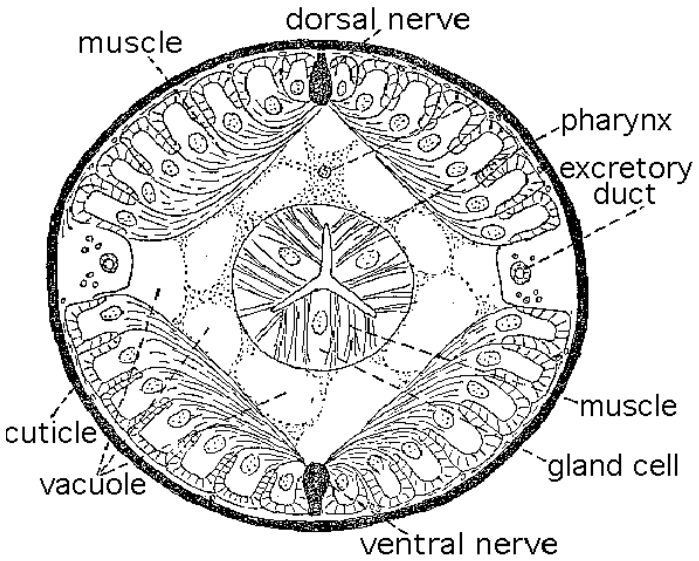
- Nuevas actualizaciones a través de las listas de nombres de dominio
- Atacante inyectará nuevo software a través de la red P2P
- Contenido: *nada bueno*

Referencias

- SRI International, http://mtc.sri.com/Conficker/
- Microsoft, http://microsoft.com/conficker
- Symantec Security Response Blog, https://forums2.symantec.com/t5/blogs/blogpage/blog-id/malicious_code
- Honeynet Project, http://www.honeynet.org/files/KYE-Conficker.pdf
- CAIDA, http://www.caida.org/research/security/ms08-067/conficker.xml
- esCERT, http://escert.upc.edu/index.php/web/es/publicacion,584,1.html
- Conficker Working Group, http://www.confickerworkinggroup.org/

Gracias especiales a:

A. Kaplan y todo el CERT.AT
Wikipedia Commons
CENTR



sanz@denic.de