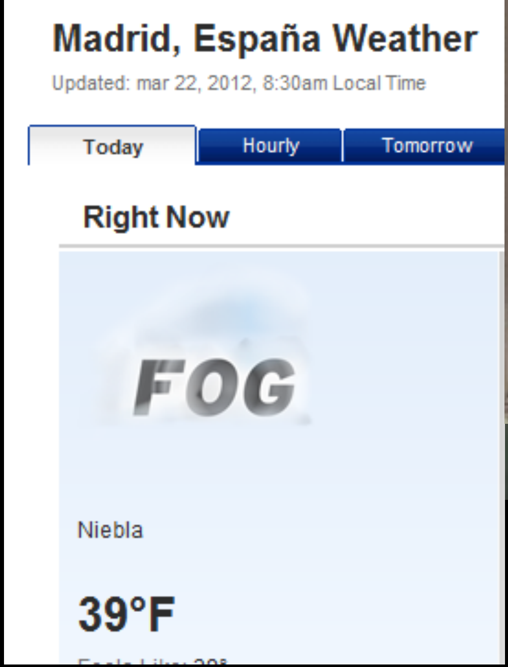
Excel (and Office apps) Kills the Citrix (or Terminal Services) Star

Chema Alonso
(@chemaalonso)
chema@informatica64.com

Español

I’m disappointed



Madrid, España Weather

Updated: mar 22, 2012, 8:30am Local Time

Right Now

FOG

Niebla

39°F

Feels Like: 39°

We want in exchange:

PORSCHE
STUTTGART

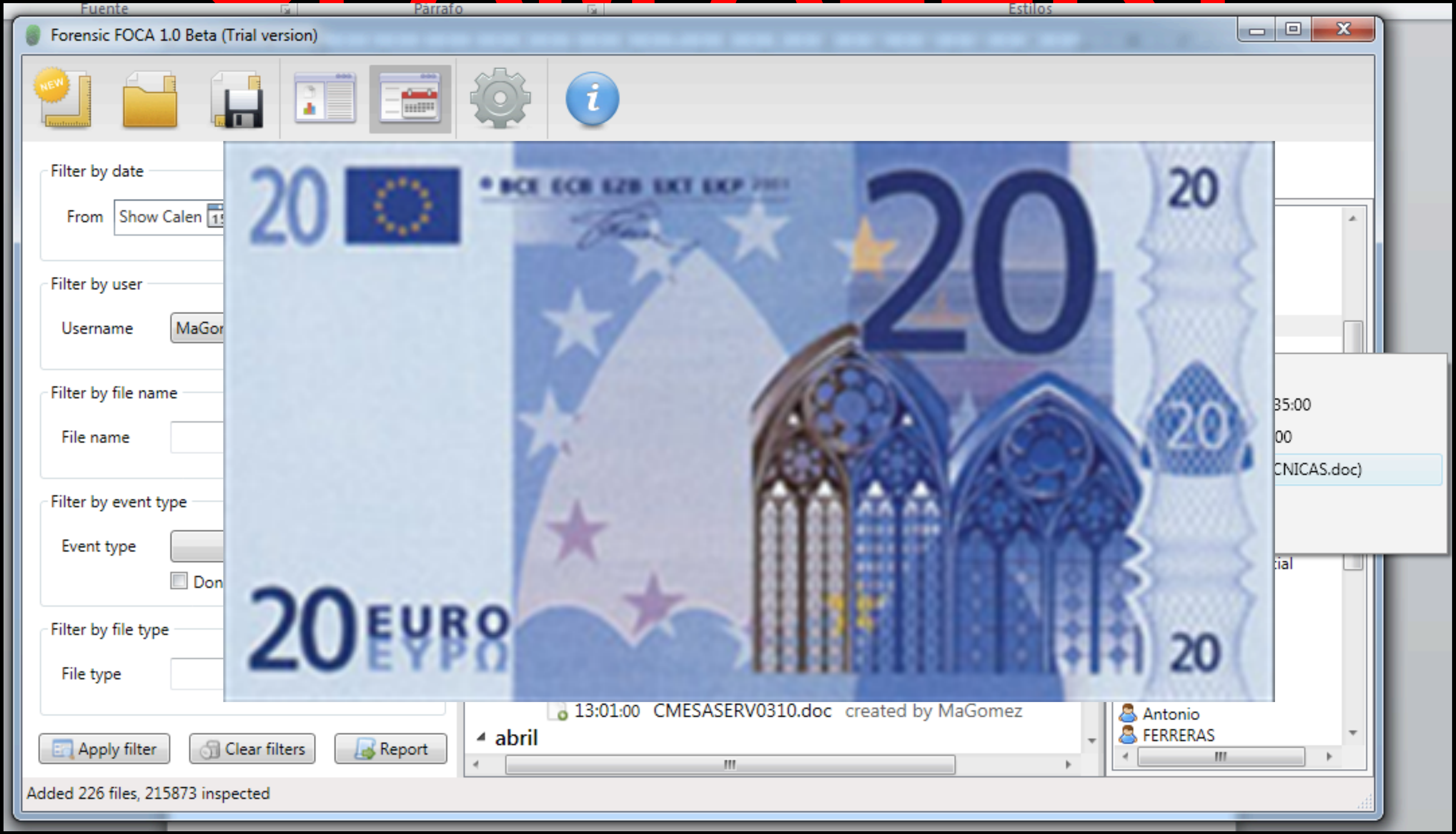
Mercedes-Benz

Who?

About

- Working at INFORMATICA64.COM
- http://www.informatica64.com

SPAM ALERT



From: Show Calen

Username: MaGor

File name:

Event type:

□ Don

File type:

35:00

00

CNICAS.doc)

tial

13:01:00 CMESASERV0310.doc created by MaGomez

abril

Antonio

FERRERAS

Added 226 files, 215873 inspected

http://www.informatica64.com/forensicfoca/

What

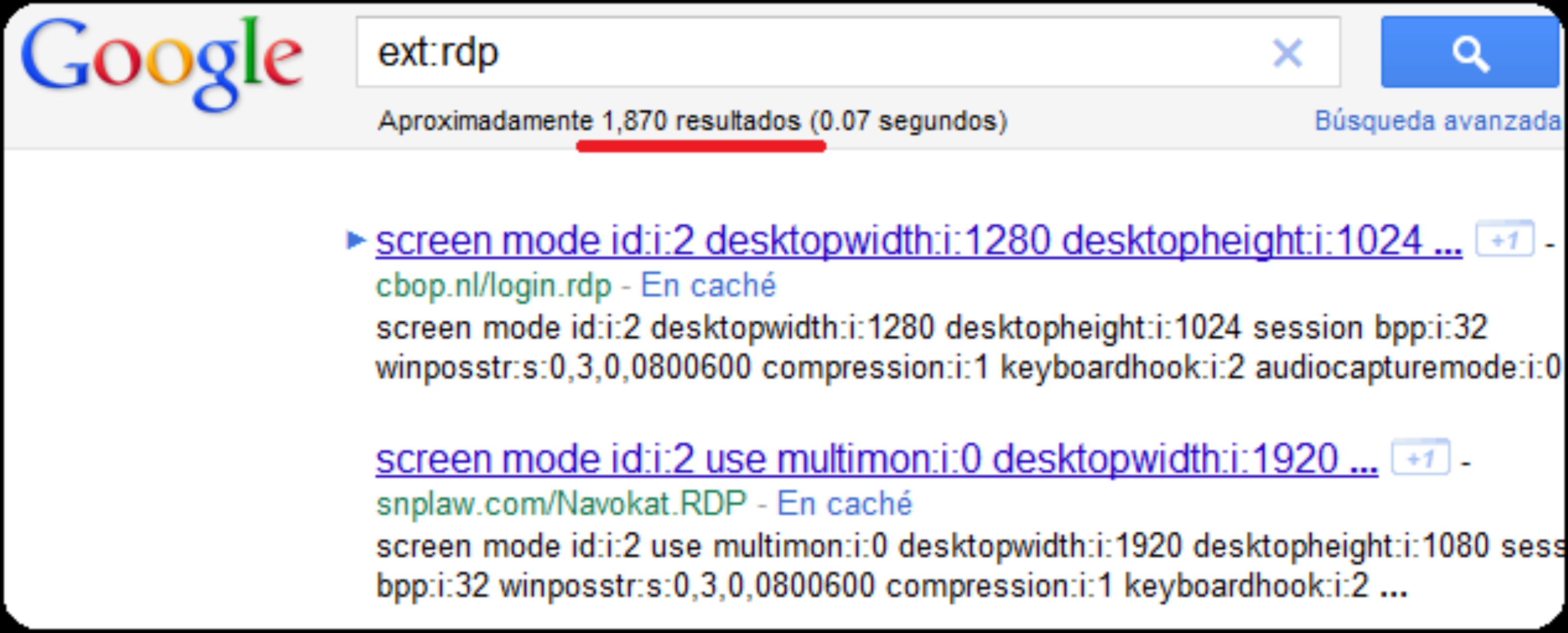
?

Terminal Applications

Kung-Fu Panda Talk

Why?

RDP



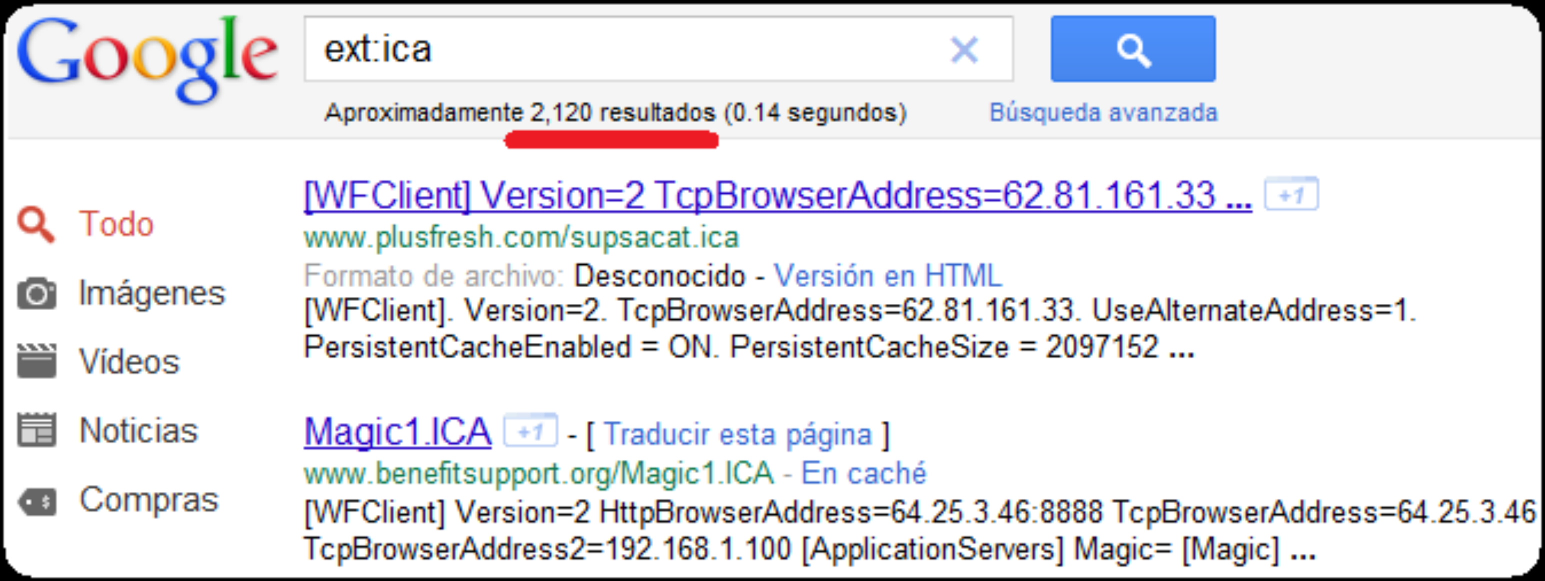
ext:rdp

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

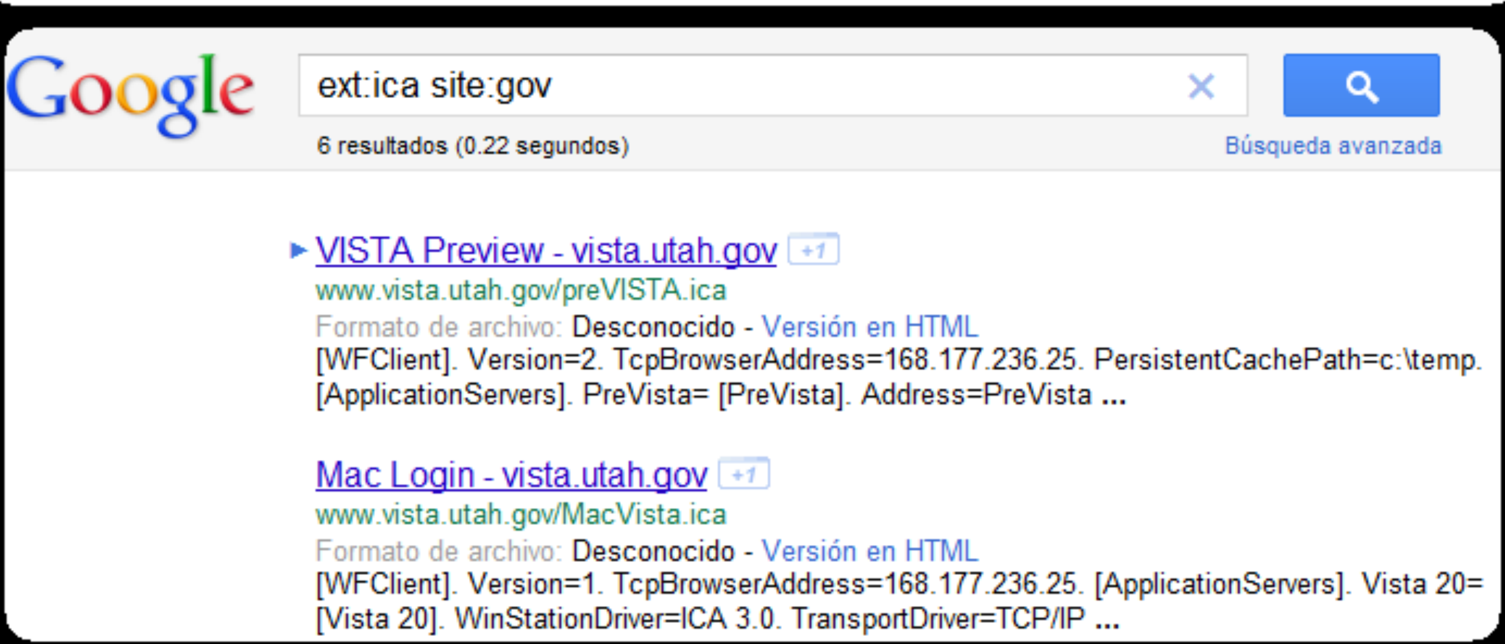


ext:ica

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] ...



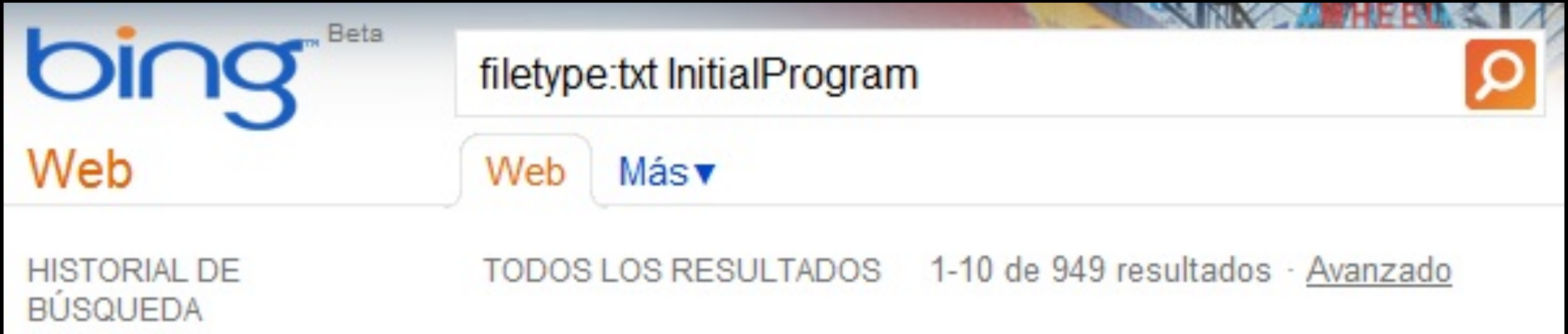
ext:ica site:gov

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 ...

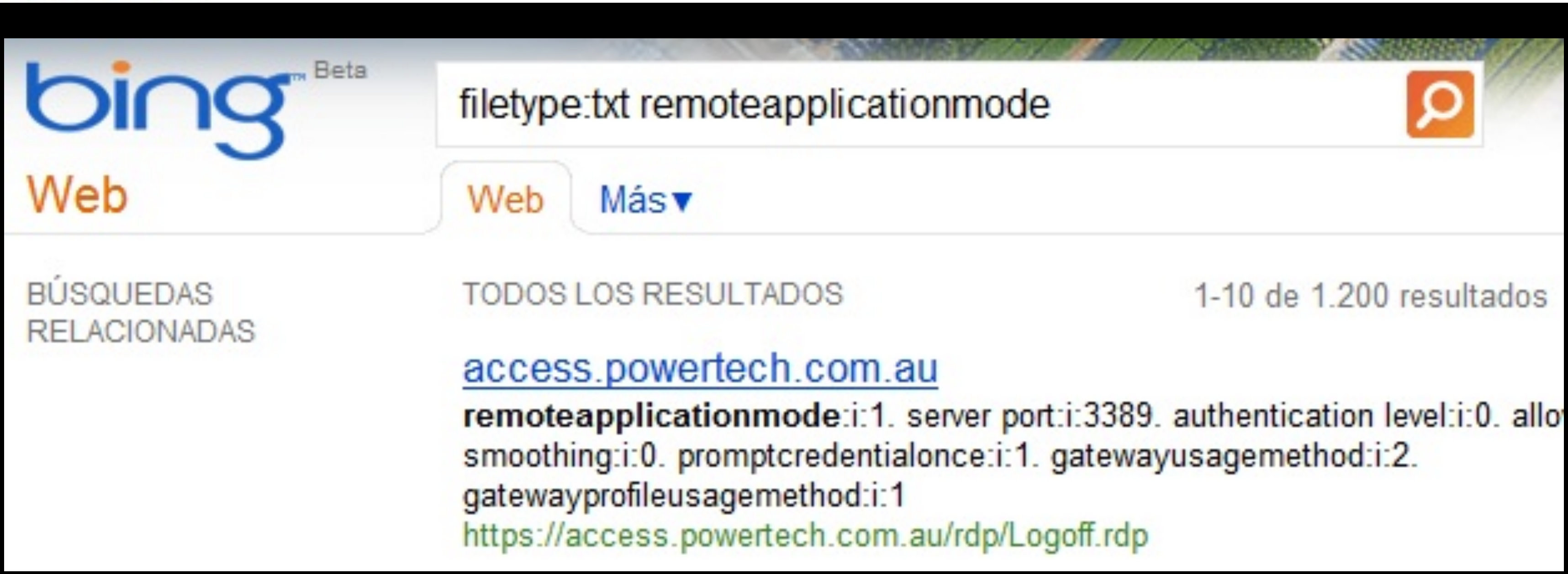
Mac Login - vista.utah.gov
www.vista.utah.gov/MacVista.ica
Formato de archivo: Desconocido - Versión en HTML
[WFClient]. Version=1. TcpBrowserAddress=168.177.236.25. [ApplicationServers]. Vista 20= [Vista 20]. WinStationDriver=ICA 3.0. TransportDriver=TCP/IP ...

Using Bing



filetype:txt InitialProgram

1-10 de 949 resultados · Avanzado



filetype:txt remoteapplicationmode

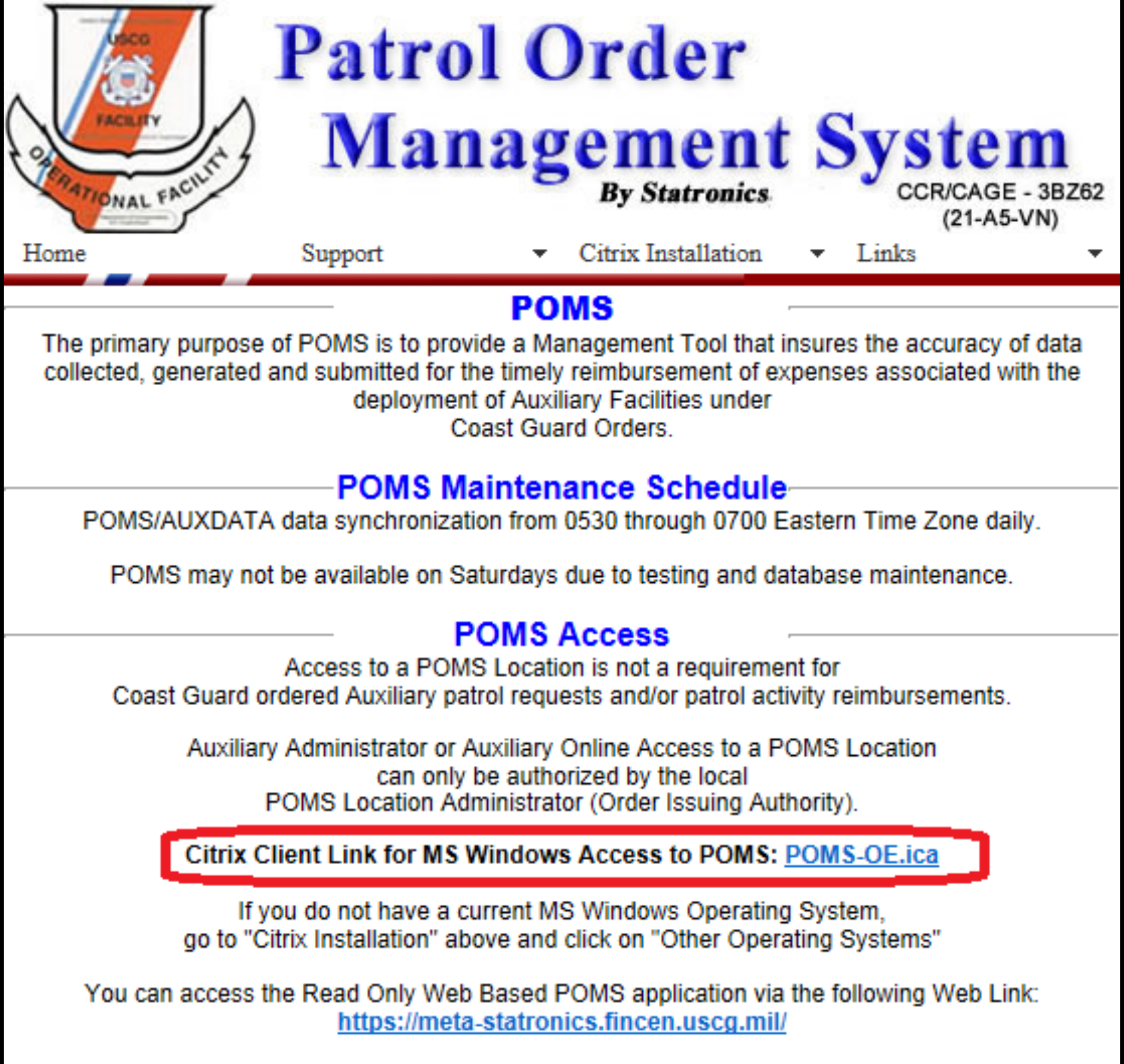
1-10 de 1.200 resultados

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

Goverment Sites



Patrol Order Management System

By Statronics

CCR/CAGE - 3BZ62
(21-A5-VN)

POMS

The primary purpose of POMS is to provide a Management Tool that insures the accuracy of data collected, generated and submitted for the timely reimbursement of expenses associated with the deployment of Auxiliary Facilities under
Coast Guard Orders.

POMS Maintenance Schedule

POMS/AUXDATA data synchronization from 0530 through 0700 Eastern Time Zone daily.

POMS may not be available on Saturdays due to testing and database maintenance.

POMS Access

Access to a POMS Location is not a requirement for
Coast Guard ordered Auxiliary patrol requests and/or patrol activity reimbursements.

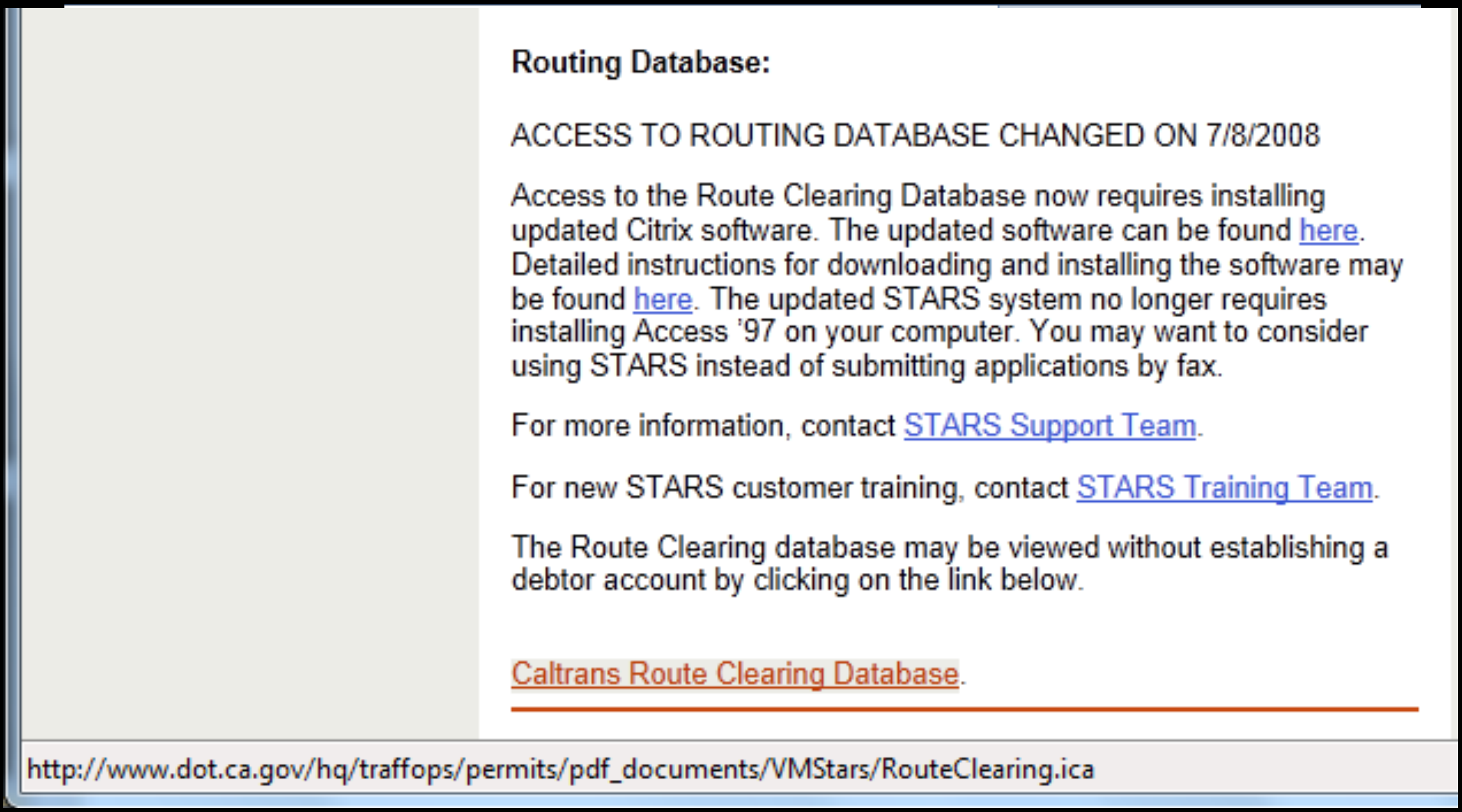
Auxiliary Administrator or Auxiliary Online Access to a POMS Location
can only be authorized by the local
POMS Location Administrator (Order Issuing Authority).

Citrix Client Link for MS Windows Access to POMS: POMS-OE.ica

If you do not have a current MS Windows Operating System,
go to "Citrix Installation" above and click on "Other Operating Systems"

You can access the Read Only Web Based POMS application via the following Web Link:
https://meta-statronics.fincen.uscg.mil/

Goverment Sites



Routing Database:

ACCESS TO ROUTING DATABASE CHANGED ON 7/8/2008

Access to the Route Clearing Database now requires installing updated Citrix software. The updated software can be found here. Detailed instructions for downloading and installing the software may be found here. The updated STARS system no longer requires installing Access '97 on your computer. You may want to consider using STARS instead of submitting applications by fax.

For more information, contact STARS Support Team.

For new STARS customer training, contact STARS Training Team.

The Route Clearing database may be viewed without establishing a debtor account by clicking on the link below.

Caltrans Route Clearing Database.

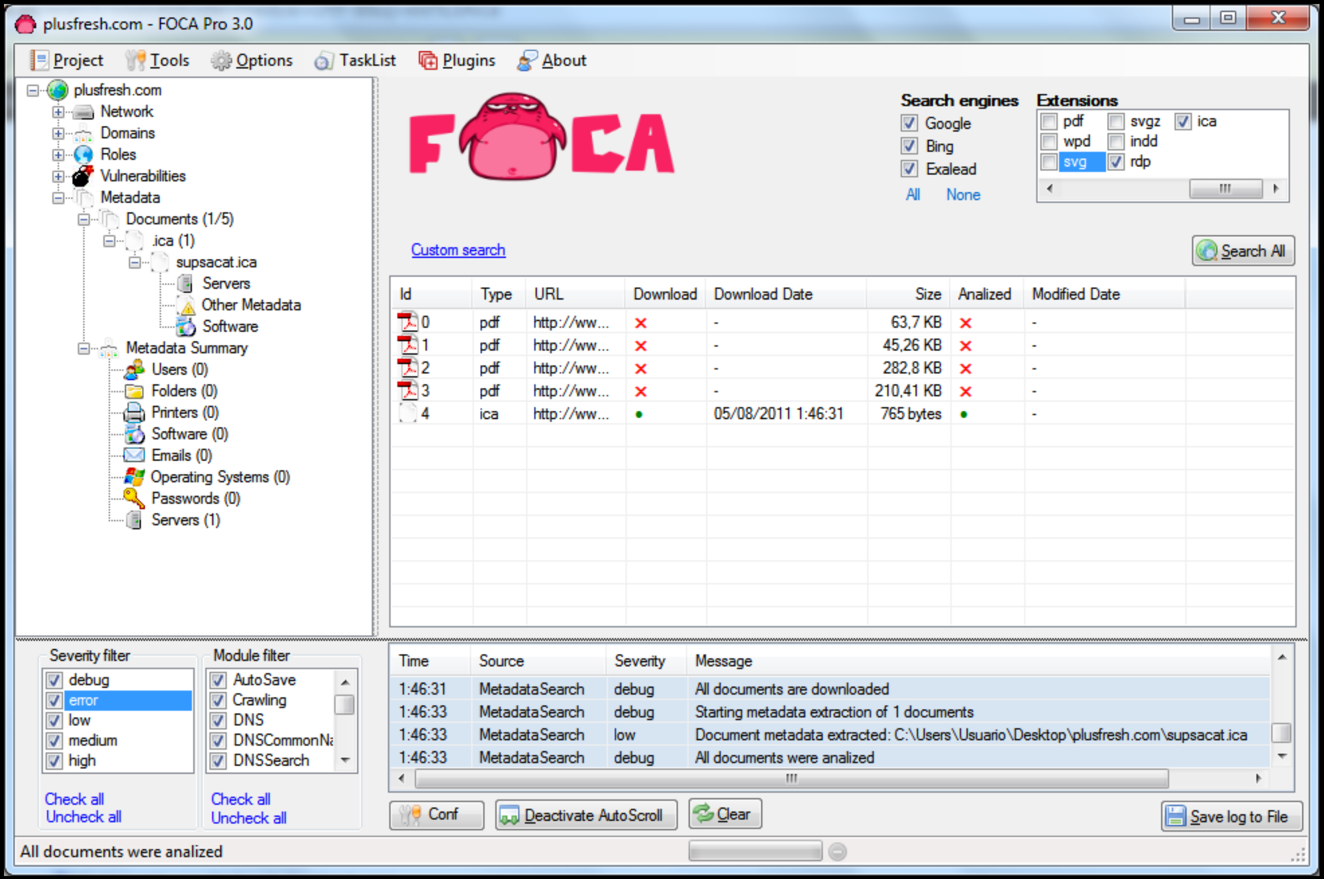
http://www.dot.ca.gov/hq/traffops/permits/pdf_documents/VMStars/RouteClearing.ica

Secure?

Verbosity

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

Verbosity



- plusfresh.com
  - Network
  - Domains
  - Roles
  - Vulnerabilities
  - Metadata
    - Documents (1/5)
      - .ica (1)
        - supsacat.ica
          - Servers
          - Other Metadata
          - Software
    - Metadata Summary
      - Users (0)
      - Folders (0)
      - Printers (0)
      - Software (0)
      - Emails (0)
      - Operating Systems (0)
      - Passwords (0)
      - Servers (1)

Search engines: ☑ Google ☑ Bing ☑ Exalead

Extensions: □ pdf □ svgz ☑ ica □ wpd □ indd □ svg ☑ rdp

Id	Type	URL	Download	Download Date	Size	Analized	Modified Date
0	pdf	http://ww...	✗	-	63,7 KB	✗	-
1	pdf	http://ww...	✗	-	45,26 KB	✗	-
2	pdf	http://ww...	✗	-	282,8 KB	✗	-
3	pdf	http://ww...	✗	-	210,41 KB	✗	-
4	ica	http://ww...	●	05/08/2011 1:46:31	765 bytes	●	-

Severity filter: ☑ debug ☑ error ☑ low ☑ medium ☑ high

Module filter: ☑ AutoSave ☑ Crawling ☑ DNS ☑ DNSCommonNa ☑ DNSSearch

Time	Source	Severity	Message
1:46:31	MetadataSearch	debug	All documents are downloaded
1:46:33	MetadataSearch	debug	Starting metadata extraction of 1 documents
1:46:33	MetadataSearch	low	Document metadata extracted: C:\Users\Usuario\Desktop\plusfresh.com\supsacat.ica
1:46:33	MetadataSearch	debug	All documents were analized

All documents were analized

9th of April: FOCA PRO Online Seminar in english

http://www.informatica64.com/foca.aspx

Book and get one of the most lovely FOCA PRO 3.1

Sorry, No CLI, No Linux version Yet

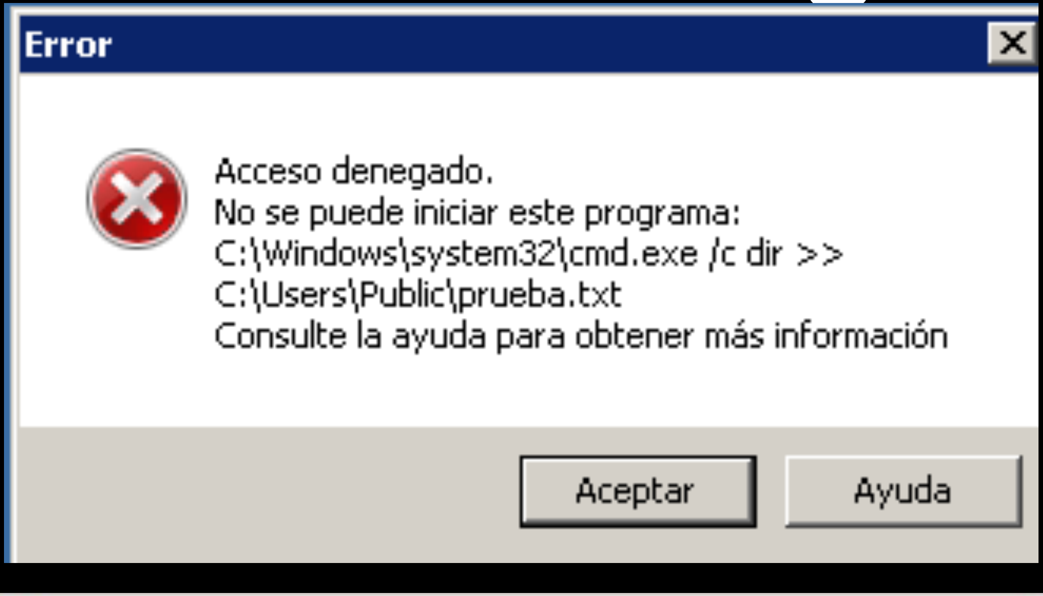
Verbosity

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

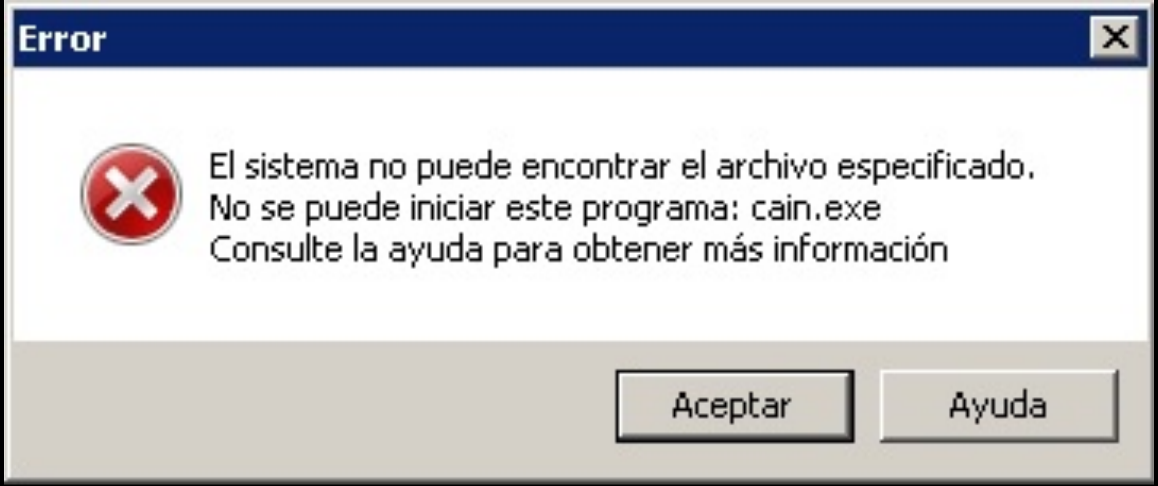
Terminal Services

- Remoteapplicationmode
  - 0 -> Desktop
  - 1 -> Only App
- What app?
  - Alternate Shell (RDP < v 6.0)
  - RempoteApplicationProgram (RDP v 6.0++)

Terminal Services Error Messages

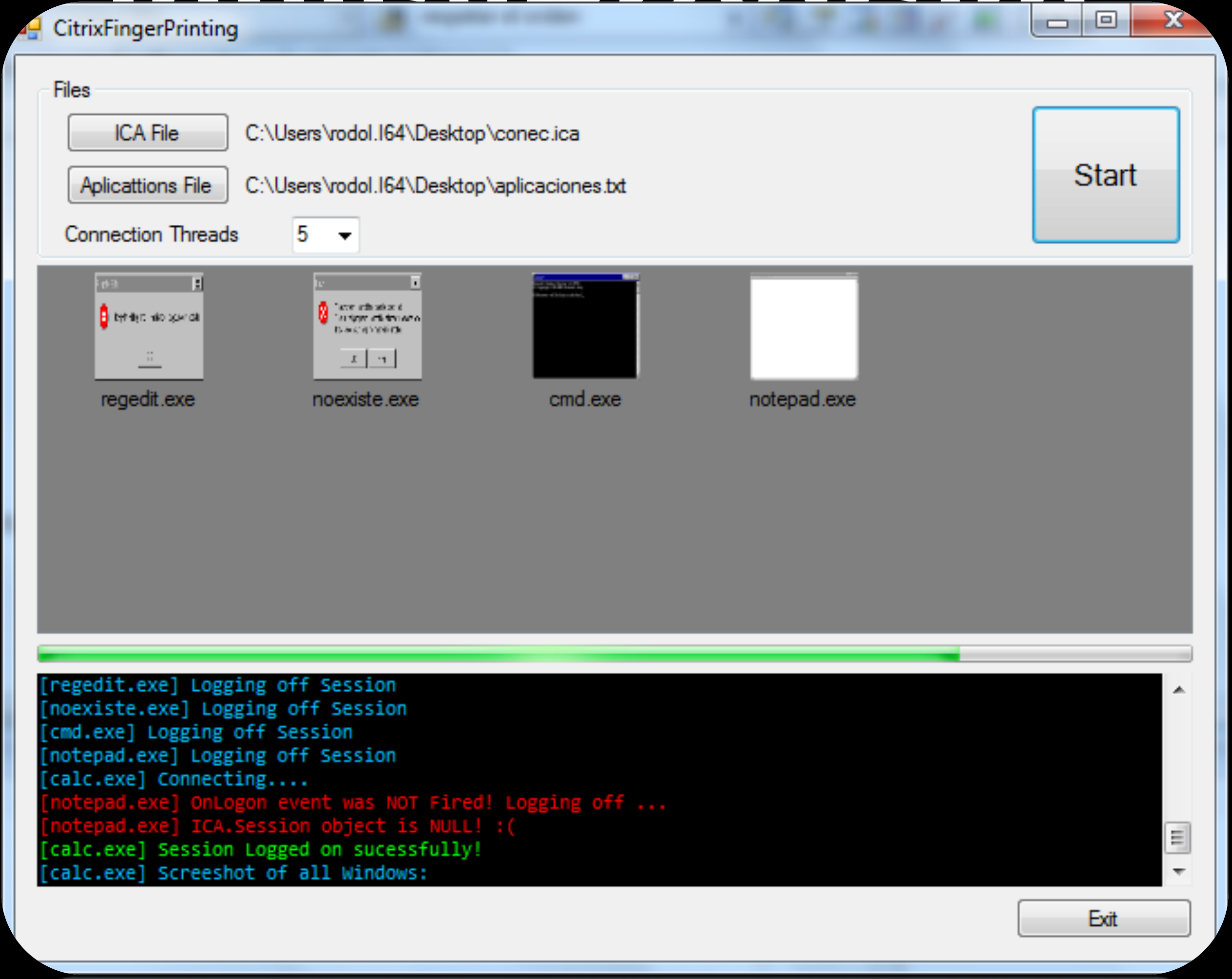


Acceso denegado.
No se puede iniciar este programa:
C:\Windows\system32\cmd.exe /c dir >>
C:\Users\Public\prueba.txt
Consulte la ayuda para obtener más información



El sistema no puede encontrar el archivo especificado.
No se puede iniciar este programa: cain.exe
Consulte la ayuda para obtener más información

Computer Assited Citrix Apps InnitalProgram



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

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

Connection Threads: 5

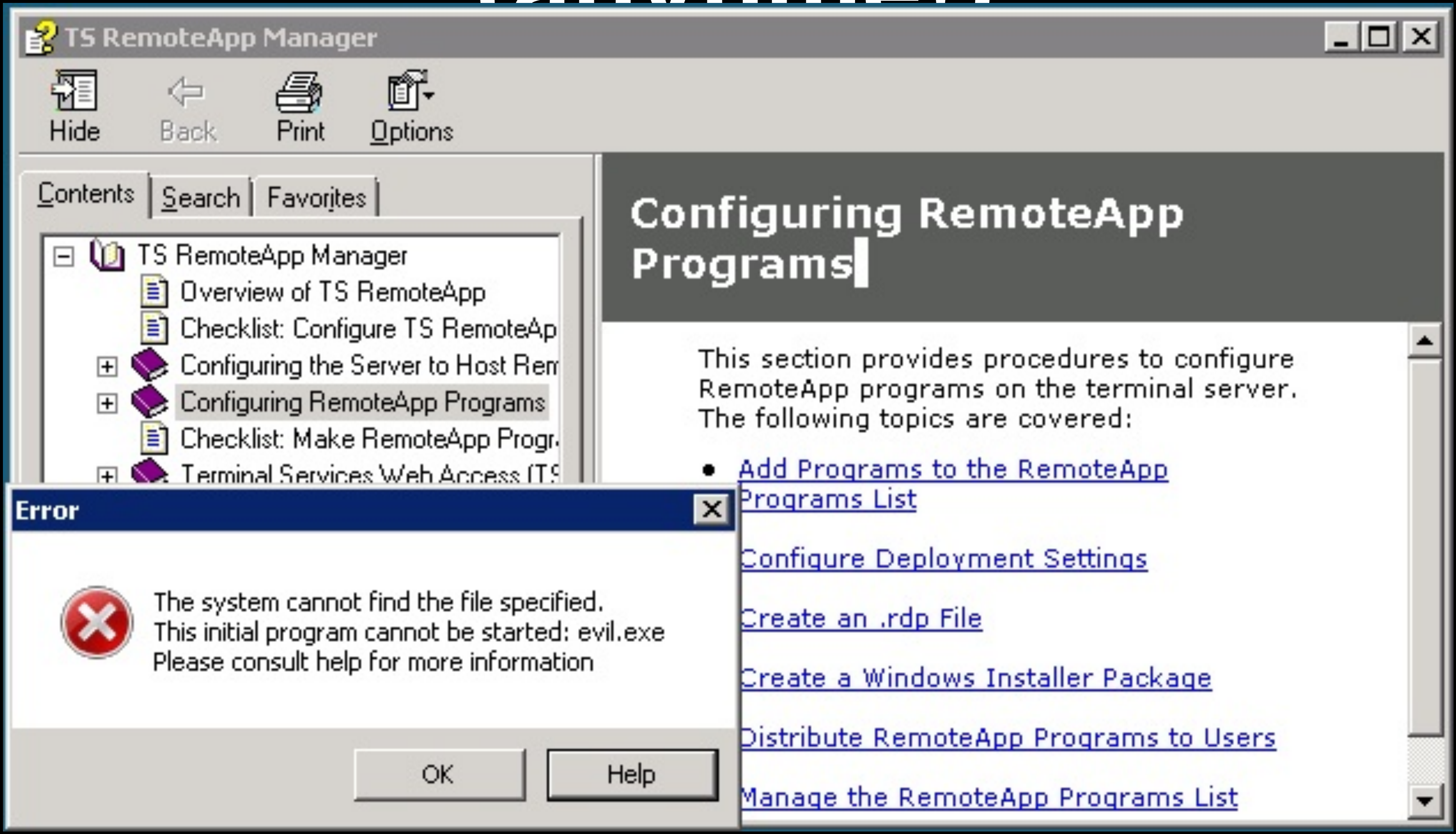
```
[regedit.exe] Logging off Session
[noexiste.exe] Logging off Session
[cmd.exe] Logging off Session
[notepad.exe] Logging off Session
[calc.exe] Connecting....
[notepad.exe] OnLogon event was NOT Fired! Logging off ...
[notepad.exe] ICA.Session object is NULL! :(
[calc.exe] Session Logged on sucessfully!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

Playing the Piano

Playing the Piano

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

Window Server 2008 wants to help you!! (anytime!)


TS RemoteApp Manager
Hide
Back
Print
Options
Contents
Search
Favorites
TS RemoteApp Manager
Overview of TS RemoteApp
Checklist: Configure TS RemoteAp
Configuring the Server to Host Rem
Configuring RemoteApp Programs
Checklist: Make RemoteApp Progr
Terminal Services Web Access (TS

Configuring RemoteApp Programs

This section provides procedures to configure RemoteApp programs on the terminal server. The following topics are covered:

- Add Programs to the RemoteApp Programs List

  Configure Deployment Settings

  Create an .rdp File

  Create a Windows Installer Package

  Distribute RemoteApp Programs to Users

  Manage the RemoteApp Programs List

Error

The system cannot find the file specified.
This initial program cannot be started: evil.exe
Please consult help for more information

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?

Demo Servers

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

Bosses love EXCEL

VBA

Excel 1:

The power of VBA

Software Restriction Policies

- Too many consoles
  - Cmd.exe
  - Windows Management Instrumentation
  - PowerShell
  - Jscript
  - Cscript..
  - ….

Software Restriction Policies

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

Software Restriction Policies

- Too many consoles,
  - (Even frOm other OS)
  - Reactos….

Excel

2

forbidden Consoles

Security Polices for Excel Macros

1) Disable VBA

- Secure but it´s not REAL Excel

2) Security for macros

- No macros
- signed macros
- Case by case
- All macros

Excel

3

No macros!

Excel 4

Only Signed-macros

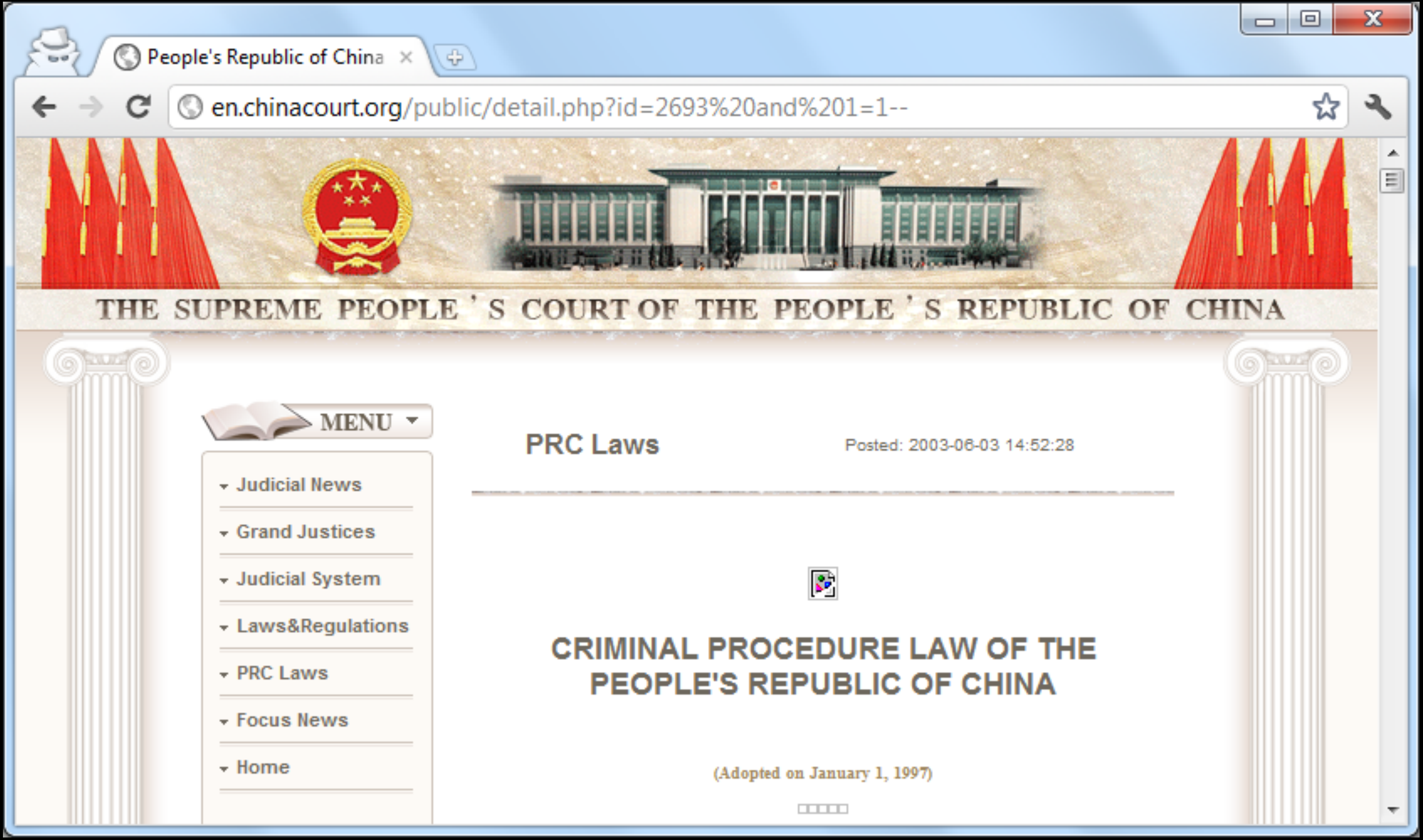
Risky

?

Start the III World War

- Find a bug in a DHS Computer
- Trust in your Rogue CA
- Generate an attacking URL in the CRL (attacking China, for example)
- Sign an excel file with your rogue CA
- Send a digital ly-signed excel file to someone relevant!

Something like…



en.chinacourt.org/public/detail.php?id=2693%20and%201=1--

THE SUPREME PEOPLE'S COURT OF THE PEOPLE'S REPUBLIC OF CHINA

PRC Laws

Posted: 2003-06-03 14:52:28

CRIMINAL PROCEDURE LAW OF THE PEOPLE'S REPUBLIC OF CHINA

(Adopted on January 1, 1997)

Just kidding

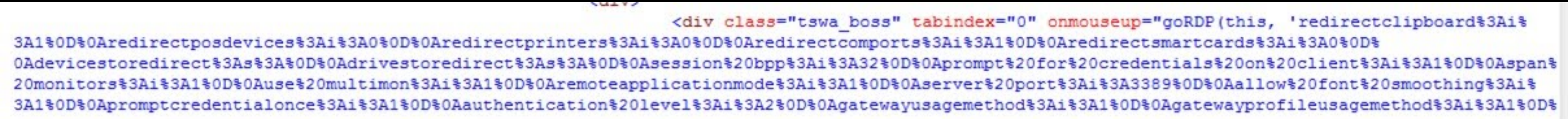
Final demo

Solutions

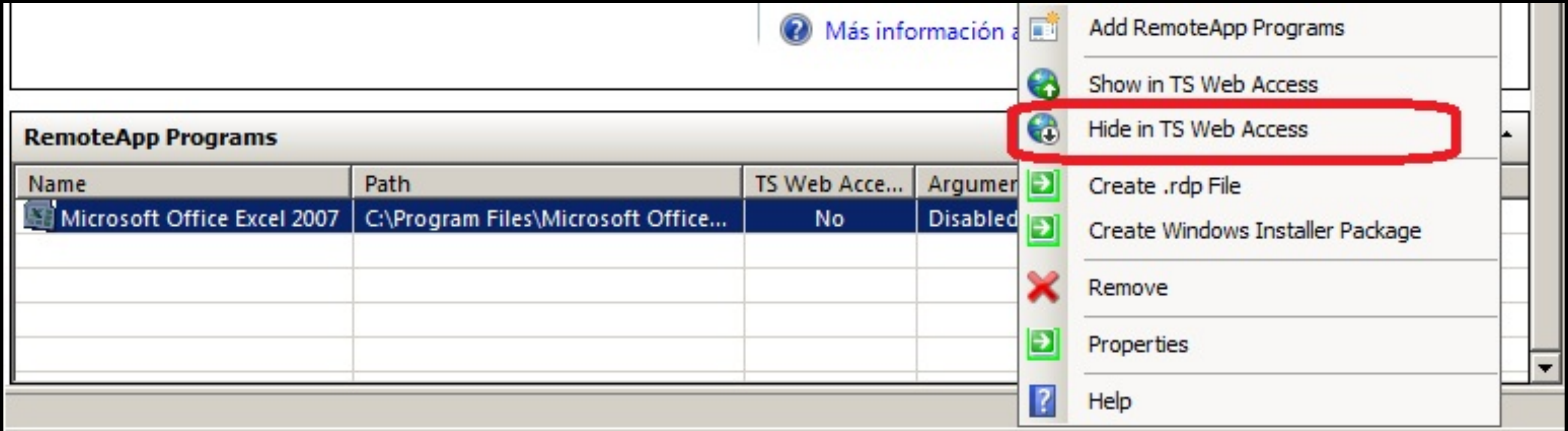
- Re-evaluate your Remote App connections
- No alerts at all in Excel (and all the rest of apps you publish)
- No trusted locations in user-profiles
- No shared remote users
- Trust in nobodoy…
- Sorry, not even in nobody

How may paths do you have?

- TS Web Access
  - –Hidden means not-removed



```
                                        <div class="tswa_boss" tabindex="0" onmouseup="goRDP(this, 'redirectclipboard%3Ai%
3A1%0D%0Aredirectposdevices%3Ai%3A0%0D%0Aredirectprinters%3Ai%3A0%0D%0Aredirectcomports%3Ai%3A1%0D%0Aredirectsmartcards%3Ai%3A0%0D%
0Adevicestoredirect%3As%3A%0D%0Adrivestoredirect%3As%3A%0D%0Asession%20bpp%3Ai%3A32%0D%0Aprompt%20for%20credentials%20on%20client%3Ai%3A1%0D%0Aspan%
20monitors%3Ai%3A1%0D%0Ause%20multimon%3Ai%3A1%0D%0Aremoteapplicationmode%3Ai%3A1%0D%0Aserver%20port%3Ai%3A3389%0D%0Aallow%20font%20smoothing%3Ai%
3A1%0D%0Apromptcredentialonce%3Ai%3A1%0D%0Aauthentication%20level%3Ai%3A2%0D%0Agatewayusagemethod%3Ai%3A1%0D%0Agatewayprofileusagemethod%3Ai%3A1%0D%
```



RemoteApp Programs

Name	Path	TS Web Acce...	Argumen
Microsoft Office Excel 2007	C:\Program Files\Microsoft Office...	No	Disabled

Contact information

- Chema Alonso
  - chema@informatica64.com
  - http://www.elladodelmal.com
  - @chemaalonso
- http://www.informatica64.com

Special Thanks to

- Juan Garrido “Silverhack”
  - jgarrido@informatica64.com
  - http://windowstips.wordpress.com
- Didier Stevens
  - http://blog.didierstevens.com/2010/02/04/cmd-dll/
- Shanit Gupta
  - http://www.blackhat.com/presentations/bh-usa-08/Gupta/BH_US_08_Gupta_Got_Citrix_Hack_IT.pdf
- PDP
  - http://www.blackhat.com/presentations/bh-europe-08/Petkov/Presentation/bh-eu-08-petkov.pdf

?