Symantec

vb 2012 DALLAS

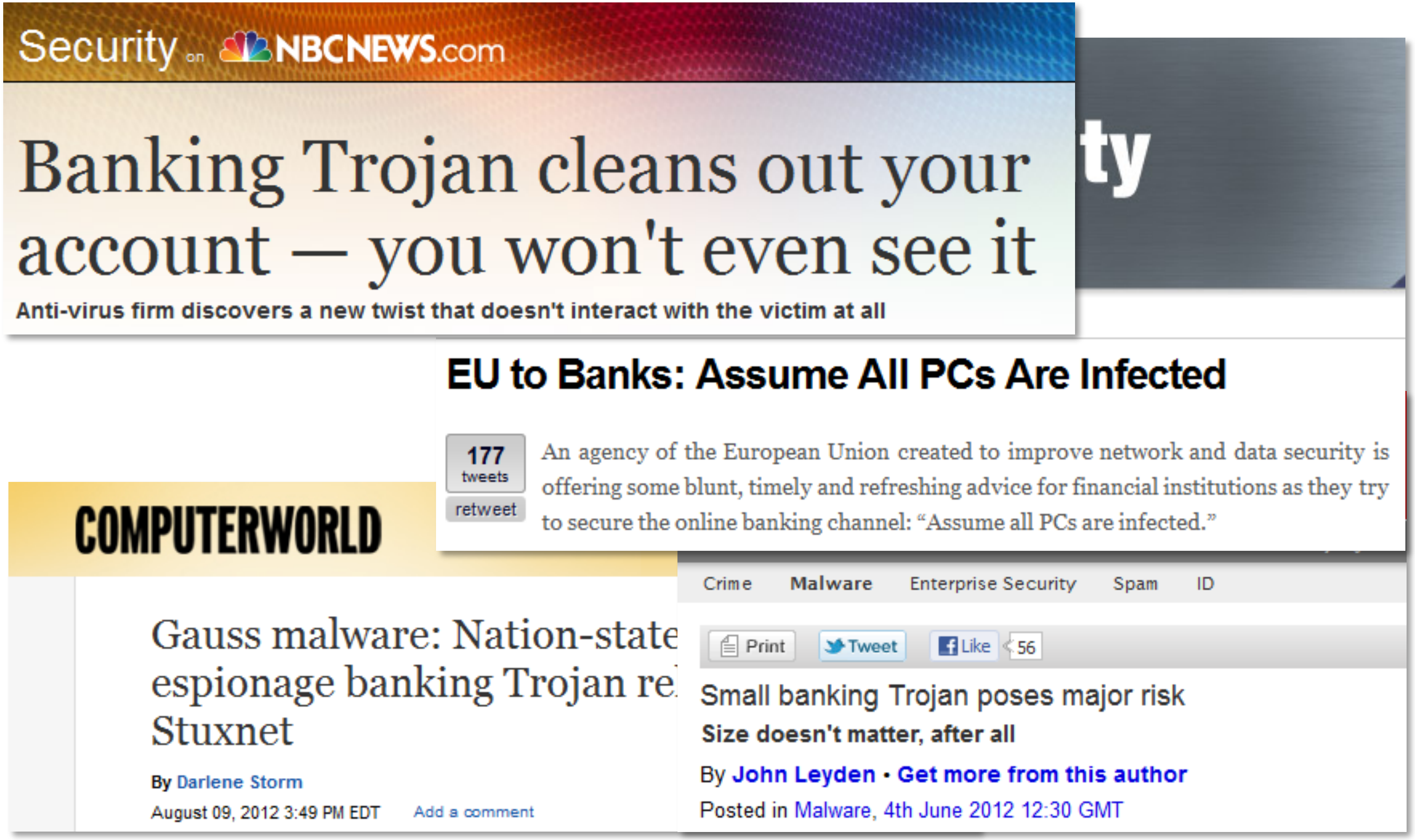
26 - 28 September 2012

Where do we stand with banking Trojans today?

Candid Wüest

Symantec Global Security Response

It‘s about banks…



Banking Trojan cleans out your account — you won't even see it

Anti-virus firm discovers a new twist that doesn't interact with the victim at all

EU to Banks: Assume All PCs Are Infected

An agency of the European Union created to improve network and data security is offering some blunt, timely and refreshing advice for financial institutions as they try to secure the online banking channel: “Assume all PCs are infected.”

Gauss malware: Nation-state espionage banking Trojan re Stuxnet

By Darlene Storm

August 09, 2012 3:49 PM EDT Add a comment

Small banking Trojan poses major risk

Size doesn't matter, after all

By John Leyden • Get more from this author

Posted in Malware, 4th June 2012 12:30 GMT

Agenda

- Distribution
- New features
- Webinject MITB
- Automated fraud
- Mobile banking
- C&C infrastructure
- Conclusion

So what is all the fuss about?

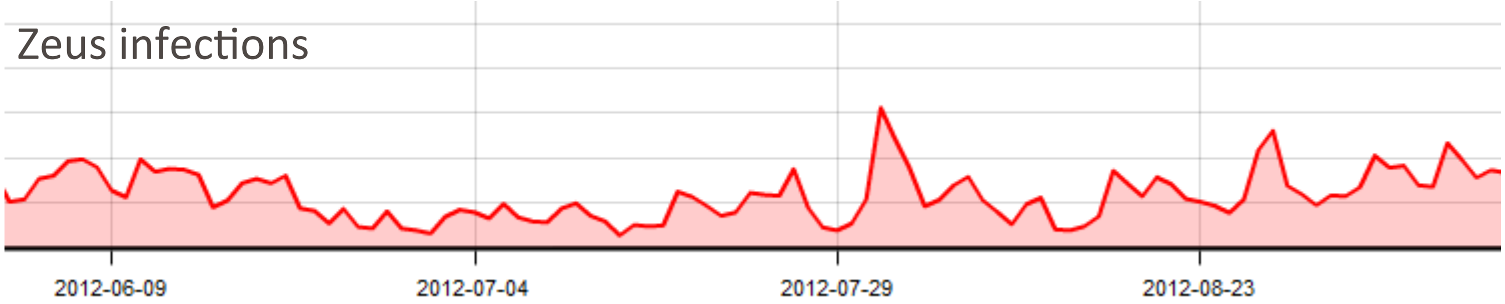
Not a new Problem!

- 2003: Infostealer.Bancos very active
- Virus Bulletin article in 2005

But how bad is it today?

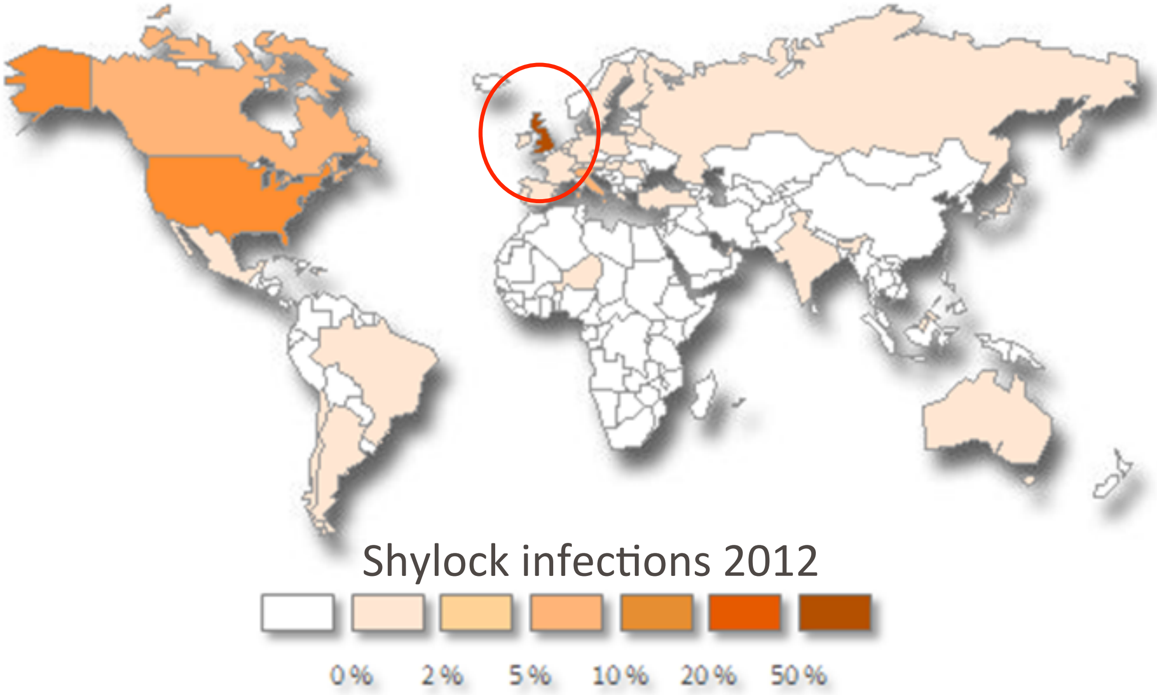
- Zeus (Citadel, Ice IX, Murofet, Licat, Gameover)

  > 1 Million Zeus infection/year
- SpyEye, Carberp, Tatanarg, Shylock, Cridex, Bebloh



Distribution

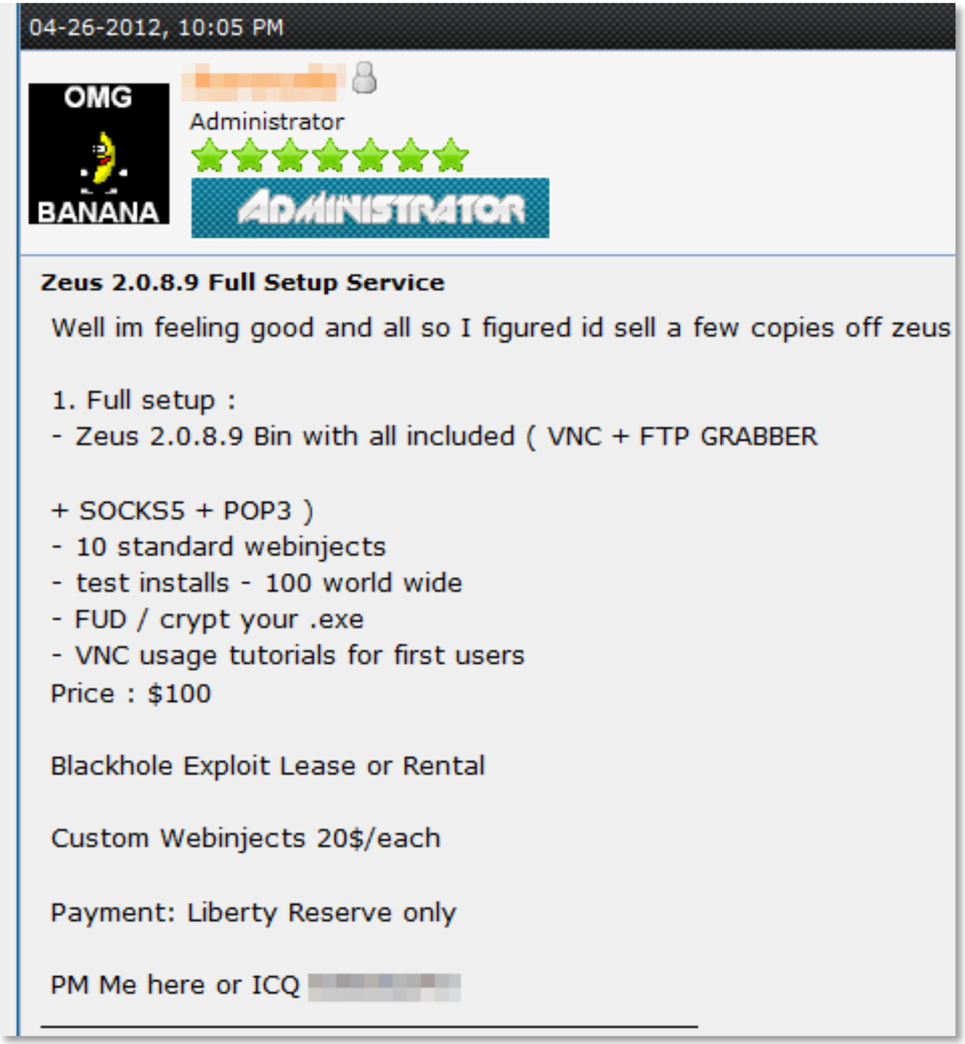
- Some are local – some are global
- Shylock in UK, Carberp in Russia, Tinba in Turkey and Bebloh Germany
- Some target 300 URLs – in total 7 common families targeted 683 URLs


Shylock infections 2012

Infection vector

The usual suspects:

- Webattack toolkits
  - Filtering victims by IP
  - May check for mouse activity
  - Rented as a service
- Email with attachments
- Email with malicious link
  - Especially after data breaches



04-26-2012, 10:05 PM

[redacted]

Administrator

Zeus 2.0.8.9 Full Setup Service

Well im feeling good and all so I figured id sell a few copies off zeus

1. Full setup :
- Zeus 2.0.8.9 Bin with all included (VNC + FTP GRABBER

+ SOCKS5 + POP3)
- 10 standard webinjects
- test installs - 100 world wide
- FUD / crypt your .exe
- VNC usage tutorials for first users

Price : $100

Blackhole Exploit Lease or Rental

Custom Webinjects 20$/each

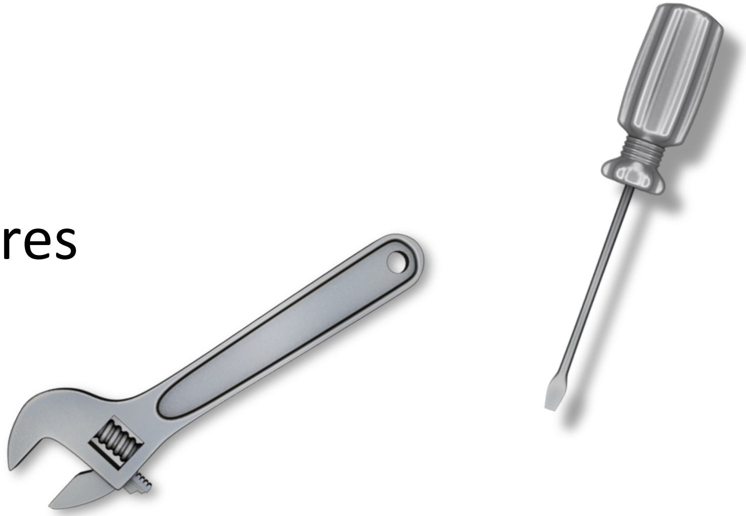
Payment: Liberty Reserve only

PM Me here or ICQ [redacted]

Adapted features

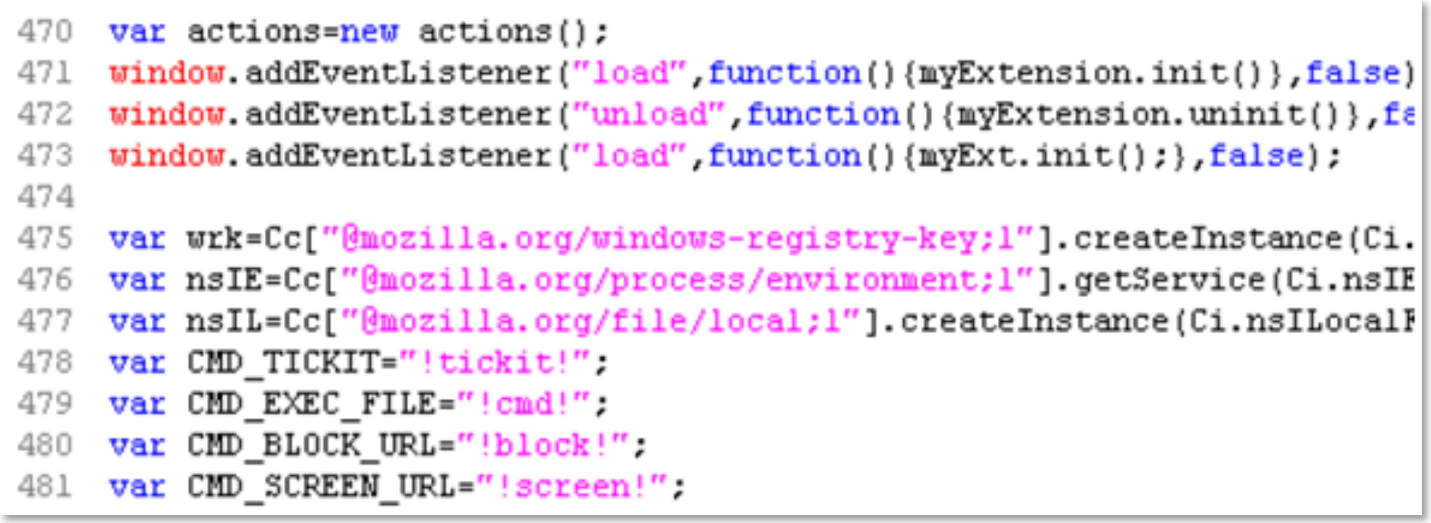
General Bot functionality evolved a bit:

- Can run as Guest account (e.g. Zeus)
- Local re-encryption, binding to machine
- Change encryption of config to thwart automated analysis
  - For example replace RC4 with AES
- Only steal once from a bot
- Different banks need different features



Different Ideas: Neloweg Firefox Extension

- Creates new WSCInstallNameSpace to load its DLL with Winsock2
- With Firefox present it will drop a FF extension (.xpi)
- Bot interacation is done within the browser by the FF extension
- Steals stored passwords and enables „webinjects“

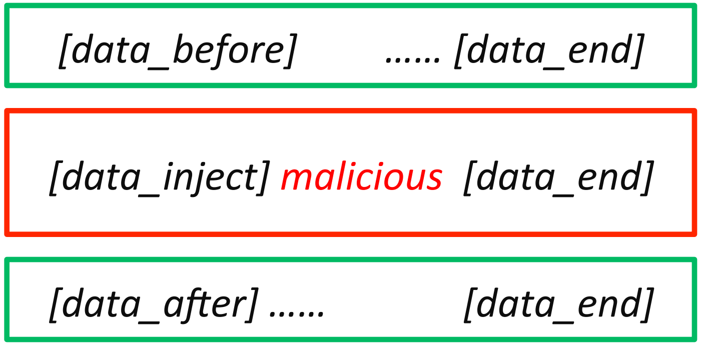


```
var actions=new actions();
window.addEventListener("load",function(){myExtension.init()},false)
window.addEventListener("unload",function(){myExtension.uninit()},fa
window.addEventListener("load",function(){myExt.init();},false);

var wrk=Cc["@mozilla.org/windows-registry-key;1"].createInstance(Ci.
var nsIE=Cc["@mozilla.org/process/environment;1"].getService(Ci.nsIE
var nsIL=Cc["@mozilla.org/file/local;1"].createInstance(Ci.nsILocalF
var CMD_TICKIT="!tickit!";
var CMD_EXEC_FILE="!cmd!";
var CMD_BLOCK_URL="!block!";
var CMD_SCREEN_URL="!screen!";
```

Webinjects – MITB Attacks

- Add or remove HTML/JS elements - simple and powerful!
- Syntax shared between multiple Trojans, e.g. Zeus & SpyEye
- Hooking: nspr4.dll, wininet.dll, WS2_32.dll
- Trojans may change IE settings to allow mixed content without warning



[data_before] …… [data_end]

[data_inject] malicious [data_end]

[data_after] …… [data_end]

Webinjects

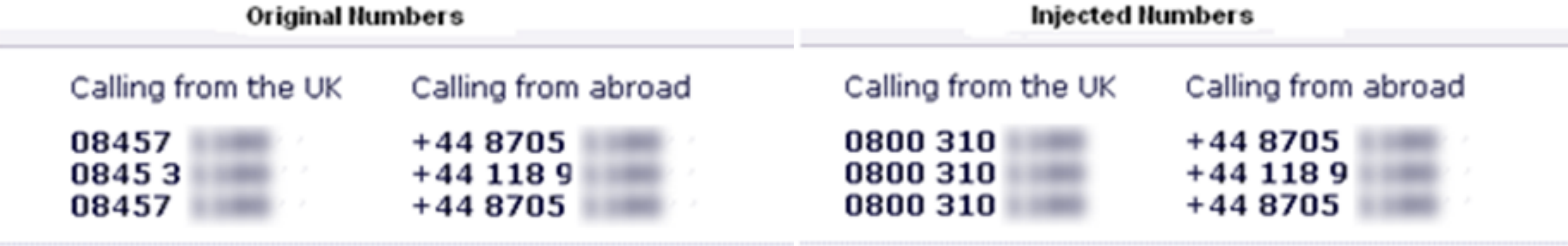
- Custom Webinjects are sold for $10-100

> SpyEye 1.3.48 Private
> […]
> Full installation including all injects mentioned above: 100 LR or WS
> **Custom Inject** coding for your own needs: **50LR** (Per Inject)

> We sell already made webinjects for Zeus/Spyeye. We can develope **webinjects to your needs** if you provide logins for testing it. Injects can be made on for any country and any language if you provide details for it. Injects are sold encrypted and you can`t modify them.
> […]
> Price for one inject is now **60 WMZ/LR**
> Updated/modify of injects 20 lr each.

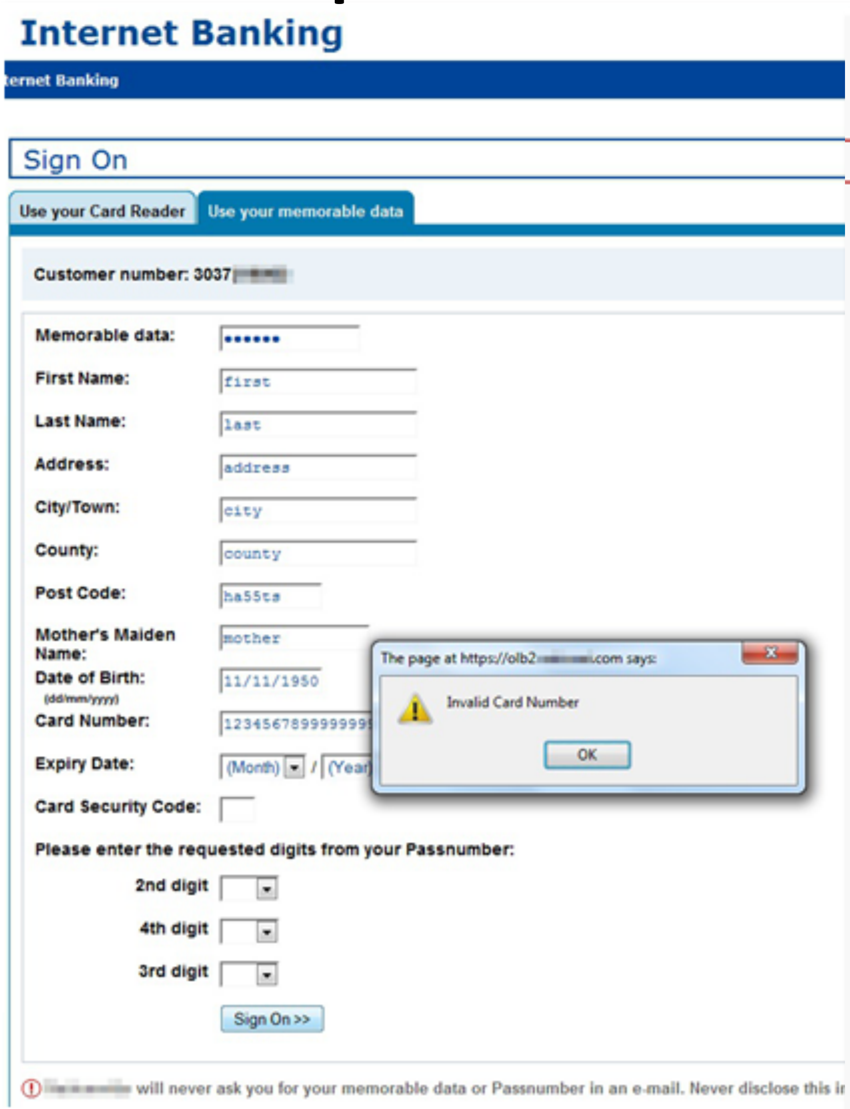
Webinjects: Obfuscation Tricks

- Display a maintenance or „please wait“ window
- Cleanup the balance and transaction history
- Add a fake chat window or fake contact info
- Block access to security websites
- Bruteforce web logins



Original Numbers		Injected Numbers	
Calling from the UK	Calling from abroad	Calling from the UK	Calling from abroad
08457 [redacted]	+44 8705 [redacted]	0800 310 [redacted]	+44 8705 [redacted]
0845 3 [redacted]	+44 118 9 [redacted]	0800 310 [redacted]	+44 118 9 [redacted]
08457 [redacted]	+44 8705 [redacted]	0800 310 [redacted]	+44 8705 [redacted]

The simple ones steal CCs



Internet Banking

ernet Banking

Sign On

Customer number: 3037[redacted]

Memorable data:	••••••
First Name:	first
Last Name:	last
Address:	address
City/Town:	city
County:	county
Post Code:	ha55ts
Mother's Maiden Name:	mother
Date of Birth: (dd/mm/yyyy)	11/11/1950
Card Number:	123456789999999
Expiry Date:	(Month) / (Year
Card Security Code:	

Please enter the requested digits from your Passnumber:

2nd digit

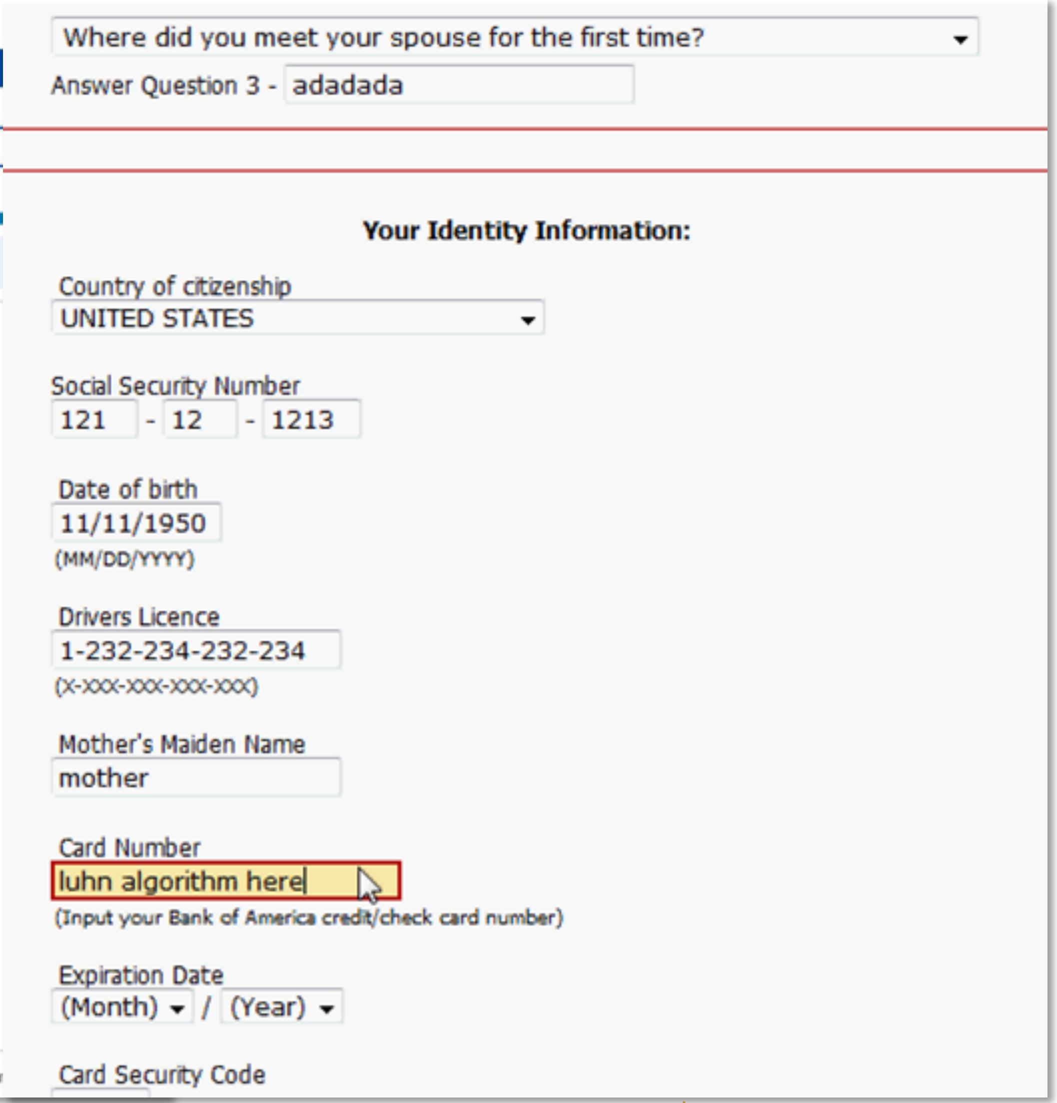
4th digit

3rd digit

The page at https://olb2[redacted].com says:

Invalid Card Number

[redacted] will never ask you for your memorable data or Passnumber in an e-mail. Never disclose this i



Where did you meet your spouse for the first time?

Answer Question 3 - adadada

Your Identity Information:

Country of citizenship
UNITED STATES

Social Security Number
121 - 12 - 1213

Date of birth
11/11/1950
(MM/DD/YYYY)

Drivers Licence
1-232-234-232-234
(X-XXX-XXX-XXX-XXX)

Mother's Maiden Name
mother

Card Number
luhn algorithm here
(Input your Bank of America credit/check card number)

Expiration Date
(Month) / (Year)

Card Security Code

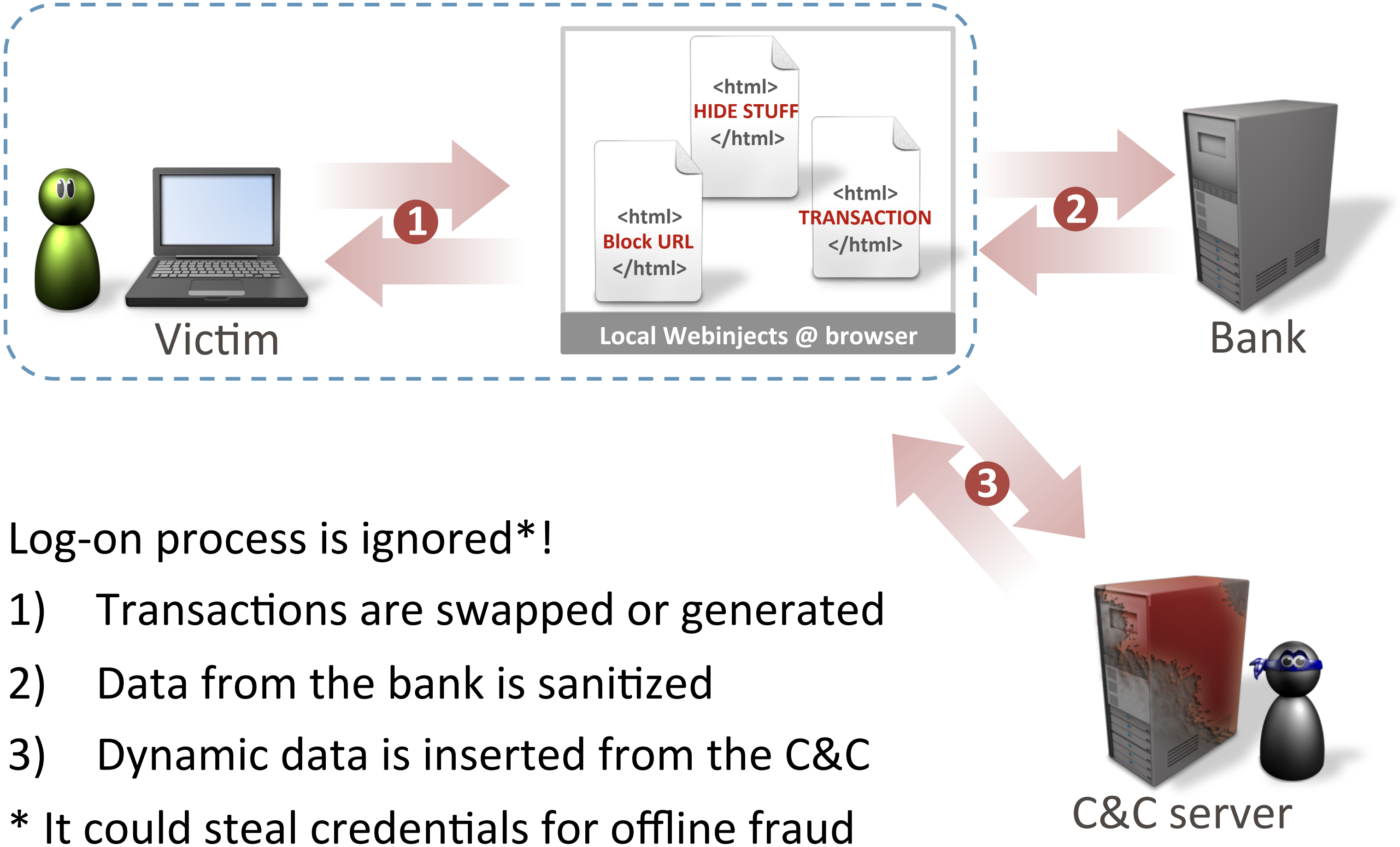
Automated MITB Transactions

The smart ones make automated transactions on the client

- Steal a percentage of the highest balance or a fixed amount
  - Usually less then 5K to stay under money laundry detection
- Money mule accounts are loaded on-the-fly from C&C server
- Some simulate user behavior (browsing, menu clicking) in order to fool anomaly detection

This can bypass, virtual keyboards, anti-keylogger, OTP iTAN, mTAN (when no transaction verification is done)

Webinject MITB



Log-on process is ignored*!

1) Transactions are swapped or generated

2) Data from the bank is sanitized

3) Dynamic data is inserted from the C&C

* It could steal credentials for offline fraud

Social Engineering Tricks

Let the user beat the system:

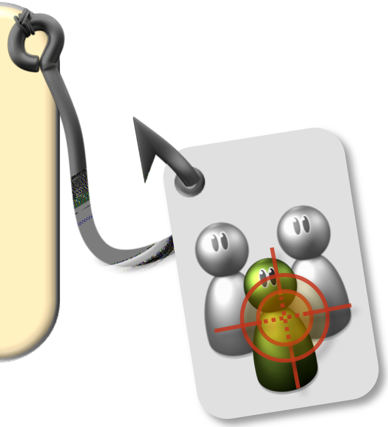
- Perform a „test“ transaction (Tatanarg)
- Revert a „false“ transaction (Zeus)
- Change corresponding mobile number and let user confirm it

Dear user,

there has been a transaction error

Please revert the following transaction

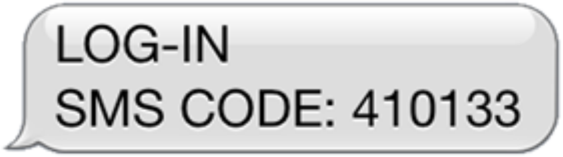
in order to unblock your account.



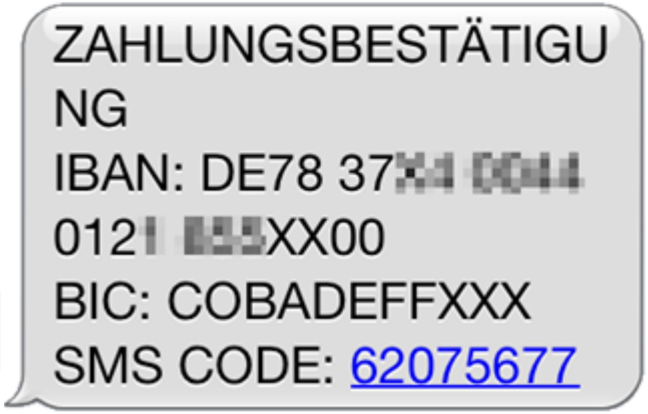
Mobile Authentication

- Mobile Transaction Authentication Number (mTAN)
  - Popular method for online banking, often only used for authentication
- Zeus & SpyEye mobile modules
  - (2010: Android, Blackberry, Symbian, Windows Mobile)
- Main Trojan will ask for mobile number and model
- Forward all SMS to C&C server

Annuls transaction signing,
as user does not see it!



LOG-IN
SMS CODE: 410133



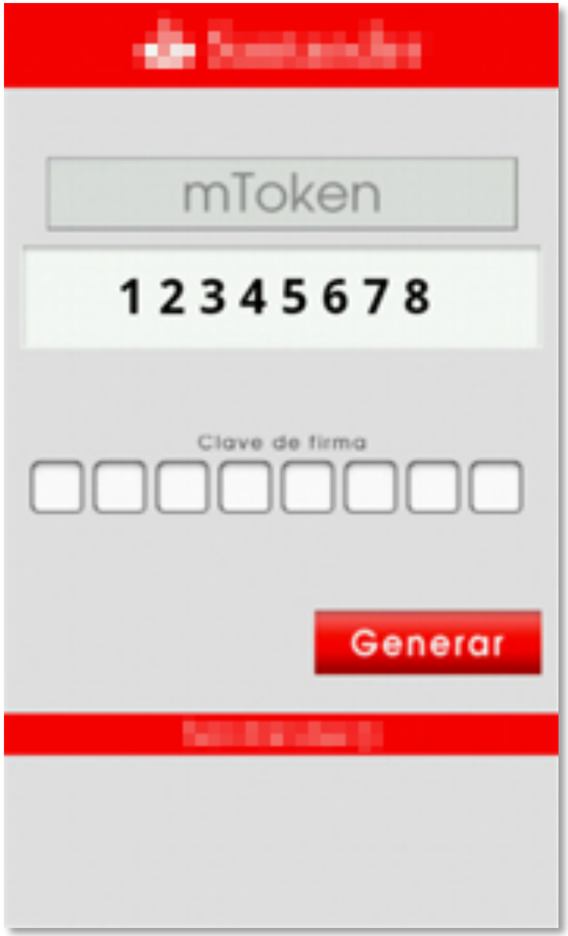
ZAHLUNGSBESTÄTIGU
NG
IBAN: DE78 37[redacted]
012[redacted]XX00
BIC: COBADEFFXXX
SMS CODE: 62075677

Mobile Banking

- Some banks have started to deploy mobile banking solutions
  - Complete transactions from your mobile
  - OutOfBand authentication is no longer OOB if mobile is used!
  - Devices are often unprotected

Example:

- Pose as standalone OTP generator and ask for credentials -> full access



Command & Control Infrastructure

A simple PHP webfront is still the most common C&C server

Usually HTTP/S traffic with encrypted content (XOR, RC4, AES, ...)

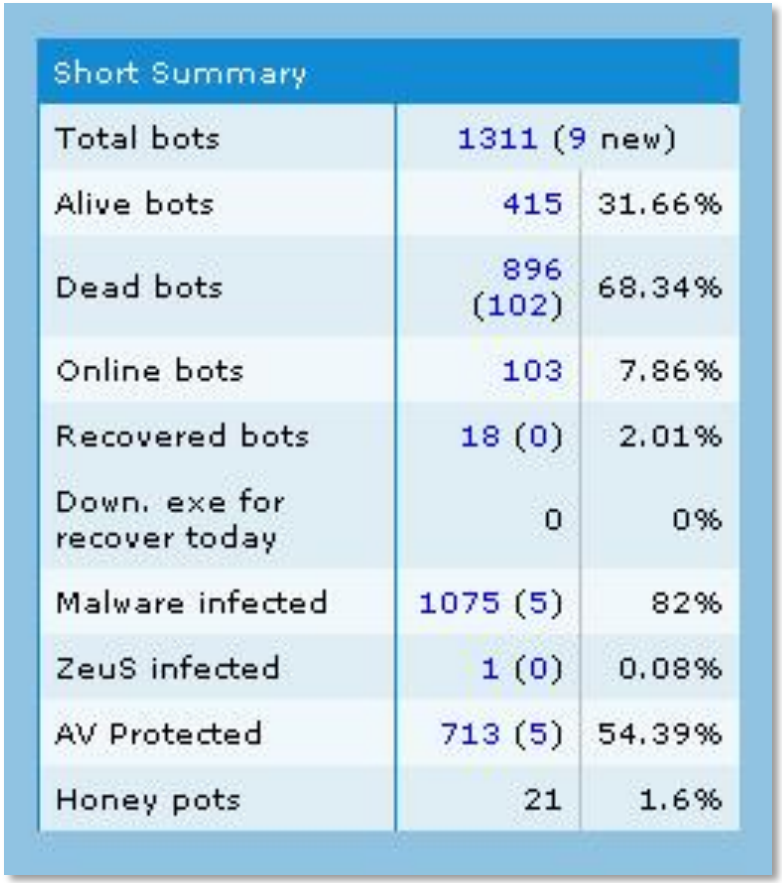
But we have seen:

- Zeus operator that used stolen cloud service as C&C server
- Zeus operator that used a hidden TOR service as C&C server
- Zeus variant that uses P2P network

Protect Your Assets

Citadel - Module MiniAV ($ 100)

- Allows you to **clean your PC** from someone else's bot Malware,
- the module is activated every 4 hours and **remove all of the Zeus**-modification systems, such as Zeus1, 2, Ice9, etc.
- Vitality of your build go up a few times, it is recommended to those who have met in my logs wrong gates and uses traffic exchanges. In the near future will add a signature to remove feykav and substitution issue.



Short Summary		
Total bots	1311 (9 new)	
Alive bots	415	31.66%
Dead bots	896 (102)	68.34%
Online bots	103	7.86%
Recovered bots	18 (0)	2.01%
Down. exe for recover today	0	0%
Malware infected	1075 (5)	82%
ZeuS infected	1 (0)	0.08%
AV Protected	713 (5)	54.39%
Honey pots	21	1.6%

Tatanarg controller statistics

Conclusion

They didn‘t change much, because it still works!

- MITB with webinjects is very powerful
- More stealth & obfuscation features
  - Encryption, C&C protection, P2P, …
- More automation
  - Dynamic money mule loading, transaction swapping, …
- More social engineering
  - Because there is no patch for it ;-)

The banks added a lot of fraud protection on the backend

Thank you for your attention!

CANDID_WUEEST@SYMANTEC.COM

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.