

掃吧你！從協議面抓出機歪的 遠端桌面後門

orange@chroot.org

About Me



- 蔡政達 aka Orange
- CHROOT 成員
- DEVCORE Security Consultant
- HITCON, PHPCONF, PYCON ...等講師
- 揭露過 Microsoft, Django, Yahoo ...等漏洞
- 專精於駭客手法、Web Security 與網路滲透

水議題? 老議題?

old issue ?

yes, it is.

遠端桌面後門?

Remote Desktop Backdoor ?

遠端桌面 "相黏鍵" 後門?

Remote Desktop "StickKeys" Backdoor ?

遠端桌面後門?

- 透過再未輸入有效登入憑證的狀況下，使用作業系統自帶的功能繞過限制。

安裝方法

- C:\windows\system32\sethc.exe
 - shift * 5
- C:\windows\system32\utilman.exe
 - Windows + U
- C:\windows\system32\osk.exe
 - 輔助鍵盤
- ...

安裝方法 v1

- 直接覆蓋

- copy /y cmd.exe C:\windows\system32\sethc.exe
- copy /y cmd.exe :\\windows\system32\dlldatacache
\\sethc.exe
- takeown /f sethc.exe
- echo y | cacls sethc.exe /G administrator:F

安裝方法 v2

- 映像劫持

- EXEC master..xp_regwrite

- 'HKEY_LOCAL_MACHINE',

- 'SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Image File Execution Options\sethc.exe',


- 'debugger',

- 'reg_sz',

- 'C:\windows\system32\cmd.exe'

如果要用圖片來說明

Log On to Windows




Microsoft
Windows Server 2003 R2
Datacenter x64 Edition

Copyright © 2005 Microsoft Corporation Microsoft

User name:

Password:

Log On to Windows



Microsoft
Windows Server 2003 R2
Datacenter Edition

Copyright © 2005 Microsoft Corporation Microsoft

User name:

StickyKeys X

Pressing the SHIFT key 5 times turns on StickyKeys. StickyKeys lets you use the SHIFT, CTRL, ALT, or Windows Logo keys by pressing one key at a time.

To keep StickyKeys on, click OK.
To cancel StickyKeys, click Cancel.
To deactivate the key combination for StickyKeys, click Settings.

Log On to Windows



Microsoft
Windows Server 2003 R2
Datacenter x64 Edition

Copyright © 2005 Microsoft Corporation

Microsoft

User name:

Password:

C:\WINDOWS\system32\sethc.exe

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

```
C:\WINDOWS\system32>net user orange orange /add_
```

Log On to Windows



Microsoft
Windows Server 2003 R2
 Enterprise Edition

Microsoft

tion

Microsoft

Windows Task Manager

File Options View Help

Applications Processes Performance Networking Users

Image Name	User Name	CPU	Mem Usage
sethc.exe	SYSTEM	00	5,676 K
ctfmon.exe *32	Administrator	00	160 K
logon.scr	LOCAL SERVICE	00	2,372 K
ctfmon.exe	Administrator	00	436 K
wmiprvse.exe	NETWORK SERVICE	00	9,056 K
explorer.exe	Administrator	00	3,300 K
vssvc.exe	SYSTEM	00	5,744 K
svchost.exe	SYSTEM	00	5,524 K
rdpclip.exe	Administrator	00	452 K
wmiprvse.exe	NETWORK SERVICE	00	25,420 K
csrss.exe	SYSTEM	00	4,308 K
alg.exe	LOCAL SERVICE	00	4,376 K
wmiprvse.exe	SYSTEM	00	8,052 K
winlogon.exe	SYSTEM	00	7,452 K
svchost.exe	SYSTEM	00	7,588 K
XenGuestAgent.exe	SYSTEM	00	43,096 K
Ec2Config.exe	SYSTEM	00	47,344 K
cmd.exe	Administrator	00	120 K
svchost.exe	NETWORK SERVICE	00	5,940 K

Show processes from all users

End Process

Processes: 38

CPU Usage: 0%

Commit Charge: 336M / 2433M

Cancel

Shut Down...

Options <<

Log On to Windows



Local Disk (C:) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Home Search Folders

Address Go Links

System Tasks

- Hide the contents of this drive
- Add or remove programs
- Search for files or folders

File and Folder Tasks

- Make a new folder
- Publish this folder to the Web
- Share this folder

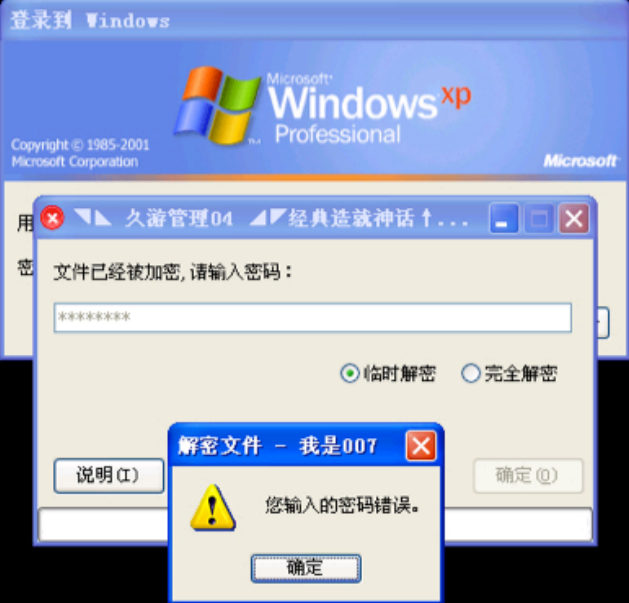
Other Places

- My Computer
- My Documents
- My Network Places

Details

ADFS	Documents and Settings
Program Files	Program Files (x86)
WINDOWS	wmpub

當然，笨蛋才不加密



登录到 Windows



Copyright © 1985-2001
Microsoft Corporation

Microsoft

用户名 (U):

密码 (P):

确定

取消

选项 (O) >>

登录到 Windows



Copyright © 1985-2001
Microsoft Corporation

Microsoft

用户名 (U):

密码 (P):

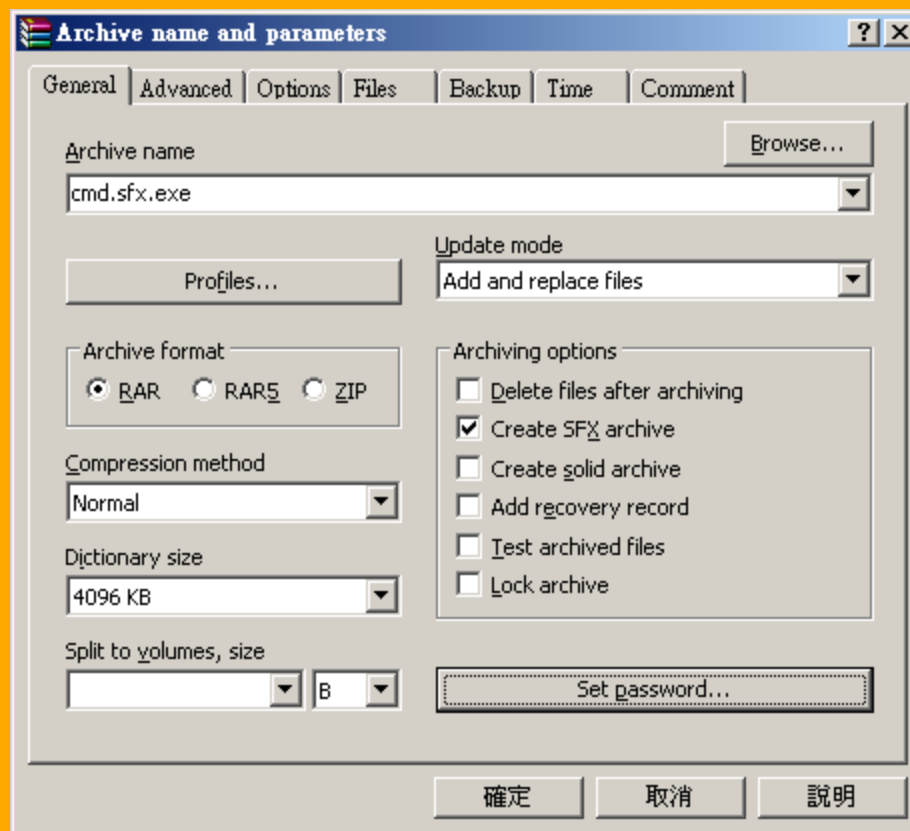
确定

取消

选项 (O) >>

test1234

當然，有些也是可以被繞過的



Enter password [X]

Archiving with password

Enter password

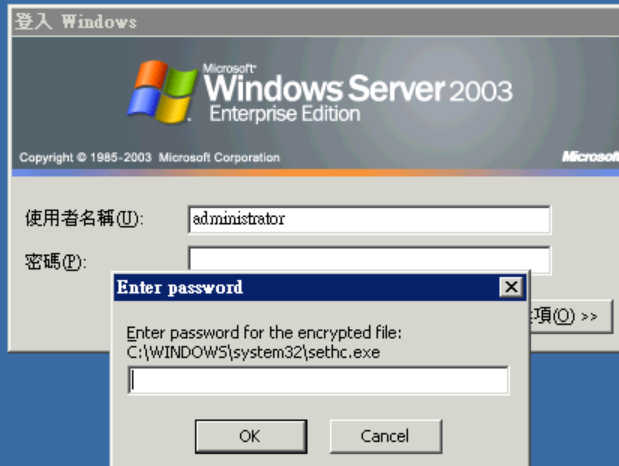
Reenter password for verification

Show password

Encrypt file names


Organize passwords...

OK Cancel Help



登入 Windows

WinRAR self-extracting archive



Checksum error in the encrypted file C:\WINDOWS\system32\sethc.exe. Corrupt file or wrong password.

Destination folder
C:\WINDOWS\system32 Browse...

Extraction progress

Extract Cancel

登入 Windows

WinRAR self-extracting archive

Checksum error in the encrypted file C:\WINDOWS\system32

瀏覽資料夾

Select destination folder

- 桌面
- 我的文件
- 我的電腦
- 網路上的芳鄰

建立新資料夾(M) 確定 取消

Browse...

Extract Cancel

SYSTEM

- 管理您的伺服器
- 命令提示字元
- Windows 檔案總管
- 記事本
- 所有程式 (A) ▶

- 我的電腦
- 控制台 (C)
- 系統管理工具
- 印表機和傳真
- 說明及支援 (H)
- 搜尋 (S)
- 執行 (R)...
- Windows 安全性 (W)

登出 (L) 關機 (U)

登入 Windows



Copyright © 1985-2003 Microsoft Corporation

使用者名稱 (U):

密碼 (P):

確定 取消 選項 (O) >>

到檔案或項目 %/idlist,552:3300,C:\WINDOWS\system32\config\systemprofile\My'。請檢查鍵入的名稱是否正確，再試一次。要搜尋 [開始] 按鈕，然後按 [搜尋]。

確定

建立新資料夾 (M) 確定 取消

Browse...

Extract Cancel



Windows 2000 輸入法漏洞

講古



What I Want to Do ?

What I Want to Do ?

- RDP Scanner
 1. RDP Info
 2. Check Backdoor
 3. Maybe check weak password
- `./rdp_scan 0.0.0.0/0`

有沒有工具可以檢測這種後門?

當需要批量檢查時怎麼辦?

From BH 03

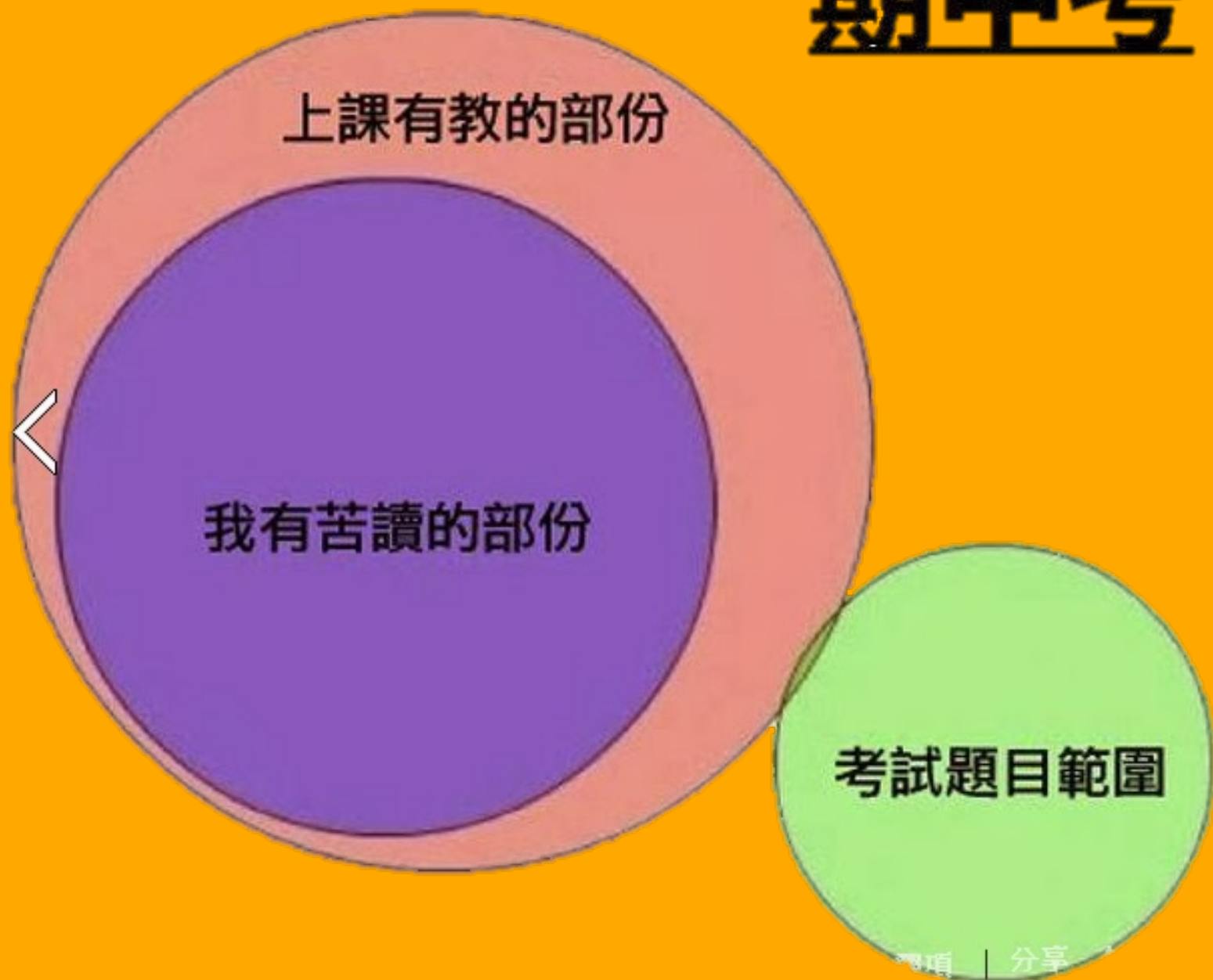
- Windows 2000 mstsc.exe has an undocumented API
 - mstsc.exe /CLXDLL=clxtshar.dll
 - smclient.exe (Windows 2000 resource toolkit)
- TSGrinder
- RDP Risk Checker
 - by xtiger

開始研究 RDP Protocol

研究方法?

- 微軟貌似有出 RDP Spec
 - MS-RDPBCGR (Basic Connectivity and Graphics Remoting)
 - MS-RDPEGDI
 - MS-RDPERP
 - MS-RDPNSC
 - ...

期中考



研究方法?

- 從 Open Source 開始研究?
 - RDesktop
 - Proper-JavaRDP / Lixia-JavaRDP
 - FreeRDP

RDP Protocol

- Connection Negotiation
 - Native RDP
 - TLS
 - NLA

RDP Protocol

- **MCS - Multipoint Communication Service**
 - Create channel
 - Join channel
 - Clipboard, sound, Device redirect, File sharing ...

RDP Protocol

- **Security Exchange**
 - **Encryption Mode**
 - FIPS 140-1
 - RSA with RC4 (40, 128 bit key)
 - **Exchange Public Key and Client/Server Random**

RDP Protocol

- RDP Setting Exchange
 - Client Info
 - username, password, hostname ...
 - xfreerdp -n client_hostname <IP>
 - Capabilities
 - Orders Support ?
 - Font, Color, Keyboard, Pointer, Cache ...

RDP Protocol

- RDP Command
 - PDU DATA
 - Bitmap, Control, Sync, Pointer, Disconnect ...
 - Orders
 - Line, Rectangle, Polygon, Glyph ...
 - Client Data
 - Point, Keyboard

Glyph

相黏鍵

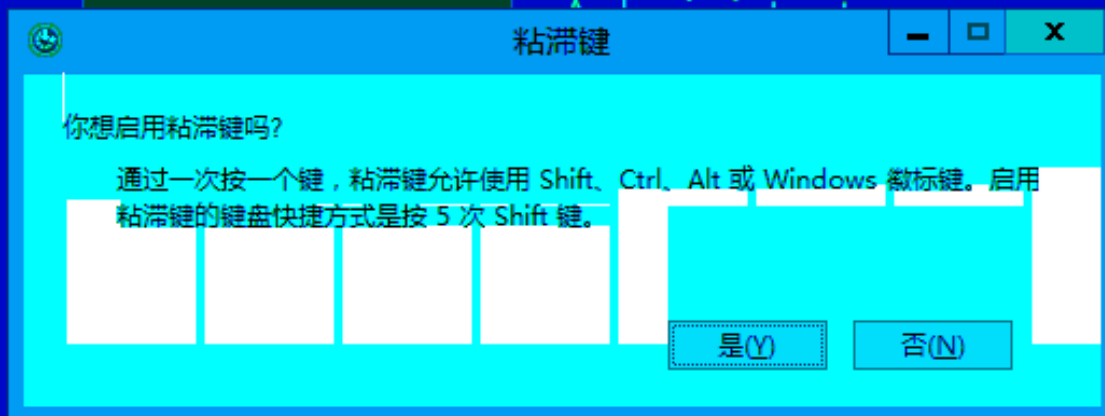
按下 SHIFT 鍵五次會啟動相黏鍵的功能。相黏鍵可讓您使用 SHIFT、CTRL、ALT 或 Windows 標幟按鍵。每次只按一個按鍵。

如果要持續啟動相黏鍵，請按 [確定]。
如果要取消相黏鍵

確定

取消

Bitmap



RDP Weak Password Cracker

RDP Weak Password Cracker

- RDP Setting Exchange - Client Info
 - 1 次
- 模擬 Key Type
 - 5 次

RDP Info Scanner

感覺滿簡單的

RDP Info Scanner

- 從最初的幾個交互連線可獲得的資訊
 - RDP Version (4, 5)
 - Protocol (RDP, TLS, NLA)
 - Encrpytion (RSA+RC4 or FIPS 140-1 ?)
 - Certificate
 - 至於 Windows version 呢?

RDP Info Scanner v1

- 一開始從 RDP 版本行為差異做區分
 - RSA_INFO_LENGTH
 - 376 # Vista+
 - 184 # XP / 2003
 - Slow-Path
 - Windows 8+ do not support
 - Bell PDU
 - Windows 2008 R2+ do not support
 - BPP - Bits per Pixel
 - Windows 8+ do not support BPP lower than 16

RDP Info Scanner v2

- File System Virtual Channel Extension
 - [header 4 bytes]
 - [version major] [version minor]
 - [client ID 4 bytes]
 - Version major **MUST** be set to 0x0001
 - Version minor
 - 0x02 # Win 2000
 - 0x05 # Win XP sp1/sp2, Win 2003 sp1
 - 0x06 # Win XP sp3
 - 0x10 # Win 2003 sp2

RDP Backdoor Scanner

一開始我以為很簡單...

RDP Backdoor Scanner

- Orders 內有個 Fast glyph
- 可以 parse 出 ASCII 的字元
- 接著只要寫個白名單當沒出現關鍵字就顯示有問題就好

相

直到我遇見這個



(3) after the right sequence, the password input box appear.

(1) click <setting> button

(2) click <cancel> button

WTF...

接下來開始想還有什麼方式

Screenhost ?

- RDP new version not support Fast Glyph

聲音?

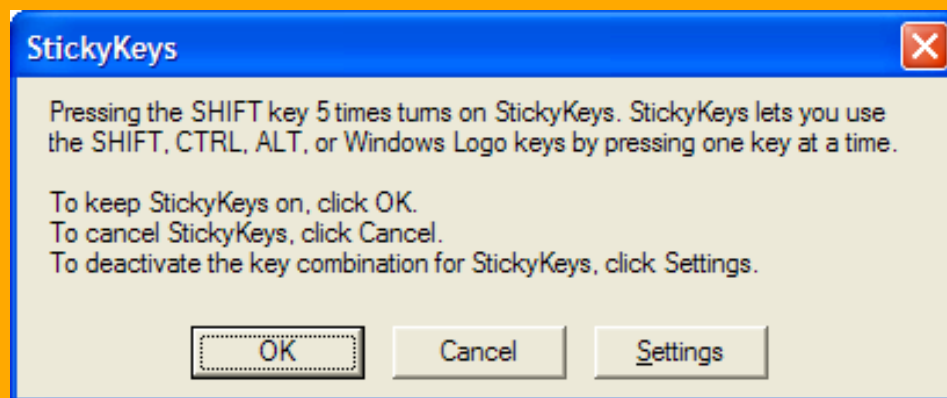
- Bell PDU
- RDP Version 7 不支援 Bell PDU
 - 改用 Sound Channel 代替

行為?

- sethc.exe 會有防止重複執行功能，而一般後門鮮少會加上
 - FindWindowEx # 2003 ...
 - CreateMutex # 2008 +

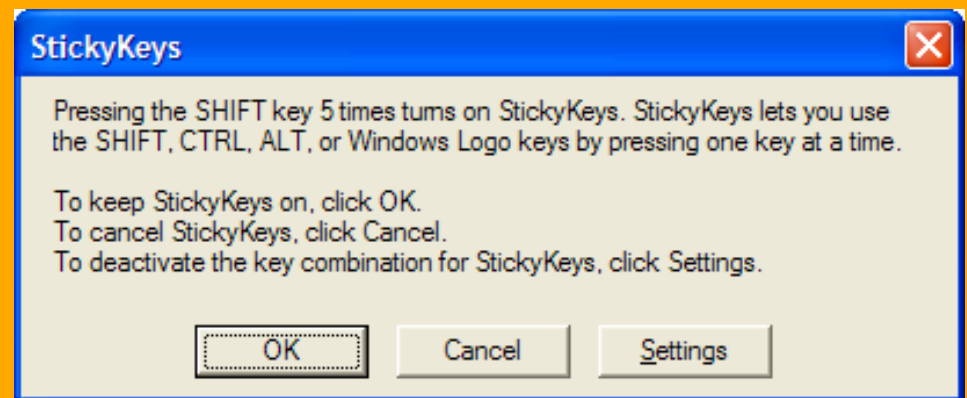
行為(Original)

- Send KeyDown SHIFT * 5



行為(Original)

- SendKeyDown SHIFT * 5
- SendKeyDown SHIFT * 5



行為(Original)

- Send KeyDown SHIFT * 5
- Send KeyDown SHIFT * 5
- Send KeyDown ESC

行為(Original)

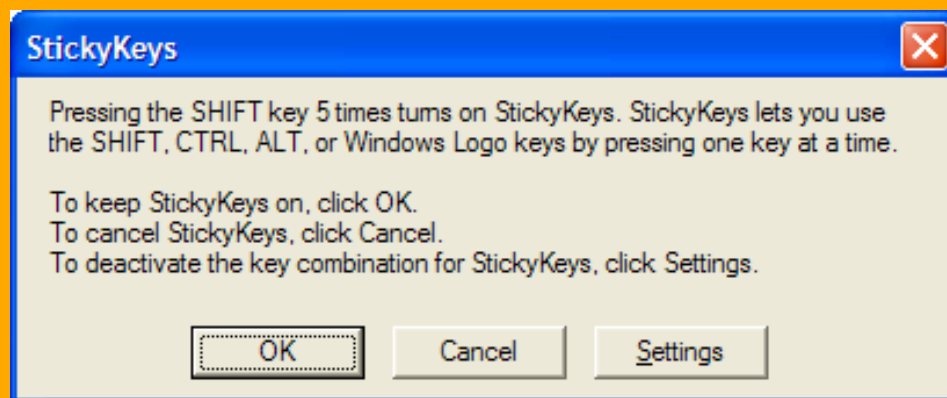
- Send KeyDown SHIFT * 5
- Send KeyDown SHIFT * 5
- Send KeyDown ESC
- Send KeyDown ESC



Connection
Close

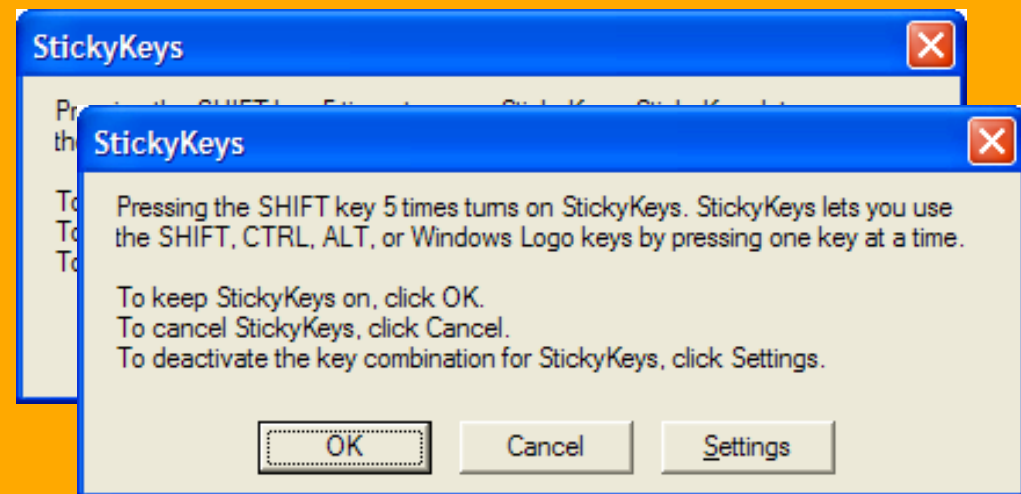
行為(Backdoor)

- Send KeyDown SHIFT * 5



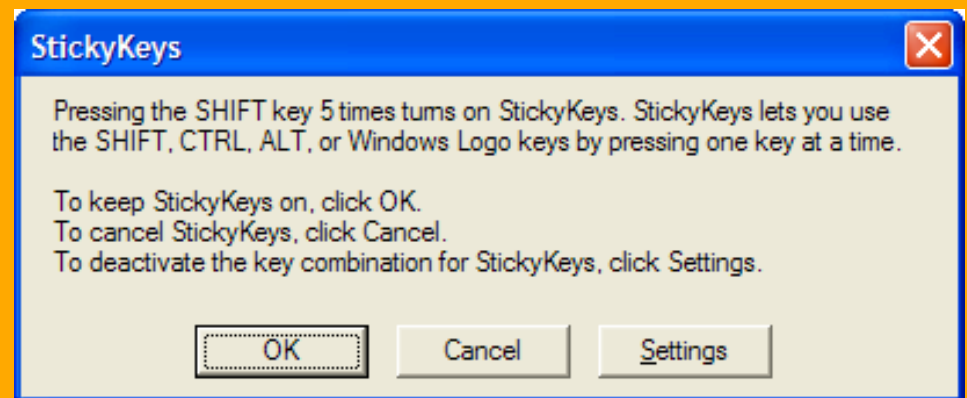
行為(Backdoor)

- Send KeyDown SHIFT * 5
- Send KeyDown SHIFT * 5



行為(Backdoor)

- Send KeyDown SHIFT * 5
- Send KeyDown SHIFT * 5
- Send ESC * 1



行為(Backdoor)

- Send KeyDown SHIFT * 5
- Send KeyDown SHIFT * 5
- Send ESC * 1
- Send ESC * 1

行為(Backdoor)

- Send KeyDown SHIFT * 5
- Send KeyDown SHIFT * 5
- Send ESC * 1
- Send ESC * 1

- Waiting ...



Connection
Timeout

看起來滿給力的

但唯一的問題...

Exception

- Windows XP work
- Windows 2003 work
- Windows Vista work
- Windows 7 work
- Windows 2008 not work ...
- Windows 2008 R2 work

sethc.exe of Windows 2008

- 就只有這個版本沒有檢查重複執行...
- Windows 2003
 - FindWinodwEx
- Windows 2008 R2
 - CreateMutex
- Windows 2008
 -

```
rdp-py-imp — bash — 80x24
Orange-2:rdp-py-imp Orange$ python r.py -s 140.119.98.5

Enaro RDP Tool ver 0.1
by orange@chroot.org

Infomation ->
[-] connect to 140.119.98.5 on port 3389
[-] connect success !
[*] rdp_protocol          -> native RDP
[*] encryption           -> rc4 128-bit
[*] encryption_level     -> medium
[*] rsa_info_length      -> 1322
[*] server_bpp           -> 8
[*] windows_version      -> 2003/sp2
[-] shift sended !
[-] shift sended !
[-] esc sended !
[-] esc sended !

Result ->
[-] backdoor not found :(

Orange-2:rdp-py-imp Orange$
```


Conclusion

- 歡迎加入，收集樣本
- 有更好的檢測方法歡迎提供：)

Thanks