Verkkorikollisuus ja rahaliikenne

Mikko Hyppönen
Tutkimusjohtaja
F-Secure Oyj


F-SECURE
© 2005 Mikael Albrecht

Tietoverkkorikollisen monet kasvot

Harrastelija

Rikollinen

Aktivisti / Terroristi

Vakoilija / Teollisuusvakoilija

Virukset ja kriittinen infrastruktuuri

Virus	Liikenne	Sähkönjakelu	Perusjärjestelmät	Pankit
Slammer	Kolme kansainvälistä lentokenttää ilmoitti häiriöistä	Saastutti Ohiolaisen ydinvoimalan sisäverkon	Hätäpuhelimet nurin Seattlessa	Bank of American pankki-automaatti-verkko nurin
Blaster	Mm. Air Canadan ja Finnairin järjestelmissä ongelmia, CSX:n junaliikenne seis	New Yorkin sähköverkko-operaattori NY ISO:n verkko saastui	Lukuisia RPC-pohjaisia SCADA-verkkoja kaatui	Lukuisia Windows-pohjaisia pankki-automaatti-verkkoja saastui
Sasser	Kaikki junaliikenne Australiassa pysähtyi, ongelmia Deltan ja British Airwaysin lentojen kanssa	Hong Kongin hallituksen voimalaitos-yksikön verkot saastuivat	Saastui: Iso-Britannian rajavartiosto, Heatrhown lentokenttä, kaksi sairaalaa Ruotsissa	Pankit sulkivat oviaan Euroopassa, Aasiassa ja Amerikassa

Entä tilanne Suomessa?

Tietokonevirusten pelätään katkaisevan sähköt sydäntalve

Liikenneministeriö m
suuryrityksiä tietotu

▶ Virukset uhkaavat sähkön jakelua ja pankkien järjestelmiä

Tietokonevikojen aiheuttamia ongelmia syksyn aikana

▶ Virukset tukkivat sähköyhtiöiden viesti
Yhdysvaltojen sähkökatkon korjaustöitä

Pekka Pekkala
HELSINGIN SANOMAT

▶ Liikenne- ja viestintäministeriö on erittäin huolestunut erilaisten tietokonevirusten aiheuttamista ongelmista, jotka vaikuttavat suoraan suomalaisten arkeen.

Se on lähettänyt yhdessä Huoltovarmuuskeskuksen

Ennen vanhaan meidän tarvitsi varoa vain niitä rikollisia jotka olivat meitä lähellä

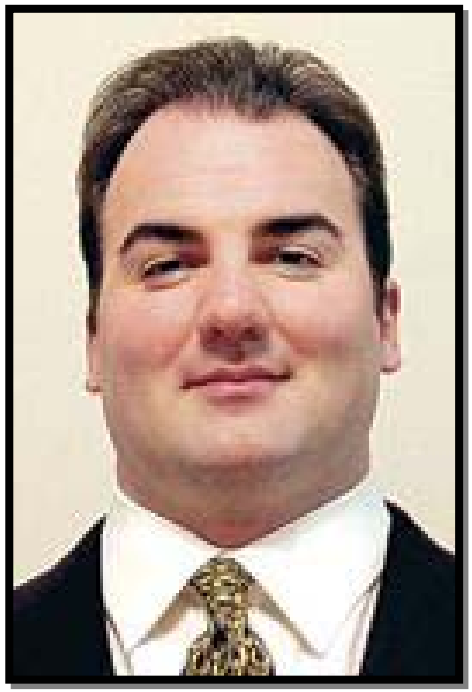
Päävastustajamme ennen...

Chen-Ing Hau
CIH-viruksen kirjoittaja

Joseph McElroy
Murtautui Fermi National Accelerator Lab -asetutkimuskeskukseen

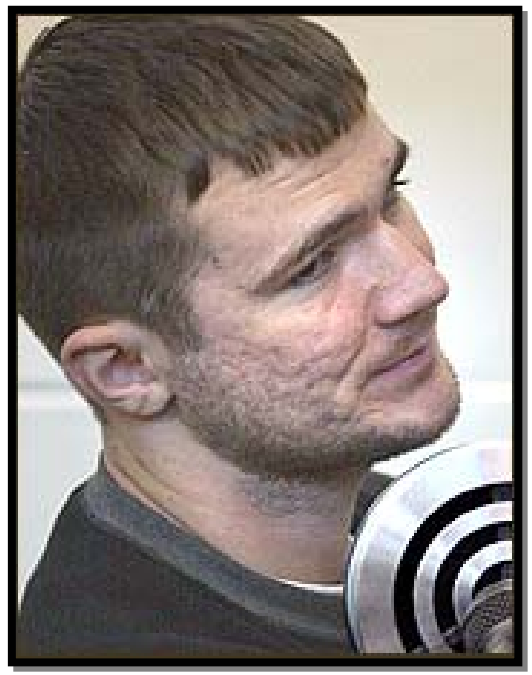
Benny
29A-virusryhmän avainjäseniä

Päävastustajamme tänään



Jeremy Jaynes
- miljonääri.
- roskapostittaja

Jay Echouafni
- toimitusjohtaja
- verkkohyökkäyksien suunnittelija



Andrew Schwarmkoff
- venäläinen mafioso
- phishing-viestien lähettäjä

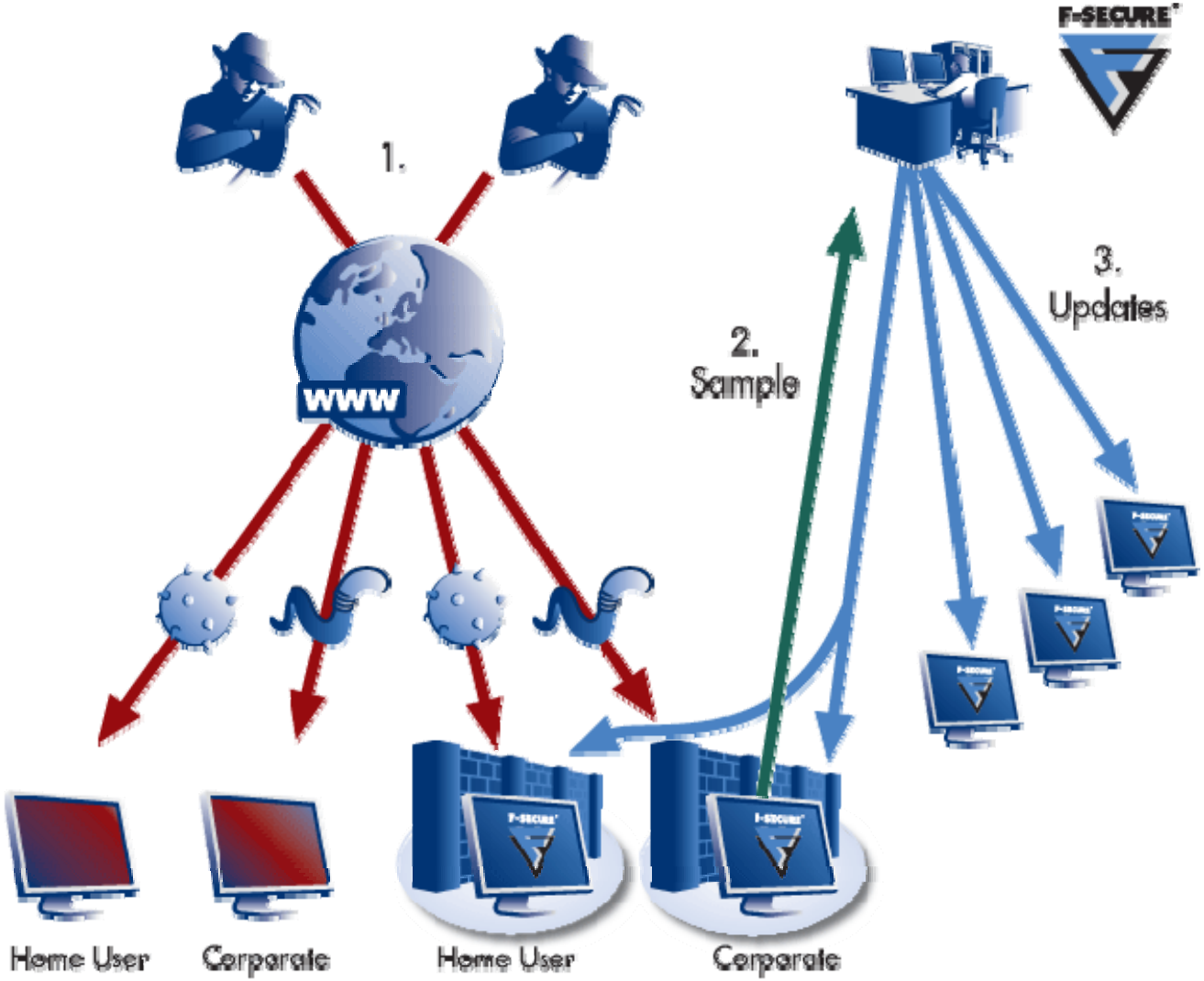
F-SECURE®

Alexander Petrov, Denis Stepanov

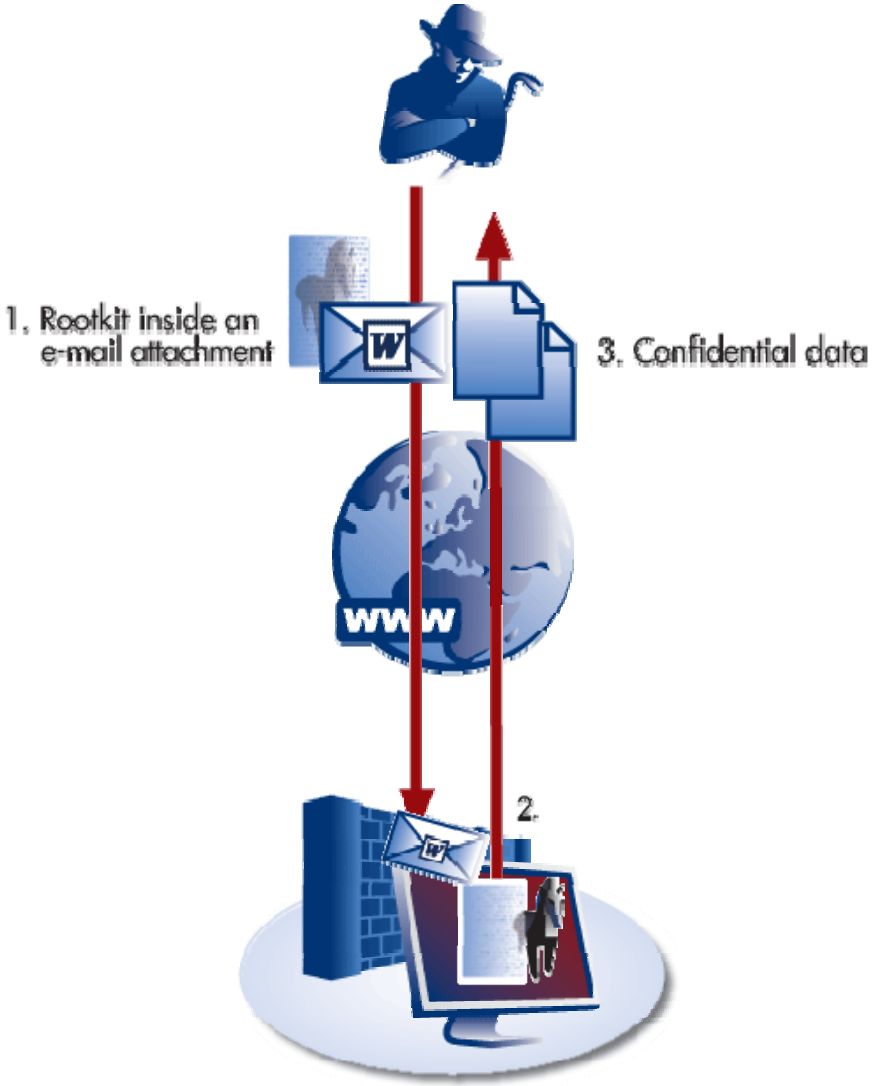
Verkkorikollisuus on koko IT-alan nopeimmin kasvava sektori

Suunnatut hyökkäykset

Perinteiset hyökkäykset



Suunnatut hyökkäykset - vakoilu



Suunnattuja hyökkäyksiä

Joulukuu 2005: Yhdysvallat

Maaliskuu: 2006. Englanti

Huhtikuu 2006: Saksa

Toukokuu 2006; Ruotsi

Kesä 2006: Suomi

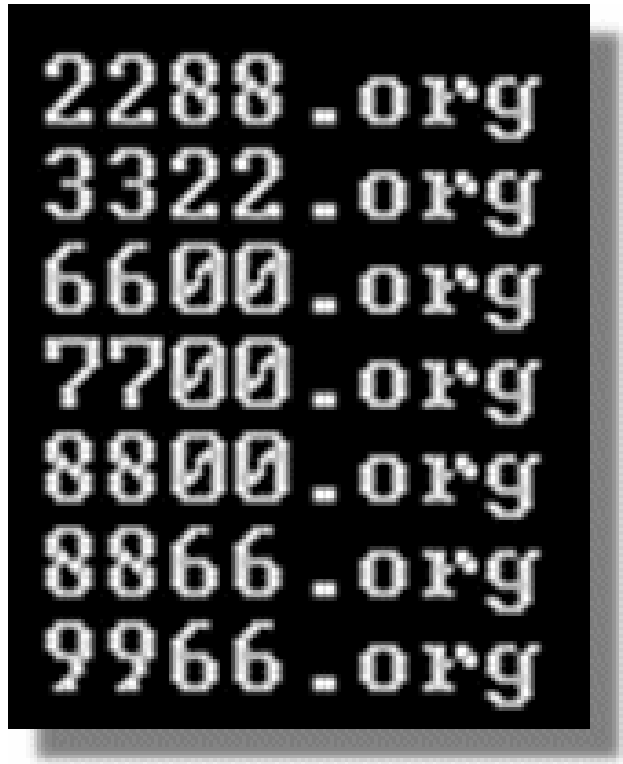
Marraskuu 2006: Ruotsi

Marraskuu 2006: Suomi

Tammikuu 2007: Yhdysvallat

Helmikuu 2007: Yhdysvallat

Maaliskuu 2007: Viro



F-SECURE®

Phishing

PayPal

Enter Information → Done

Personal Account Update

Email Address*:

Password*:

Email Address and Password
You will use these to log in to PayPal.

Please enter your full email address, for example, **name@domain.com**

Your password must be at least 8 characters long and is case-sensitive. Please do not enter accented characters.

First Name*:

Last Name*:

Address*:

City*:

State*:

ZIP Code*: (5 or 9 digits)

Country*: -- Choose a Country --

Personal Information
Please enter your name and address as they are listed for your debit card, credit card, or bank account.

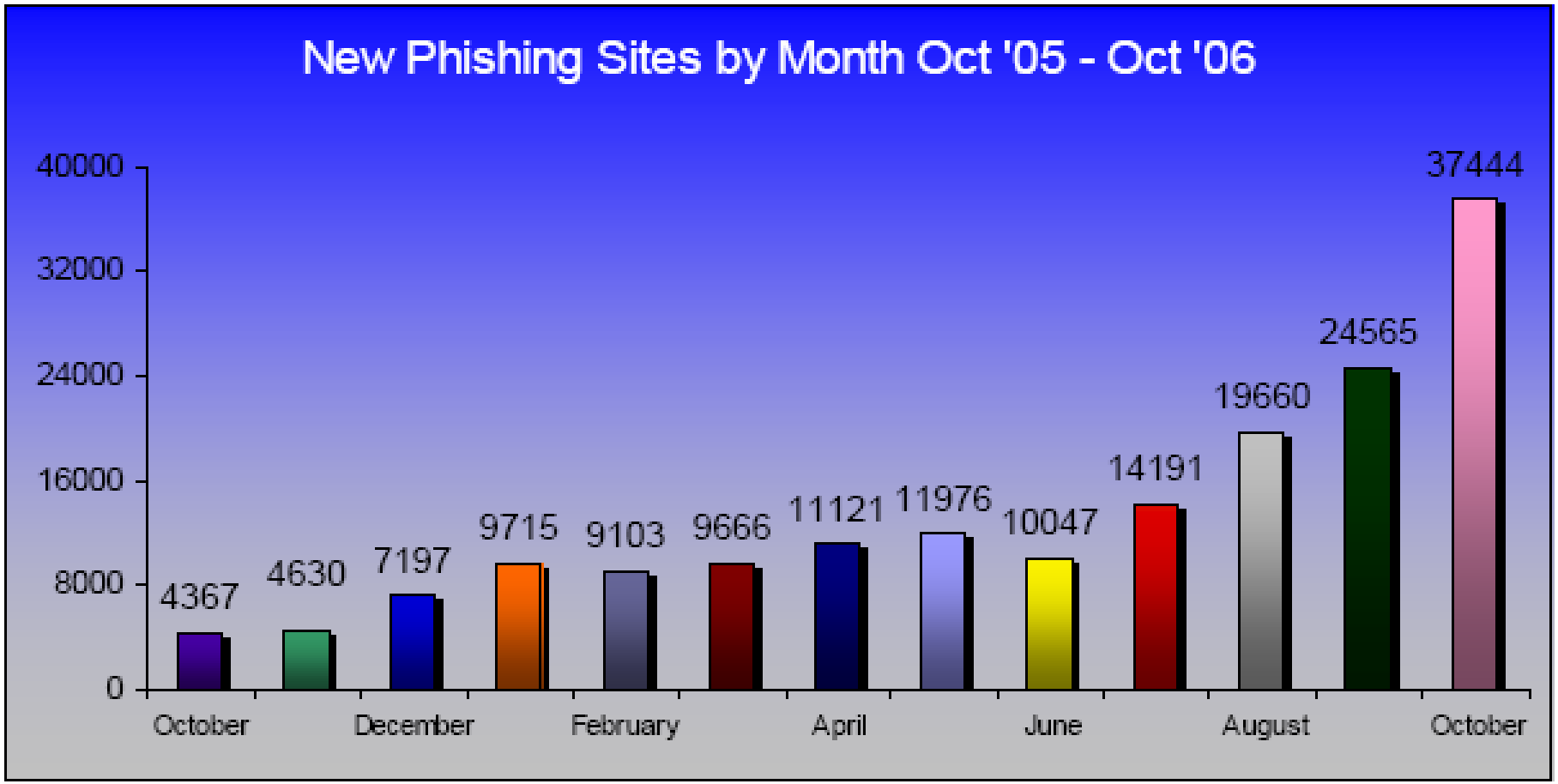
Card Number*:

Expiration Date*: - - - - - -

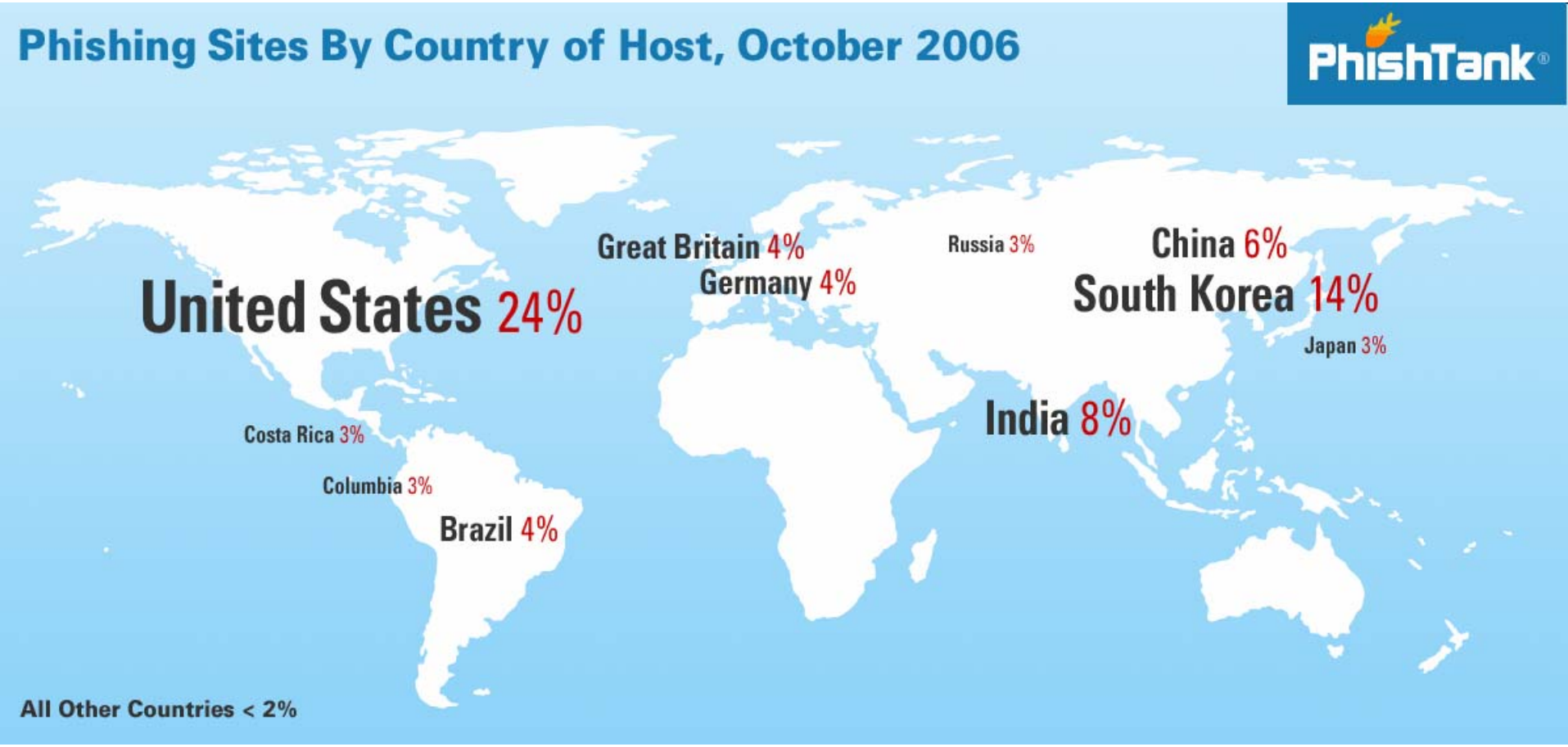
Card Verification Number*:

ATM PIN Number* (Credit Card Validation):

Card Information
Please enter your credit card number, card verification number, expiration date exactly as they appear on your credit card and PIN number.



Source: Anti-Phishing Working Group


Phishing Sites By Country of Host, October 2006
PhishTank
United States 24%
Great Britain 4%
Germany 4%
Russia 3%
China 6%
South Korea 14%
Japan 3%
India 8%
Costa Rica 3%
Columbia 3%
Brazil 4%
All Other Countries < 2%

F-SECURE

Pankki-troijalaiset

Snatch

Haxdoor

Torpig

Apophis

Bancos…

nologies » Nuclear grabber ::

« : A311 Death : »

A311 Death это профессиональная система удалённого администрирования с кучей возможностей.

Помните, что постоянное совершенствование средств защиты требует постоянный приток новых технологий тестиро
ТОЛЬКО свежее spyware способно обеспечить уровень функциональности, адекватный текущим потребностям.

-==::==-

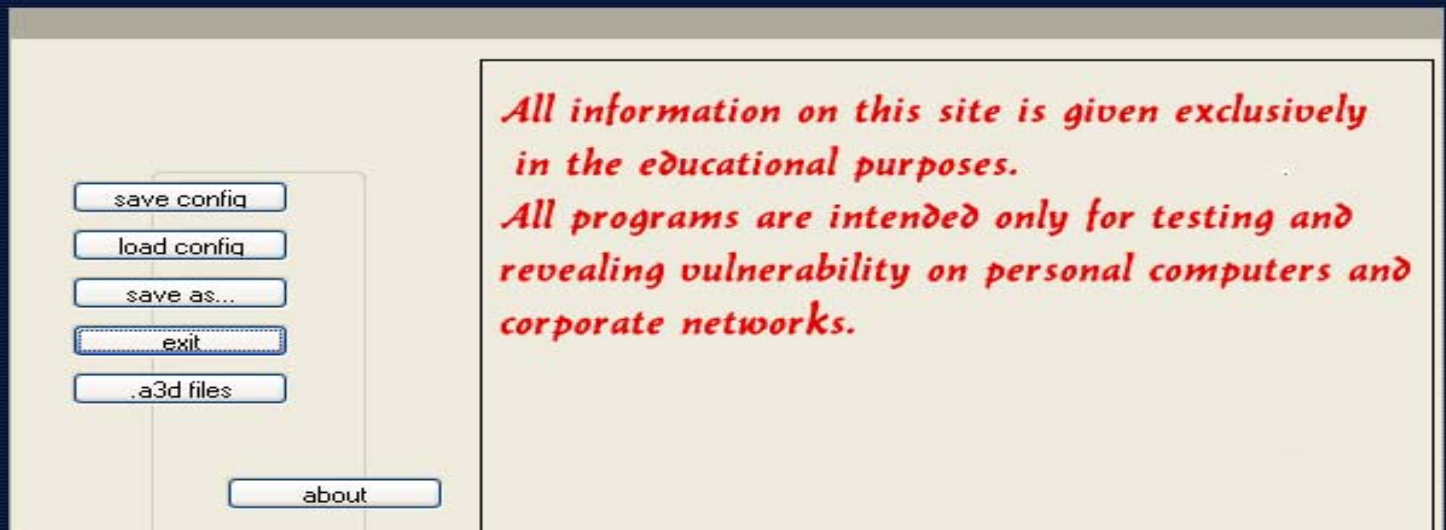
- !!! теперь возможен заказ с ПРОФЕССИОНАЛЬНОЙ админкой для организации сокс-сервиса

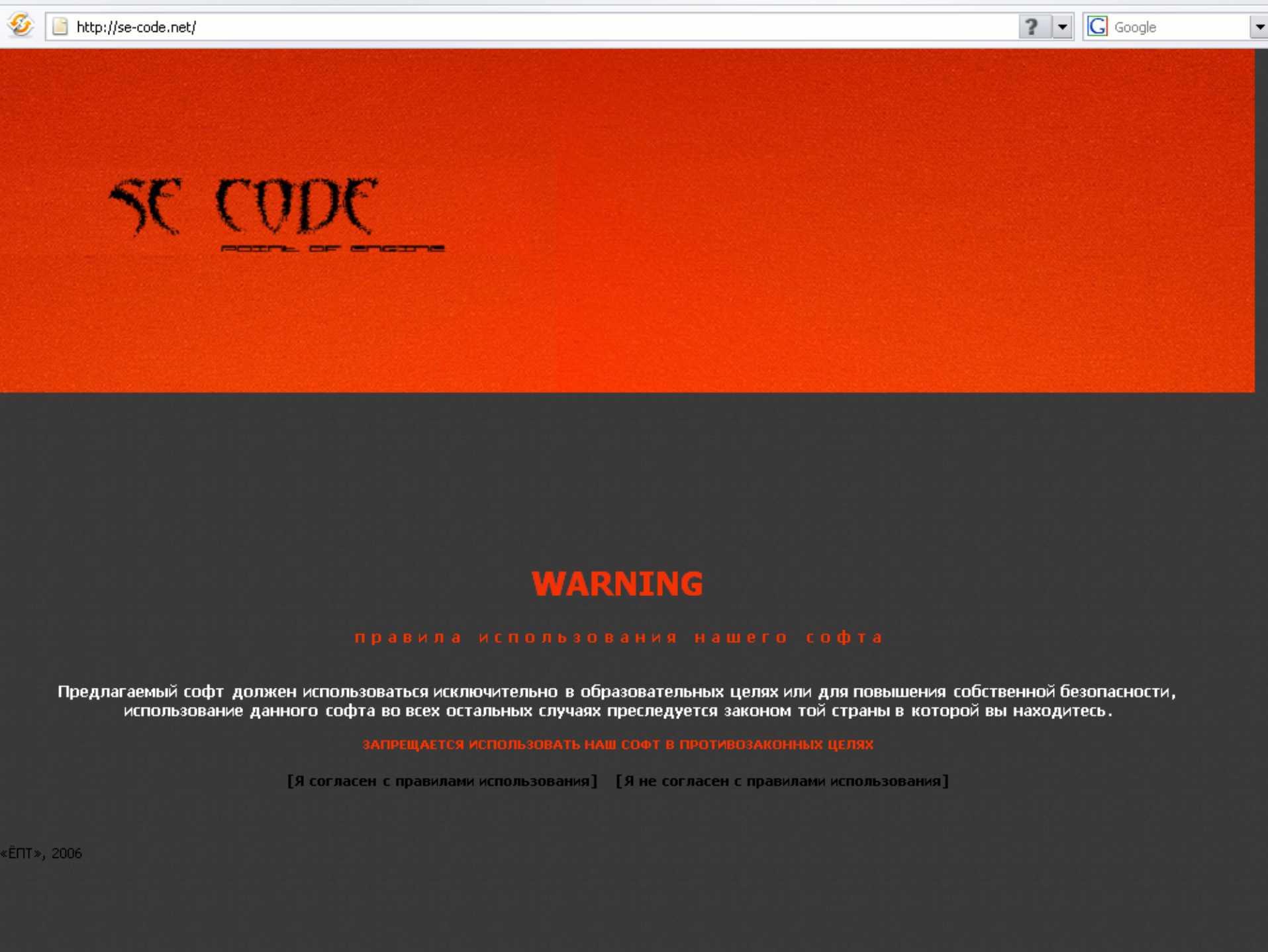
- СВЕЖАЯ GEO база (IP to country-state-sity)
- система аккуантов и установка лимитов (срок действия аккуанта, количество взятых проксей)
- вывод соксов для пользователей в поштучном виде типа 197.59.***.***
- поиск и фильтрация по соксам
- в цену входит установка на сервер

цена 250 $

посмотреть скриншоты

*** установка производится ТОЛЬКО на технически подготовленные сервера




http://se-code.net/
Google
SE CODE
POINT OF ENGINE
WARNING
правила использования нашего софта
Предлагаемый софт должен использоваться исключительно в образовательных целях или для повышения собственной безопасности, использование данного софта во всех остальных случаях преследуется законом той страны в которой вы находитесь.
ЗАПРЕЩАЕТСЯ ИСПОЛЬЗОВАТЬ НАШ СОФТ В ПРОТИВОЗАКОННЫХ ЦЕЛЯХ
[Я согласен с правилами использования] [Я не согласен с правилами использования]
«ЁПТ», 2006

www.bci.cl telemarch.bancamarch.es www.bdd.cl directnetbusiness.dexia.be www.bancoparis.cl www.bancoo
*banistmo.com *bancocuscatlan.com express.bancoaliado.com bcnet.bcocontinental.com 440strand.com *ban
secure.baoffshore.com *deltabank.net internetbanking.firstcaribbeanbank.com portal4.*.dk *sydbank.dk
*internationalbanking.barclays.com *dexia.be **www511.sampo.fi** *.netbanking.ch www.optionsxpress.com.s
ubadirect.com 217.117.9.49 **solo*.nordea.fi www*.sampo.fi** ubaplc.com *.pictet.com ihb.*.ch inba-html.g
private.lombardodierdarierhentsch.com *bcge.ch *bcvs.ch inba.bcf.ch sobanet.baloise.ch *mygottardo.c
banking.tkb.ch onba.zkb.ch *banking.*.ch *carnegiebanking.com www.biaonline.lu *secure.lcf-rothschild
*ebanking.millenniumbank.gr *ebank.emporiki.gr *egnatiateller.egnatiabank.gr www.eurobank.gr www.eur
*.vv.sebank.se *staalbankiers.nl *robecodirect.nl *ingbank.nl *kasweb.com *dhbbank.com *rabobank.nl
*.sebank.se *.snet.lu *.sparbankenfinn.se *.sparebank1.no */cmserver
*abcbrasil.com.br *abnamro.be *abnamro.ch *abnamro.com *abnamro.lu *abnamro.nl *abnamroprivatebanking
*bancofar.es *bancopostaonline.poste.it *bancoreal.com.br *bankenverband.li *banking.agkb.ch *banquec
*bnpparibas.com *bpiexpresslink.com *bpitrade.com *bradesco.com.br *bradescori.com.br *businessonline
*capitalone.com *cashproweb.com *cdg.citibank.de *cey-ebanking.com *channel-e.com.my *chinatrust.com.
*citibusinessonline.da-us.citibank.com *citidirect-eb.citicorp.com *cmserver* *commercebank.com *comm
danskebank *danskebank.dk *dnbnor* *dnbnor.no *dollarbank.com *eastwestbanker.com *ebank.hsbc.co.uk
ecashman *edb.com *exact4web* *fiibg.com *fineco.it *fiservsa4.com *frostbank.com *gemoneybank* *ha
*ikanobanken.se *insularlife.com.ph *iurisbank.com *jobtoasterspain.com *juliusbaer.com *kaupthing*
*lasallebank.com *latpro.com *mandtbank.com *metrobankdirect.com *mystreetscape.com *net.hsbc.com *ni
onlineserv *onlinetreasurymanager* *optionsxpress.com.sg *paypal.com *plusgirot.se *portalbank.no
*privatebanking.info *produbanco.com *raiffeisendirect.ch *redfcu.org *ruralvia.com *sampo.fi *sanost
*sparebank1.no *standardchartered.com.hk *surepayroll.com *terra.as *trabajo.org *trustweb.com *ucpb.
*vault.melloninvestor.com *vip.lasallebank.com *vr-*ebanking.de *webcashmgmt* a.photofile.ru abnamro.
achpayments.wachovia.com allianceach.com amdirect.ambg.com.my areasegura.banif.es arubabank.com asp2.
authzone.virtualbank.com b2b.ccb.cn banca.cajaen.es bancae.caixapenedes.com bancainternet.bancocredic
bancolombia.olb.todo1.com banesnet.banesto.es banking.*sparkasse*.de banking.1822direkt.com banking.b
banking.berliner-sparkasse.de banking.bw-bank.de banking.degussa-bank.de banking.firsttennessee.* ban
banking.oberbank.de banking.postbank.de banking.privatbank.at banking.raiffeisen.at banking.santander
bankingportal.*.de bankingportal.kreissparkassealtenkirchen.de bankingportal.ksk-birkenfeld.de bankin
bankingportal.naspa.de bankingportal.sparkasse-ger-kandel.de bankingportal.sparkasse-rhein-haardt.de
bbv.webank.it bireysel.hsbc.com.tr brokerage.bankingonline.de brokerage.comdirect.de brokerage.lbbw.c
business.memberdirect.net businessbanking*.tdcommercialbanking.com businessbillpay-e.com businessnet.
caixadirecta.cgd.pt canada-connexis.bnpparibas.com caonline.credito-agricola.pt carenet.fnfismd.com c
cashmanagement.firstambank.com cashproweb.com cbf.cd.citibank.fr chaseonline.chase.com cib.ebanking-s
citidirect-eb.citicorp.com client.manulifebank.com cn.bochk.com co.caixabank.fr coma.comdirect.de con
connex.bdc.ca corporate-internet-banking.dbs.com cs.directnet.com csfb.com cspehb*.cd.citibank.es ctr
digibanker.securitybank.com direct.bankofamerica.com DISABLED-citibusinessonline.da-us.citibank.com e
easylink.bankofbermuda.com eb2.dexia.sk ebaer.juliusbaer.com ebancoval.bancoval.es ebank.sghambros.co

Verkon alamaailma


The Theft Services -> bank accounts for sale - Opera
File Edit View Bookmarks Widgets Feeds Tools Help
wl blog mess intra wiki kl vt descs Rtr stats meets mass solo TV rad fsc1 comp gfsc ghyp gfsbl digi isc amp world ropas sfix kvid dig
https://forum.theftservices.com/index.php?showtopic=4280
TService AG (DE)
Google
Article 19 of Universal Declaration of Human Rights
Pages: (3) [1] 2 3 (Go to first unread post)
AddReply
NewTopic
NewPoll
bank accounts for sale
Track this topic | Email this topic | Print this topic
tabbot
Posted: Jan 27 2006, 12:29 AM
Quote
Verified for Bank Accounts Logins
Group: Verified Vendor
Posts: 14
Member No.: 3407
Joined: 24-January 06
any US bank accounts for sale
Balance from 3k and above -40$
Regular Brokerage accounts from 3k and above - 70$
Lots of different brokerage accounts from 3k and above with signature - 100$
In stock accounts from other countries: CA, AU, NZ, FR, TR etc. – price negotiable
Also I can check for other countries that interest you, please drop links to my icq
bank accounts for sale
icq 258-954-710
www.accs-info.com
PM
Email
ICQ

Selling dumps[EU]

Author	Message
0xc0040bd6 Verified Seller Joined: 22 Nov 2006 Posts: 4	Posted: Thu Nov 23, 2006 8:50 pm Post subject: Selling dumps[EU] QUOTE **EU Dumps:** Random from these banks: SEB - 60€ NORDEA - 60€ SWEDBANK - 60€ HANDELSBANKEN - 60€ **F.A.Q:** What is the minimal sum of the deal with you? -Today the minimal sum of the deal is ten pieces, meaning 600€. What is the format of the dumps? -This first week it's track 1 and track 2, but in a week it will be all three. How long does it take to recieve the dumps? -It depends if im online, then instant delivery. Do you give discount if buy lots? -Yes, sure.

Logins&Cob From Drax

Drax

Australian Logins Verified Provider

Group: Verified Vendor
Posts: 100
Member No.: 3641
Joined: 16-March 06

Posted: Jun 22 2006, 11:26 PM

I'm offering for sale Bank Logins of various countries, and limited supply of cobs.

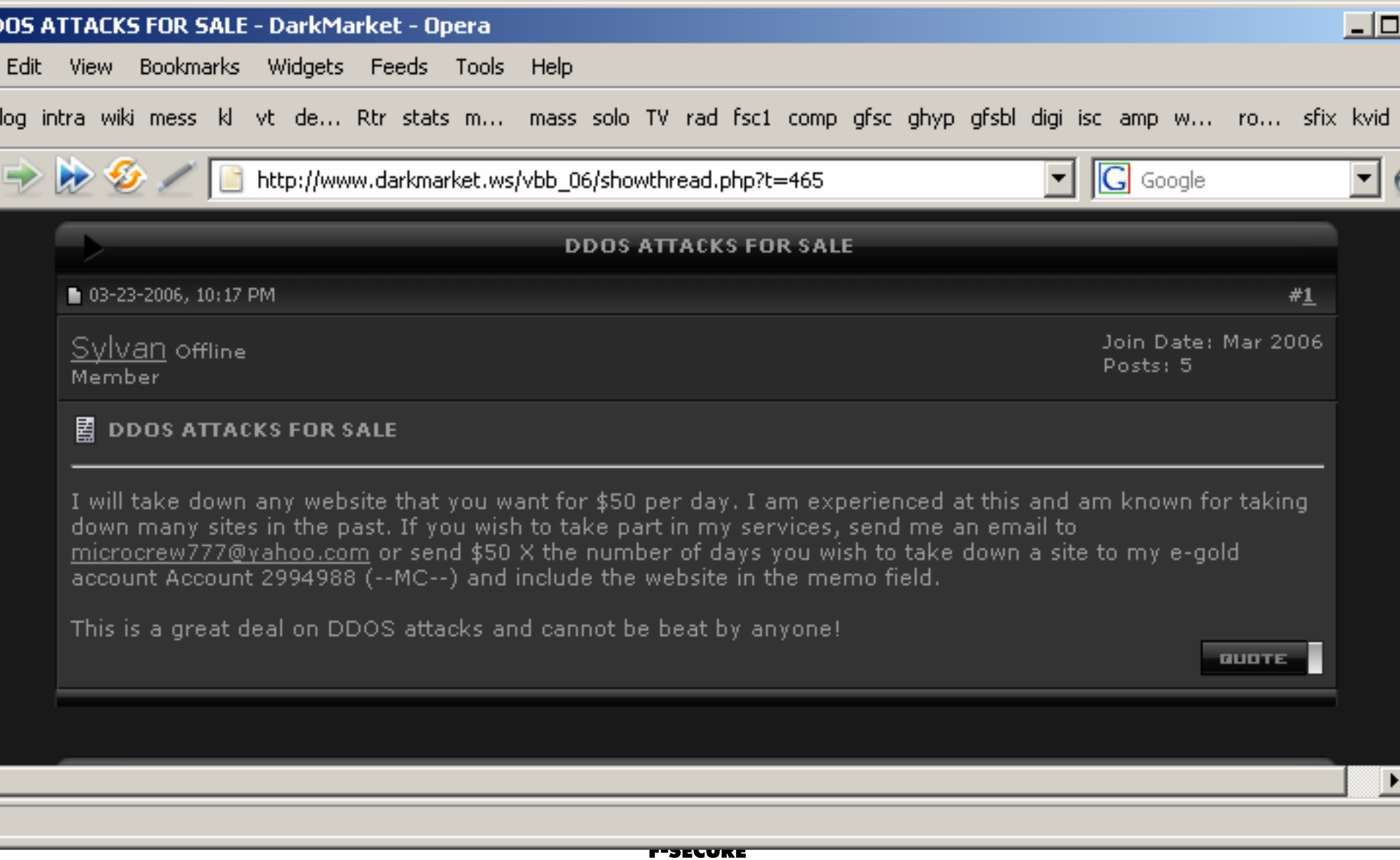
Logins:
USA - Citi, Washington Mutual, Wachovia, Boa, Chase
Australia - Commonwealth, National
United Kingdom - HSBC, Lloyds
Canada - TD Canada Trust

Some other's in stock, Ask me if you need something specific.

Cobs:
Discover

I only have Discover & Chase in stock now, Contact me if there is a specific cob you interested in.

Prices:
Contact for price.


OS ATTACKS FOR SALE - DarkMarket - Opera
Edit View Bookmarks Widgets Feeds Tools Help
log intra wiki mess kl vt de... Rtr stats m... mass solo TV rad fsc1 comp gfsc ghyp gfsbl digi isc amp w... ro... sfix kvid
http://www.darkmarket.ws/vbb_06/showthread.php?t=465
Google
DDOS ATTACKS FOR SALE
03-23-2006, 10:17 PM
#1
Sylvan offline
Member
Join Date: Mar 2006
Posts: 5
DDOS ATTACKS FOR SALE
I will take down any website that you want for $50 per day. I am experienced at this and am known for taking down many sites in the past. If you wish to take part in my services, send me an email to microcrew777@yahoo.com or send $50 X the number of days you wish to take down a site to my e-gold account Account 2994988 (--MC--) and include the website in the memo field.
This is a great deal on DDOS attacks and cannot be beat by anyone!
QUOTE

Verkkohyökkäykset Virossa ja Suomessa

ZYKLON
security team

Menu

» news
» releases
» papers
» links
» crew
» services
» defaces

#zyklon

Friends

The Hack
Zombiexe AREA
DamageLab
Art of Hack Security Team
.:[KZ TeaM]:.
TGBR Hack Team
S-TEALS.ORG
WDTeaM.RU

По вопросам обмена ссылками стучать: *408304*

News:

1

DDoS Attacker

Дата: 28.04.2007 **Написал:** zombiexe

релиз **DDoS Attacker** многопоточный, поддержка Socks 4, Socks 5.
Написан на Delphi
Скачать TCP/IP DDoS Attacker
Special for attacking fuc*ing Estonian sites.

Новости команды

Дата: 12.04.2007 **Написал:** zombiexe

1. Craft покинул команду ...
2. Релиз MySQL Bruter - Скачать
3. Идет набор в команду (желающим вступить - связаться со мной по icq 408304)

Обновление FTP-informer

Дата: 18.01.2007 **Написал:** Craft

Обновился FTP-informer, а точнее обновилась самая важная фича - это просмотр ТИЦ и PR сайта, качайте: FTP-informer v 1.1

Новогодние релизы

Дата: 06.01.2007 **Написал:** Zyklon Team

FTP-informer от Craft'a - чекает ТИЦ и pR сайта ,
работает со списком , фидбек для покупки/продажи
Скачать : FTP-informer v 1.0

Web-Shells checker - чекаем на живучесть web-шеллы, также работает с инклуд шеллами, работа со списком, написан на PHP
Скачать : Web-Shells checker

Сборщик паролей на C++

Дата: 18.10.2006 **Написал:** [N3oxh]

Offline

OrcPower

Ньюсмейкер

Комментариев: 85

Offline

#11 Заголовок: 2007-04-29 16:41:28

++
"Ты не согласен с политикой эстонии??? Ты думаешь, что ты лично не влияешь на ситуацию???
Ты МОЖЕШЬ повлиять на нее в интернете! Просто введи в гугле "site:.ee правительство" (вместо слова правительство любой интересующий запрос для поиска по эстонским сайтам). Выбери понравившийся сайт (не русскоязычный!!!), нажми (пуск -> выполнить-> cmd) и вводи "ping -n 5000 -l 10000 эстонский_сайт -t". ОК. ВСЕ!!!
пример: " ping -n 5000 -l 1000 www.riik.ee -t"
Это 3 элементарных действия, после которых многие эстонские сайты просто перестанут работать!!! Сайт правительства эстонии уже не работает. Кто следующий? Решать тебе!!!
Отомстим за издевательства эстонского правительства!!!
Разошли это сообщение по всему контакт-листу, вставь в ЖЖ, отпости на форумах. Пусть эстония знает, что Россия своих не бросает!
На 9ое МАЯ планируется повтор данной акции! Не
дай унизить своих соотечественников, отомсти за издевательства!!!"
++
nnm.ru (c)

OrcPower

Ньюсмейкер

Комментариев: 85

Offline

#12 Заголовок: 2007-04-29 16:44:16

Банки эстонии
https://www.hanza.net
http://www.sampo.ee
bankofestonia.info
www.krediidipank.ee/
http://www.nordea.ee

#13 Заголовок: 2007-04-29 17:42:01

Yhteenveto - tietoturvauhat

Hyökkääjät etsivät heikoimman kohteen

Phishing on edelleen suuri kansainvälinen ongelma

Pankkitroijalaiset ovat se todellinen suuri haaste

Pankit ovat näkyvä kohde DDoS-hyökkäyksille

Kun tarvitaan todellista korkean tason tietoturvaa, laitteet tulee eristää julkisista verkoista

Kriittisten ympäristöjen rakentaminen Windowsin päälle arveluttavaa

F-SECURE®

BE SURE.