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
Why?
RDP
Cítrix
Using Bing
Secure?
verbosity

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

• Attacker can:
  – modify conf files
  – Generate error messages
  – Fingerprinting all software

• Example: C.A.C.A.
Computer Assisted Citrix Apps
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 Address
  – Ctrl + p – Print
  – Right Click (Shift + F10)
  – Save Image As
  – View Source
  – F1 – Jump to URL…
Playing the Piano

• Too, Too, Too many shortcuts:
  - ALT GR + SUPR = CTRL + ALT + SUP
  - CTRL + F1 = CTRL + ALT + SUP
  - CTRL + F3 = TASK MANAGER

• Sticky Keys
Easy?
Paths?
Minimum Exposure Paths

• There are as many paths as published 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
  - Necessary to download 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