Outsmarting Researchers: Fraudsters and Their Security Practices

by Julia Karpin and Avi Shulman
June 2015
F5 Networks
Outsmarting Researchers: Fraudsters and Their Security Practices

by Julia Karpin and Avi Shulman
June 2015
F5 Networks
Fraudsters

WHAT DO WE WANT?  LOTS OF MONEY!

WHEN DO WE WANT IT?  NOW!

WHAT WILL WE DO TO GET IT?  WRITE SOME CODE...?
History of an Arms Race

Fraudsters
Keyloggers
Phishing
Webinjects
Man in the Mobile
VNC\RAT

banking security
Virtual Keyboards
SSL (digital certificates)
Smartcards\mTAN
Fingerprinting
Brainwaves
History of an Arms Race

- Fraudsters
- Keyloggers
- Phishing
- Webinfects
- Man in the Mobile
- VNC\RAT
- banking security
- Virtual Keyboards
- SSL (digital certificates)
- Smartcards\mTAN
- Fingerprinting
- Brainwaves
History of an Arms Race

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

Fraudsters
Keyloggers
Phishing
Webinfects
Man in the Mobile
VNC\RAT

banking security
Virtual Keyboards
SSL (digital certificates)
Smartcards\mTAN
Fingerprinting
Brainwaves
WANTED
By The FBI

$3,000,000 Reward

SpyEye author
30 years in prison

SpyEye botmaster
30 years in prison

carberp author
10 years in prison
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
Protected mode is turned off for the Internet zone.

Don't show this message again  Turn on Protected mode

Protected mode is turned off for the Internet and Restricted sites zones.

Don't show this message again  Turn on Protected mode
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 motherf*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
- Webinjests configuration (AES, blowfish, steganography)
- C&C communication (https, RC4)
Server-Side Enforcement

- Geolocation IP filtering
- Server-side webinjects
Index of /panel

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

Authentication Required

The server http://*redacted* requires a username and password. The server says: Admin Center.

User Name: [ ]
Password: [ ]

[Log In] [Cancel]
THANK YOU!

Questions?
References

- http://larslohmann.blogspot.co.il/2013/05/protected-mode-warning.html
- https://amiunique.org/fp
Outsmarting Researchers: Fraudsters and Their Security Practices

by Julia Karpin and Avi Shulman
June 2015
F5 Networks