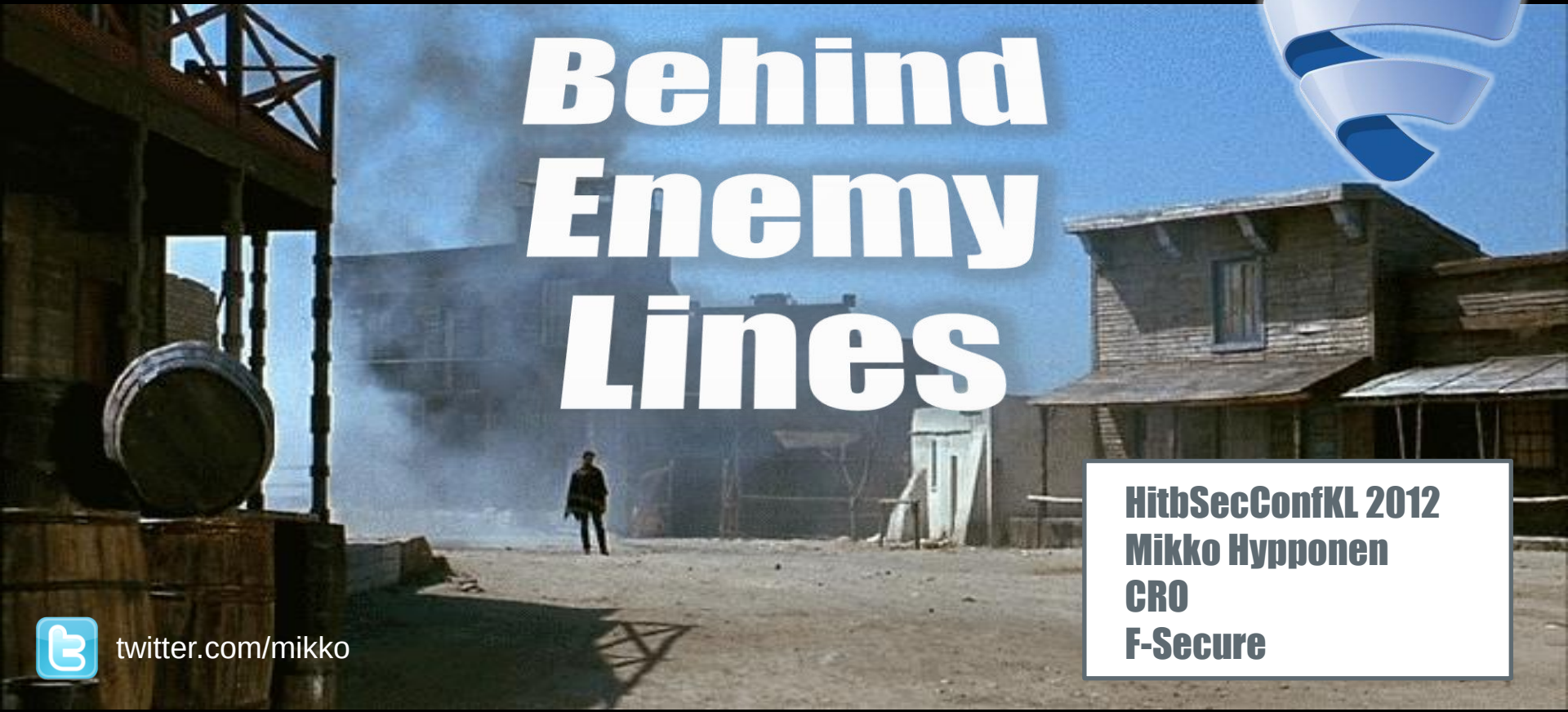


HitbSecConfKL 2012
Mikko Hypponen
CRO
F-Secure

twitter.com/mikko


htc

The Three Main Sources of Cyber Attacks

Criminals

Hactivists

Governments

F-Secure.

Criminals

F-Secure


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, Karjamaa küla

AADRESS	AADRESS	AADRESS
Kuremarja alajaam	Kuremarja tee 8	Kuremarja tee 2
Biopuhasti	Kuremarja tee 6	Kuremarja tee 1
Kuremarja tee 12	Kuremarja tee 4	Võgana Pluss
Kuremarja tee 10	Kuremarja tee 3	

Peipsi järv

Jõgevamaa, Palamuse vald, Ehavere küla

AADRESS
Põdralaane

Tartumaa, Luunja vald

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

Tartu linn

AADRESS
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

Tartumaa, Tähtvere vald, Tähtvere küla

AADRESS
Meika
Tõllu

Tartu

Võrts-järv

Tartu maakond, Haaslava vald, Haaslava küla

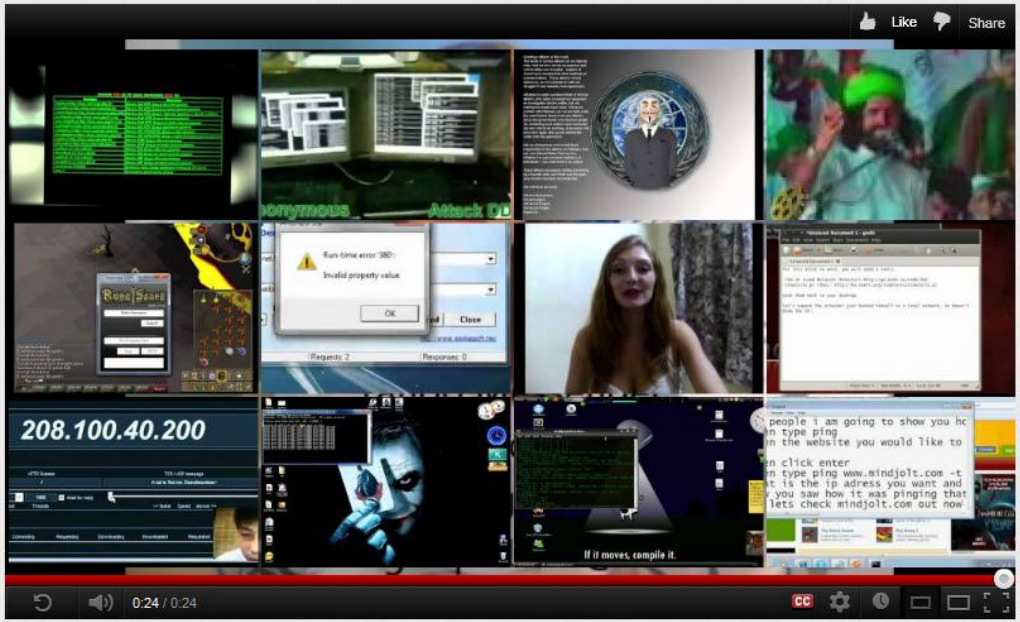
AADRESS	AADRESS	AADRESS	AADRESS

YouTube

Browse | Upload

Gwapo's Professional DDOS Service (Take down websites for long term)

Gwapologist | Subscribe | 4 videos



Lataa video

Like | Share

16,778

456 likes, 110 dislikes

As Seen On:

Uploaded by Gwapologist on Jan 4, 2012

Service Website : http://www.ddosservice.org/

Email Us : gwapo@hackforums.net

DDoS Attack Tools
by ArborNetworks
7,774 views

How To DDOS Runescape by
by CrisizRS
10,134 views

How to do a DOS attack using LOIC
by renzadude
41,490 views

Anonymous DDos Attack
by KHOFACHpaltalk
65,870 views

How to Ddos IP or URL (BEST WAY)
by DomTheChosenOne
25,517 views

How to make a Ping of Death attack.
by bobbyprculovski
59,821 views

Gwapo's Professional DDOS Se × | Gwapo's Professional DDOS Se ×

www.youtube.com/watch?v=ySdaJbgO5gc

YouTube | Browse | Upload

Gwapo's Professional DDOS Service (Take down websites for long term)

Gwapologist | Subscribe | 4 videos

Uploaded by Gwapologist on Jan 4, 2012

Service Website : http://www.ddosservice.org/

Email Us : gwapo@hackforums.net

456 likes, 110 dislikes

As Seen On:

DDoS Attack Tools
by ArborNetworks
7,774 views

How To DDOS Runescape by
by CrisizRS
10,134 views

How to do a DOS attack using LOIC
by renzadude
41,490 views

Anonymous DDos Attack
by KHOFACHpaltalk
65,870 views

How to Ddos IP or URL (BEST WAY)
by DomTheChosenOne
25,517 views

How to make a Ping of Death attack.
by bobbyprculovski
59,821 views

Start date: End date: Apply Autoupdate interval: **10 sec.**

STATISTIC

TOTAL INFO

450216 HITED **148233** HOSTS **18997** LOADS **14.61%** LOADS

TODAY INFO

21899 HITED **8663** HOSTS **978** LOADS **12.74%** LOADS

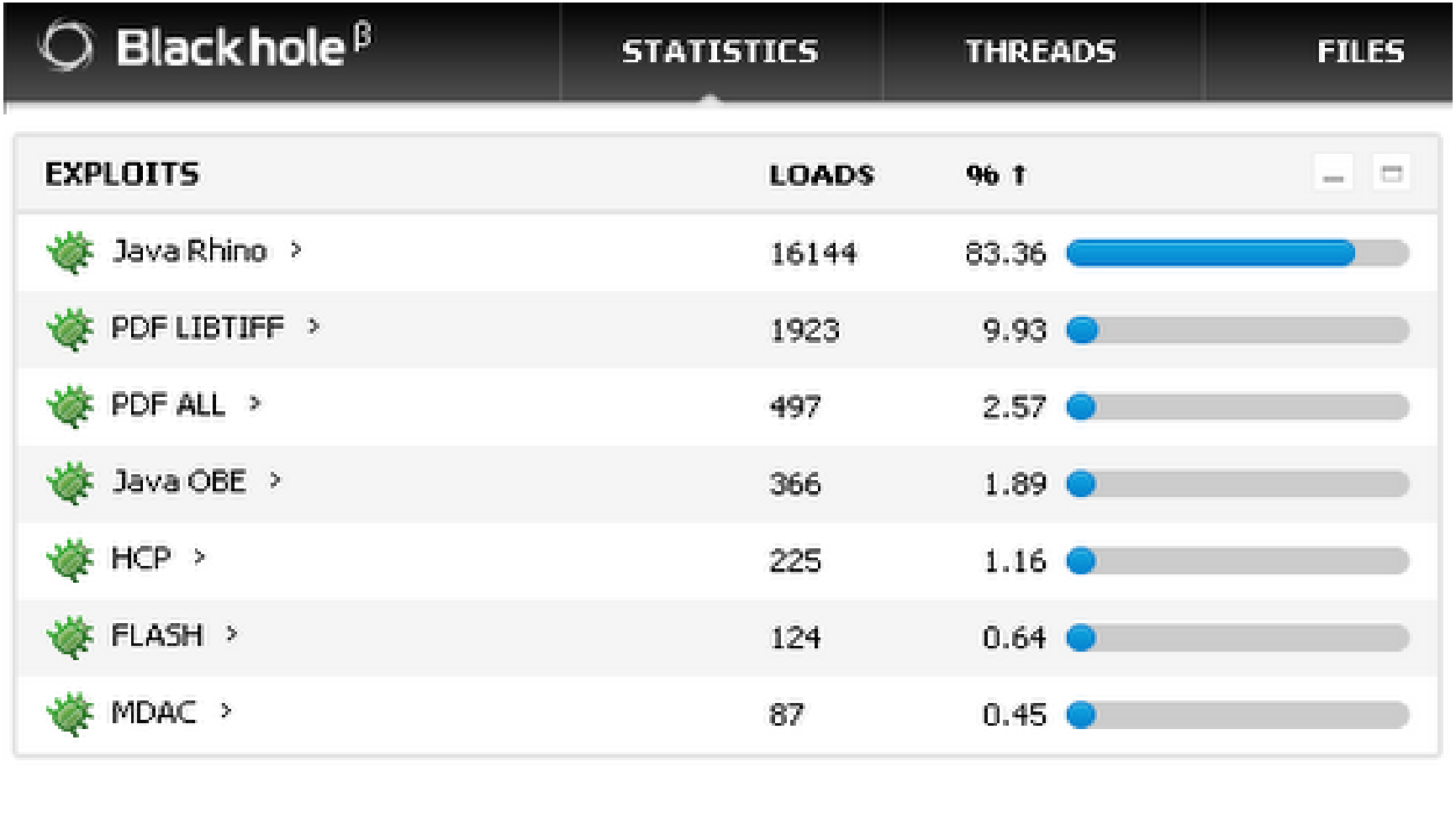
OS	HITS	HOSTS	LOADS ↑	%
Windows 7	228122	81851	9227	12.50
Windows XP	107502	34616	5607	19.06
Windows Vista	88850	30063	4303	16.04
Windows 2003	538	105	27	27.55
Windows 2000	368	70	9	13.24
Windows NT	178	47	3	8.82
Windows 98	24	17	3	17.65
Linux	7773	1259	1	0.19
Mac OS	16845	2862	0	0.00

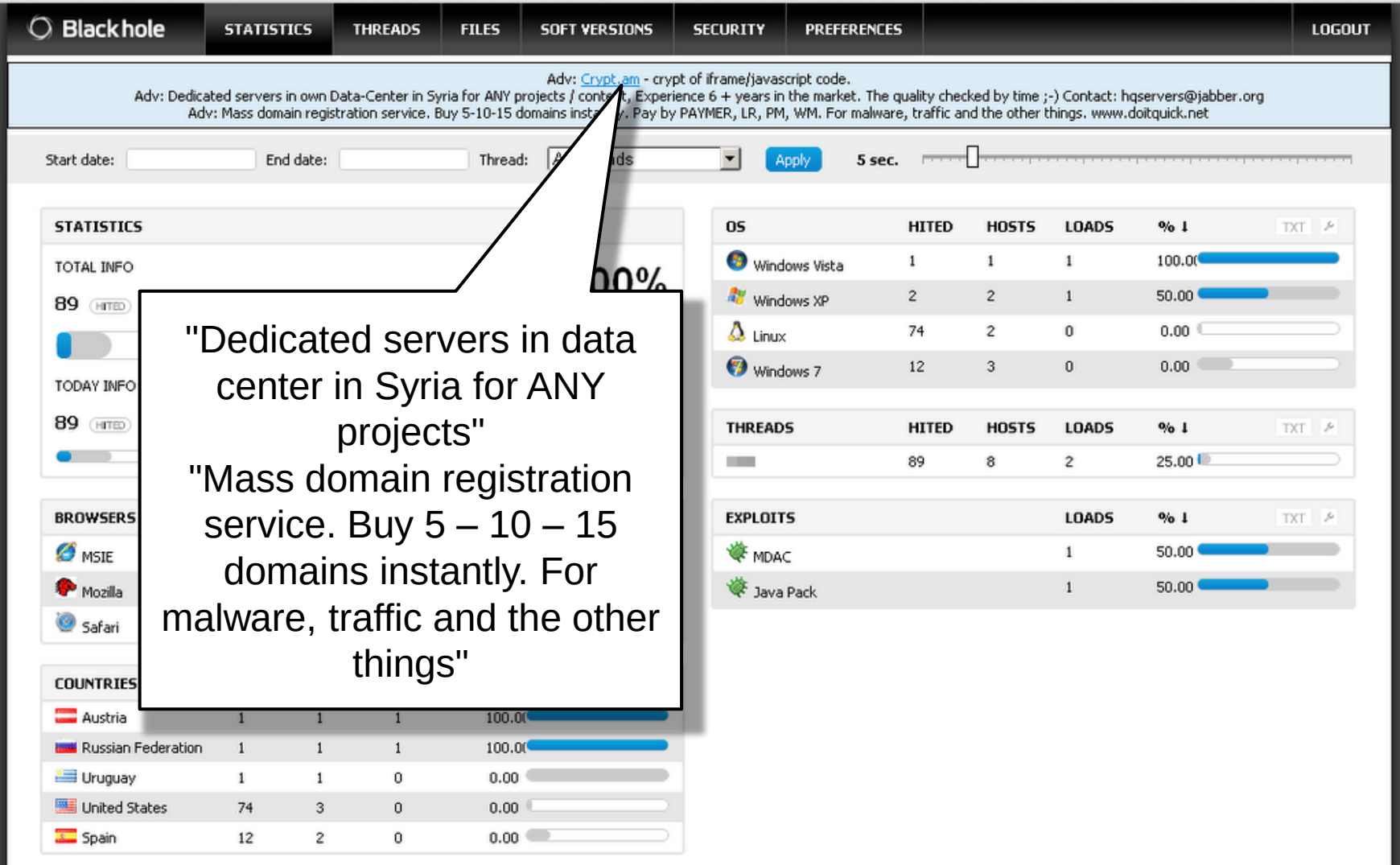
THREADS ↑	HITS	HOSTS	LOADS	%
default ›	369	88	0	0.00
PT_DOR ›	319647	40022	6927	25.47
PT_DIGITAL ›	87724	79502	8088	10.18
NO ›	7707	6590	2335	39.08

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


Blackhole β
STATISTICS
THREADS
FILES
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


Blackhole
STATISTICS
THREADS
FILES
SOFT VERSIONS
SECURITY
PREFERENCES
LOGOUT
Adv: Crypt.am - crypt of iframe/javascript code.
Adv: Dedicated servers in own Data-Center in Syria for ANY projects / content, Experience 6 + years in the market. The quality checked by time ;-) Contact: hqservers@jabber.org
Adv: Mass domain registration service. Buy 5-10-15 domains instantly. Pay by PAYMER, LR, PM, WM. For malware, traffic and the other things. www.doitquick.net
Start date:
End date:
Thread:
Apply
5 sec.
STATISTICS
TOTAL INFO
89 HITED
TODAY INFO
89 HITED
BROWSERS
MSIE
Mozilla
Safari
COUNTRIES
Austria 1 1 1 100.0
Russian Federation 1 1 1 100.0
Uruguay 1 1 0 0.00
United States 74 3 0 0.00
Spain 12 2 0 0.00
OS HITED HOSTS LOADS % ↓ TXT
Windows Vista 1 1 1 100.0
Windows XP 2 2 1 50.00
Linux 74 2 0 0.00
Windows 7 12 3 0 0.00
THREADS HITED HOSTS LOADS % ↓ TXT
89 8 2 25.00
EXPLOITS LOADS % ↓ TXT
MDAC 1 50.00
Java Pack 1 50.00
"Dedicated servers in data center in Syria for ANY projects"
"Mass domain registration service. Buy 5 – 10 – 15 domains instantly. For malware, traffic and the other things"

195.189.22 × 195.189.22 × 195.189.22 × 195.189.22 × 195.189.22 × 195.189.22 × 195.189.22 × 195.189.22 × 195.189.22 × 195.189.22 × 195.189.22 × 195.189.22 ×

195.189.227.227/DE/

BUNDESPOLIZEI

NATIONAL CYBER CRIMES UNIT

ACHTUNG!!!

Achtung!!!

Das Betriebssystem wurde im Zusammenhang mit Verstoßen gegen die Gesetze der Bundesrepublik Deutschland gesperrt!

Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet "**193.110.109.30**" mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen
Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

IP:193.110.109.30
Location: Finland, Helsinki
ISP: F-Secure OYj

Um die Sperre des Computers aufzuheben, sind Sie dazu verflichtet eine Strafe von 100 Euro zu zahlen.

Die Zahlung per Ukash begleichen:

Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK).

Solte das System Fehler melden, so müssen Sie den Code per Email einzahlung@inter-bundeskriminalamt.eu versenden.

Ukash Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich beifolgenden Tankstellen: Agip, Avia, Esso, OMV, Ql und Westfalen.

AVIA Agip Esso OMV Q1 Westfalen

Epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call- Shops, in denen Sie dieses Logo sehen.

epay

OK

Polizia di Stato

Polizia postale e delle comunicazioni

Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

C.N.A.I.P.I.C

Attenzione!!!

È stata rivelata un'attività illegale. Il sistema operativo è stata bloccata per una violenza delle leggi della Repubblica Italiana!

È stata fissata una seguente violazione: Dal tuo indirizzo IP "193.110.109.30" era eseguito un accesso alle web-pagine contenenti la pornografia, la pornografia minorile, zoofilia, nonché la violenza dei bambini. Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile.

Dalla posta elettronica era effettuato anche la distribuzione dello spam con un senso recondito terroristico.
Il bloccaggio di computer serve per troncare l'attività illegale dalla parte tua.

I tuoi dati:	**IP:193.110.109.30** Posizione: Finland, Helsinki ISP: F-Secure OYj

Per togliere il bloccaggio devi pagare una multa di 100 euro.

Effettuare il pagamento tramite l'Ukash.

Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK)

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica deposito@cyber-gdf.net.

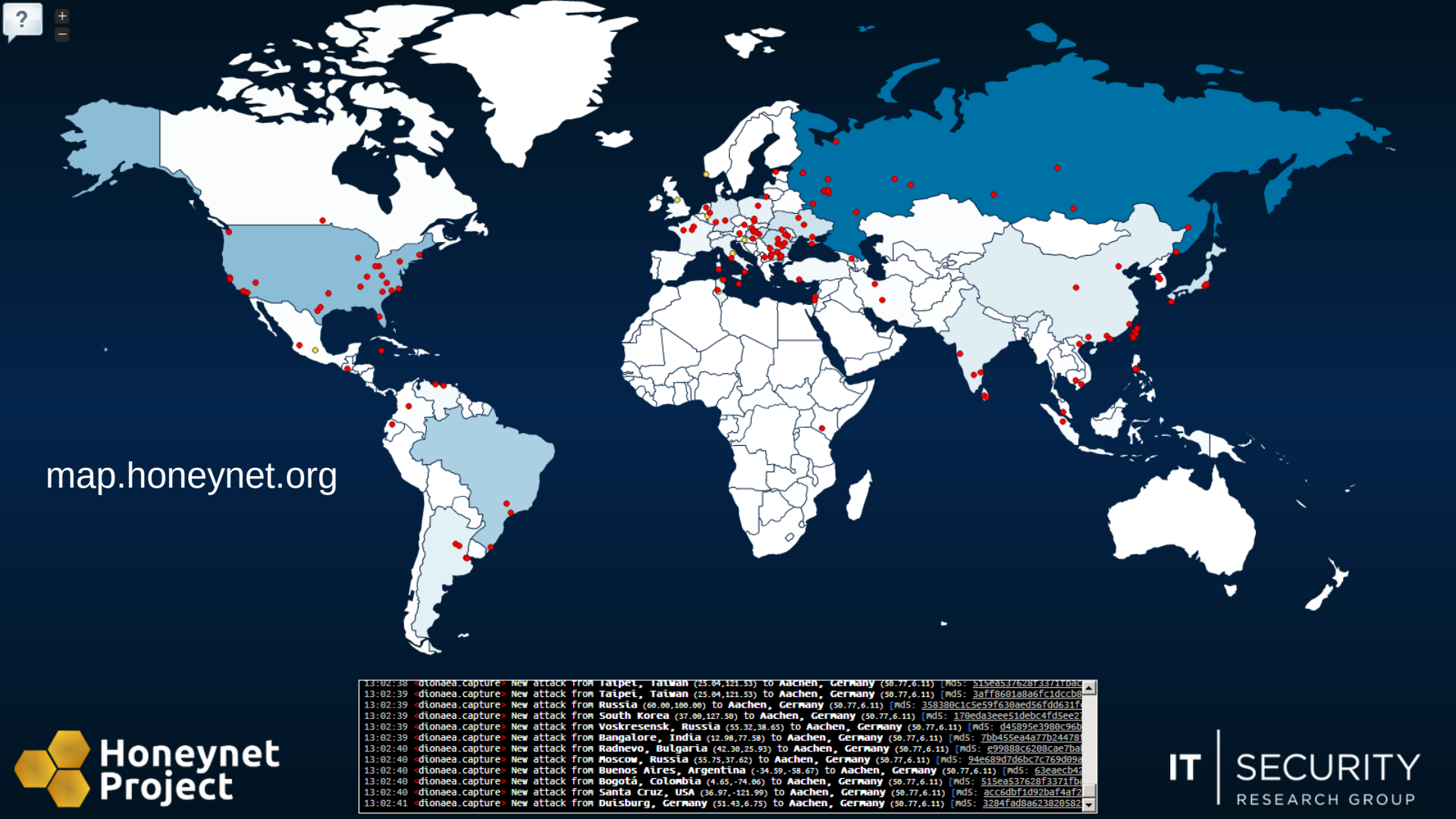
Ukash Dove passo trovare Ukash?

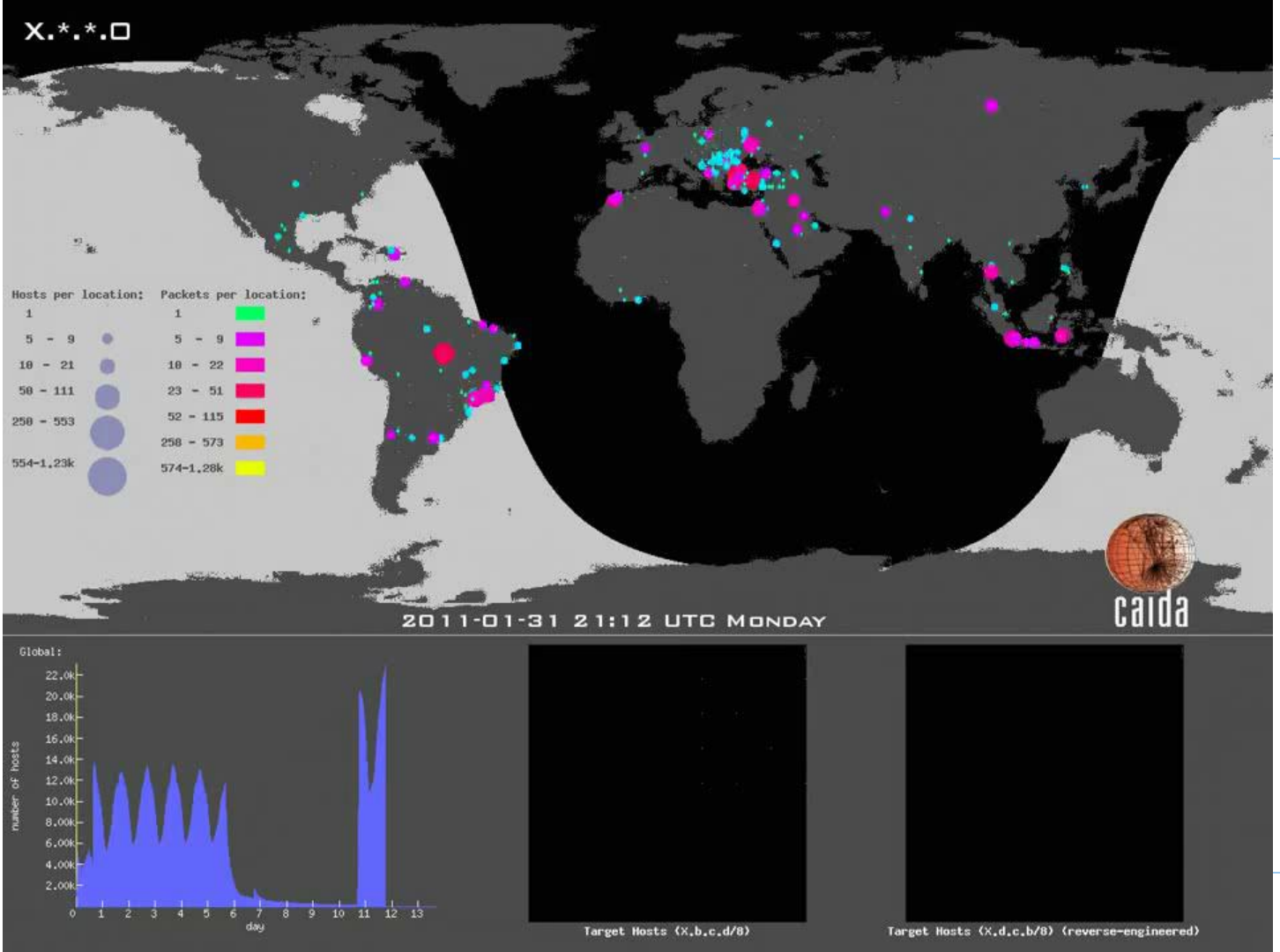
Puoi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, stazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di terminale **Epay**, **Epipoli**.

Recati presso il punto vendita dotato di terminale **Epay**, **Epipoli** a te piu vicino. Richiedi un voucher in contanti al negoziante. Il negoziante dovra stampare e consegnarti un voucher Ukash con codice PIN da 19 cifre.

epay - Voucher Ukash sono disponibili da migliaia di negozi con un terminal epay.
Epipoli - Voucher Ukash sono disponibili da migliaia di negozi con un terminal Epipoli.

OK


map.honeynet.org
13:02:38 <dionaea.capture> New attack from Taipei, Taiwan (25.04,121.53) to Aachen, Germany (50.77,6.11) [md5: 515ea537628f3371fba
13:02:39 <dionaea.capture> New attack from Taipei, Taiwan (25.04,121.53) to Aachen, Germany (50.77,6.11) [md5: 3aff8601a8a6fc1dccb8
13:02:39 <dionaea.capture> New attack from Russia (60.00,100.00) to Aachen, Germany (50.77,6.11) [md5: 358380c1c5e59f630aed56fdd631f
13:02:39 <dionaea.capture> New attack from South Korea (37.00,127.50) to Aachen, Germany (50.77,6.11) [md5: 170eda3eee51debc4fd5ee27
13:02:39 <dionaea.capture> New attack from Voskresensk, Russia (55.32,38.65) to Aachen, Germany (50.77,6.11) [md5: d45895e3980c96b
13:02:39 <dionaea.capture> New attack from Bangalore, India (12.98,77.58) to Aachen, Germany (50.77,6.11) [md5: 7bb455ea4a77b244781
13:02:40 <dionaea.capture> New attack from Radnevo, Bulgaria (42.30,25.93) to Aachen, Germany (50.77,6.11) [md5: e99888c6208cae7ba
13:02:40 <dionaea.capture> New attack from Moscow, Russia (55.75,37.62) to Aachen, Germany (50.77,6.11) [md5: 94e689d7d6bc7c769d09a
13:02:40 <dionaea.capture> New attack from Buenos Aires, Argentina (-34.59,-58.67) to Aachen, Germany (50.77,6.11) [md5: 63eaecbb42
13:02:40 <dionaea.capture> New attack from Bogotá, Colombia (4.65,-74.06) to Aachen, Germany (50.77,6.11) [md5: 515ea537628f3371fba
13:02:40 <dionaea.capture> New attack from Santa Cruz, USA (36.97,-121.99) to Aachen, Germany (50.77,6.11) [md5: acc6dbf1d92baf4af2
13:02:41 <dionaea.capture> New attack from Duisburg, Germany (51.43,6.75) to Aachen, Germany (50.77,6.11) [md5: 3284fad8a623820582
Honeynet Project
IT SECURITY RESEARCH GROUP



Sality

Sipscan

F-Secure


Zeroaccess KML
file available from
F-Secure Weblog

Ring0 bundle (Zerokit) for control million-strong botnet

Ring0 bundle (Zerokit) for control million-strong botnet

Author	Message
ring0 Joined: 21 May 2011 Posts: 12 Rep: 1752	**Ring0 bundle (Zerokit) for control million-strong botnet** QUOTE I want to introduce new crazy **ring0 bundle** (**Zerokit** or **0kit**) 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 priveleges: 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. - Intuitively clear interface of admin-panel. - Protection against the abstraction of Admin Panel. - Impossibility of detection of the bundle in the working system by any of known AV/rootkit scanner, owing to the use of author's technologies of concealment. The unique opportunity of detection exists only at loading with livecd or scanning of a disk from the other computer. Thus the opportunity of detection is also extremely improbable, as own algorithms of a mutation are used. ** Start of a file from the memory allows to bypass all modern proactive protection and AV-scanners, that is, there is no necessity to crypt a file.* *** Protected storehouse is the original ciphered file system in which the certain quantity of files which will be started from the memory at each start of the OS can be stored.* The bundle consists of: - **Bootkit.** It is responsible for the start of the basic modules at a stage of loading of OS. - **Driver.** It is responsible for all infrastructure and implements componental business-logic on the basis of so-called mod (functional unit). That is, the driver is not a legacy driver (monolithic), and consists of the set of mods that allows to operate the bundle with maximum of flexibility, and to protect (hard to reverse), update and expand it. - **Dropper.** At the current moment it brake out all machines with the patches till January, 8th, 2011, except for XP x32/x64 where reloading is initiated. If the systems distinct from XP have latest updates reloading is initiated as well. - User friendly Admin Panel.

Case **cg4ng3dn5**

- 4 million home DSL routers in Braz il
- Huawei, ZyXel, D-Link, Linksys, Netgear…
- Cross Site Request Forgery (CSRF) to be performed in the administration panel of the ADSL modem
- Changing the DNS servers to malicious ones
- Some Brazilian ISPs had more than 50% of users affected

```
<body onLoad=javascript:document.form.submit()>
<form action="http://192.168.1.1/password.cgi";
  method="POST" name="form">
<input type="hidden" name="sptPassword" value="cg4ng3dn5">
<input type="hidden" name="usrPassword" value="cg4ng3dn5">
<input type="hidden" name="sysPassword" value="cg4ng3dn5">
</form>
</body>
```

CSRF

Achieving Together

EchoLife HG520b

- Status
- Basic
  - ADSL Mode
  - WAN Setting
  - LAN Setting
  - DHCP
  - NAT
  - IP Route
  - Wireless Lan
  - ATM Traffic
- Advanced
- Tools

DHCP

DHCP Settings	
DHCP	Server
Client IP Pool Starting Address	192.168.1.2
Size of Client IP Pool	253
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Remote DHCP Server	N/A
DHCP Lease Time	1 Days 0 Hours 0 Min

DHCP Table

Host Name	IP Address	MAC Address	Status
	192.168.1.5	Manual Config	Static
dell	192.168.1.2		Auto
Dell2	192.168.1.3		Auto
Dell2	192.168.1.4		Auto

Submit

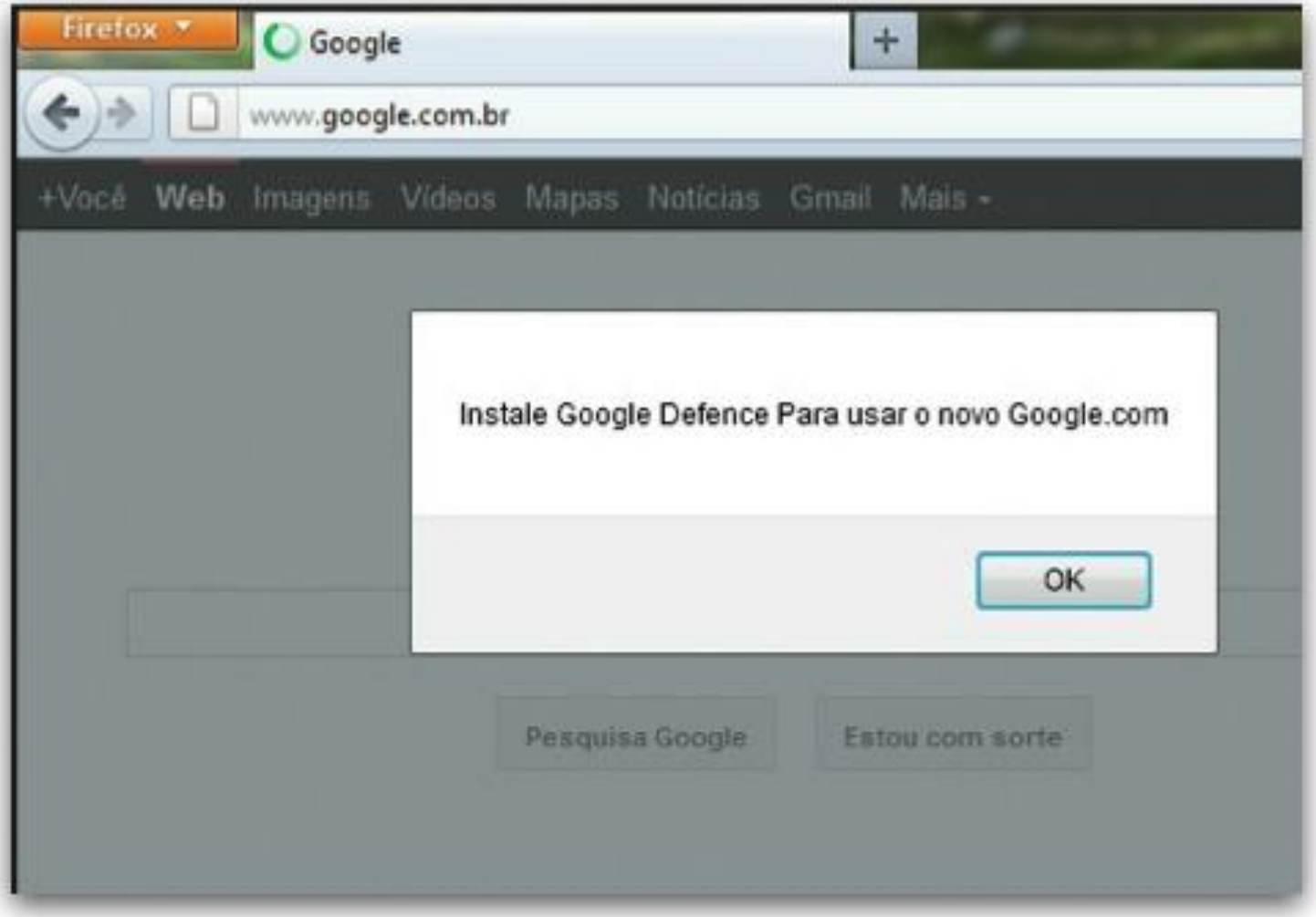


Image from Securelist.

- google.com/GoogleDefence.exe
- facebook.com/ChromeSetup.exe
- facebook.com/Activex_Components.exe
- msn.com/ChromeSetup.exe

5. Monitoring the integrity of files the bot.

- **Server-side bot functions:**

    1. Socks 4/4a/5 server with support for UDP and IPv6.
    2. Backconnect for any service (RDP, Socks, FTP, etc.) on the infected machine. I.e. may gain access to a computer that is behind a NAT, or, for example, which has prohibited connections by a firewall. For this feature to work there are used additional applications that run on any Windows-server on the Internet, which has a dedicated IP.
    3. Getting a screenshot of your desktop in real time.

- **Intercepting HTTP/HTTPS-requests from wininet.dll (Internet Explorer, Maxton, etc.), nspr4.dll (Mozilla Firefox) libraries:**

    1. Modification of the loaded pages content (HTTP-inject).
    2. Transparent pages redirect (HTTP-fake).
    3. Getting out of the page content the right pieces of data (for example the bank account balance).
    4. Temporary blocking HTTP-injects and HTTP-fakes.
    5. Temporary blocking access to a certain URL.
    6. Blocking logging requests for specific URL


Krypton
Texas Hold'em NL - $0.50/$1
Current hand: 665493614
Last hand:
Disconnection protection: 1
kohle74
$40.47
Wardancer
$117.30
kamikazi8
$204.63
Tay0
$37
Total pot: $46.50
2
10
A
A
8
$40
$6.50
fishermansam
$53.40
PoRTuAA
$148
Rrrappe
$98.45
capzio
$101.30
Suicidalistic
Stout ($85.40)
manekoAA
$163.40, Folded

Hactivists

IRC.ANONOPS.LI
#OPMALAYSIA
PORT: 6667

WEDNESDAY,
JUNE 15
7 : 30 PM
GMT

TARGET: HTTP://WWW.MALAYSIA.GOV.MY

OPERATION MALAYSIA

@anonymouSabu
The Real Sabu

@mikko Do you remember about 3 years ago - a bar named Baker's in downtown Helsinki? Summertime or so.

@mikko
Mikko Hypponen

@anonymouSabu ...no, I don't think I do.

GeoHot / George Hotz
Comex / Nicholas Allegra


DON'T WORRY
WE'RE FROM
THE INTERNET

Governmental attacks

```
00 00 00 00    iexplore.exe....
25 64 2E 25    firefox.exe.%d.%
19 94 96 94    d.%d.%d.I♥ô◘↓öûö
45 81 93 1F    (ôâ♦h(¿§.╢ö☻Eüô▼
44 55 4D 4D    ┘ï¾¡ô§2ô....DUMM
49 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.
```

```
[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]
```

sample.pdf - Adobe Reader

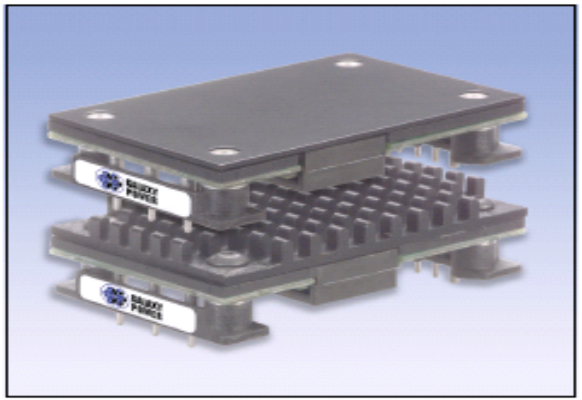
File Edit View Document Tools Window Help

1 / 7 73.3% Find

GALAXY POWER Incorporated

DORADO HV

High-efficiency DC/DC Converter
48V Input, 18V to 34VDC Output, 3A Output



The Dorado HV is also available with an optional low profile heatsink for improved thermal

- Suitable for Fan Motor Control
- Industry Standard Quarter Brick Pinout and Footprint
- Typical Efficiency: 87% at 3A, 34V
- Droop Feature Allows Current Sharing
- Very Low Common-mode Noise for a Commercial DC/DC Converter
- Two-stage Input Filter
- Constant Switching Frequency
- Remote Sense
- Single Board Design
- Optional Low Profile Heatsink for Improved Thermal Performance
- Header with M3 Metal Inserts for

جنگ سایبری

نگاهی به مهمترین حملات سایبری درجهان

نبرد مجازی، یا جنگ سایبری، به نوعی از نبرد اطلاق می‌گردد که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای به عنوان ابزار استفاده می کنندجنگ اطلاعاتی با انقلاب اطلاعات ظهور پیدا کرده‌است.این انقلاب به دلیل دامنه وسیع و تاثیرات گسترده آن می‌تواند سبک نوینی از جنگ را ارائه بدهد.

انواع نفوذگران

White hat hackers
هکرهای کلاه سفیدیا هکر خوب، متخصصین شبکه هستند که چاله‌های امنیتی شبکه را پیدا می کنند

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

Gray hat hackers
هکرهای کلاه خاکستری حد وسط دو تعریف بالا می باشند

Pink hat hackers
هکرهای کلاه صورتی افراد کم سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت دیگران می پردازند

انواع حملات

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 می‌پردازد.

افزودن اطلاعات یا Fabrication
در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند.

وقفه Interruption
در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.

ایران
نام حمله: STUXNET
تاریخ: ۲۰۰۹ - ۲۰۱۰
هدف: سیستم های صنعتی
آسیب: ویروسی شدن چند رایانه، اخلال 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
۲۰۰۷، تاریخ
وب سایت دولت ،بانک ها و روزنامه ها، آسیب
برای چندین ساعت غیر فعال شد

روسیه

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

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

هند
GHOSTNET، نام حمله
۲۰۰۹-۲۰۰۷، تاریخ
سفارتخانه های بسیاری از، هدف
کشور ها نظیر آمریکا،
دفتر تبعیدیان تبت
نامعلوم،نفوذ به رایانه کاربران، آسیب

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

چین

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

حمایت دولتی	توانمندی
دور از ذهن	کم
بعید	متوسط
پذیرفتنی	زیاد
محتمل	
قطعی	

طراحی از :
www.infographics.ir | کپی برداری تنها با ذکر منبع مجاز است

منبع : NewScientist


Nuclear physics lost it's innocence in 1945

Computer science lost it's innocence in 2009


Manzariyeh Airport
Baqerabad
1
2
3
4


Turbine Bldg
Electrical Bldg
A
Boushehr Nuclear Power Plant
نیروگاه اتمی بوشهر
Emergency Feedwater Bldg
Auxiliary Bldg
Ventilation Chimney
Solid Waste Bldg

J. of Nuclear Sci. and Tech.
No. 55, pp. 1-7, 2011

مجله علوم و فنون هسته‌ای
شماره ۵۵، صفحات ۷-۱، ۱۳۹۰

تأثیر باربرودتی سیستم خنک‌کننده بر روی عملکرد ماشین سانتریفوژ

مجید آقایی*[۱و۲]، سیدجابر صفدری[۱]، محمدحسن ملاح[۱]، جواد کریمی‌ثابت[۱]، محمد اتوکش[۲]

۱- پژوهشکده چرخه سوخت هسته‌ای، پژوهشگاه علوم و فنون هسته‌ای، سازمان انرژی اتمی ایران، صندوق پستی: ۸۴۸۶-۱۱۳۶۵، تهران - ایران

۲- دانشکده مهندسی انرژی، دانشگاه صنعتی شریف، صندوق پستی: ۱۱۳۶۵-۱۱۱۵۵، تهران - ایران

چکیده: در این مقاله اثر بار برودتی یک سیستم خنک‌کننده بر روی عملکرد ماشین سانتریفوژ مورد مطالعه قرار گرفته است. افزایش بار برودتی سیستم، از طریق تغییر دما و دبی حجمی آب ورودی انجام پذیرفته است. نتایج به دست آمده نشان می‌دهد که تأثیر افزایش بار برودتی از طریق کاهش دما یا افزایش دبی آب ورودی، بر روی واحد کار جداکنندگی (SWU)، ضرایب غنی‌سازی (α) و تهی‌سازی (β) جزیی است. در ضمن بار برودتی سیستم خنک‌کننده نباید از یک مقدار کمینه کم‌تر باشد چرا که عدم دفع گرمای تولیدی توسط مجموعه‌ی محرک ماشین سبب افزایش دمای قطعات مکانیکی و نهایتاً تخریب آن‌ها می‌گردد.

واژه‌های کلیدی: *ماشین سانتریفوژ، شیب دما، بار برودتی سیستم خنک‌کننده، غنی‌سازی اورانیم*

www.aeoi.org.ir/Portal/Home/

سازمان | فیلم و نشریات | خدمات | کتابخانه | تعامل با کاربران | سایر | ارتباط با سازمان

تاریخ و زمان

یکشنبه 1 مرداد 1391 04:19:46

نظرسنجی | اوقات شرعی

ماه رمضان ماه ضیافت الهی

آلبوم تصاویر

گزیده اخبار مجتمع‌هاي سوخت مجاري راكتور تحقيقاتي 40 مگاواتي اراك ساخته شد

رویدادها | اطلاعیه‌ها | اخبار هسته‌اي رسانه‌ها | فراخوان | مناقصه و مزایده

چهارشنبه 1391/4/28
اولین سالگرد شهید صنعت هسته‌ای، مهندس داریوش رضایی نژاد برگزار می‌گردد

چهارشنبه 1391/4/14
مسجد شهداي هسته اي سازمان انرژي اتمي ايران افتتاح شد

چهارشنبه 1391/4/14
اصلاحیه شماره 2/ کانون بازنشستگان سازمان انرژي اتمي دوره‌هاي آموزش حفاظت در برابر .اشعه برگزار می‌نماید

شنبه 1391/4/3

چهارشنبه 1391/5/11

واكنش عباسي به ادعاي حمله سايبري به تاسيسات هسته‌يي ايران

رييس سازمان انرژي اتمي انتشار خبري كه مدعي حمله سايبري به تاسيسات هسته‌يي ايران شده بود، را نادرست خواند.

به گزارش خبرنگار خبرگزاري دانشجويان ايران (ايسنا)، فريدون عباسي در حاشيه جلسه هيات دولت در پاسخ خبرنگاري كه به انتشار خبري در يكي از خبرگزاري‌هاي خارجي مبني بر حمله سايبري به تاسيسات هسته‌يي ايران و پخش موزيك اشاره كرد، گفت: آيا شما اين خبر را باور مي‌كنيد؟!

رييس سازمان انرژي اتمي در ادامه تصريح كرد: اگر شما اين خبر را باور نمي‌كنيد؛ بنابراين چنين چيزي نيست.

وي در مواجهه با سوالات خبرنگاران مبني بر اعلام خبري جديد از سازمان انرژي اتمي گفت: ما مشغول انجام كارهاي‌مان هستيم.

به گزارش خبرگزاري دانشجويان ايران (ايسنا)، خبرگزاري "نووستي" اوايل مرداد گزارش داد: ميكو هيپونن، مدير شركت ضد ويروس فنلاندي اف.سكيور(F-Secure) در وبلاگ اين شركت از تلاش براي حمله جديد سايبري به واحدهاي هسته‌يي ايران خبر داد. اين حمله دو سال پس از حمله با ويروس رايانه‌يي "استاكس نت" انجام گرفته است.

به ادعاي هيپونن، او از يك دانشمند ايراني كه در سازمان انرژي اتمي ايران كار كرده و نامش به دلايل امنيتي ذكر نمي شود، نامه‌اي دريافت كرده است كه در آن درباره حمله جديد سايبري به واحدهاي هسته‌يي ايران اطلاع داده مي‌شود .در اين نامه ادعا شده است كه دو سايت هسته‌يي ايران دوباره با ويروس رايانه‌يي مورد حمله قرار گرفته است .در اين نامه همچنين تاكيد شده كه در اين حمله از ابزار موسوم به" Metasploit Framework " استفاده شده است كه اغلب توسط مهاجمان به كار برده مي‌شود.

ميكو هيپونن مدعي شد كه هنوز هيچ يك از حقايق ذكر شده در اين نامه مورد تاييد قرار نگرفته ولي ثابت شده است كه اين نامه از طريق شبكه سازمان انرژي اتمي ايران ارسال شده بود.

منبع: ايسنا

نسخه قابل چاپ
نظر بدهيد
RSS | بيشتر

Gauss encryption

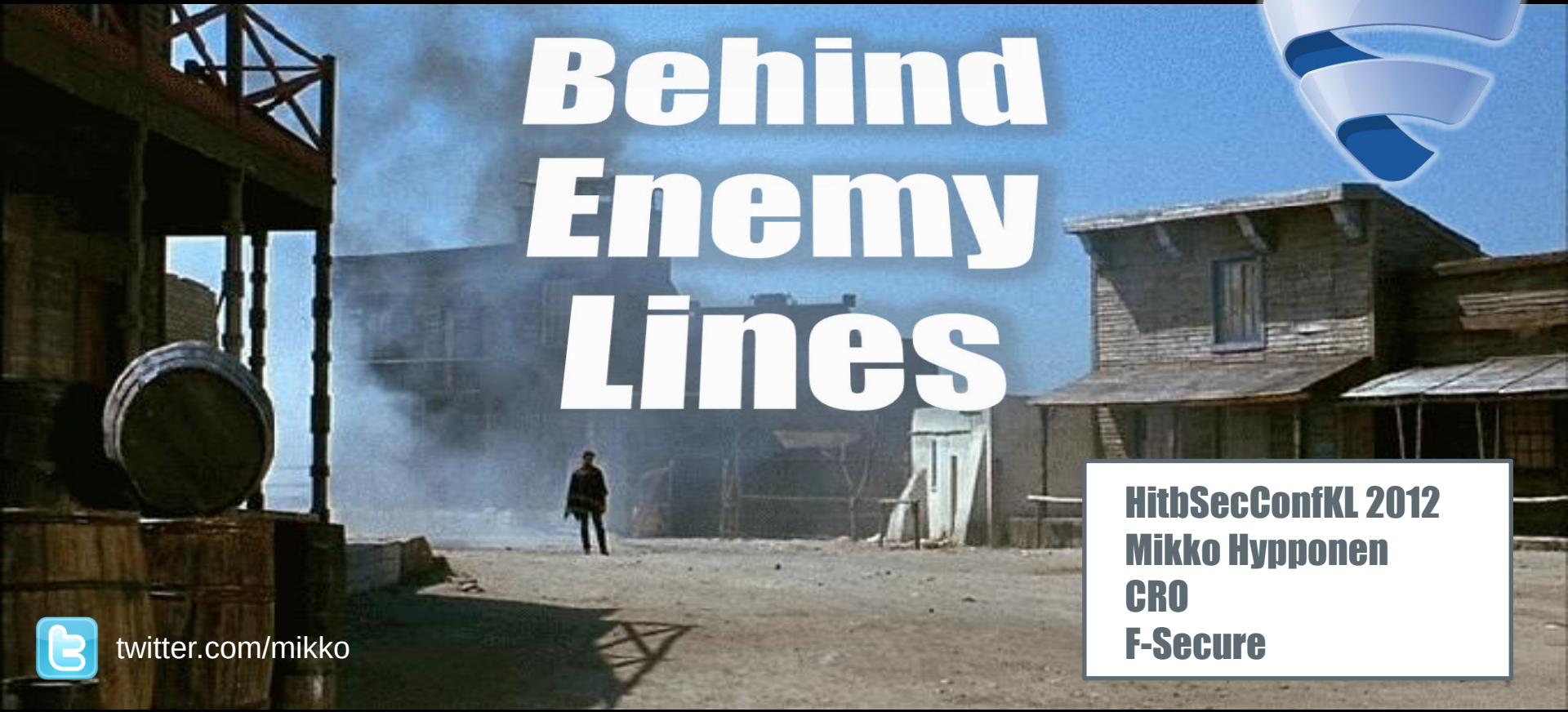
```
mov             ecx, (LENGTHOF tToCrypt)-1
mov             edx, OFFSET tToCrypt
mov             ebx, OFFSET tEncrypt
L1:
    mov                     eax, [edx]
    XOR                     eax, ACDCh
    not                     eax

    mov                     [ebx], eax
    inc                     edx

    inc                     EBX


LOOP L1

mov             edx, OFFSET tOutEncr
call            WriteString
mov             edx, OFFSET tEncrypt
call            WriteString
call            Crlf
ret
```



HitbSecConfKL 2012
Mikko Hypponen
CRO
F-Secure

twitter.com/mikko