Bosses love Excel … hackers too!

Juan Garrido "Silverhack"

Chema Alonso (@chemaalonso)

INFORMATICA64.COM

Who?

About

- Security Researchers
- Working at INFORMATICA64
- http://www.informatica64.com

What?

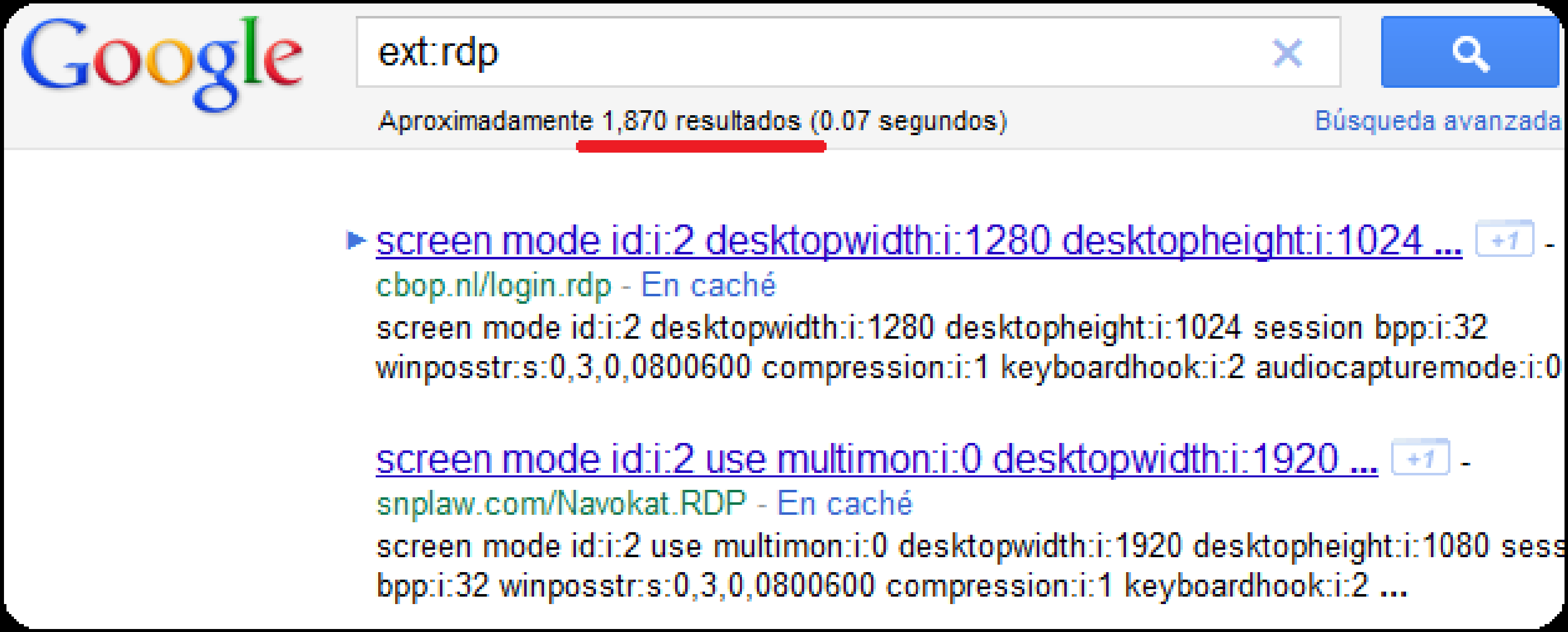
Terminal Applications

CITRIX®

Windows
Terminal Services

why?

RDP



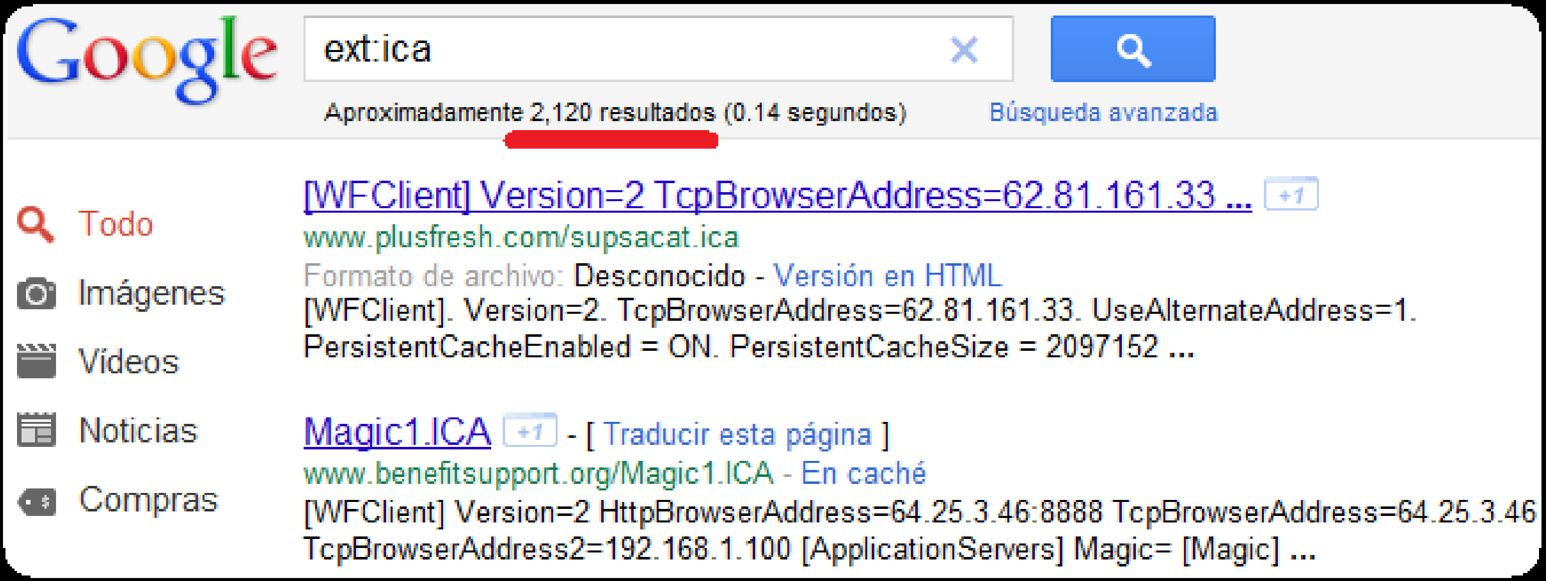
ext:rdp

Aproximadamente 1,870 resultados (0.07 segundos)

screen mode id:i:2 desktopwidth:i:1280 desktopheight:i:1024 ... +1 -
cbop.nl/login.rdp - En caché
screen mode id:i:2 desktopwidth:i:1280 desktopheight:i:1024 session bpp:i:32 winposstr:s:0,3,0,0800600 compression:i:1 keyboardhook:i:2 audiocapturemode:i:0

screen mode id:i:2 use multimon:i:0 desktopwidth:i:1920 ... +1 -
snplaw.com/Navokat.RDP - En caché
screen mode id:i:2 use multimon:i:0 desktopwidth:i:1920 desktopheight:i:1080 sess bpp:i:32 winposstr:s:0,3,0,0800600 compression:i:1 keyboardhook:i:2 ...

Citrix

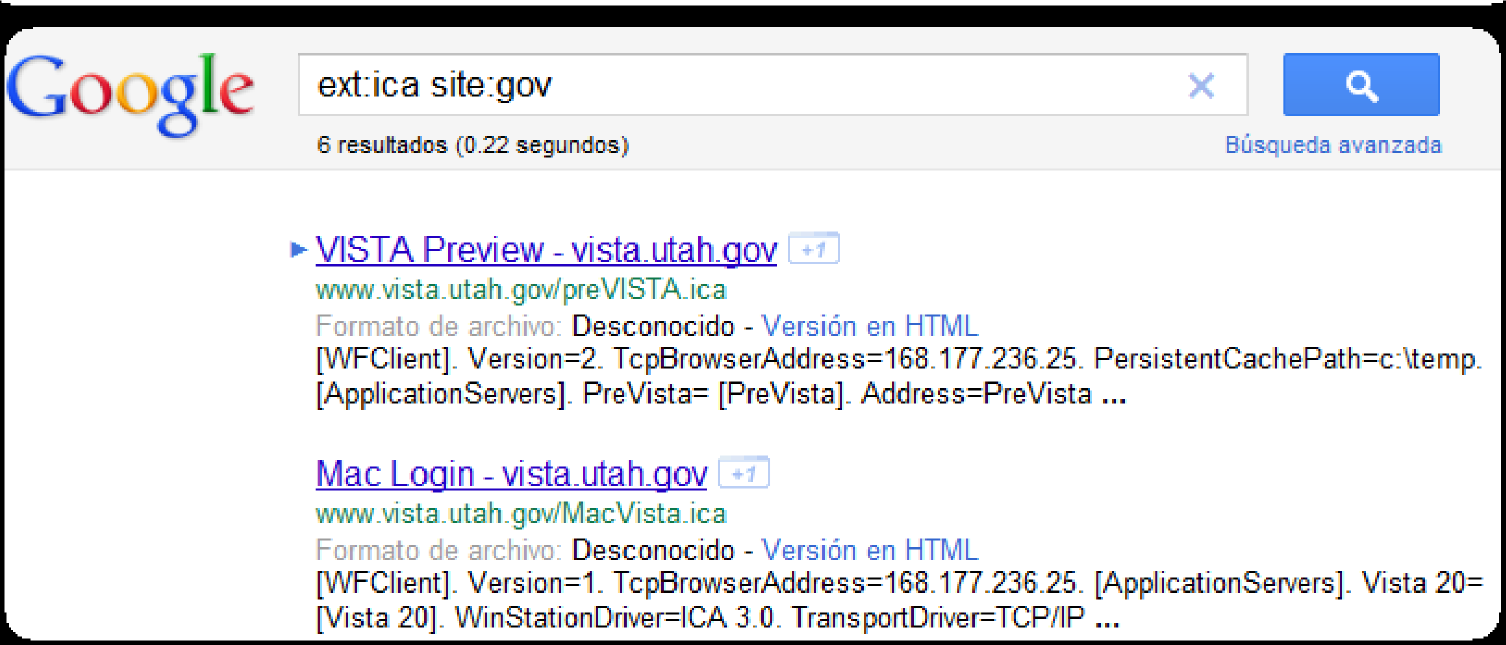


ext:ica

Aproximadamente 2,120 resultados (0.14 segundos)

[WFClient] Version=2 TcpBrowserAddress=62.81.161.33 ...
www.plusfresh.com/supsacat.ica
Formato de archivo: Desconocido - Versión en HTML
[WFClient]. Version=2. TcpBrowserAddress=62.81.161.33. UseAlternateAddress=1. PersistentCacheEnabled = ON. PersistentCacheSize = 2097152 ...

Magic1.ICA - [Traducir esta página]
www.benefitsupport.org/Magic1.ICA - En caché
[WFClient] Version=2 HttpBrowserAddress=64.25.3.46:8888 TcpBrowserAddress=64.25.3.46 TcpBrowserAddress2=192.168.1.100 [ApplicationServers] Magic= [Magic] ...



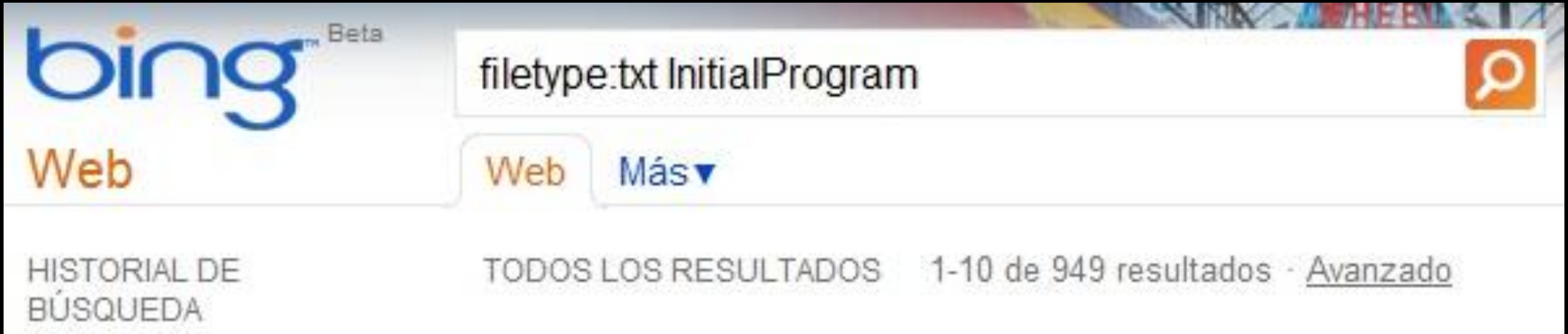
ext:ica site:gov

6 resultados (0.22 segundos)

VISTA Preview - vista.utah.gov
www.vista.utah.gov/preVISTA.ica
Formato de archivo: Desconocido - Versión en HTML
[WFClient]. Version=2. TcpBrowserAddress=168.177.236.25. PersistentCachePath=c:\temp. [ApplicationServers]. PreVista= [PreVista]. Address=PreVista ...

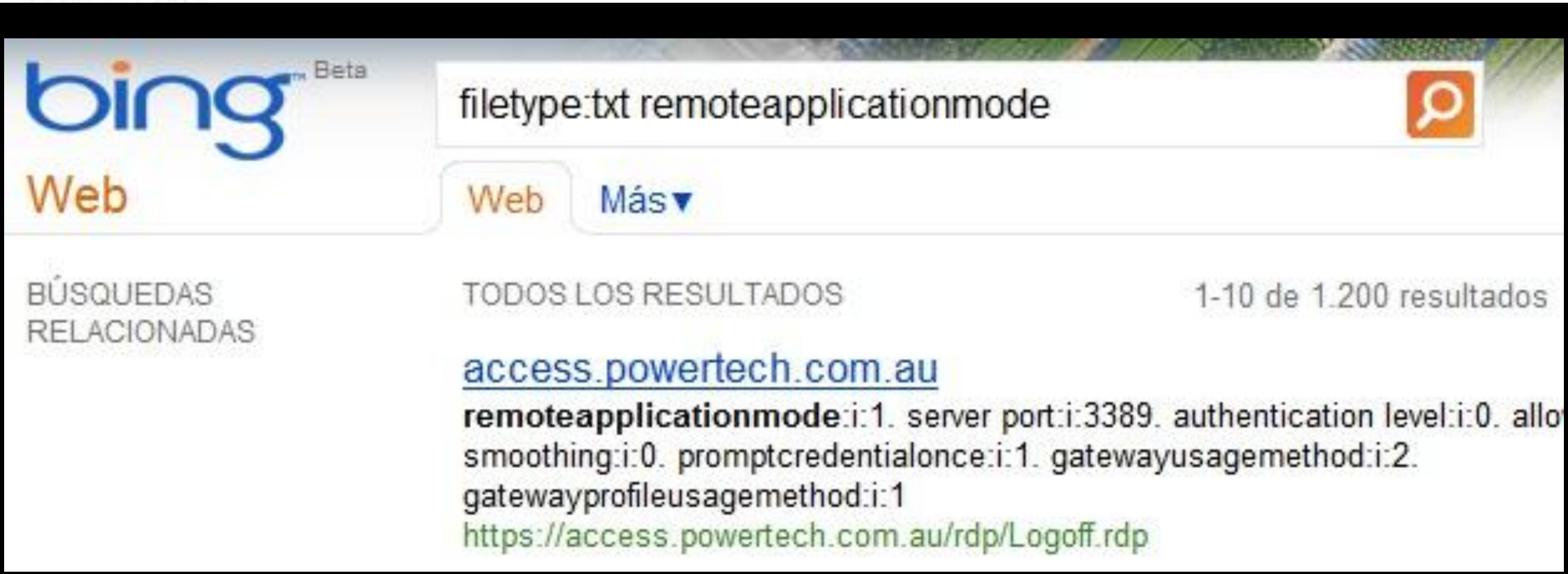
Mac Login - vista.utah.gov
www.vista.utah.gov/MacVista.ica
Formato de archivo: Desconocido - Versión en HTML
[WFClient]. Version=1. TcpBrowserAddress=168.177.236.25. [ApplicationServers]. Vista 20= [Vista 20]. WinStationDriver=ICA 3.0. TransportDriver=TCP/IP ...

Using Bing



filetype:txt InitialProgram

TODOS LOS RESULTADOS 1-10 de 949 resultados · Avanzado



filetype:txt remoteapplicationmode

TODOS LOS RESULTADOS 1-10 de 1.200 resultados

access.powertech.com.au

remoteapplicationmode:i:1. server port:i:3389. authentication level:i:0. allo smoothing:i:0. promptcredentialonce:i:1. gatewayusagemethod:i:2. gatewayprofileusagemethod:i:1

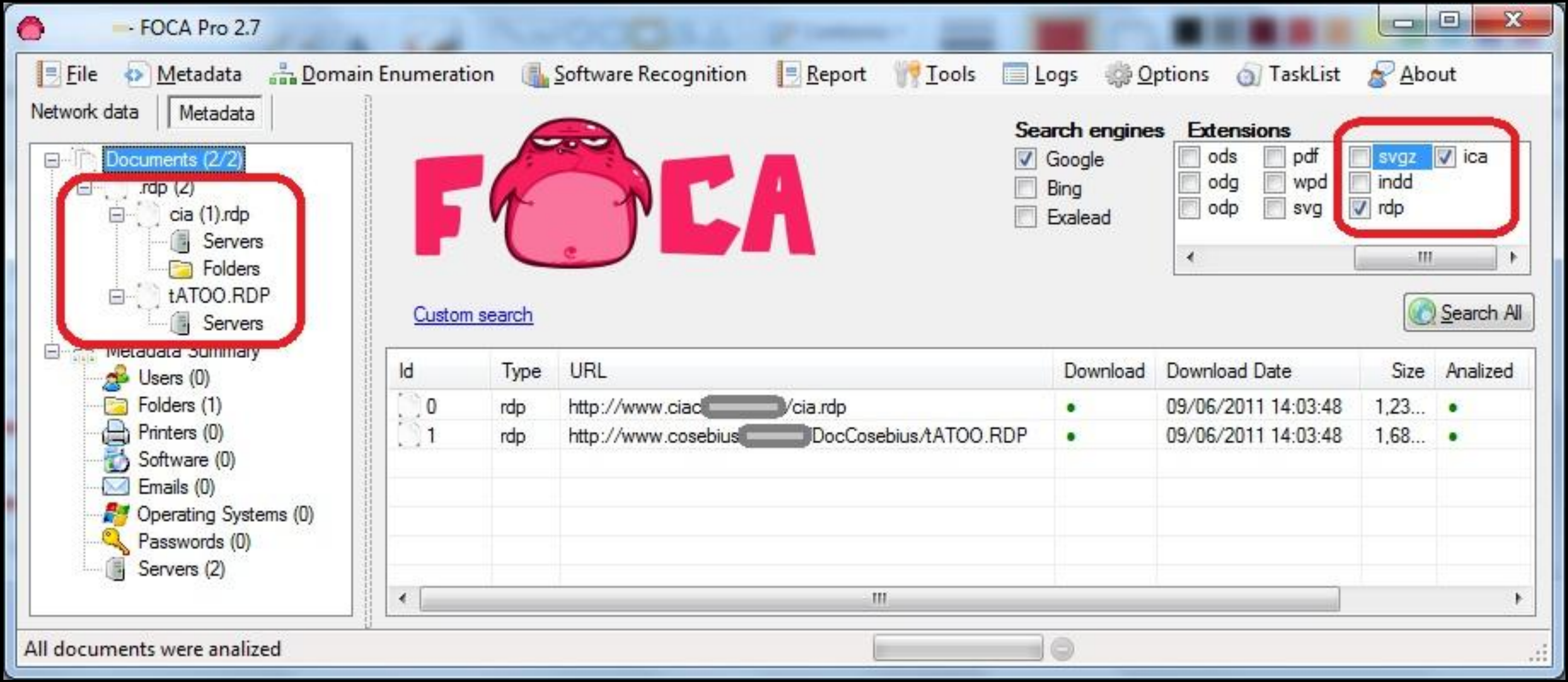
https://access.powertech.com.au/rdp/Logoff.rdp

Secure?

Verbosity

- Conf -files are too verbosity
  - Internal IP Address
  - Users & encrypted passwords
  - Internal Software
  - Perfect for APTs
    - 0-day exploits
    - Evilgrade attacks

Verbosity



- Documents (2/2)
  - .rdp (2)
    - cia (1).rdp
      - Servers
      - Folders
    - tATOO.RDP
      - Servers
- Metadata Summary
  - Users (0)
  - Folders (1)
  - Printers (0)
  - Software (0)
  - Emails (0)
  - Operating Systems (0)
  - Passwords (0)
  - Servers (2)

Search engines

☑ Google
□ Bing
□ Exalead

Extensions

□ ods □ pdf □ svgz ☑ ica
□ odg □ wpd □ indd
□ odp □ svg ☑ rdp

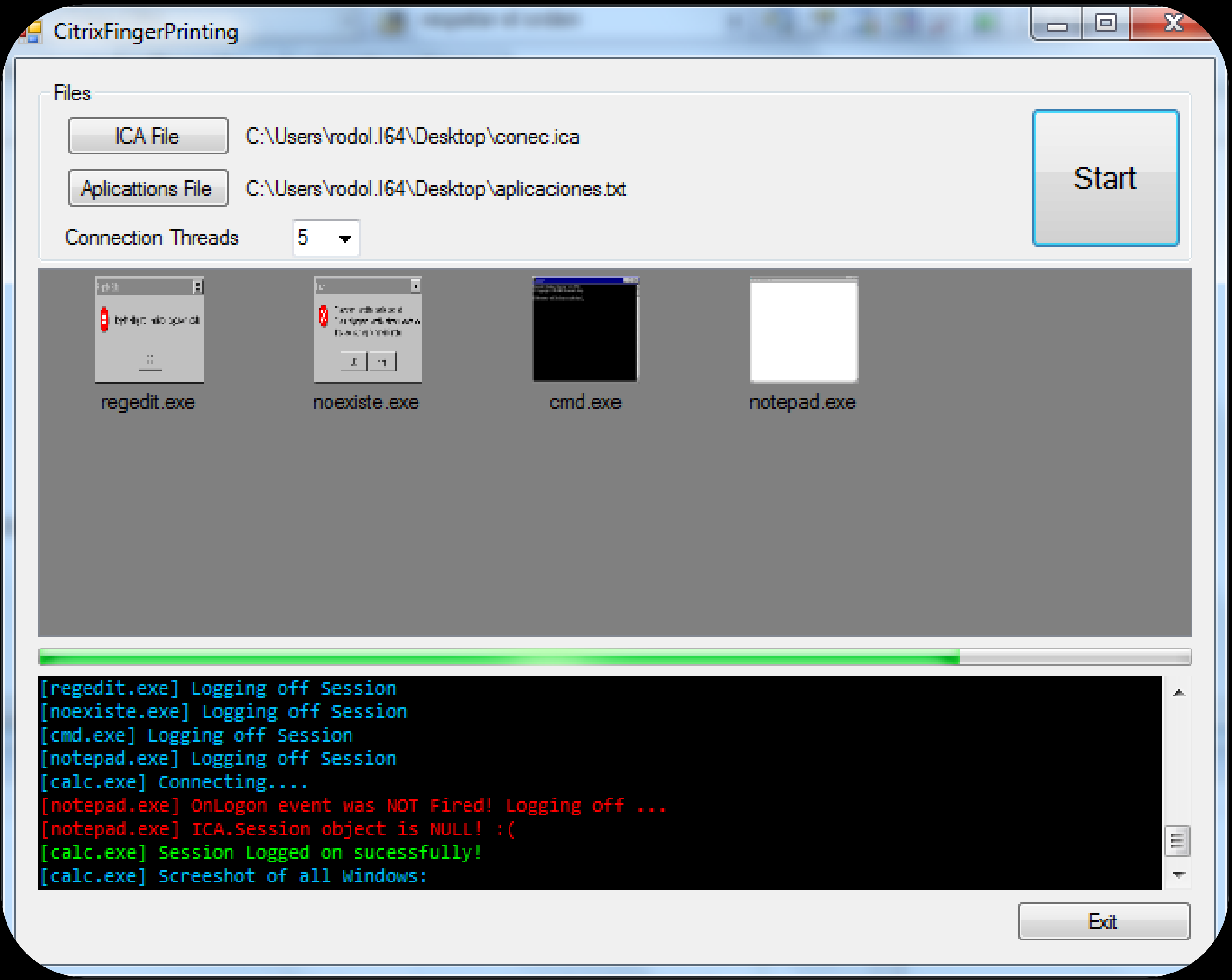
Id	Type	URL	Download	Download Date	Size	Analized
0	rdp	http://www.ciac[redacted]/cia.rdp	•	09/06/2011 14:03:48	1,23...	•
1	rdp	http://www.cosebius[redacted]DocCosebius/tATOO.RDP	•	09/06/2011 14:03:48	1,68...	•

All documents were analized

Verbosity

- Attacker can:
  - –modify conf files
  - –Generate error messages
  - –Fingerprinting all software
    - Example: C.A.C.A.

Computer Assited Citrix Apps



ICA File C:\Users\rodol.I64\Desktop\conec.ica

Aplicattions File C:\Users\rodol.I64\Desktop\aplicaciones.txt

Connection Threads 5

```
[regedit.exe] Logging off Session
[noexiste.exe] Logging off Session
[cmd.exe] Logging off Session
[notepad.exe] Logging off Session
[calc.exe] Connecting....
[notepad.exe] OnLogon event was NOT Fired! Logging off ...
[notepad.exe] ICA.Session object is NULL! :(
[calc.exe] Session Logged on sucessfully!
[calc.exe] Screeshot of all Windows:
```

Hash Stealing

- Modify the Conf file
- Run a remote app in a rogue Server
- Sniff the hash

Playing the Piano

Playing the Piano

- Too many links
  - Specially running on Windows 2008
- Too many environment variables
  - %SystemRoot%
  - %ProgramFiles%
  - %SystemDrive%

Playing the Piano

- Too many shortcuts
  - Ctrl + h – Web History
  - Ctrl + n – New Web Browser
  - Shift + Left Click – New Web Browser
  - Ctrl + o – Internet Addres
  - Ctrl + p – Print
  - Right Click (Shift + F10)
  - Save Image As
  - View Source
  - F1 –Jump to URL…

Playing the Piano

- Too , Too , Too many shorcuts:
  - ALT GR+SUPR = CTRL + ALT + SUP
  - CTRL + F1 = CTRL + ALT + SUP
  - CTRL + F3 = TASK MANAGER
- Sticky Keys

Easy?

Paths?

Minimun Exposure Paths

- There are as many paths as pulbished apps
- Every app is a path that could drive to elevate privileges
- Complex tools are better candidates
- Excel is a complex tool

Excel as a Path

- Office Apps are complex
- Too many security policies
  - Necesary to donwload extra GPOS
- Too many systems by default
  - No Security GPOs
  - Allowing non-signed Macros
  - Allowing third-part-signed macros
  - Allowing CA to be added

Excel 1

Software Restriction Policies

- Forbidden apps
  - Via hash
  - Via path
- App Locker
  - Using Digital Certificates
- ACLs

Software Restriction Policies

- Too many consoles
  - Cmd.exe
  - Windows Management Instrumentation
  - PowerShell
- Even consoles from other OS
  - ReactOS

Excel 2

Risky?

Start the III World War

- Find a bug in a DHS Computer
- Getting to the OS
- Sing an excel file with a rogue CA
- Generate an attacking URL in the CRL to attack… China
- Send a digital signed-excel file…

Just kidding

Contact information

- Juan Garrido “Silverhack”
  - jgarrido@informatica64.com
- Chema Alonso
  - chema@informatica64.com
  - @chemaalonso
- http://www.informatica64.com