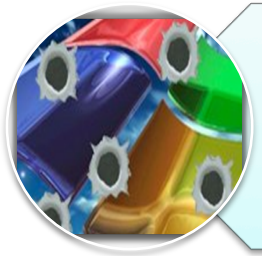
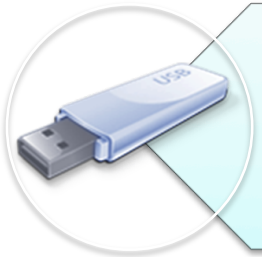

F-SECURE®
Case
Conficker
Black Hat 2009
Las Vegas
Mikko Hypponen
Chief Research Officer
F-Secure Corp

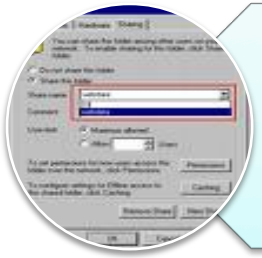
Conficker / Downadup spreading vectors



MS08-067
Vulnerability in Server service

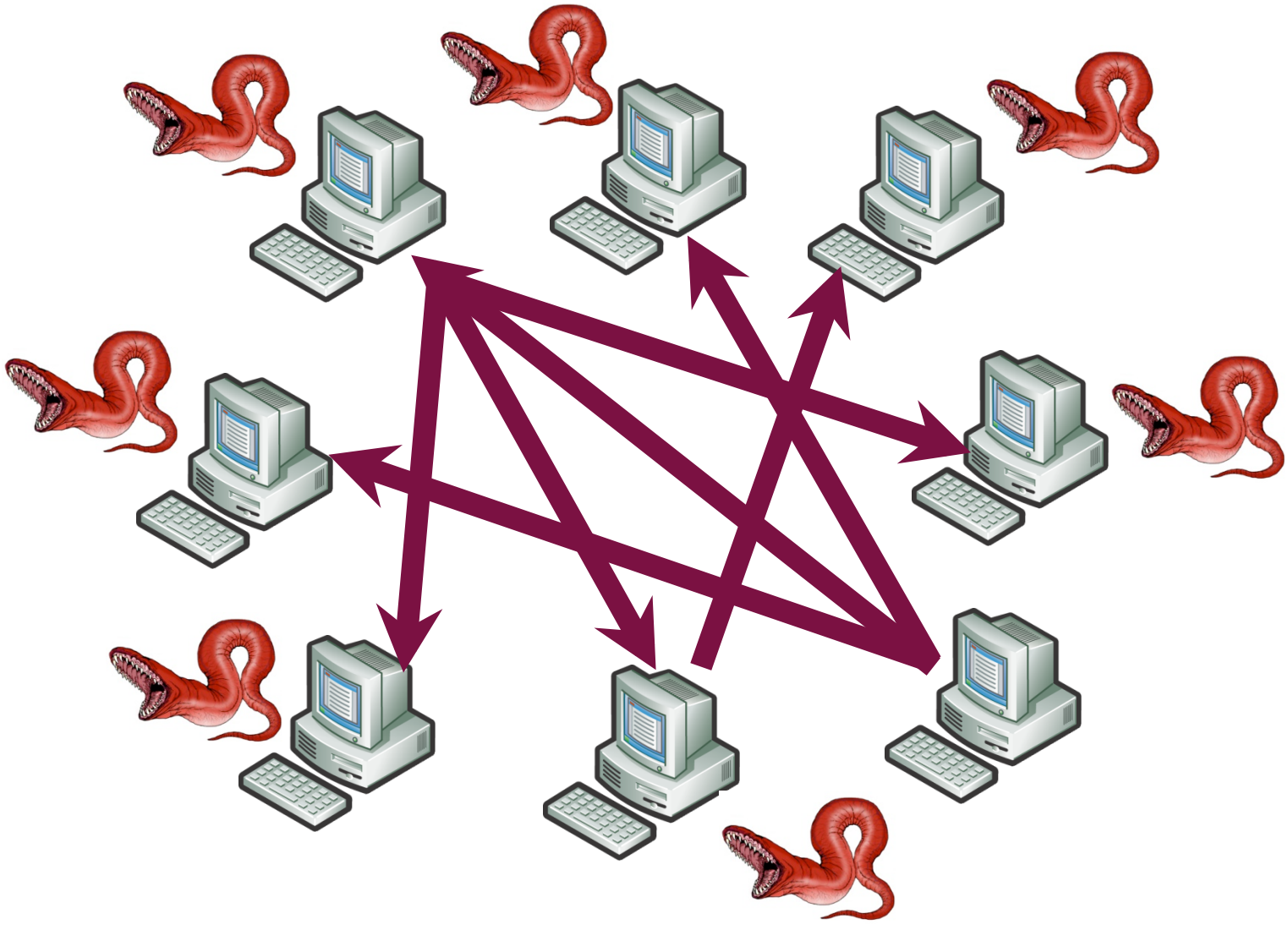


USB-Flash drives
Autorun & Autoplay



ADMIN$ shares

F-SECURE®



abc123

academia

access

account

Admin

admin

admin1

admin12

admin123

adminadmin

administrator

anything

asddsa

asdfgh

IP range : 91.199.104.0 - 91.199.104.255
Network name : BITDEFENDER

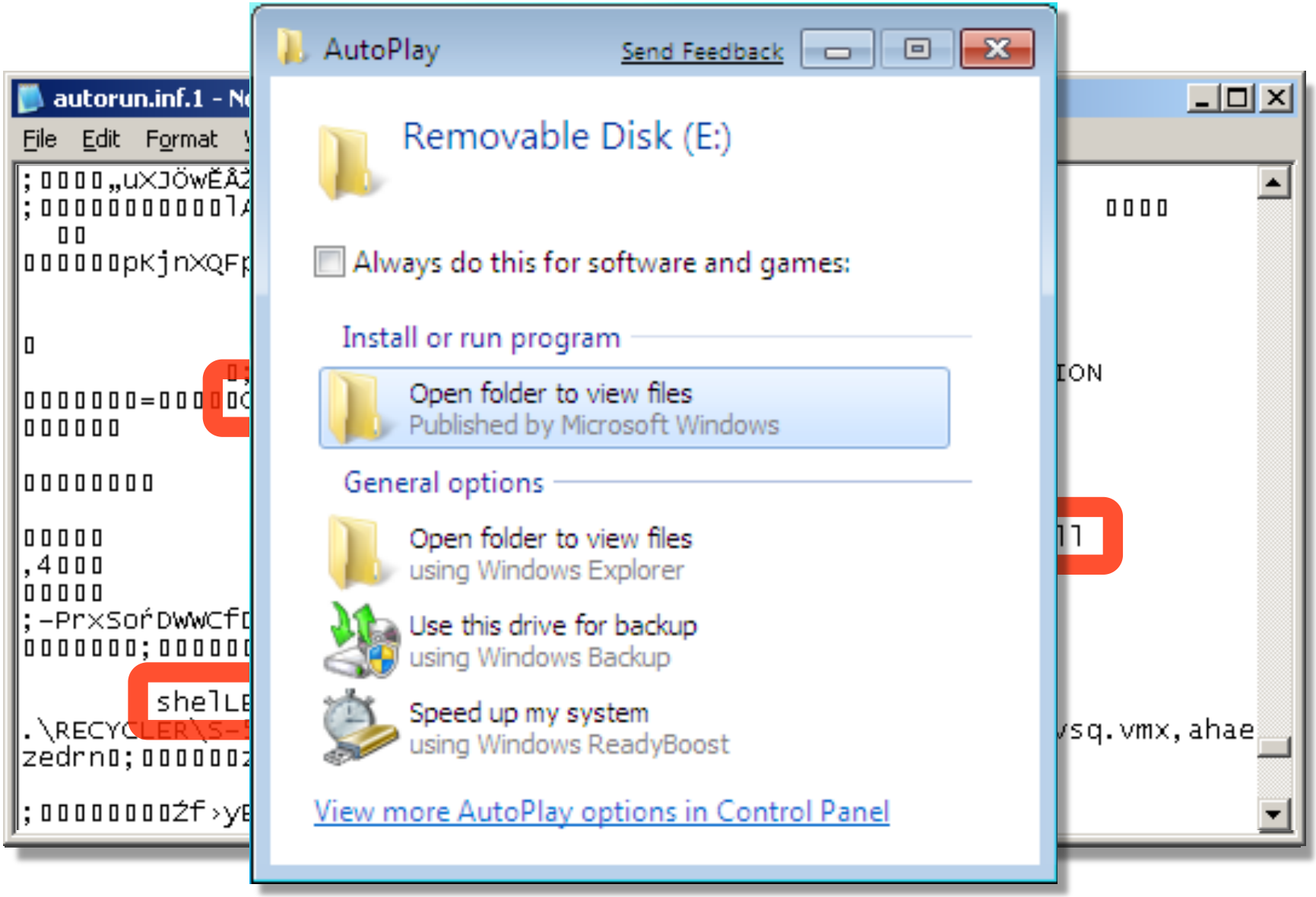
IP range : 192.88.209.0 - 192.88.209.255
Network name : CERT-NET
Abuse E-mail : cert@cert.org

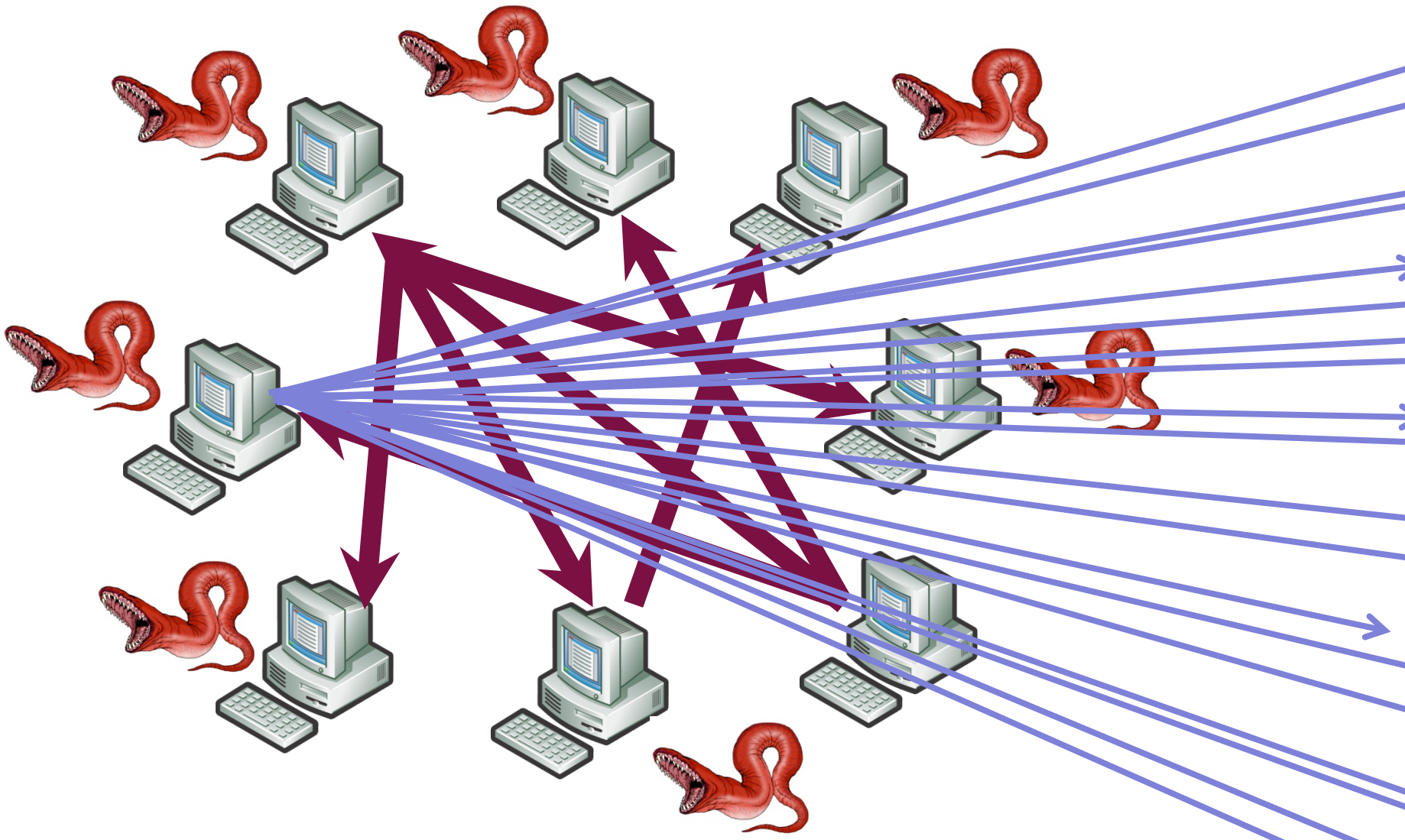
IP range : 207.242.88.0 - 207.242.88.255
Infos : COMPUTER ASSOCIATES

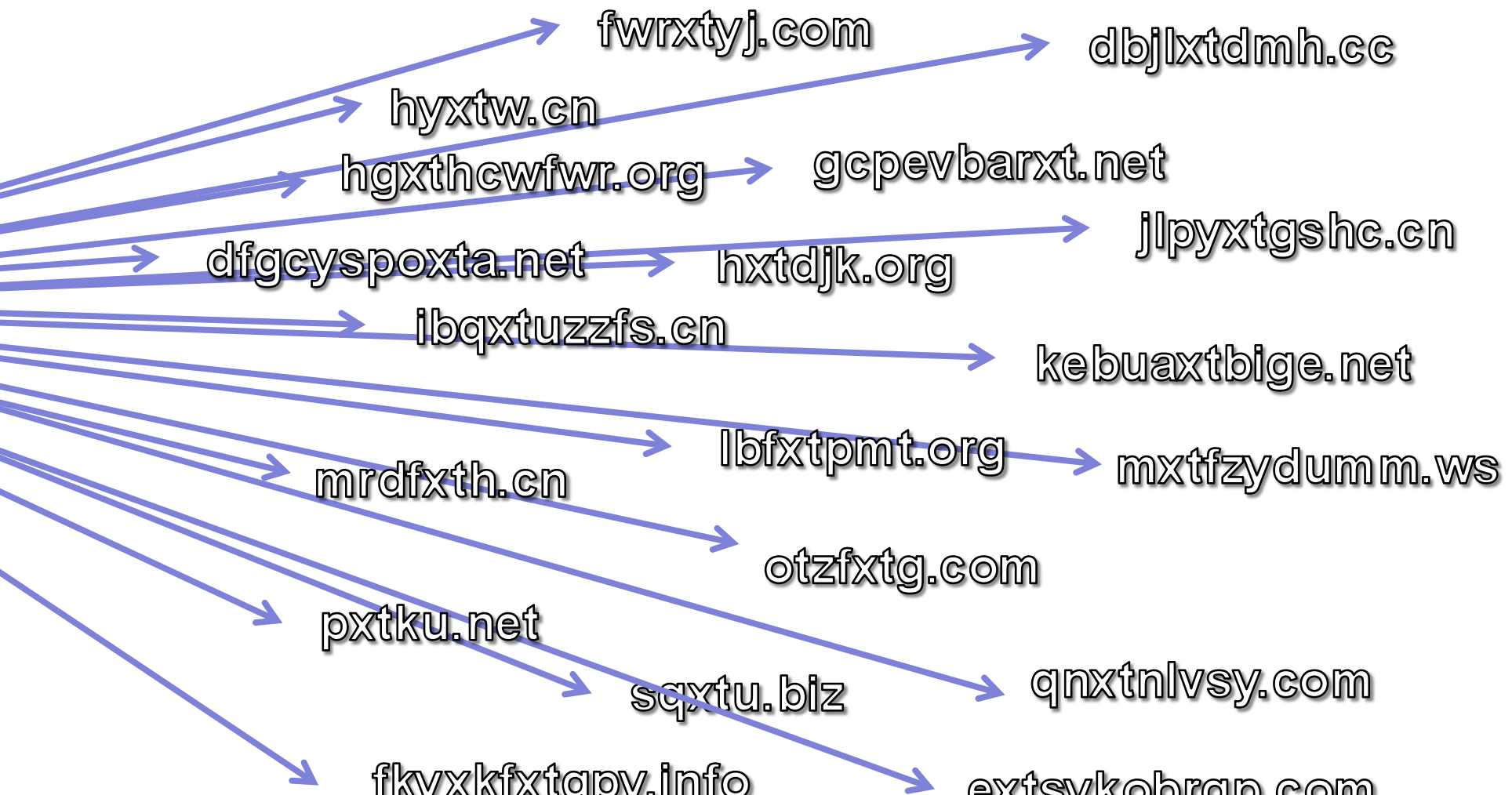
IP range : 72.32.7.88 - 72.32.7.95
Infos : ESET LLC
Infos : 1172 Orange Ave

IP range : 204.118.23.96 - 204.118.23.127
Infos : FRISK Software International

IP range : 65.200.212.0 - 65.200.212.255
Infos : F-Secure Inc.
Infos : 100 Century Center Court
Infos : Suite 700
Infos : San Jose
Infos : CA
Infos : 95112


autorun.inf.1 - No
File Edit Format
AutoPlay
Send Feedback
Removable Disk (E:)
Always do this for software and games:
Install or run program
Open folder to view files
Published by Microsoft Windows
General options
Open folder to view files
using Windows Explorer
Use this drive for backup
using Windows Backup
Speed up my system
using Windows ReadyBoost
View more AutoPlay options in Control Panel




fwrxtyj.com
dbjlxtdmh.cc
hyxtw.cn
hgxthcwfwr.org
gcpevbarxt.net
jlpyxtgshc.cn
dfgcyspoxta.net
hxtdjk.org
ibqxtuzzfs.cn
kebuaxtbige.net
lbfxtpmt.org
mxtfzydumm.ws
mrdfxth.cn
otzfxtg.com
pxtku.net
qnxtnlvsy.com
sqxtu.biz
fkyxkfxtgpy.info
extsykobrqp.com

8,976,038


F-SECURE®
Conficker.C

Confick... | Antiviru... | F-Secur... | F-Secur... | F-Secur... | F-Secur... | F-Secur...

http://www.confickerworkinggroup.org/wiki/

CONFICKER WORKING GROUP

Search Go

Big View Text Size – 0 +

- Home
- Edit
- History
- Recent Changes

- **HomePage**
- Calendar
- Public Relations
- Press Releases

Assistance

- Enterprise
- Service Providers
- TLD Operators
- Network Detection

Information

- FAQ
- Infection Distribution
- Infection Tracking
- Malicious Sites
- Repair Tools
- **Check for Infection**

- Contact us

edit SideBar

Home Page

« January 2009 · July 2009 »

Calendar:

- No entries for May 2009.
- 01.04.2009: Conficker.C is Live and well
- 29.03.2009: Conficker Working Group Web is Prepared

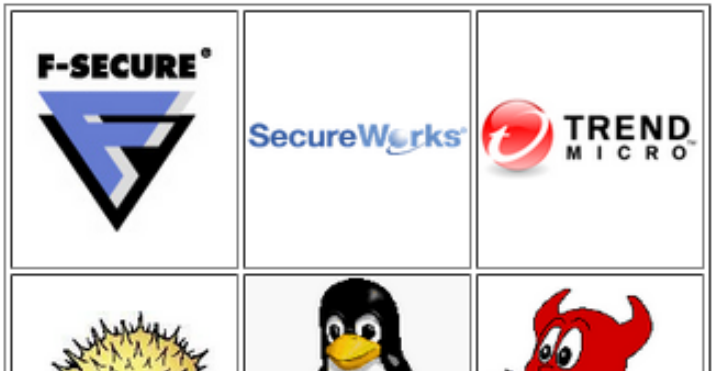
Newest first Oldest first

Check to see if you are infected

Thanks to Joe Stewart from SecureWorks for his awesome work.

Check for Infection

On this page... (hide)



Working Group Members

Afilias
AOL
Arbor
Cisco
ESET
F-Secure
Facebook
Global Domains International
ICANN
Internet Storm Center
Internet Systems Consortium
Juniper
Kaspersky
McAfee
Microsoft
Neustar
NIC Chile
SecureWorks
Shadowserver
SRI International
Support Intelligence
Symantec
Team Cymru
Trend Micro
Verisign

Calendar/Blog

February 2009
29 · March 2009
01 · April 2009
May 2009

fwrxtyj.com

dbjlxtdmh.cc

hyxtw.cn

hgxthcwfwr.org

gcpevbarxt.net

jlpyxtgshc.cn

dfgcyspoxta.net

hxtdjk.org

ibqxtuzzfs.cn

kebuaxtbige.net

lbfxtpmt.org

mrdfxth.cn

mxtfzydumm.ws

otzfxtg.com

pxtku.net

sqxtu.biz

qnxtnlvsy.com

fkyxkfxtgpy.info

extsykobrqp.com

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

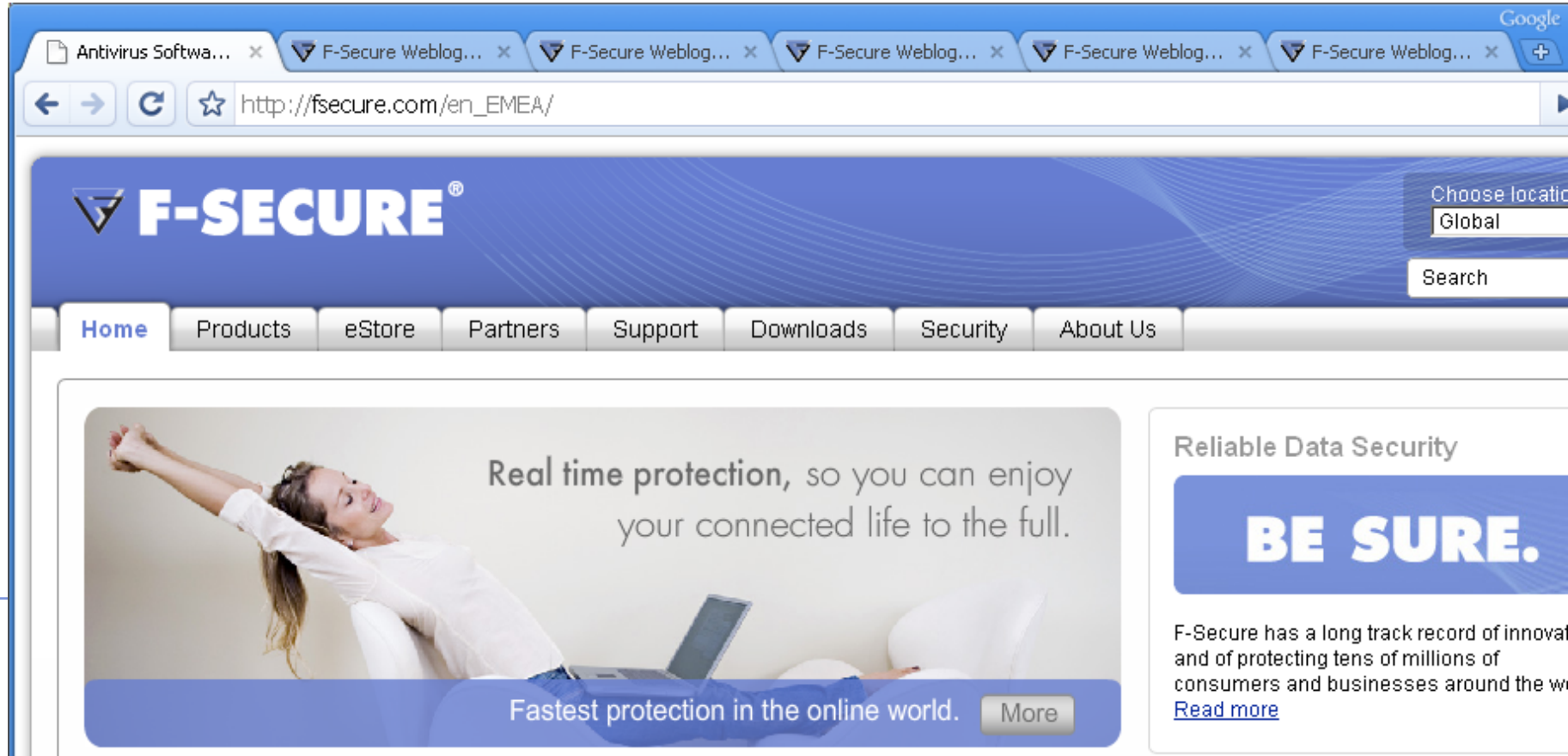
.sc .sg .sh .sk .su .tc .tj .tl .tn .to .tw .us .vc .vn

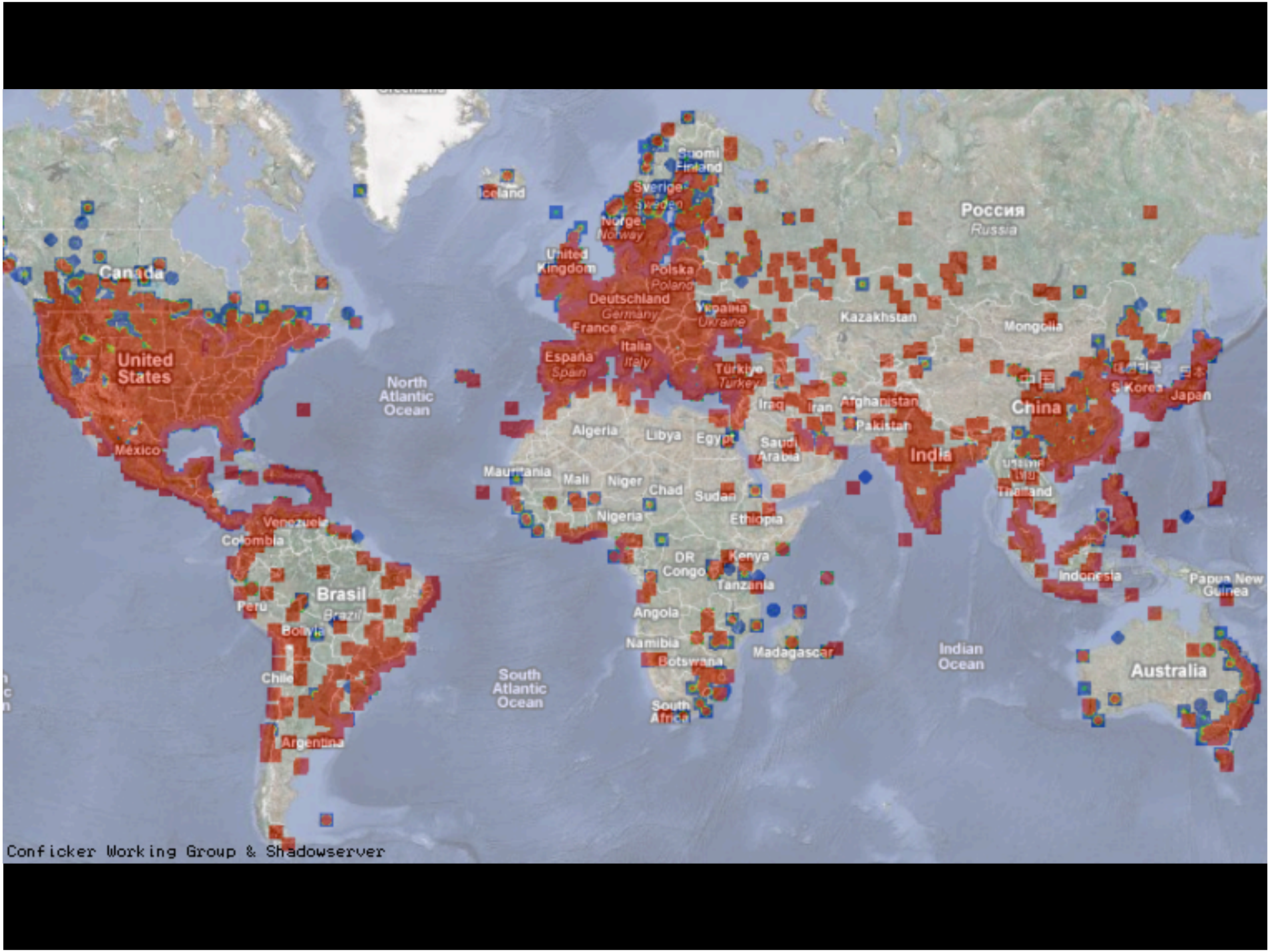
The bad boys keep watching us

Conficker.C blocked access to domains containing "**f-secure**"

So we created **fsecure.com** in addition of **f-secure.com**

Conficker.E blocks both **f-secure** and **fsecure**




Canada
United States
México
Россия
Russia
Kazakhstan
Mongolia
China
India
Japan
S. Korea
Indonesia
Papua New Guinea
Australia
Brasil
Brazil
Peru
Bolivia
Chile
Argentina
Colombia
Venezuela
Iceland
Suomi Finland
Sverige
Norge Norway
United Kingdom
Polska Poland
Deutschland Germany
France
España Spain
Italia Italy
Türkiye Turkey
Ukraina Ukraine
Algeria
Libya
Egypt
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Saudi Arabia
Iraq
Iran
Afghanistan
Pakistan
DR Congo
Kenya
Tanzania
Angola
Namibia
Botswana
South Africa
Madagascar
North Atlantic Ocean
South Atlantic Ocean
Indian Ocean
Conficker Working Group & Shadowserver


Why?


F-SECURE®
Case
Conficker
Black Hat 2009
Las Vegas
Mikko Hypponen
Chief Research Officer
F-Secure Corp