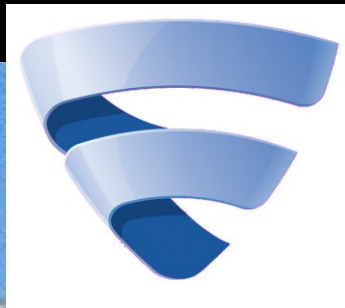


State Of The Net



Internetdagarna
Mikko Hyppönen
CRO
F-Secure



twitter.com/mikko

The Three Main Sources of Cyber Attacks

Criminal



Hactivist



Government





Criminals



Matjaz skorjanc







●● Tõenäoliselt läheb arestimisele ligi 150 kinnistut, millest valdav osa on prokuratuuri hinnangul soetatud kuritegelikul teel saadud rahaga. Nende müügitulu võib minna riigikassasse.

Tallinn, Pirita tee 26f

korter
basseiniruum ja saun
spordisaal nr 77
spordisaal nr 78
2 garaaži

Ida-Virumaa, Alajõe vald, Karjamäe küla

ADDRESS

Kuremarja alajaam
Biopuhasti
Kuremarja tee 12
Kuremarja tee 10

ADDRESS

Kuremarja tee 8
Kuremarja tee 6
Kuremarja tee 4
Kuremarja tee 3

ADDRESS

Kuremarja tee 2
Kuremarja tee 1
Võgana Pluss

Peipsi järv



Tartu linn

ADDRESS

Narva mnt 78/80/
82 / Staadioni tn 4
Põik tn 14
Põik tn 12
Lai tn 6
Turu tn 63
Ringtee tn 83
Ringtee tn 89
Raudtee tn 114B
Fortuuna tn 22
Fortuuna tn 25
Jaama tn 34
Veski tn 34

Jõgevamaa, Palamuse vald, Ehavere küla

ADDRESS

Põdralaane

Tartumaa, Tähtvere vald, Tähtvere küla

ADDRESS

Meika
Tõllu

Tartumaa, Luunja vald

ADDRESS

Põvvatu tee l1
Hobunurme tee l2
Hobunurme tee l1
Hobunurme tee 29
Hobunurme tee 31
Hobunurme tee 27
Hobunurme tee 25
Hobunurme tee 23
Hobunurme tee 22
Hobunurme tee 21
Hobunurme tee 20
Hobunurme tee 19
Hobunurme tee 18
Hobunurme tee 17a
Hobunurme tee 17
Hobunurme tee 16

Tartu maakond, Haaslava vald, Haaslava küla

ADDRESS

ADDRESS

ADDRESS

ADDRESS

Võrts-
järv



Adv: Sell Domains! Fast and cheap! Domains .in - 6 wnz
 Adv: Chinese domains with the best price!

Start date: End date: [Apply](#) Autoupdate interval: **10 sec.**

STATISTIC

TOTAL INFO

450216 HITED 148233 HOSTS 18997 LOADS

14.61%

TODAY INFO

21899 HITED 8663 HOSTS 978 LOADS

12.74%

OS	HITS	HOSTS	LOADS ↑	%
Windows 7	228122	81851	9227	12.50
Windows XP	107502	34616	5607	19.06
Windows Vista	88850	30063	4303	16.04
Windows 2003	538	105	27	27.55
Windows 2000	368	70	9	13.24
Windows NT	178	47	3	8.82
Windows 98	24	17	3	17.65
Linux	7773	1259	1	0.19
Mac OS	16845	2862	0	0.00

THREADS ↑	HITS	HOSTS	LOADS	%
default >	369	88	0	0.00
PT_DOR >	319647	40022	6927	25.47
PT_DIGITAL >	87724	79502	8088	10.18
NO >	7707	6590	2335	39.08

EXPLOITS

LOADS

% ↑

Java Rhino >	16144	83.36
PDF LIBTIFF >	1923	9.93
PDF ALL >	497	2.57
Java OBE >	366	1.89
HCP >	225	1.16
FLASH >	124	0.64
MDAC >	87	0.45

BROWSERS ↓

HITS

HOSTS

LOADS

%

Chrome >	112654	18305	16	0.46
Firefox >	93164	39359	5490	13.97
MSIE >	217897	87742	13594	15.51
Mozilla >	1299	301	0	0.00
Opera >	2718	969	7	15.91
Safari >	22467	4301	6	0.79

COUNTRIES

HITS

HOSTS ↑

LOADS

%








Portugal	404183	117583	14949	14.19
Italy	34498	23705	1713	9.17
Norway	7703	6587	2335	39.08
United States	2353	224	0	0.00
Iceland	57	37	0	0.00
Poland	152	20	0	0.00
Netherlands	38	14	0	0.00

EXPLOITS

LOADS

% ↑



 Java Rhino >	16144	83.36	<div><div></div></div>
 PDF LIBTIFF >	1923	9.93	<div><div></div></div>
 PDF ALL >	497	2.57	<div><div></div></div>
 Java OBE >	366	1.89	<div><div></div></div>
 HCP >	225	1.16	<div><div></div></div>
 FLASH >	124	0.64	<div><div></div></div>
 MDAC >	87	0.45	<div><div></div></div>



OBS !

IP: [REDACTED]
Location: Sweden, [REDACTED]
IPS: [REDACTED]

Din dator är låst - för ett eller flera skäl som anges nedan.

Du har brutit mot lagen "om upphovsrätt och närstående rättigheter" (Video, Musik, Software) eftersom du har olagligt använt och / eller distribuerat innehåll som skyddat för upphovsrätt och därmed du har brutit mot **§128 Straffrätt Sverige**.

§128 Straffrätt Sverige föreskriver ett straff **från 2 till 500 gånger** minimilönen eller fängelse från **2 till 8 år**.

Du har tittat eller distribuerat ett pornografiskt innehåll som är förbjudet (**Child Porno / Zoofilia och etc**). Det är ett brott mot **§202 Straffrätt Sverige**.

§ 202 Straffrätt Sverige föreskriver fängelse för en period av **4 till 12 år**.
Från din dator gjordes en olaglig tillgång till uppgifter eller du

§208 Straffrätt Sverige föreskriver ett straff till **100.000€** eller fängelse för en period av **från 4 till 9 år**.

Eftersom från din dator gjordes olagligt tillträde utan din vetskap, är det möjligt att din dator blev infekterad med skadlig programvara. Det heter också att du bryter mot lagen om "En försummelse att använda en dator."

§210 Straffrätt Sverige föreskriver ett straff **från 2000€ till 8000€**.

Eftersom från din dator (också om utan din vetskap) gjordes spam - sendning eller andra olagliga verksamheter med mål att göra en vinst, är det möjligt att din dator blev infekterad med skadlig programvara.

Videoinspelning

PÅ



Kod:

Summan:

 500 kr

1	2	3	4	5	6	7	8	9	0
---	---	---	---	---	---	---	---	---	---

Ersätta Ukash

Var kan jag köpa en Ukash?

Du kan få Ukash från hundratusentals globala platser, på nätet, från plånböcker, från kiosker och uttagsautomater.



195.189.227.227/US/



Computer Crime & Intellectual Property Section United States Department of Justice

USA.gov

Attention!

This operating system is locked due to the violation of the federal laws of the United States of America! Following violations were detected:

Your IP address is "193.110.109.30". This IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

Your details:

IP:193.110.109.30

Location: Finland, Helsinki
ISP: F-Secure OYj

To unlock the computer you are obliged to pay a fine of \$ 100.

You must pay the forfeit through Paysafecard:

To do this, you should enter the 16 digits resulting code (if necessary with a password) in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

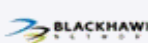
If an error occurs, send the codes to address
surcharge@cyber-usa-police.gov.

 **paysafecard**
pay cash. pay safe.

Where can I buy Paysafecard?

Paysafecard is available from 350,000 sales outlets worldwide, in the United States from IPP, epay, precash and blackhawk outlets.

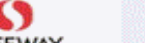
 **payXchange**

 **BLACKHAWK**

 **epay**

 **VONS**

 **Tom Thumb**

 **ShopRite**

 **SAFEWAY**

 **King Kullen**

 **PRICE RITE**

 **Dominick's**

 **Randalls**

 **PRE CASH**

 **GENUARDIS**

OK

83.233.180/24 (Relakks)



RELAKKS

Protect yourself and your family against surveillance. Simply preserve your integrity online with a hidden IP-number via proxy and VPN-encryption.

[THE SERVICE](#)[SIGN UP](#)[FAQ](#)[ABOUT US](#)[LOG IN](#)

How it works

The Service consists of an encrypted VPN tunnel between your computer and RELAKKS. The IP-number you receive from your existing ISP is only used to connect your computer to RELAKKS, from there on RELAKKS substitute your existing IP-number with a new IP-number from RELAKKS. This gives you a number of advantages:

- Your existing ISP will not be able to intercept and track your applications or communication
- Your existing ISP can not limit what you can do nor limit what information you can access
- Other organizations or individuals can't intercept or track your applications or communication.

"For Swedish authorities to force RELAKKS to hand over traffic data including your RELAKKS IP at a specific point in time, they will have to prove a case with the minimum sentence of two years imprisonment.

Regarding inquiries from other parties than Swedish authorities RELAKKS will never hand over any kind of information"



Ring0 bundle (Zerokit) for control million-strong botnet

Goto page 1, 2, 3, 4 Next

Post Reply

darkode.com Forum Index » Projects

[View previous topic](#)

[View next topic](#)

Ring0 bundle (Zerokit) for control million-strong botnet

Author

Message

ring0

✱ Ring0 bundle (Zerokit) for control million-strong botnet

QUOTE

I want to introduce new crazy **ring0 bundle (Zerokit or Okit)** for control million-strong botnet.

Breaking down **all** nowadays-existing firewall with **full network blocking** (bypassing in ring0).

Existence of the bundle is **not detected** by any of the antiviruses (the list <http://www.matousec.com/projects/proactive-security-challenge/results.php>), antirootkit-utilities (Tuluka, GMER, RKU, RootkitRevealer) also see nothing.

Features:

- Start of *.exe, *.dll (*.dll is in a pre-alpha stage) and shellcodes in a context of the chosen process.
- Start of files from a disk and from the memory* (start from memory is in a pre-alpha stage).
- Start of files with specified privileges: CurrentUser and NT SYSTEM/AUTHORITY.
- Granting the protected storehouse** for off-site (your) ring3-solutions for permanent existence in the system without need of crypt.
- Survivability of the bundle, down to a reinstallation of the system.
- All the components are stored outside of a file system and are invisible to OS.

Joined: 21 May 2011

Posts: 12

Rep: 1752





Hactivists



SONY®

GeoHot / George Hotz
Comex / Nicholas Allegra





**DON'T WORRY
WE'RE FROM
THE INTERNET**



Browse

ANONYMOUS: #OpPirateBay

AnonymousWorldOps



Subscribe

49 videos



Lataa video



Like



Add to

Share



31,860



Published on Oct 1, 2012 by AnonymousWorldOps

Greetings SWEDEN!

189 likes, 21 dislikes



PASTEBIN

Follow @pastebin



create new paste



trending pastes



Volvo Targeted - #OpPirateBay + #Op

BY: A GUEST ON SEP 4TH, 2012 | SYNTAX: NONE | SIZE:

[DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#)



1.

Volvo Login

2.

3.

4. 1. <http://login.trucks.volvo.com/tpreset.as>

5. 2. <http://asci.srv.volvo.com/>

6. 3. <http://www.tech.volvo.com/std/login.jsp>

7. 4. <http://brctan097.rds.volvo.com/>

8. 5. <https://www.volvocenews.volvo.com/en/use>

9. 6. <https://ideaprod4.srv.volvo.com/idea.use>

10. 7. <http://munktellmuseet.volvo.com/login.ht>

11. 8. <http://web.volvo.com/welcome/login.swf>

12. 9. <http://segotn2208.rds.volvo.com/login/>

13. 10. <http://mmi.volvo.com/CustSpec/VolvoCE/1>

TO OUR FELLOW ANONS, /B/ROS AND INTERNET
IT HAS COME TO OUR ATTENTION THAT SWEDISH GOVERNMENT
HAVE **RAIDED** PRQ SERVERS IN ORDER TO SHUT DOWN NUMEROUS
FILE SHARING AND TORRENT WEBSITES **THIS HAS**
THIS IS UNACCEPTABLE ANONYMOUS **GONE TO FAR!**
SAYS STOP TO THIS NOW
ON FRIDAY THE

5TH OCTOBER
14:30 CET
WE ARE DOING
OUR BIGGEST OP
IN OUR HISTORY



IRC:

WEBCHAT.VOXANON.ORG
#OPPIRATEBAY

TOGETHER WE CAN **STOP**
INTERNET **CENSORSHIP**



Mikko Hyppönen

@mikko

Web server dies as thousands of journalists around the world try to access sweden.se at the same time to see if it's under attack.

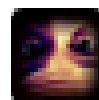
← Reply 🗑 Delete ★ Favorite

85

RETWEETS

16

FAVORITES





Mikko Hyppönen

@mikko

Note: DDoS attacks against the websites of the police, army, government, parliament etc are NOT attacks against 'critical infrastructure'.

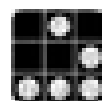
← Reply 🗑 Delete ★ Favorite

85

RETWEETS

18

FAVORITES





Governmental attacks

00	00	00	00	ieopera.exe...
00	00	00	00	ieexplore.exe...
25	64	2E	25	firefox.exe.%d.%
19	94	96	94	d.%d.%d.I♥☐↓öüö
15	81	93	1F	<ôâ*h<¿§.↓ öΘEüô▼
14	55	4D	4D	⌵î¼;ô§2ô.....DUMM
19	43	50	21	Y!DUMMY.SYS!ICP!
2D	72	32	64	94062...C3PO-r2d
54	00	00	00	2-POE...%s %d...
54	20	48	54	CONNECT %s=%d HT
FF	FF	FF	FF	TP/1.0.....
74	6F	6E	2E	TTntRadioButton.
00	00	00	00	U...1.01

[c:\virus\zapftis\fsav . /archive
F-Secure Anti-Virus Command Line Scanner, version 9.20.15330
Scans files and system for malware
Copyright © 2001-2009, F-Secure Corporation

Results of virus scanning:

C:\virus\zapftis\scuinst\scscuints.exe_ Infection: Backdoor:W32/R2D2.A

Scanned

Files: 28

Not scanned: 0

Result

Viruses: 1

Time: 00:10

[c:\virus\zapftis]■

جنگ سایبری

نگاه به مهمترین حملات سایبری در جهان

نبرد مجازی، یا جنگ سایبری، به نوعی از نبرد اطلاق می گردد که طرفین جنگ در آن از رایانه و شبکه های رایانه ای به عنوان ابزار استفاده می کنند جنگ اطلاعاتی یا انقلاب اطلاعات ظهور پیدا کرده است. این انقلاب به دلیل دامنه وسیع و تاثیرات گسترده آن می تواند سبک نوینی از جنگ را ارائه بدهد.



شنود یا Interception

در این روش نفوذگر به شکل مخفیانه از اطلاعات نسخه برداری می کند.

تغییر اطلاعات یا Modification

در این روش نفوذگر به دستکاری و تغییر اطلاعات می پردازد.

افزودن اطلاعات یا Fabrication

در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می کند.

وقفه یا Interruption

در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می شود.

White hat hackers

هکرای کلاه سفید یا هکر خوب، متخصصین شبکه هستند که چاله های امنیتی شبکه را پیدا می کنند

Black hat hackers

هکرای کلاه سیاه اشخاصی هستند که با وارد شدن به شبکه و دستبرد اطلاعات یا جاسوسی کردن، سوءاستفاده می کنند

Gray hat hackers

هکرای کلاه خاکستری حد وسط دو تعریف بالا می باشند

Pink hat hackers

هکرای کلاه صورتی افراد کم سواد هستند که با چند نرم افزار خرابکارانه به آزار و اذیت دیگران می پردازند

نام حمله، STUXNET
تاریخ، ۲۰۰۹ - ۲۰۱۰
هدف، سیستم های صنعتی
آسیب، ویروسی شدن چند رایانه، اختلال در فعالیت
نیروگاه هسته ای

رژیم
صهیونیستی

گرجستان

علت، جنگ اوستیای جنوبی
تاریخ، ۲۰۰۸
آسیب، وب سایت دولت گرجستان
برای چندین ساعت غیر فعال شد

استونی

یابود جنگ شوروی، علت
و انتخاب تالین به عنوان پایتخت
تاریخ، ۲۰۰۷
وب سایت دولت، بانک ها و روزنامه ها، آسیب
برای چندین ساعت غیر فعال شد

روسیه

حمایت دولتی
دور از ذهن
پدید
پذیرفتنی
محتل
قطعی

نوآندمی
کم
متوسط
زیاد



نام حمله، AURORA
تاریخ، ۲۰۰۹
فعالان حقوق بشر چینی، هدف
پایگاه فناوری مستقر در آمریکا
سرقت رمز عبور کاربران گوگل، آسیب
به خطر افتادن ایمیل فعالان

نام حمله، BYZANTINE CANDOR
تاریخ، ۲۰۰۲-۲۰۰۹
هدف، نیروی های نظامی و سازمان های
دولتی آمریکا
آسیب، سرقت بخش زیادی از اطلاعات حساس



نام حمله، GHOSTNET
تاریخ، ۲۰۰۷-۲۰۰۹
سفارتخانه های بسیاری از کشورها نظیر آمریکا، هدف
دفتر تبعیدیان ثبت
نامعلوم، نفوذ به رایانه کاربران، آسیب

نام حمله، Shadow in the cloud
تاریخ، ۲۰۰۹-۲۰۱۰
هدف، دفاتر دولتی هند و ثبت، دفتر سازمان ملل
آسیب، تبعیدیان ثبت و مکاتبات
محرمانه دولت هند به خطر افتاد



نام حمله، WIKILEAKS TAKE DOWN
تاریخ، ۲۰۱۰
علت، انتشار اسناد محرمانه
آسیب، قطعی مکرر سایت
غیر فعال کردن دامنه سایت





ATIC ET 2005

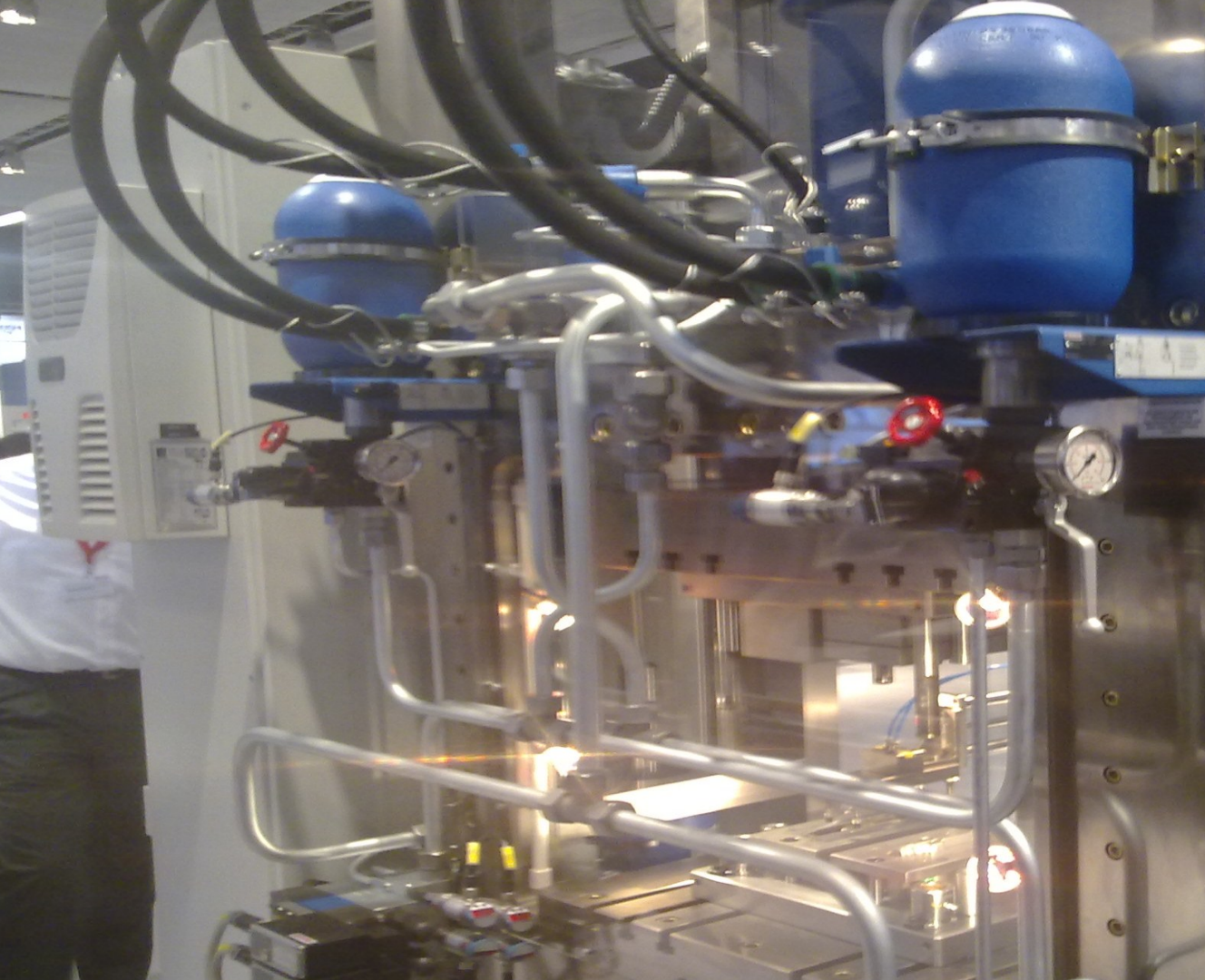
S7-400
7-3
443-1 adv.





esser – überall.







Turbine Bldg

Electrical Bldg

A
Boushehr
Nuclear
Power Plant
نیروگاه اتمی بوشهر

Emergency
Feedwater Bldg

Auxiliary
Bldg

Ventilation
Chimney

Solid
Waste Bldg

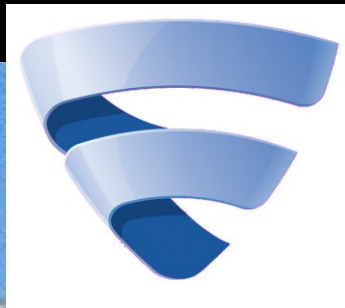
Flame







State Of The Net



Internetdagarna
Mikko Hyppönen
CRO
F-Secure



twitter.com/mikko