

SantaCare Managed WebSecurity Palvelu turvallista Web-liikennettä varten

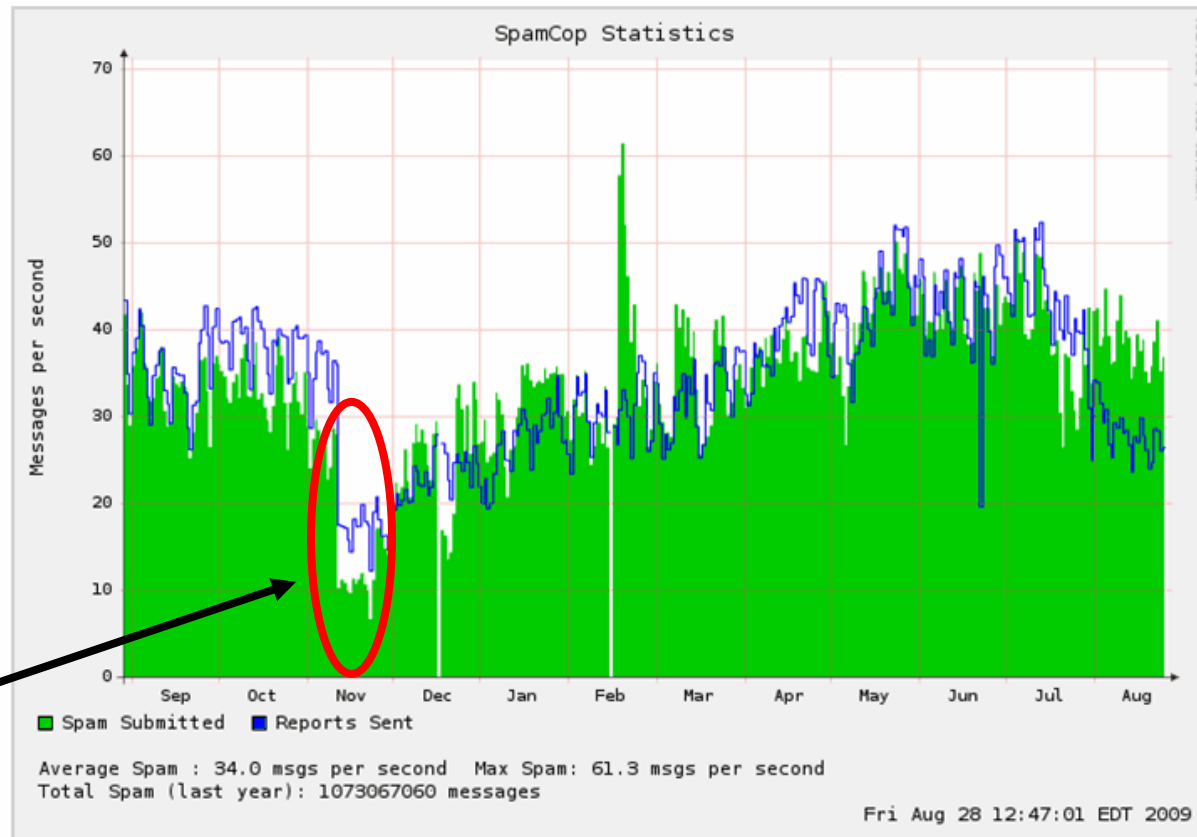
***Mikko Tammiruusu
Security Consultant***

**Cisco Expo
2009**

Tietoturvatapahtumia – SPAM:in kasvu

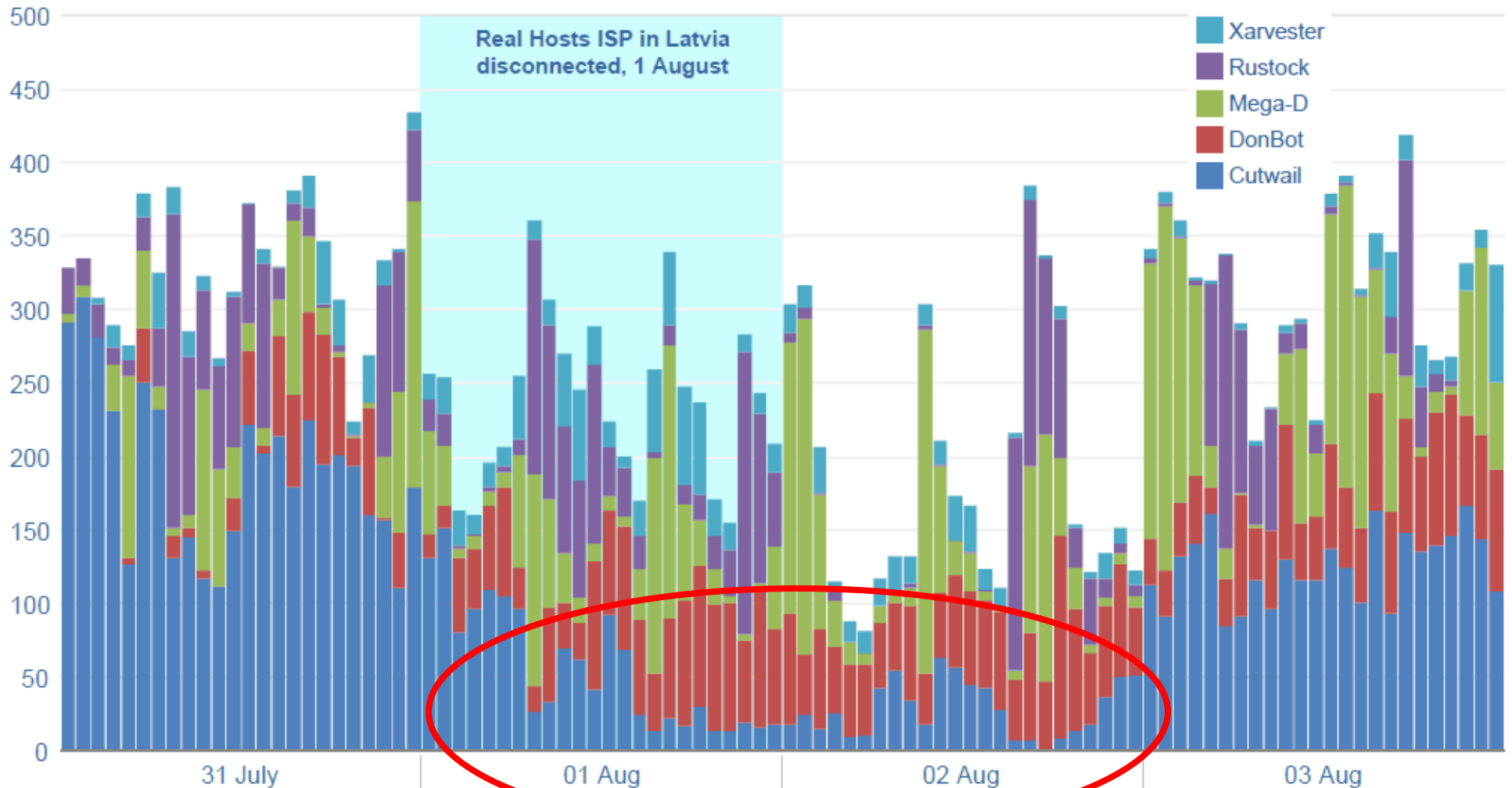
spamcop.net

Report Spam Filtered Email Blocking List Statistics Login



McColo

Tietoturvatapahtumia – Top-5 botnets



Tietoturvatapahtumia – Real Host ja Zeus



**WORLDWIDE CVV
&
BANK LOGINS**

CREDIT CARDS CVV2

- United States 1\$
- United States + DOB 5\$
- United Kingdom 4\$
- United Kingdom + DOB 15\$
- Europe 8\$
- Europe + DOB 15\$
- Asia 6\$

Bank logins

- Abbey Bank - 5%
- Lloyds pers.biz.offshore bank - 3%
- Hsbc , First direct - 3%
- Co-Operative - 5%
- Smile - 5%
- Egg bank - 6%
- Citibank Uk - 10%
- Egg Bank - 6%
- Cb/Yb-Online - 5%

Europe Bank Logins in Stock .

FULLZ

- UK FULLZ in stock , Capone and MBNA
- Online access + MMN+DOB+CVV+EXP+CC 5%

Payment Accept & Delivery

- Webmoney.com - Libertyreserve.com - PerfectMoney.com
- MoneyBookers.com - 10\$ min order,
- Western Union - Recieve in 1 min !!!

All stuffs delivery instant after payment by ICQ/Email/Upload.
I dont sell by 1 Card , if u need ask me i will give you some free.

UK PAYPAL

Without mail:
Unverified - 5\$
Verified - 10\$

With Mail:
Unverified - 12\$
Verified - 30\$

With Balances:
10% price of balance

Online Shop - WORK .

Inside you can find :

- 10 000 WorldWide CVV
- 500 Uk Bank Logins
- 80 Paypal Accounts
- Fullz UK
- Checker For CC+DUMPS.
- Registration in ICQ with 50\$ first dep.

USA DUMPS T2

- Classic - 15\$
- Gold/plat - 30\$
- World - 35\$
- Signature - 40\$

EU DUMPS T2

- Classic - 40\$

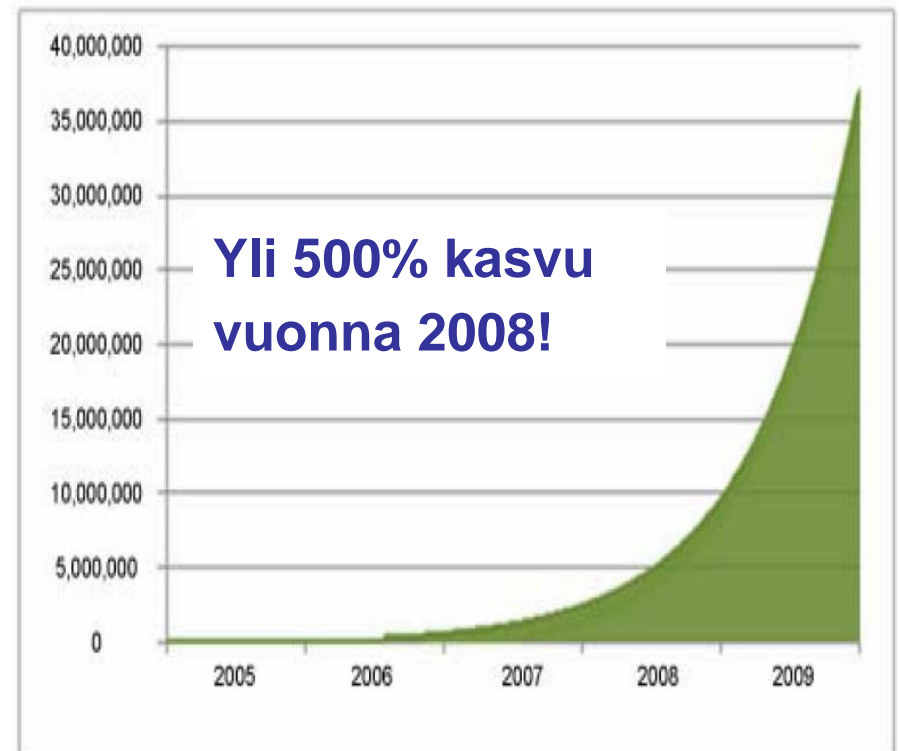
Only T2 / no d+p.

- Zeus Botnet – yksi maailman suurimmista botnet-verkoista
- Myy saastuneista koneista kerättyjä luottokortti-numeroita (0.50 USD), luottokorttien CVV/CVC-numeroita (1.0 USD), pankkien käyttäjätunnuksia yms yms
- Menetelmät ja tekniikat muistuttavat paljon RBN:n käyttämiä järjestelmiä.

Malware tänään

- Noin 90% webin kautta saaduista ongelmista on levinnyt tavallisten sivustojen ja linkkien kautta
 - Hyökkäykset ovat siirtyneet käyttämään HTTPS-liikennettä
 - >85% SPAM:stä sisältää URL:in
 - Selailun aikana tapahtuneet saastumiset jäävät usein huomaamatta
 - Pahimmat sivustot voivat sisältää yli 20000 erilaista uhkaa

Rikollisten hyökkäysten erittäin voimakas kasvu



Kaspersky Labs Nov 2008

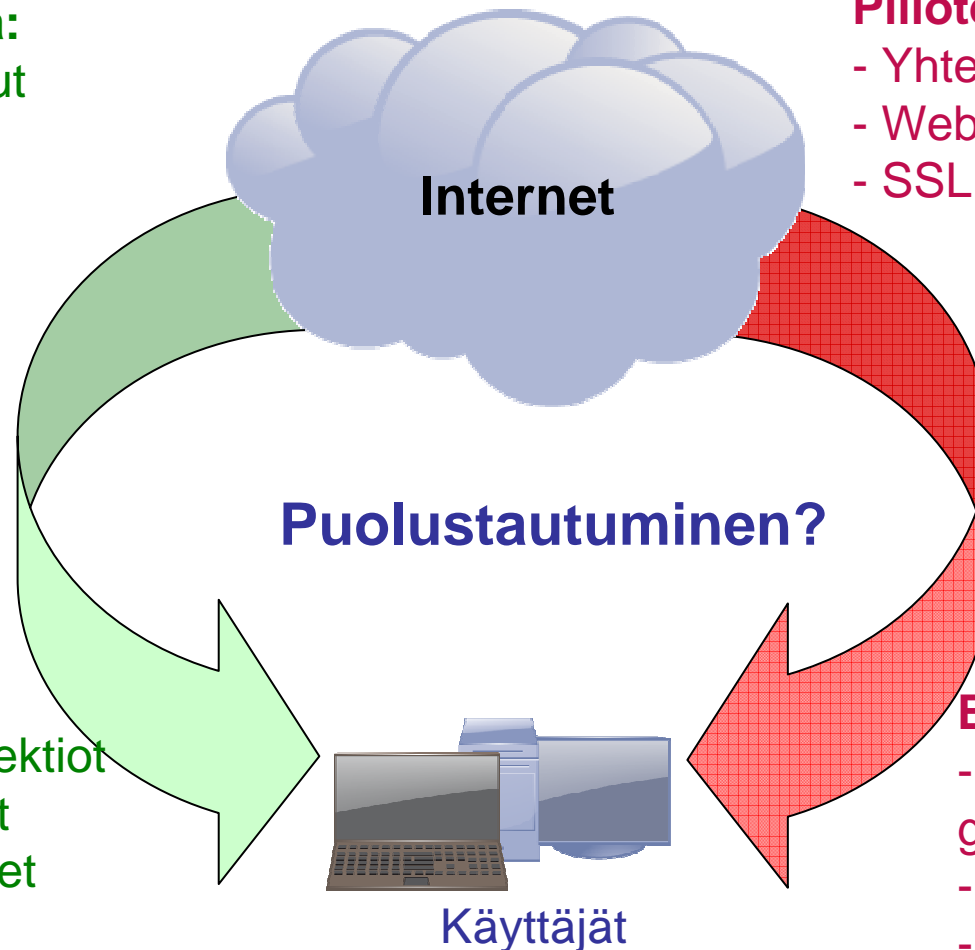
Malwaren välitysmenetelmät

Avoim menetelmä:

- Suositut web-sivut
- Ei salausta

Pilotettu menetelmä:

- Yhteistöverkostot
- Web Mail, P2P & IM
- SSL traffic



Esimerkkejä:

- iframe ja SQL injektiot
- XSS hyökkäykset
- DNS väärennykset
- Linkkihuijaukset
- Flash-parametrien väärennykset

Esimerkkejä:

- Facebook, MySpace, gmail, Twitter, Skype
- Tiedostolataukset
- Väärennetyt päivitykset

Tietoturvatapahtumia – Facebook Cooool Video



Facebook Scam ALERT: Don't Click "Cooool Video"

August 13th, 2009 | by Pete Cashmore

14 Comments

1084 tweets

retweet



post

If you receive a Facebook mail today with the subject line "Cooool Video", don't click the link. We're getting reports of a Facebook scam which causes infected users to unknowingly send out Facebook mails to their friends containing that subject line.

facebook

The links in the mails go to various places, including a blogspot blog (see screenshot below). Of course, clicking the link earns you an unpleasant dose of malware.

Facebook, to give credit where due, is becoming increasingly proficient at stomping out such scams: the last one to cause issues was around two months ago.

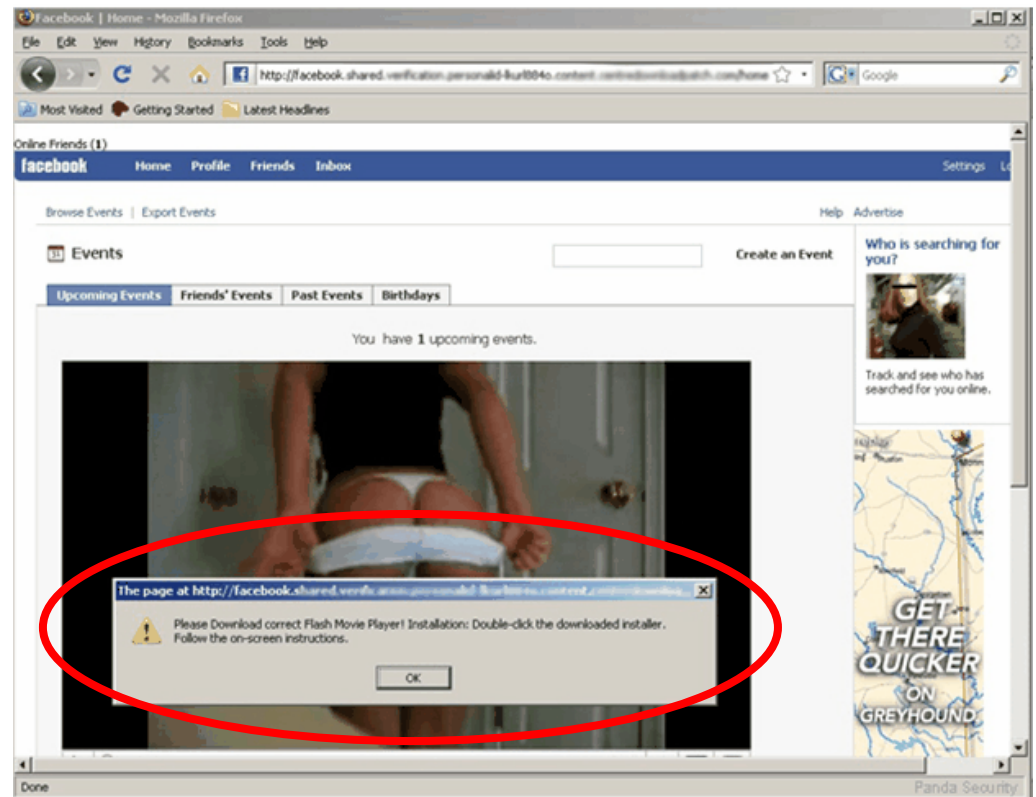
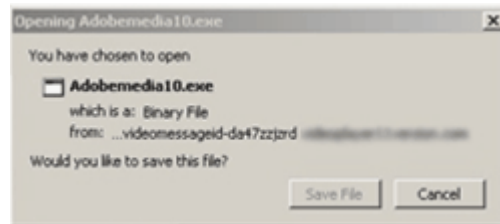
What To Do

Cooool Video

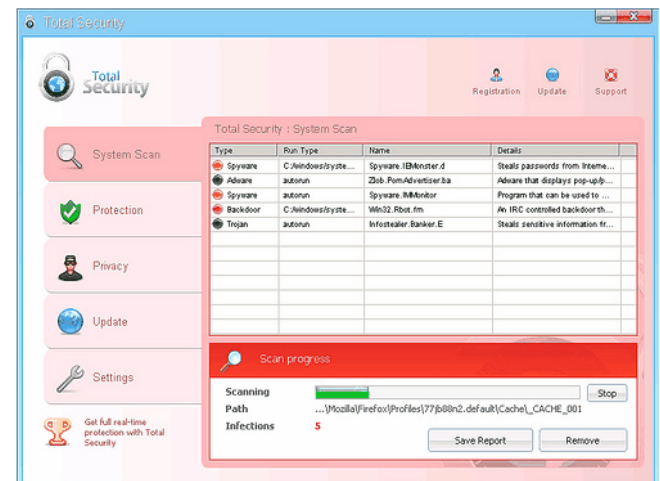
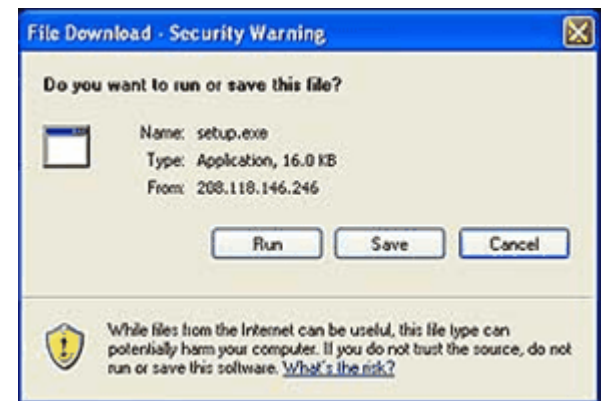
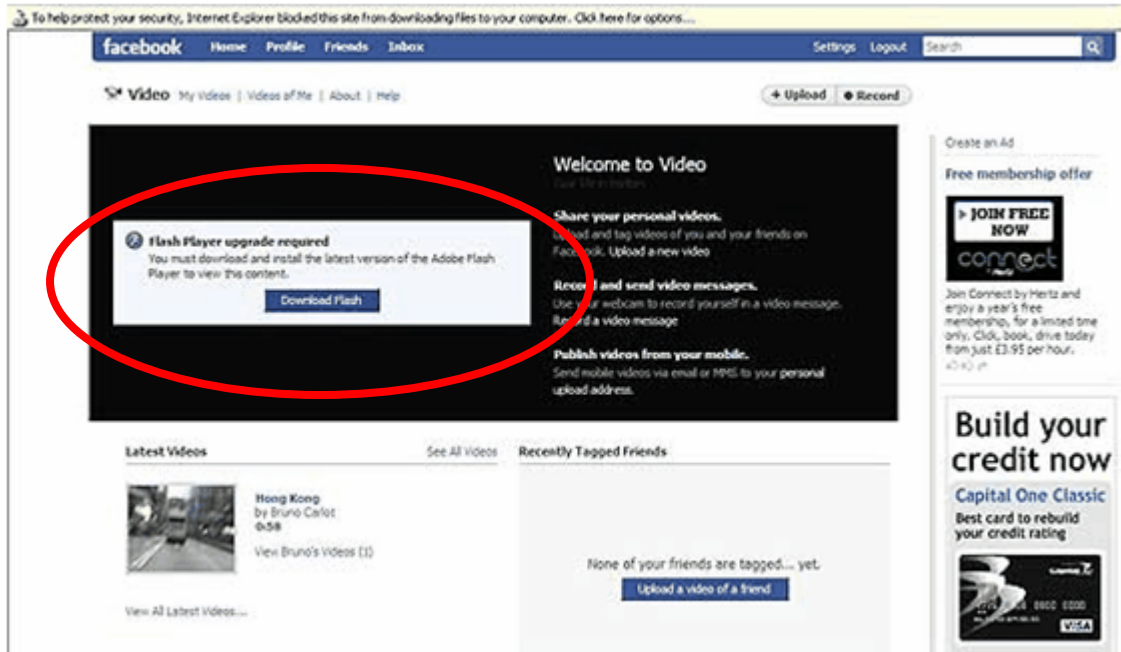
W.O.W: <http://epbsduhakpzsxjgp.blogspot.com/>

If you receive one of these Facebook mails, simply delete it – one of your friends is infected but not you. If you find, however, that your account is sending the mails:

1. As a precaution, go to your browser settings and clear your cookies.
2. Change your Facebook password
3. Make sure your antivirus software is up to date and run a full system scan



Tietoturvatapahtumia – Koobface worm (Facebook, Twitter, MySpace...)



Tietoturvatapahtumia – Koobface worm (Facebook, Twitter, MySpace...)

To help protect your security, Internet Explorer blocked this site from downloading files to your computer. [Click here for options...](#)

facebook Home Profile Friends Inbox Settings Logout Search

Video My videos | Videos of Me | About | Help Upload Record

Welcome to Video

Share your personal videos. Upload and tag videos of you and your friends on Facebook. Upload a new video

Record and send video messages. Use your webcam to record yourself in a video message. Record a video message

Publish videos from your mobile. Send mobile videos via email or SMS to your personal upload address.

Flash Player upgrade required
You must download and install the latest version of the Adobe Flash Player to view this content.
[Download Flash](#)

208.116.246.188 /bin/8/setup.exe
web.neg.md /i/captcha6.exe
web.neg.md /i/goglereg2.exe
upn1316.com /api?a=get&i=0&y=7
upn1316.com /api/tempgoo/GOO0c8be4f660bc37be8a3...

The virus downloads CAPTCHA solving application

The C&C sends the user a CAPTCHA to be solved

Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation

Enter both words below, separated by a space.

sterneff rapics

Time before shutdown: 02:50

OK

Gmail Calendar Documents Photos Reader Sites Web more

Compose Mail

Inbox (3)
Starred
Sent Mail
Drafts

Archive Report spam Delete Move to Labels More actions Refresh

Select: All, None, Read, Unread, Starred, Unstarred

msn Gmail 5 items Tag Gmail the virus...
msn Gmail 2 items Tag msn...
msn Gmail 2 items Tag msn...

Tietoturvatapahtumia – ammattimaisuus

spamcop.net

Report Spam | Filtered Email | Blocking List | Statistics | Login

45 issues
21 recipients

Abuse report sent to

Abuse report sent to	Age	Report level site
handq@citicnet.com	5.70 min.	http://www.zcukuvuy.cn/
wangjh@citicnet.com	5.70 min.	http://www.zcukuvuy.cn/
spam@ccert.edu.cn	6.32 min.	http://sendyear.com/index.php?lng=fr&cy=eu
abuse@cnc-noc.net	6.32 min.	http://sendyear.com/index.php?lng=fr&cy=eu
abuse@anti-spam.cn	6.32 min.	http://sendyear.com/index.php?lng=fr&cy=eu
spam@ccert.edu.cn	8.55 min.	http://www.undertasty.com/
abuse@anti-spam.cn	8.55 min.	http://www.undertasty.com/
abuse@cnc-noc.net	9.42 min.	http://www.undertasty.com/
spam@ccert.edu.cn	9.42 min.	http://www.undertasty.com/
anti-spam@ns.chinanet.cn.net	9.42 min.	http://www.undertasty.com/
abuse@anti-spam.cn	10.37 min.	http://www.undertasty.com/
abuse@cnc-noc.net	10.37 min.	http://www.undertasty.com/
spam@ccert.edu.cn	10.37 min.	http://www.undertasty.com/
spam@ccert.edu.cn	13.17 min.	http://mpaganix.cn/index.php?KSNWTDZQIT=3248nv
anti-spam@ns.chinanet.cn.net	13.17 min.	http://mpaganix.cn/index.php?KSNWTDZQIT=3248nv
abuse@anti-spam.cn	13.17 min.	http://mpaganix.cn/index.php?KSNWTDZQIT=3248nv
spam@ccert.edu.cn	13.52 min.	http://houmafor.com/
abuse@anti-spam.cn	13.52 min.	http://houmafor.com/
abuse@cnc-noc.net	13.52 min.	http://houmafor.com/
zhouxm@chinaunicom.cn	13.92 min.	http://ca6a6e.sqagegeb.cn/?as=DPC22311D08B62E6
zhouxm@chinaunicom.cn	13.92 min.	http://2b155.sqagegeb.cn/?ah=DPC22311D08B62E68
bao2500@gmail.com	14.52 min.	http://883c6.sqagegeb.cn/?nl=DPC22311D08B62E68
abuse@cnc-noc.net	14.52 min.	http://955.dfupebil.cn/?caygyu=73516Y43918N6B2...
bao2500@gmail.com	14.52 min.	http://5b897.dfupebil.cn/?ajaima=86W1W40342e2b...
abuse@cnc-noc.net	14.52 min.	http://e0cc.dfupebil.cn/?idumiti=5Yp256X85nPV94...
abuse@anti-spam.cn	14.52 min.	http://3ad0f5.dfupebil.cn/?owuqx=2826oXp70m587...
bao2500@gmail.com	14.52 min.	http://6f6f1.dfupebil.cn/?ipnyf=37Y6cO3529yN1z...
abuse@anti-spam.cn	14.52 min.	http://955.dfupebil.cn/?caygyu=73516Y43918N6B2...
anti-spam@ns.chinanet.cn.net	14.52 min.	http://3ad0f5.dfupebil.cn/?owuqx=2826oXp70m587...
abuse@anti-spam.cn	14.52 min.	http://e0cc.dfupebil.cn/?idumiti=5Yp256X85nPV94...

Home | Bestsellers | All products | FAQ | Contact us

USD EUR GBP CAD AUD CHF

Your cart: **\$0.00** (0 items) [Proceed to Checkout](#)

Pharma Bonus

Canadian Pharmacy

#1 Internet Online Drugstore

- Special Offer
- Free Viagra samples
- 4 pills for every order
- 12 pills for order >\$300

Product list

VIAGRA For Order more than \$300: 12 VIAGRA PILLS **FREE** For other Orders: 4 VIAGRA PILLS

Viagra + Cialis \$69.99	Cialis \$198.40	Viagra \$229.84
10 x Viagra 100 mg 10 x Cialis 20 mg	60 pills 20 mg +4 Free pills	120 pills 100 mg + 4 free pills + free delivery
ORDER NOW	ORDER NOW	ORDER NOW

Search by name:

Today's bestsellers

Viagra Our price \$1.15	Cialis Our price \$1.99	Accutane \$0.79
Viagra Professional Our price \$1.57	Cialis Professional Our price \$4.17	Clomid \$0.58
Viagra Super Active+	Cialis Super Active+	Prednisone \$0.37
		Levitra

- Erectile Dysfunction
- Male Enhancement
- Anti-Acidity
- Anti-Allergic/Asthma
- Anti-Depressant/Anti-Anxiety
- Anti-Diabetic
- Anti-Fungal
- Anti-Herpes
- Antibiotics
- Blood Pressure/Cholesterol
- Body-Building
- Dental Whitening
- Erection packs
- Female Enhancement
- General Health

Order The Cheapest Medications Now! - Windows Internet

<http://www.undertasty.com/>

File Edit View Favorites Tools Help

Order The Cheapest Medications Now!

Ratkaisumalleja – mainesuodatus



IronPort Email and Web Security

HOME THREAT OVERVIEW TOP SENDERS REPUTATION LOOK UP HELP

Cisco IronPort SenderBase Security Network

WEB & EMAIL REPUTATION

Results for: www.undertasty.com (more Details)

Email Reputation Web Reputation

Web Reputation Score: **Poor** ?

Why is the reputation Poor?

These are the most common reasons:

- The website or IP address has exhibited activities that indicates it has been involved in the distribution of malware.
- The IP address associated with this Website has been linked to highly suspect behavior. By going to this site users are at high risk for getting infected with malware.
- The host has exhibited activity that indicates it has been involved in Phishing attacks.
- The host is infected by malware or otherwise compromised by spammers or another malicious group.

How does this affect me?

While many networks use SenderBase as a means for assessing their web traffic, SenderBase does not block websites.

What can I do to improve my reputation?

The information displayed on our website is meant to help you identify and resolve any issues that might be the reason for your IP's poor reputation score. Once you have taken the necessary steps to fix any known issues, your reputation score should automatically recover within a short time frame.

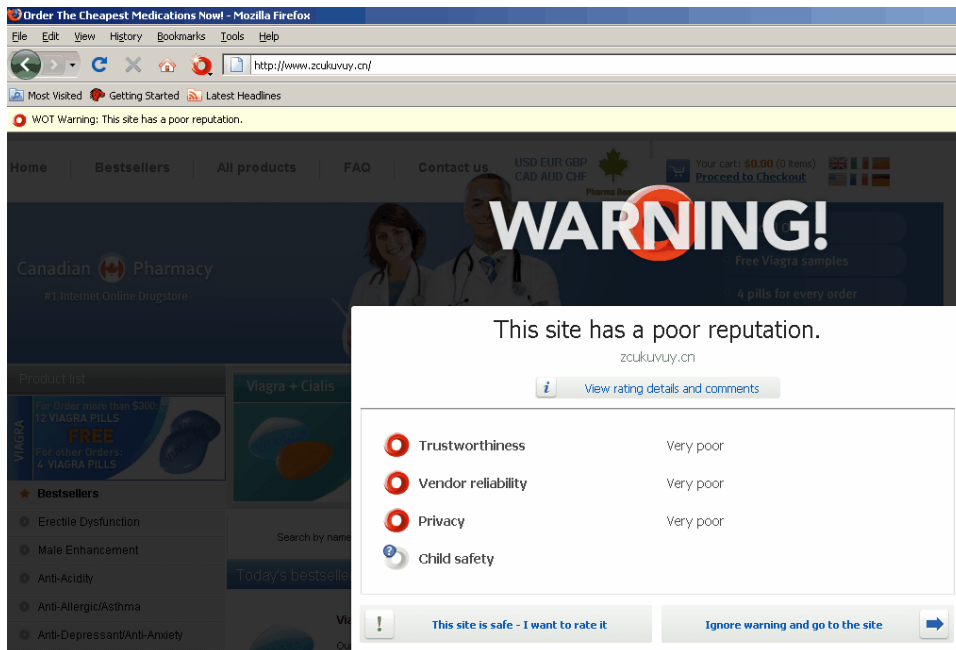
Location:



WHOIS Information

Name servers:

NS2.GALORECHIEF.COM
 NS1.GALORECHIEF.COM
 NS5.ON8.RU
 NS4.CLEARBETTER.COM
 NS6.ON8.RU
 NS3.CLEARBETTER.COM



Order The Cheapest Medications Now! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.zcukuvuy.cn/

WOT Warning: This site has a poor reputation.

Home Bestsellers All products FAQ Contact us USD EUR GBP CAD AUD CHF Your cart: 40.00 (0 items) Proceed to Checkout

WARNING!

Canadian Pharmacy #1 Internet Online Drugstore

Free Viagra samples 4 pills for every order

Product List Viagra + Cialis

FREE 12 VIAGRA PILLS 100mg 100mg 4 VIAGRA PILLS

Bestsellers

- Erectile Dysfunction
- Male Enhancement
- Anti-Acidity
- Anti-Allergic/Asthma
- Anti-Depressant/Anti-Anxiety

This site has a poor reputation.

zcukuvuy.cn

View rating details and comments

Trustworthiness	Very poor
Vendor reliability	Very poor
Privacy	Very poor
Child safety	

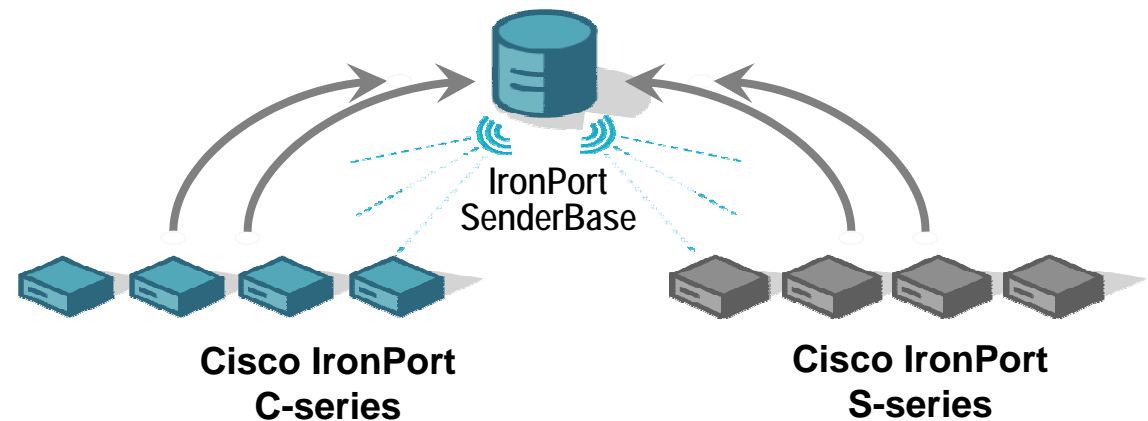
This site is safe - I want to rate it Ignore warning and go to the site

Cisco IronPort SenderBase-tietokanta



- Yli 30 miljardia kyselyä päivittäin
- Yli 150 sähköposti- ja webparametriä
- Lopputuloksena mainearvo web- ja sähköpostiliikenteelle, asteikko -10... +10

Yhdistää sähköposti- ja webliekenteen analyysit



- Tarkistamalla sekä sähköposti- että webliekennettä, havaitsemiskykyä ja –tarkkuutta parannetaan huomattavasti
- >80% SPAM:stä sisältää URL:in
- Haittaohjelmat ovat avainasemassa Botnet-verkkojen syntymisessä.
- Botnet-verkot vastaavat yli 80% koko maailman roskapostista.

SantaCare -palvelut

Ylläpitopalvelut

- Puhelin- ja sähköpostituki
- Vianrajaus
- Onsite-tuki
- Laitevaihdot
- Ohjelmistopäivitykset
- 24/7 päivystys

Hallitut palvelut

- Palomuri/VPN
- SSL VPN
- WLAN
- Sähköpostiturvallisuus
- Sovelluskiihdytys
- Turvallinen Web

Asiantuntijapalvelut

- Suunnittelu
- Käyttöönotto
- Konsultointi
- Auditoinnit
- VirtualExpert (VEX)
- Asiakaskohtaiset koulutukset

SantaCare-palvelut

SantaCare-palvelut muodostavat joustavan asiantuntijapalvelukokonaisuuden, jonka komponentteja yhdistämällä voidaan räätälöidä asiakkaalle parhaiten soveltuva kokonaisuus.

Asiakasympäristöön suunniteltu ja toteutettu verkkoratkaisu + tukipalvelut tukemaan elinkaarta

= SC Asiantuntijapalvelut + SC Ylläpitopalvelut

vai

Verkkoratkaisun hallinnoinnin ja ylläpidon ulkoistaminen SMN:lle

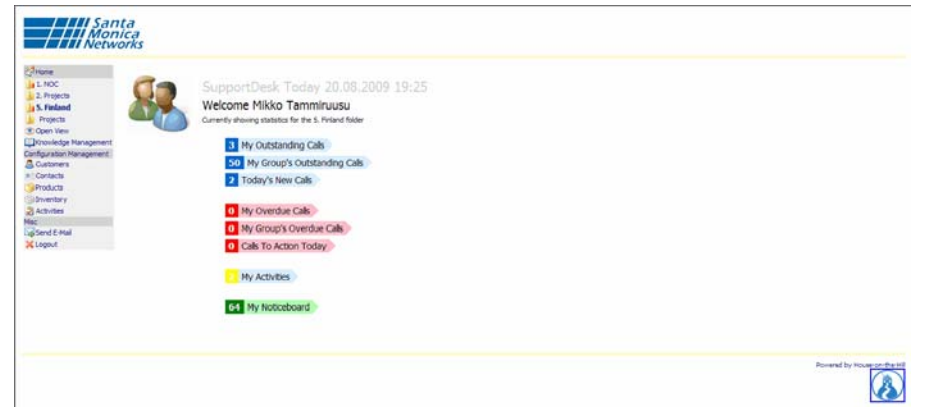
= SC Hallitut palvelut

SantaCare Managed WebSecurity

- Verkkoammattilaisten suunnittelema, implementoima ja operoima kokonaispalvelu
- Palvelu voidaan aina räätälöidä asiakkaan tarpeisiin
- Palvelua kehitetään jatkuvasti
 - Esim. uusien ohjelmistoversioiden uudet ominaisuudet, säännölliset asiakastapaamiset ja asiakkaan kehitystoiveet
- Yksi kontaktirajapinta – Santa Monica Networks NOC
- Palvelua monitoroidaan 24/7
- Useita SLA-vaihtoehtoja
- Kuukausittainen raportointi Internet-liikenteestä, tapahtumista, estetyistä sivuista, viruksista yms yms

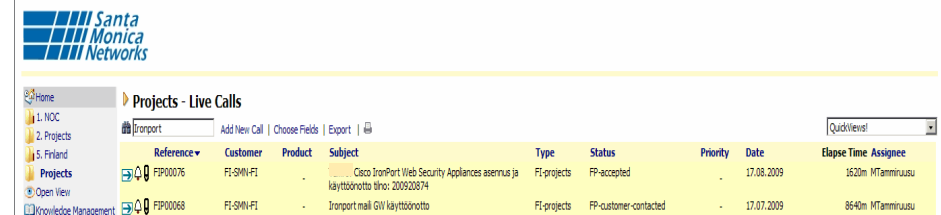
SantaCare WebPortal

- Asiakkaan pääasiallinen työkalu SantaCare-palveluiden hallintaan
- Tuki- ja muutospyynnöt auki helposti
- Inventaario laitteista, ylläpidoista ja palvelukomponenteista
- Nopeat haut kannasta



SupportDesk Today 20.08.2009 19:25
Welcome Mikko Tammi
Currently showing statistics for the S. Finland folder

- 1 My Outstanding Calls
- 2 My Group's Outstanding Calls
- 3 Today's New Calls
- 4 My Overdue Calls
- 5 My Group's Overdue Calls
- 6 Calls To Action Today
- 7 My Activities
- 8 My Hotcboard



Reference	Customer	Product	Subject	Type	Status	Priority	Date	Elapse Time	Assignee
FP00076	FI-SMN-FI		Cisco IronPort Web Security Appliances asennus ja käyttöönotto tulo: 200920874	FI-projects	FP-accepted		17.08.2009	3520m	MTammiuus
FP00068	FI-SMN-FI		Ironport mail GW käyttöönotto	FI-projects	FP-customer-contacted		17.07.2009	8640m	MTammiuus

SantaCare Managed WebSecurity - esimerkkiraportointi



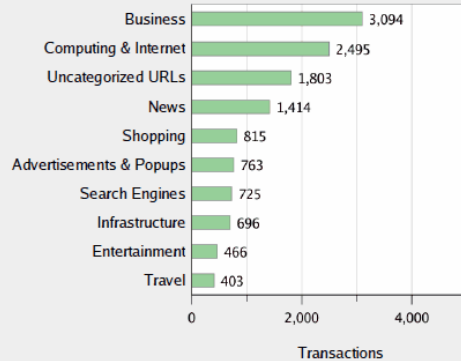
WEB SECURITY APPLIANCE

Web-liikenne – suosituimmat URL-kategoriat

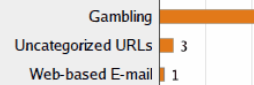
santacare-webgw.smn.fi

02 Aug 2009 00:00 to 08 Aug 2009 23:59 (GMT +0300)

Top URL Categories - Completed



Top URL Categories - Blocked



URL Category	Bandwidth		Web Transactions		
	Bandwidth Saved by Blocking	Bandwidth Used	Transactions Completed	Transactions Blocked	Total Transactions
Business	0B	14.3MB	3,094	0	3,094
Computing & Internet	0B	589.1MB	2,495	0	2,495
Uncategorized URLs	36.0KB	14.2MB	1,803	3	1,806
News	0B	24.1MB	1,414	0	1,414
Shopping	0B	6.1MB	815	0	815
Advertisements & Popups	0B	2.9MB	763	0	763
Search Engines	0B	3.1MB	725	0	725
Infrastructure	0B	937.3KB	696	0	696
Entertainment	0B	5.0MB	466	0	466
Travel	0B	6.6MB	403	0	403
Web-based E-mail	12.0KB	3.7MB	297	1	298
Blogs & Forums	0B	4.4MB	247	0	247
Motor Vehicles	0B	1.6MB	195	0	195
Reference	0B	1.3MB	190	0	190
Sports	0B	3.5MB	157	0	157
Finance & Investment	0B	201.9KB	48	0	48
Gambling	492.0KB	0B	0	41	41

SantaCare Managed WebSecurity - esimerkkiraportointi



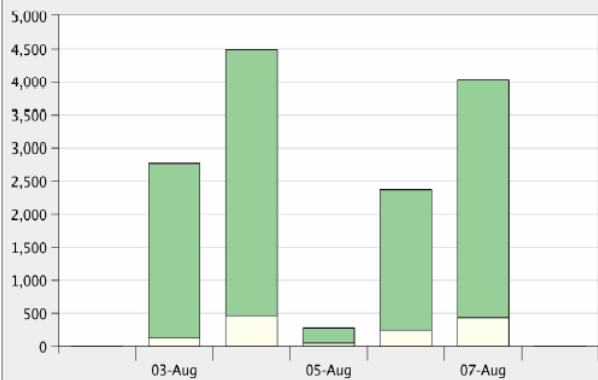
WEB SECURITY APPLIANCE

Web-liikenne - mainearvot

santacare-webgw.smn.fi

02 Aug 2009 00:00 to 08 Aug 2009 23:59 (GMT +0300)

Web Reputation Actions (Trend)



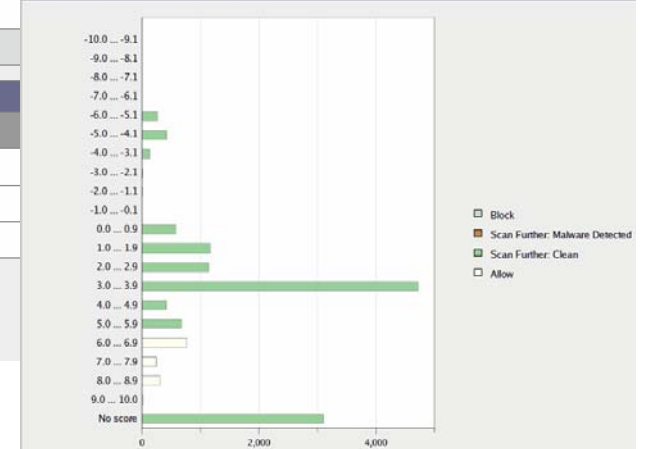
Web Reputation Actions (Volume)

Action	%	Transactions
<input type="checkbox"/> Block	0.0%	3
<input type="checkbox"/> Scan Further: Malware Detected	0.0%	0
<input checked="" type="checkbox"/> Scan Further: Clean	90.4%	12,614
<input type="checkbox"/> Allow	9.6%	
Total		

Current Configuration

Action	Current Range
Block	-10.0 to -6.0
Scan Further	-5.9 to 5.9
Allow	6.0 to 10.0

Web Reputation Actions (Breakdown by Score)



Kiitos !

**Mikko Tammiruusu
mikko.tammiruusu@smn.fi**