

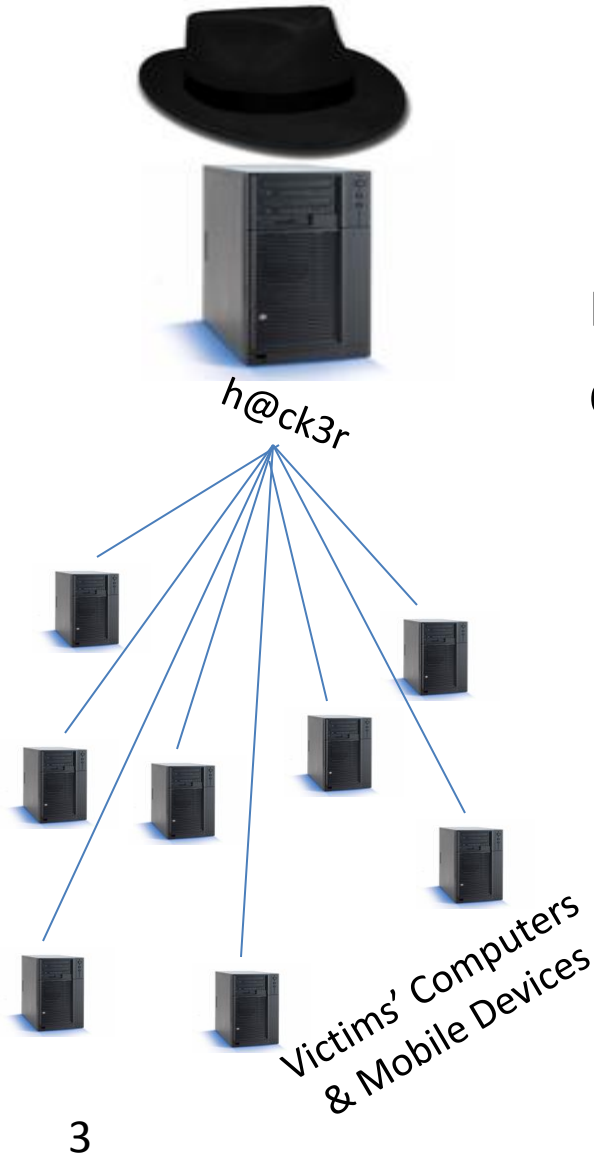


# Mobile Botnet Trends 2011 - Agenda



- What are Botnets?
- How do users get infected with malware?
- How are mobile devices at risk?
- Latest Botnet trends and functionalities

# What is a Botnet?



Multiple infected computers and mobile devices under the control of an individual Botnet Operator.




# Analysis of a Zeus Botnet Compromise

1101010  
1101000  
1101010



## *Social Engineering... 2011 Tax Season*



**Internal Revenue Service**  
United States Department of the Treasury

---

**Fraud Application**

---

**Your Progress:**

<b>1. Tax Notice Received on e-mail ✓</b>	<b>2. Tax Statement</b>
---	-------------------------

**Taxpayer ID:**  
**Tax Type: INCOME TAX**  
**Issue: Unreported/Underreported Income (Fraud Application)**

Filing and paying your federal taxes correctly and on time is an important part of living and working in the United States.  
Please review (download and execute) your tax statement:

[bot-1-2-7-19.exe](#)

**If the statement is incorrect, contact our Taxpayer Advocate Service.**

---

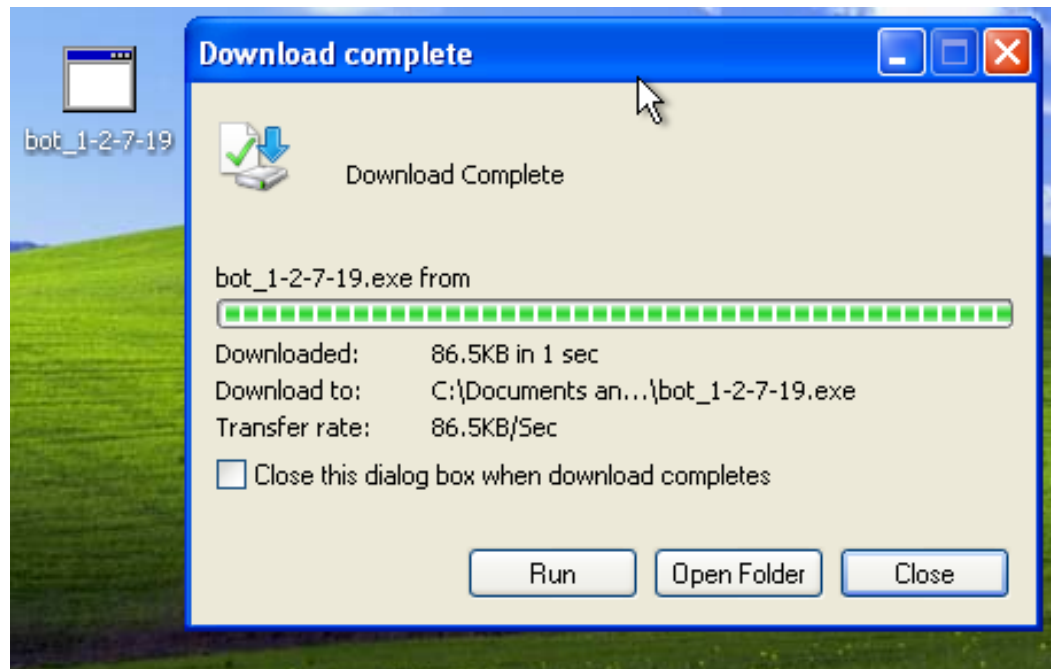
[IRS Privacy Policy](#)

# Analysis of a Zeus Botnet Compromise

1101010  
1101000  
1101010



***Social Engineering... CLICK HERE!***

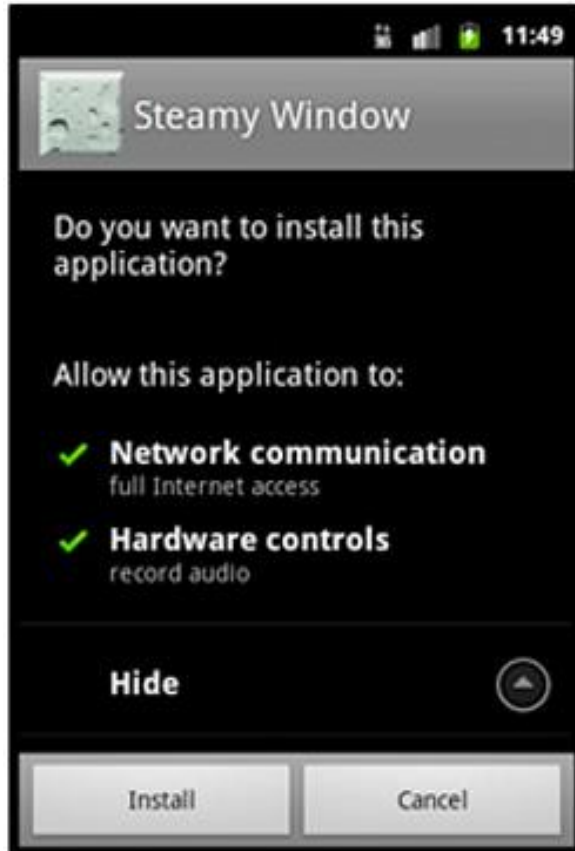


# Social Engineering for Mobile Apps

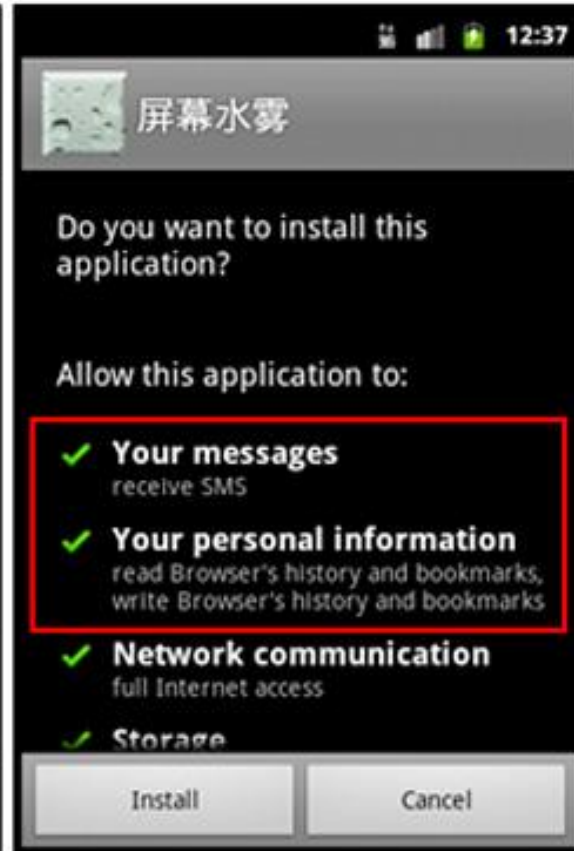
1101010  
1101000  
1101010



## Legitimate Application



## Malicious Application





# Analysis of a Zeus Botnet Compromise



## Zeus Botnet Captures Bank Login Credentials

View report (HTTPS request, 1 303 bytes)

Bot ID: mycomputer\_00130128

Botnet: -- default --

Version: 1.2.7.19

OS Version: XP Professional SP 2, build 2600

OS Language: 1033

Local time: 14.01.2010 23:07:00

GMT: +0:00

Session time: 00:26:27

Report time: 14.01.2010 23:07:55

Country: --

IPv4:

Comments for bot: -

In the list of used: No

Process name: C:\Program Files\Internet Explorer\IEXPLORE.EXE

Source: https://sitekey.bankofamerica.com/sas/signon.do?locale=en\_US

https://sitekey.bankofamerica.com/sas/signon.do?lo

Referer: https://sitekey.bankofamerica.com/sas/sig

Keys: fakeonlineid

Data:

nextAction=signon

pm\_fp=version%253D1%2526pm%255Ffpua%253Dmozilla%25

customer\_Type=MODEL

reason=

portal=

history=

cache=

dltoken=

pmbutton=false

hidstate=CO

realID=

onlineID=fakeonlineid

sitekeySignon=true

bot\_id=0E2E44DF465C41A\_7875768F2667A927

botnet=

bot\_version=2.0.8.9

ipv4=188.99.

country=DE

type=12

rtime=08:42:52 19.04.2011

time\_system=15:41:42 19.04.2011

time\_tick=00:00:57

time\_localbias=

os\_version=

language\_id=1033

process\_name=C:\Program Files\Internet Explorer\iexplore.exe

process\_user=Administrator

path\_source=https://banking./login.do

context=

Referer:

User input:

POST data:

jsOn=true

accountNumber=8

pinNumber=

action=&melden

# Analysis of a Zeus Botnet Compromise



## *Zeus Botnet Hijacks Bank Account Logins with WebInjects*

```
webinjects.txt
set_url */my.ebay.com/*CurrentPage=MyeBayPersonalInfo* GL
set_url https://www.us.hsbc.com/* GL
set_url https://www.e-gold.com/acct/balance.asp* GPL
set_url https://online.wellsfargo.com/das/cgi-bin/session.cgi* GL
set_url https://www.paypal.com/*/webscr?cmd=_login-done* GL
set_url https://www#.usbank.com/internetBanking/LoginRouter PL
set_url https://easyweb*.tdcanadatrust.com/servlet/*FinancialSummaryServlet* GL
set_url https://www#.citizensbankonline.com/*/index-wait.jsp GL
set_url https://onlinebanking.nationalcity.com/OLB/secure/AccountList.aspx GL
set_url https://www.suntrust.com/portal/server.pt*parentname=Login* GL
set_url https://www.53.com/servlet/efsonline/index.html* GL
set_url https://web.da-us.citibank.com/*BS_Id=MemberHomepage* GL
set_url https://onlineeast#.bankofamerica.com/cgi-bin/ias/*/GotoWelcome GL
set_url https://online.wamu.com/Servicing/Servicing.aspx?targetPage=AccountSummary GL
set_url https://onlinebanking#.wachovia.com/myAccounts.aspx?referrer=authService GL
set_url https://resources.chase.com/MyAccounts.aspx GL
set_url https://bancaonline.openbank.es/servlet/PProxy?* GP
set_url https://extranet.banesto.es/*/loginParticulares.htm GP
set_url https://banesnet.banesto.es/*/loginEmpresas.htm GP
set_url https://empresas.gruposantander.es/WebEmpresas/servlet/webempresas.servlets.* GP
set_url https://www.gruposantander.es/bog/sbi?*ptns=acceso* GP
set_url https://www.bbvanetoffice.com/local_bdno/login_bbvanetoffice.html GP
```



# 0-day Bots: Will your antivirus catch them?



AV Detection Rates: 25-30%

```
bot_id=ABC_7875768F84259CA4
botnet=
bot_version=2.1.0.1
ipv4=88.2.
country=ES
type=1
rtime=16:20:59 04.2011
time_system=16:18:38 04.2011
time_tick=00:02:38
time_localbias=-7:00
os_version=
language_id=1033
process_name=C:\WINDOWS\Explorer.EXE
process_user=Administrator
path_source=
context=
wininet(Internet Explorer).cookies:Path: /accou
```

Create task for Billing   Modify Cards   Tasks Statistic   Bots Monitoring  
Settings   Ban Bots   Create task for Loader   Create task for Knocker

**Hack the Planet!**

**Take your money!**

Firesale Botnet

Main Menü   Fertigstellung   About   Your Domain

Link für die Verbindung der Bots   /bot.php

**Optionen**

- Autostart
- Fake Error
- Anti Codes
- ExE Pumper
- Prozess Killer
- Icon Changer
- Rootkit
- Bypasser
- Persistent
- Spread Optionen

**Anti Codes**

- Anti Anubis
- Anti VMware
- Anti Norman
- Anti Out Post
- Anti Virtual PC
- Anti Virtual Box
- Anti Sniffer
- Anti Kaspersky
- Anti Bitdefender
- Anti Zone Alarm
- Anti Malwarebyte

**Fake Error**

Titel...  
Text...

**Prozess Killer**

exe

**Installation**

Mutex  
Install: Windows

**Bypasser**

- UAC Bypass
- Firewall Bypass
- Defender Bypass
- WiCenter Bypass

**Spread Optionen**

- USB Spread
- P2P Spread
- LAN Spread
- RAR Spread
- ICQ Spread
- MSN Spread
- Skype Spread

**Icon**

Pump: 500

```
Tue Apr 2011 18:38:19 +0400 - UPDATE for bot "magazapc! CC2F7D17" : bot_ver = 10 : md5 =  
81c26518db91b6a5a7e49665f257ee4f : dbmd5 = e4b4f01b976b7c14141be509473d9067
```

# ZITMO: Zeus In The Mobile



- 1) Victim's computer is first infected with Zeus botnet malware.
- 2) On the infected computer, HTML is injected into the web browser when a bank's login page is loaded, which requests the Model# and Telephone# of the victim's cell phone.
- 3) With this information, the attacker sends an SMS message back to the victim's phone, with a link to malware targeting their mobile device.
- 4) Once ZITMO malware is installed on the mobile device, the attacker can control both the victim's computer and smart phone.





# Mobile Malware targets all platforms



## *Infected iPhone*



## *Infected Android*



