The Trojan Money Spinner

Mika Ståhlberg, F-Secure Corporation

VB2007 Conference, Vienna

F-SECURE®

BE SURE.

What is a Banking Trojan?

- **Targets bank account transactions and information** (credentials etc.)
  - “Phishing Trojans"
  - Subcategory of Crimeware

Banker

Bancos

Haxdoor (aka A-311 Death)

Sinowal (aka Torpig aka Anserin)

Nuklus (aka Apophis)

Bzub (aka Metafisher)

Snatch

Sters (aka Briz aka VisualBreeze)

Gozi

Banking Trojan Problem

- The machine has been infected already
    - Exploits
    - Social engineering: Spam attachments
- User does not necessarily do anything wrong
    - Trojan waits until the user goes to bank
    - Can user education help?

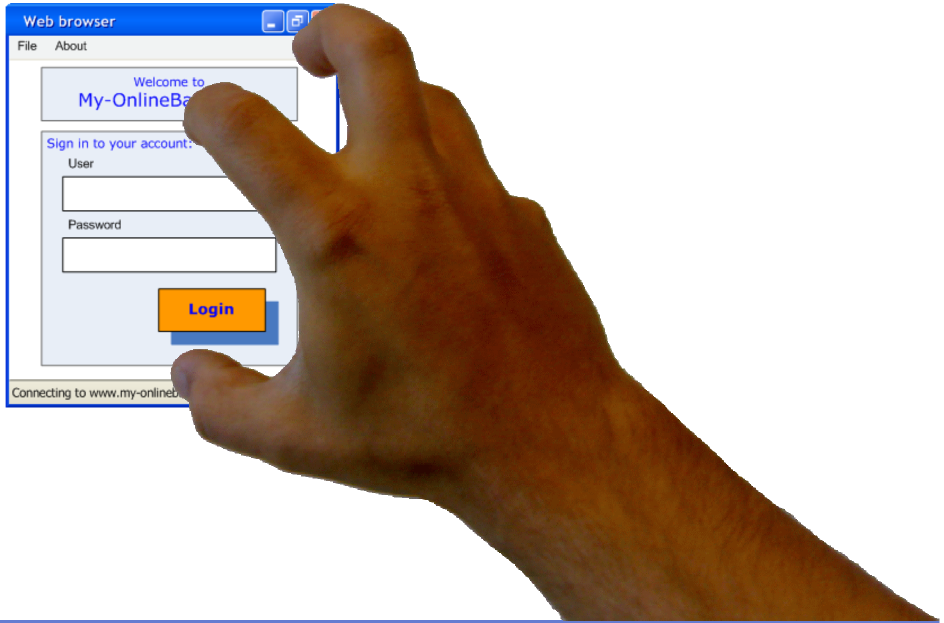
Attacking the Session

- Spying of Credentials - Attacks Used
  - Key logging
  - Local content injection
  - Form grabbing
  - Screen capture
  - Video capture
  - Fake website (pharming)
  - Man-in-the-Middle (dns changers)
  - Man-in-the-Browser

- Hijacking Sessions
  - Man-in-the-Middle (network, injection of data)
  - Man-in-the-Browser

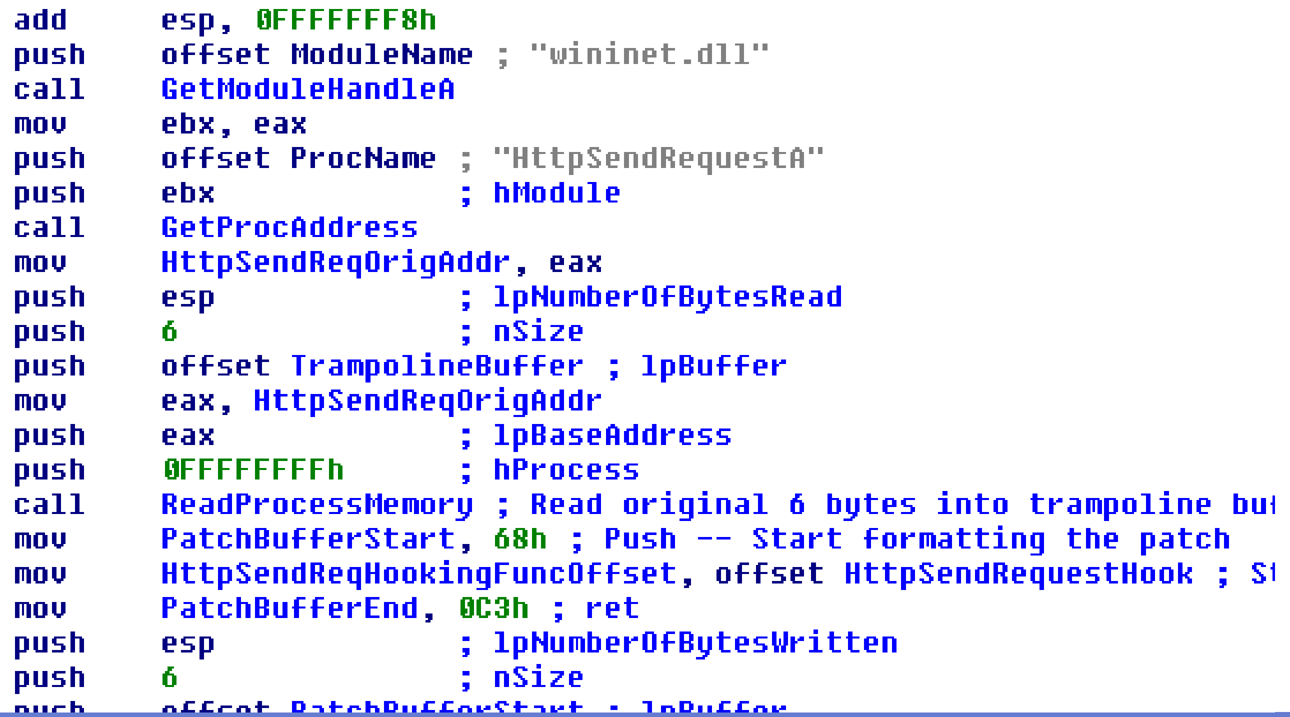
Form Grabbing

- User submits data to a legitimate banking website using web forms
- Malware monitoring the web browser can grab that data
- Form grabbing is the method of choice for capturing banking data
  - All credentials typically end up in a web form
  - Keylogging would result in a lot of useless data



Example:
Form Grabbing Using Inline Hooking

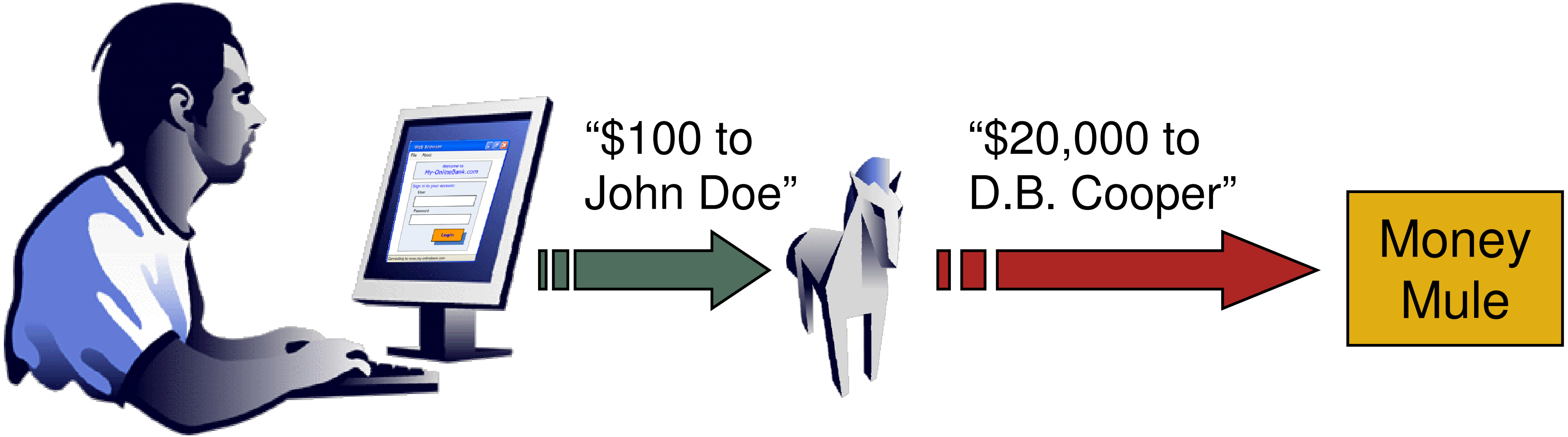
- Qhost.JE injects a DLL into Internet Explorer
- The DLL hooks HttpSendRequestA
- The hook grabs POST data and uploads it to an FTP server



```
add     esp, 0FFFFFFF8h
push    offset ModuleName ; "wininet.dll"
call    GetModuleHandleA
mov     ebx, eax
push    offset ProcName ; "HttpSendRequestA"
push    ebx             ; hModule
call    GetProcAddress
mov     HttpSendReqOrigAddr, eax
push    esp             ; lpNumberOfBytesRead
push    6               ; nSize
push    offset TrampolineBuffer ; lpBuffer
mov     eax, HttpSendReqOrigAddr
push    eax             ; lpBaseAddress
push    0FFFFFFFFh      ; hProcess
call    ReadProcessMemory ; Read original 6 bytes into trampoline bu
mov     PatchBufferStart, 68h ; Push -- Start formatting the patch
mov     HttpSendReqHookingFuncOffset, offset HttpSendRequestHook ; S
mov     PatchBufferEnd, 0C3h ; ret
push    esp             ; lpNumberOfBytesWritten
push    6               ; nSize
push    offset PatchBufferStart ; lpBuffer
```

Local Session Riding

- Browser is a trusted terminal of the online bank
    - Not maintained by the bank
- Many banks only check the credentials of the terminal on entry
- A MitB attack can hijack the authenticated session
    - Transactions can be added or modified

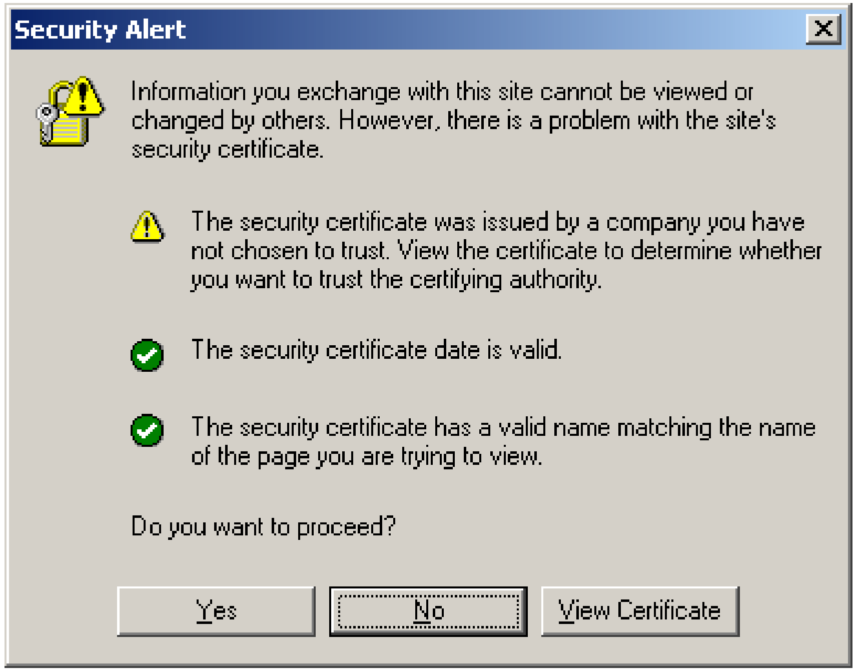

“$100 to John Doe”

“$20,000 to D.B. Cooper”

Money Mule

Pharming with Trojans

- Browser can be tricked into accessing a malicious web server
  - Hosts file poisoning
  - Hooking
- Browser will still display the correct URL
- SSL will not help
- Malware can suppress dialogs
  - Import own root certificate
  - Hook, patch
  - User imitation



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Filtering Data

- Banking trojans target data related to online banking
- Only a small fraction of web form data or typed data is relevant
    - Information glut ensues (S/N)
- Attackers are typically only interested in certain banks
    - Familiar, local banks (Brazil)
    - Lowest hanging fruit
    - Banks with a large customer base

Banking trojans are only interested in banking data; and only in a small portion of that data.

How do Banking Trojans Filter Data?

- Online banks are accessed using web browsers
- Trojan monitors browsing and activates when browser is connected to a bank

Window title enumeration using FindWindow()

BHO or Firefox Browser Extension

LSP (Layered Service Provider)

DDE (Dynamic Data Exchange) using WWW_GetWindowInfo topic

OLE (Object Linking and Embedding) using IWebBrowser2

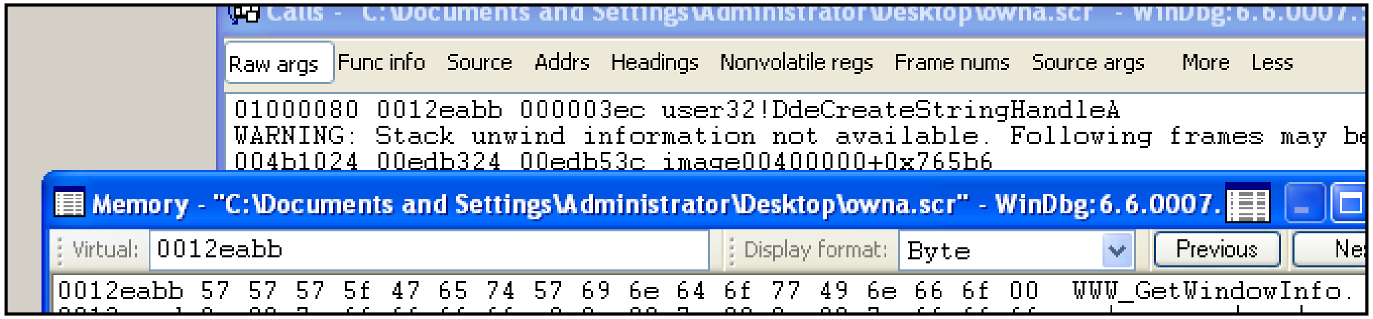
Hooking (e.g. WinInet HttpSendRequest)

Example: Detecting the start of a banking session using DDE

Banker.CJM uses DdeConnect() with topic “WWW_GetWindowInfo” to query current Browser location from “iexplore”

```
mov     [esp+24h+var_24], 24h
mov     [esp+24h+var_18], 3ECh
push    esp              ; pCC (context)
push    ebp              ; hszTopic (WWW_WindowInfo)
push    edi              ; hszService (dde string handle, name of app)
mov     eax, dword_4B8FD8
mov     eax, [eax+44h]
push    eax              ; idInst (instance id received from DdeInitialize)
call    DdeConnect
mov     ebx, eax
```

Topic:



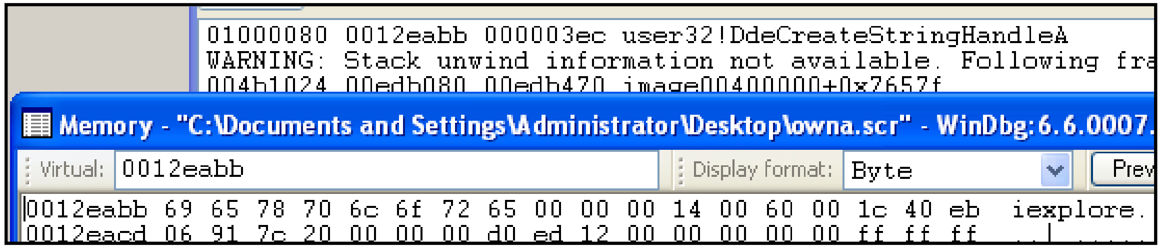
```
01000080 0012eabb 000003ec user32!DdeCreateStringHandleA
WARNING: Stack unwind information not available. Following frames may be
004b1024 00edb324 00edb53c image00400000+0x765b6
```

Memory - "C:\Documents and Settings\Administrator\Desktop\owna.scr" - WinDbg:6.6.0007.

Virtual: 0012eabb   Display format: Byte

```
0012eabb 57 57 57 5f 47 65 74 57 69 6e 64 6f 77 49 6e 66 6f 00  WWW_GetWindowInfo.
```

Service:



```
01000080 0012eabb 000003ec user32!DdeCreateStringHandleA
WARNING: Stack unwind information not available. Following fra
004b1024 00edb080 00edb470 image00400000+0x7657f
```

Memory - "C:\Documents and Settings\Administrator\Desktop\owna.scr" - WinDbg:6.6.0007.

Virtual: 0012eabb   Display format: Byte

```
0012eabb 69 65 78 70 6c 6f 72 65 00 00 00 14 00 60 00 1c 40 eb  iexplore.
0012eacd 06 91 7c 20 00 00 00 d0 ed 12 00 00 00 00 00 ff ff ff  ..|
```

Analyzing Banking Trojans

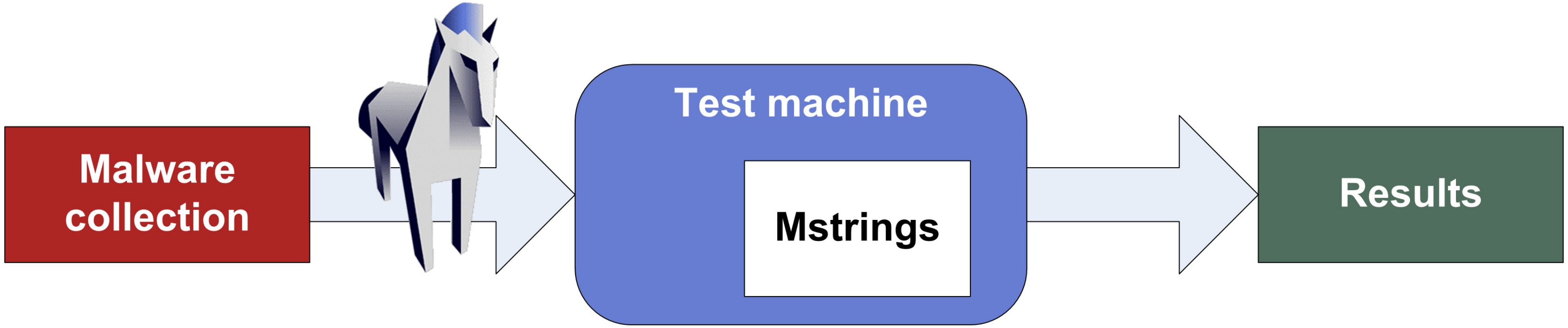
1. Banking trojans filter out data
2. Trojans detect bank sites by URLs, Windows title string and other “banking strings”
3. Strings in the binary or downloaded from web
4. Filter list is typically cleartext in memory

➔ Banking trojans contain banking URLs in one form or another

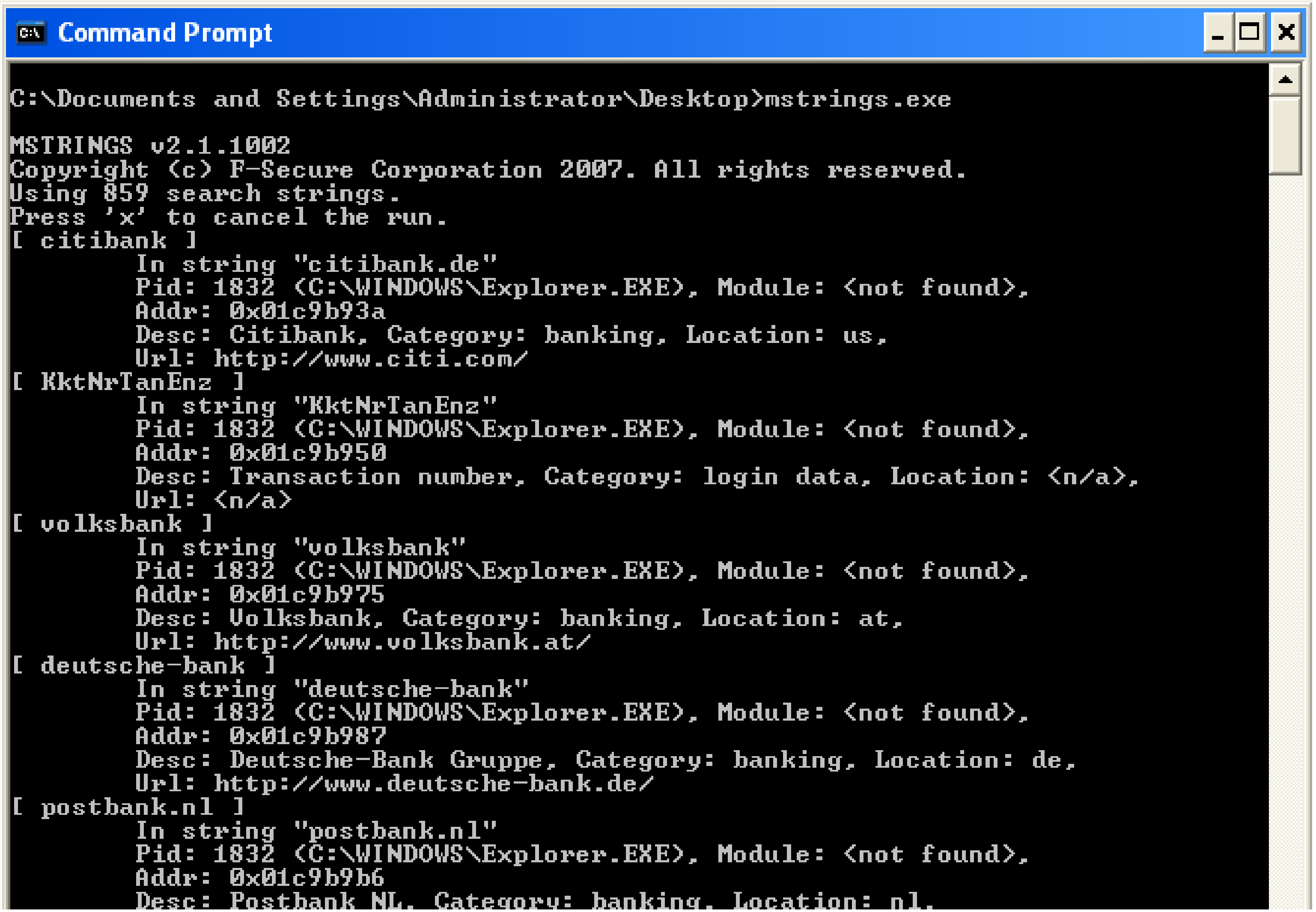
➔ Analysis and categorization of banking trojans can be improved by looking for banking strings

Mstrings

- F-Secure in-house lab tool for analyzing banking trojans
- Searches memory for known banking strings
- Features:
  - Scans both user-mode and kernel memory
  - Can automatically decrypt basic forms of encryption/obfuscation
  - Has an updatable database with white listing



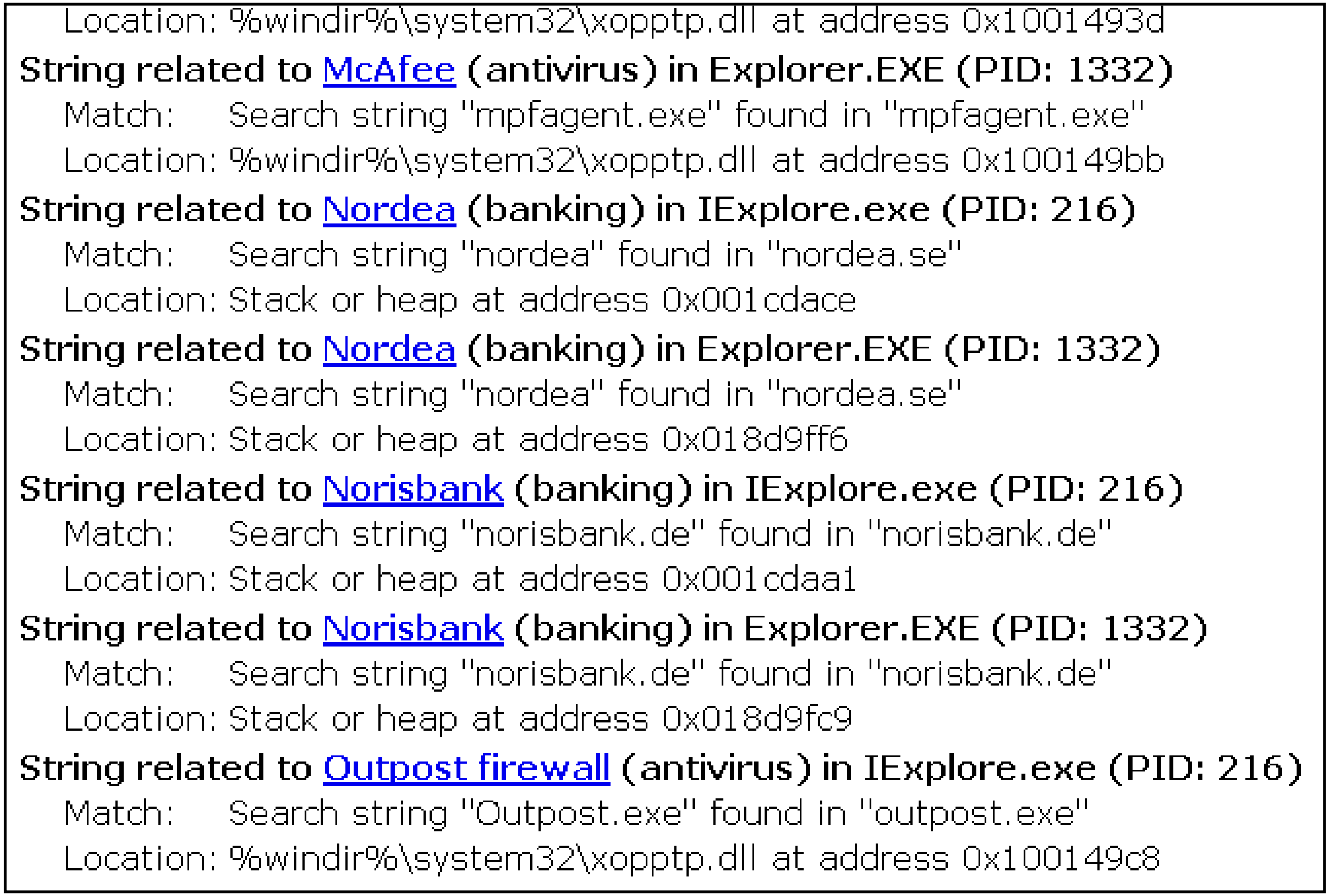
Mstrings vs. Haxdoor.KI



```
C:\Documents and Settings\Administrator\Desktop>mstrings.exe

MSTRINGS v2.1.1002
Copyright (c) F-Secure Corporation 2007. All rights reserved.
Using 859 search strings.
Press 'x' to cancel the run.
[ citibank ]
        In string "citibank.de"
        Pid: 1832 (C:\WINDOWS\Explorer.EXE), Module: <not found>,
        Addr: 0x01c9b93a
        Desc: Citibank, Category: banking, Location: us,
        Url: http://www.citi.com/
[ KktNrTanEnz ]
        In string "KktNrTanEnz"
        Pid: 1832 (C:\WINDOWS\Explorer.EXE), Module: <not found>,
        Addr: 0x01c9b950
        Desc: Transaction number, Category: login data, Location: <n/a>,
        Url: <n/a>
[ volksbank ]
        In string "volksbank"
        Pid: 1832 (C:\WINDOWS\Explorer.EXE), Module: <not found>,
        Addr: 0x01c9b975
        Desc: Volksbank, Category: banking, Location: at,
        Url: http://www.volksbank.at/
[ deutsche-bank ]
        In string "deutsche-bank"
        Pid: 1832 (C:\WINDOWS\Explorer.EXE), Module: <not found>,
        Addr: 0x01c9b987
        Desc: Deutsche-Bank Gruppe, Category: banking, Location: de,
        Url: http://www.deutsche-bank.de/
[ postbank.nl ]
        In string "postbank.nl"
        Pid: 1832 (C:\WINDOWS\Explorer.EXE), Module: <not found>,
        Addr: 0x01c9b9b6
        Desc: Postbank NL, Category: banking, Location: nl,
```

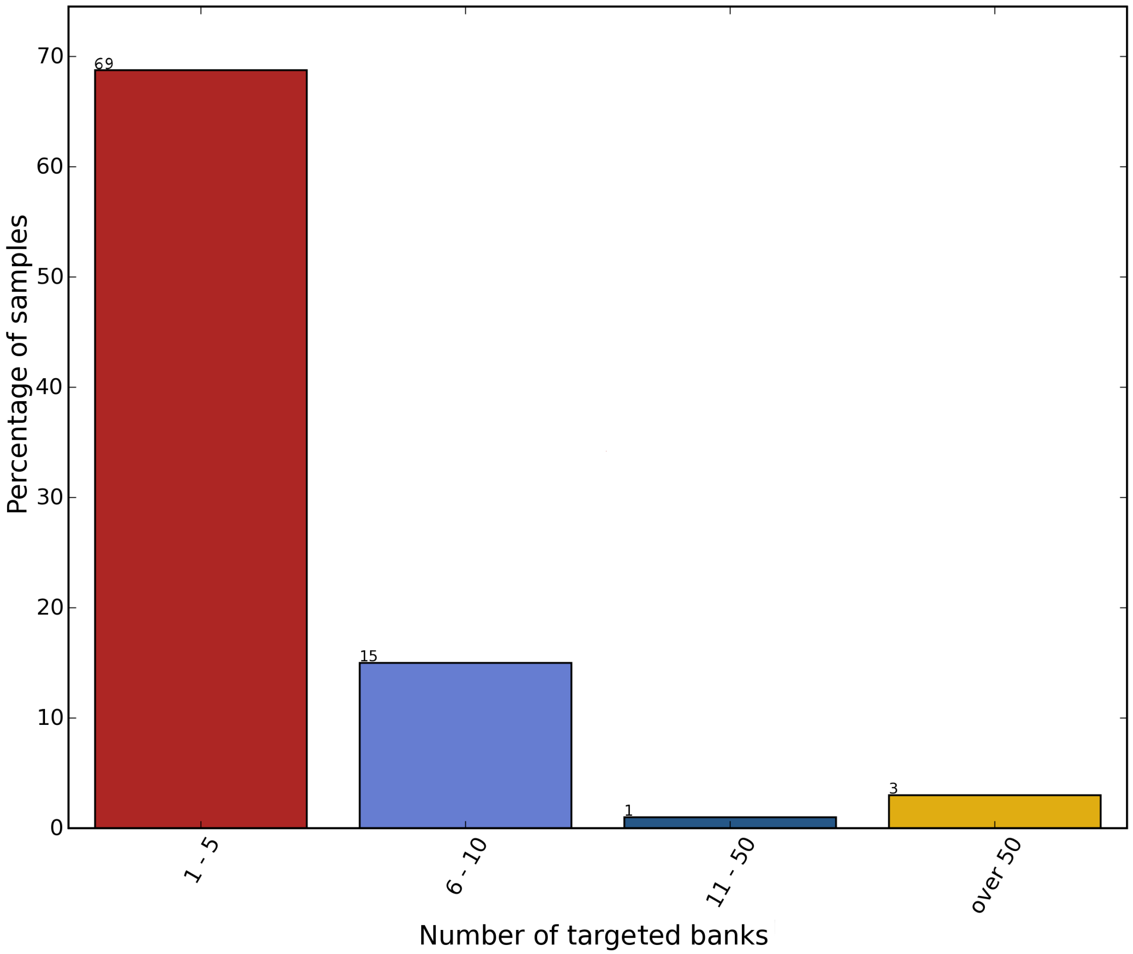
Mstrings vs. Haxdoor.KI

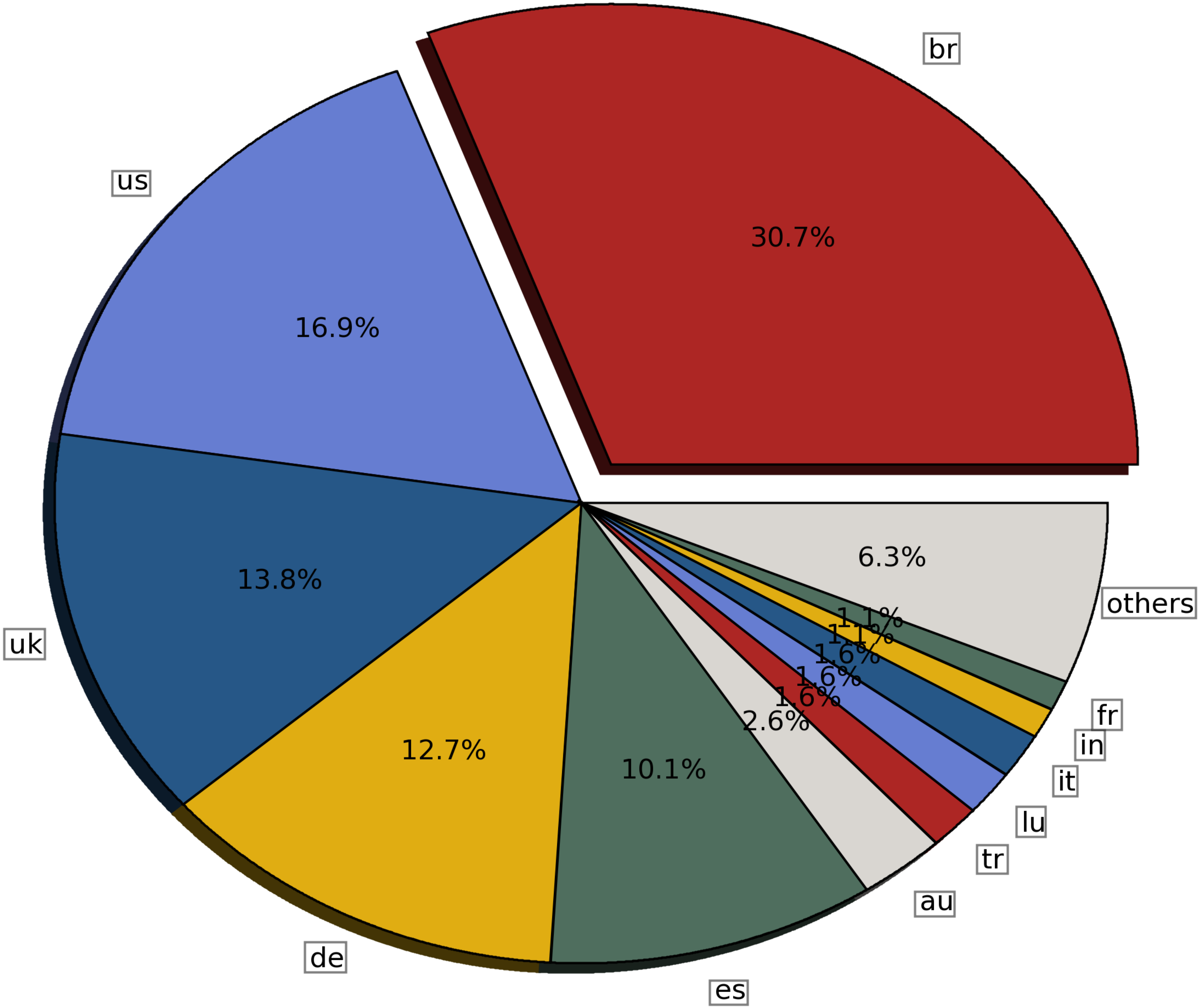


```
    Location: %windir%\system32\xopptp.dll at address 0x1001493d
String related to McAfee (antivirus) in Explorer.EXE (PID: 1332)
    Match:    Search string "mpfagent.exe" found in "mpfagent.exe"
    Location: %windir%\system32\xopptp.dll at address 0x100149bb
String related to Nordea (banking) in IExplore.exe (PID: 216)
    Match:    Search string "nordea" found in "nordea.se"
    Location: Stack or heap at address 0x001cdace
String related to Nordea (banking) in Explorer.EXE (PID: 1332)
    Match:    Search string "nordea" found in "nordea.se"
    Location: Stack or heap at address 0x018d9ff6
String related to Norisbank (banking) in IExplore.exe (PID: 216)
    Match:    Search string "norisbank.de" found in "norisbank.de"
    Location: Stack or heap at address 0x001cdaa1
String related to Norisbank (banking) in Explorer.EXE (PID: 1332)
    Match:    Search string "norisbank.de" found in "norisbank.de"
    Location: Stack or heap at address 0x018d9fc9
String related to Outpost firewall (antivirus) in IExplore.exe (PID: 216)
    Match:    Search string "Outpost.exe" found in "outpost.exe"
    Location: %windir%\system32\xopptp.dll at address 0x100149c8
```

Results from Analysis:
Target?

- Test run had 5,244 samples
- 88 had banking strings
- Typically only a limited number of banks
- Typically targeted towards certain geographical areas

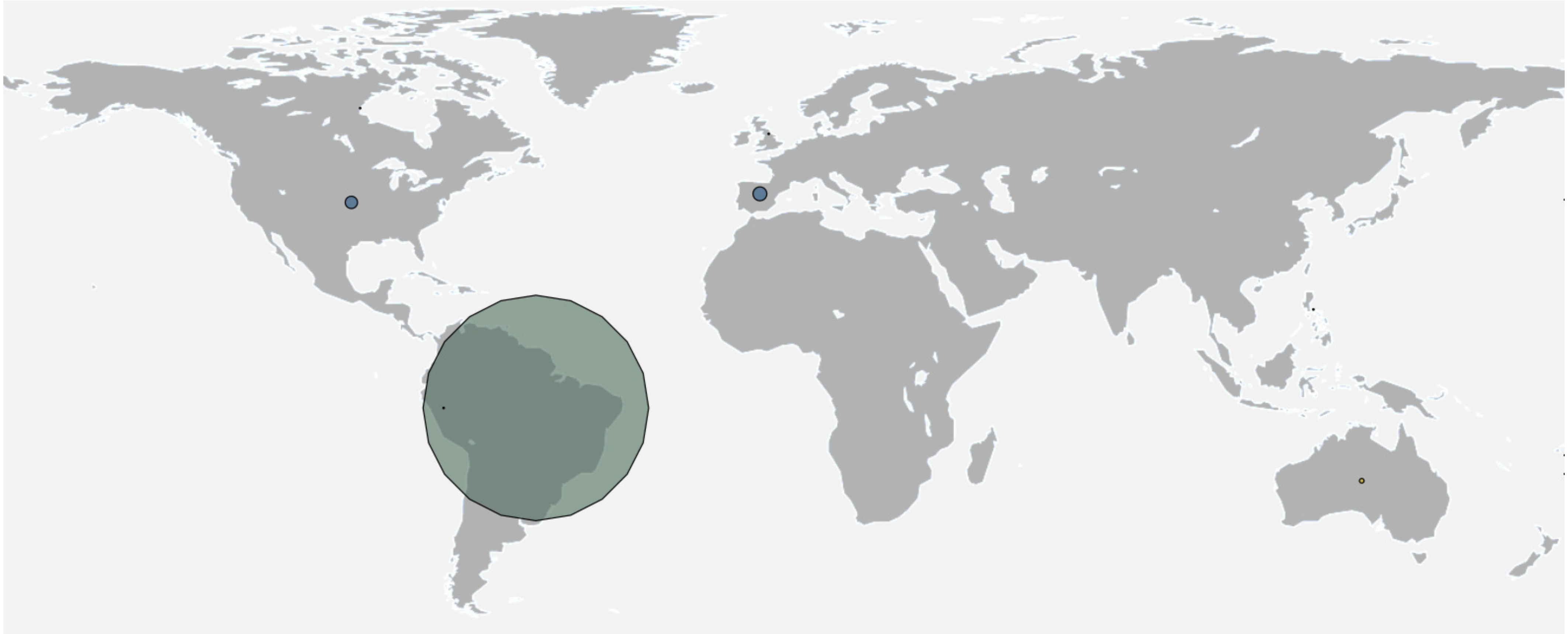



br
30.7%
us
16.9%
uk
13.8%
de
12.7%
es
10.1%
au
2.6%
tr
1.6%
lu
1.6%
it
1.6%
in
1.1%
fr
1.1%
others
6.3%

Targeted Countries

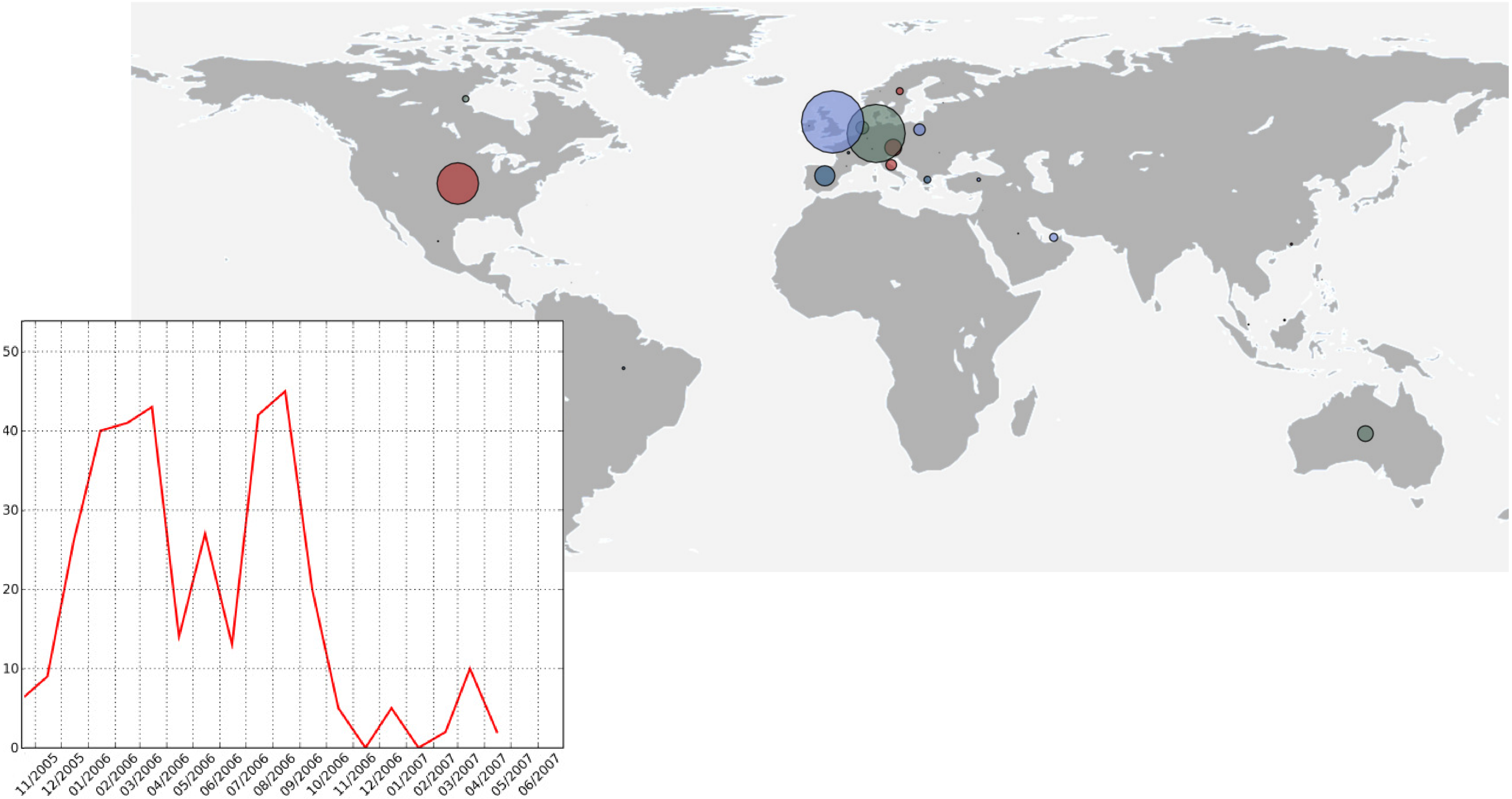
- Australia
- Austria
- Brazil
- Canada
- France
- Germany
- Greece
- Hong Kong
- India
- Ireland
- Italy
- Luxembourg
- Netherlands
- Philippines
- Poland
- Spain
- Sweden
- Turkey
- UAE
- United Kingdom
- United States

Brazilian Banking Trojans Target Brazil



Target distribution of Banker family

Target Distribution of Haxdoor Samples



Number of Haxdoor detections added per month 11/05-04/07

The Brazilian Connection

- Brazilian Banking Trojans are local
    - Not really even targeting other South American countries
- Made and distributed by local gangs
- Distribution servers are typically not in Brazil
- There are a lot of Brazilian malware in general – not just Banking Trojans
    - Big population
    - A pioneer in online banking
    - A lot of new computer users coming online every day

Problems with the String Search Approach

- Filter Strings Downloaded from a Control Server
  - No filter string included
  - Control servers may already be down

The requested URL was not found on this server.

If you entered the URL manually please check your spelling and try again.

- Strong Encryption
- Multipartite Malware
  - Plugin architecture; Configuration needs to be correct
- Server Side Filtering
  - Roel’s last minute presentation

Summary

- Banking trojan phenomenon can be analyzed by looking at which banks are being targeted
- The problem is getting worse
- Phishing has peaked already, banking trojans have not
- Multifactor authentication ➔ Local Session Riding
- Man-in-the-Browser attack problem will not be solved through user education

Thank you! Questions?

F-SECURE®

BE SURE.