

Who Hid My Desktop

DEEP DIVE INTO HVNC



Or Safran, Pavel Asinovsky

IBM Trusteer, Israel

November 2017

Agenda

- Intro
 - What is VNC.
- Part 1
 - Sessions, Window Stations, Desktops.
- Part 2
 - Financial malware.
 - hVNC.
- Part 3
 - Reversing Gozi ISFB's hVNC module.
 - Demo.
 - Detection/IOCs.

VNC & hVNC



Who are we

- IBM Security (Trusteer) Financial Malware Research Team
- Or Safran
- Pavel Asinovsky

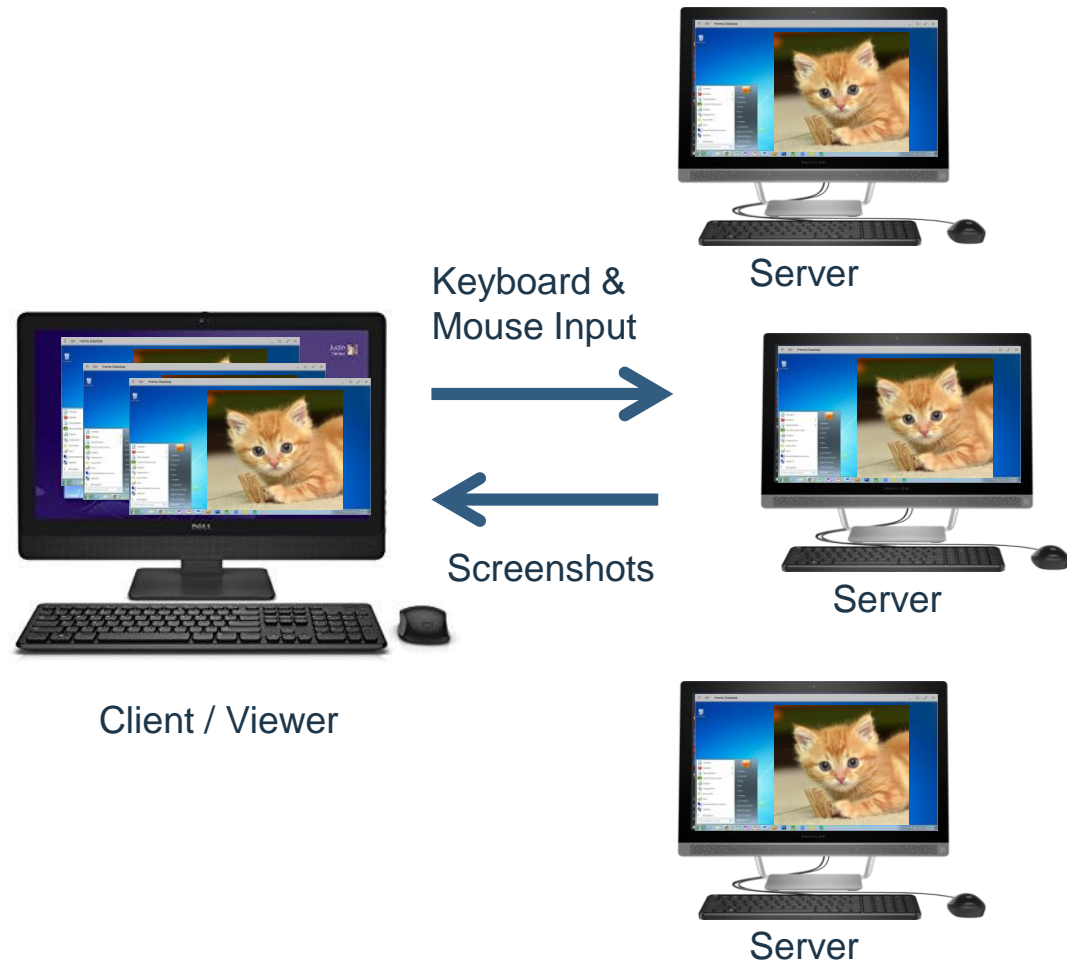
Remote Desktop Software

- Allows remote control of a computer across the network.
- Originally was used for remote technical support.
- Used for server administration, conference calls, file transfers, etc.
- Has many implementations: RDP, VNC, Citrix, LogMeIn, TeamViewer etc.

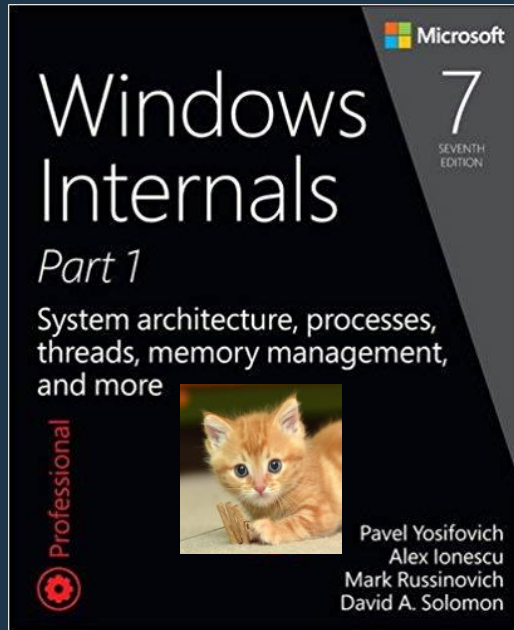


What is VNC

- Virtual Network Computing.
- Graphical desktop sharing system that uses the RFB protocol (Remote Frame Buffer).
- Composed of a server and a client.
- Platform independent.
- Default TCP port 5900.
- The desktop is shared.
- Used by many RAT (Remote Access Tool) Malware.

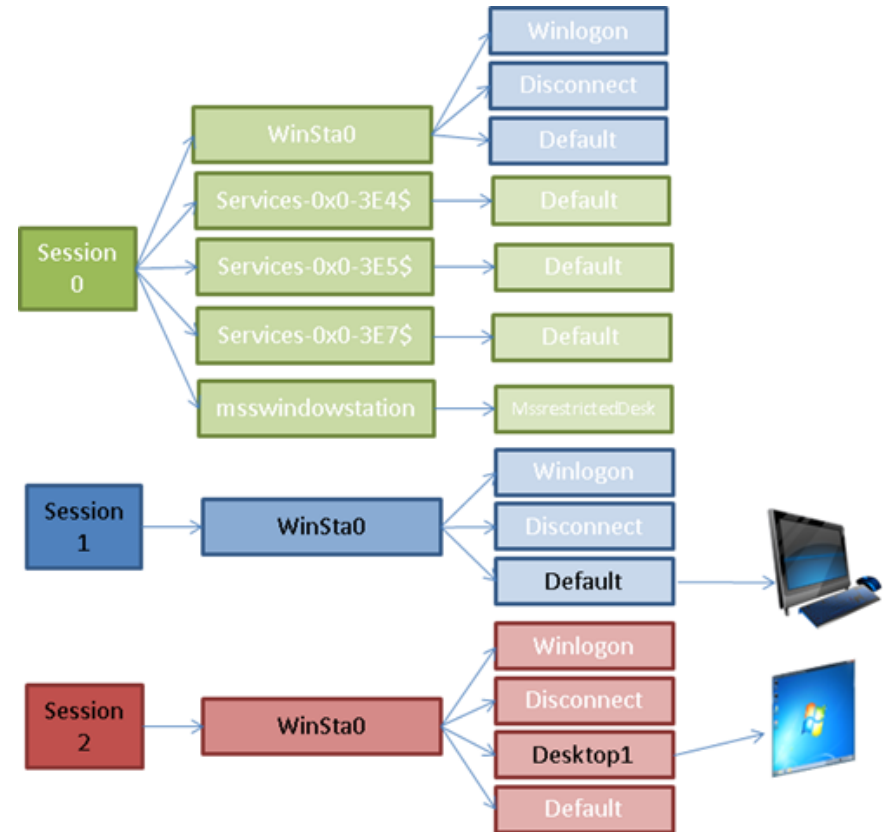


Part 1 – Sessions, Window Stations and Desktops



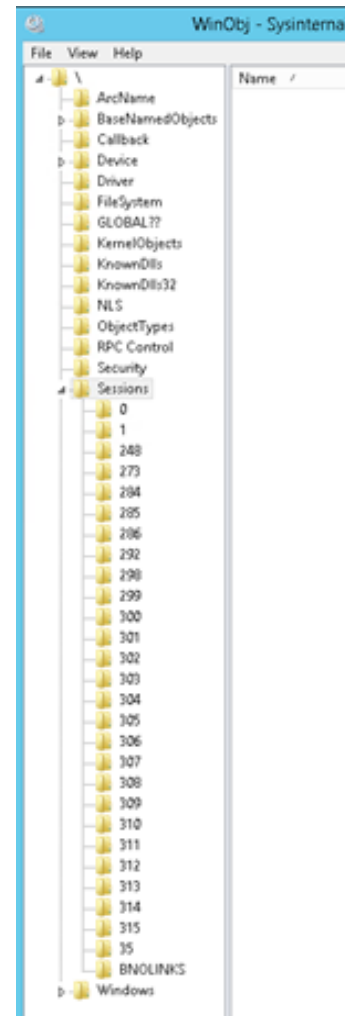
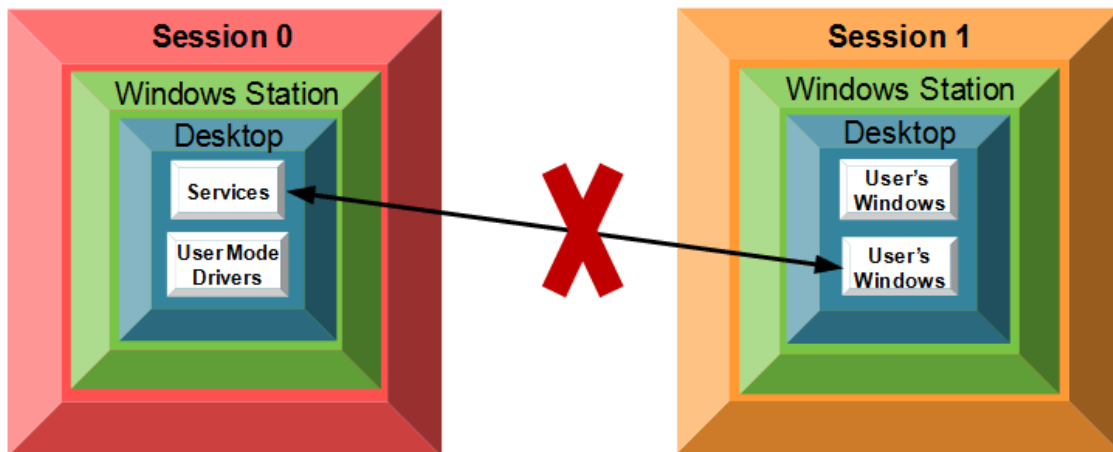
Sessions, Window Stations and Desktops

- Securable kernel objects (contain a security descriptor).
- Used as containers to manage graphical objects, provide isolation and security.
- Structured in hierarchy.
- Each session contains only one interactive window station – WinSta0.



Sessions

- Represent a single user's logon session.
- Each user is assigned with a different session.
- Session 0 is the base session (the system user session).
- Session 0 is isolated from the user sessions.



Window Stations

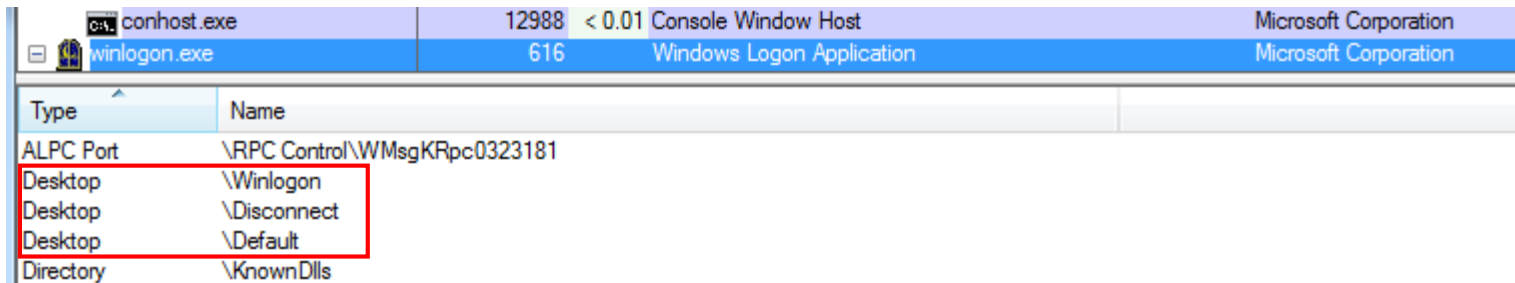
- A logical security boundary.
- Contains a clipboard, atom table, and one or more desktop objects.
- Contains the keyboard, mouse, and a display device.
- Associated with a process.
- The interactive window station (WinSta0) is the only that can display user interface or receive user input.
- Used by Chrome to implement a “Sandbox”.

The screenshot shows the Sysinternals WinObj tool interface. The top pane displays a tree view of the system's object hierarchy, with 'Sessions\2\Windows\WindowStations' selected. The right pane shows a list of window stations, with 'Service-0x0-448ab8\$' highlighted in red. The bottom pane shows a table of objects associated with the selected window station.

Type	Name
File	\Device\KsecDD
File	\Device\NamedPipe\mojo.4752.5476.18230698618931588411
File	\Device\NamedPipe\mojo.4752.6972.9424247446060851687
Directory	\KnownDlls
Desktop	\sbox_altemate_desktop_0x1290
Directory	\Sessions\2\BaseNamedObjects
Section	\Sessions\2\BaseNamedObjects\CrSharedMem_3bf150e2dfe20c79
Section	\Sessions\2\BaseNamedObjects\CrSharedMem_ba7113a2e23dd54
Section	\Sessions\2\BaseNamedObjects\CrSharedMem_ed5caada41b9799
Section	\Sessions\2\BaseNamedObjects\CrSharedMem_fe3a103e171181ca
WindowStation	\Sessions\2\Windows\WindowStations\Service-0x0-448ab8\$
WindowStation	\Sessions\2\Windows\WindowStations\Service-0x0-448ab8\$

Desktops

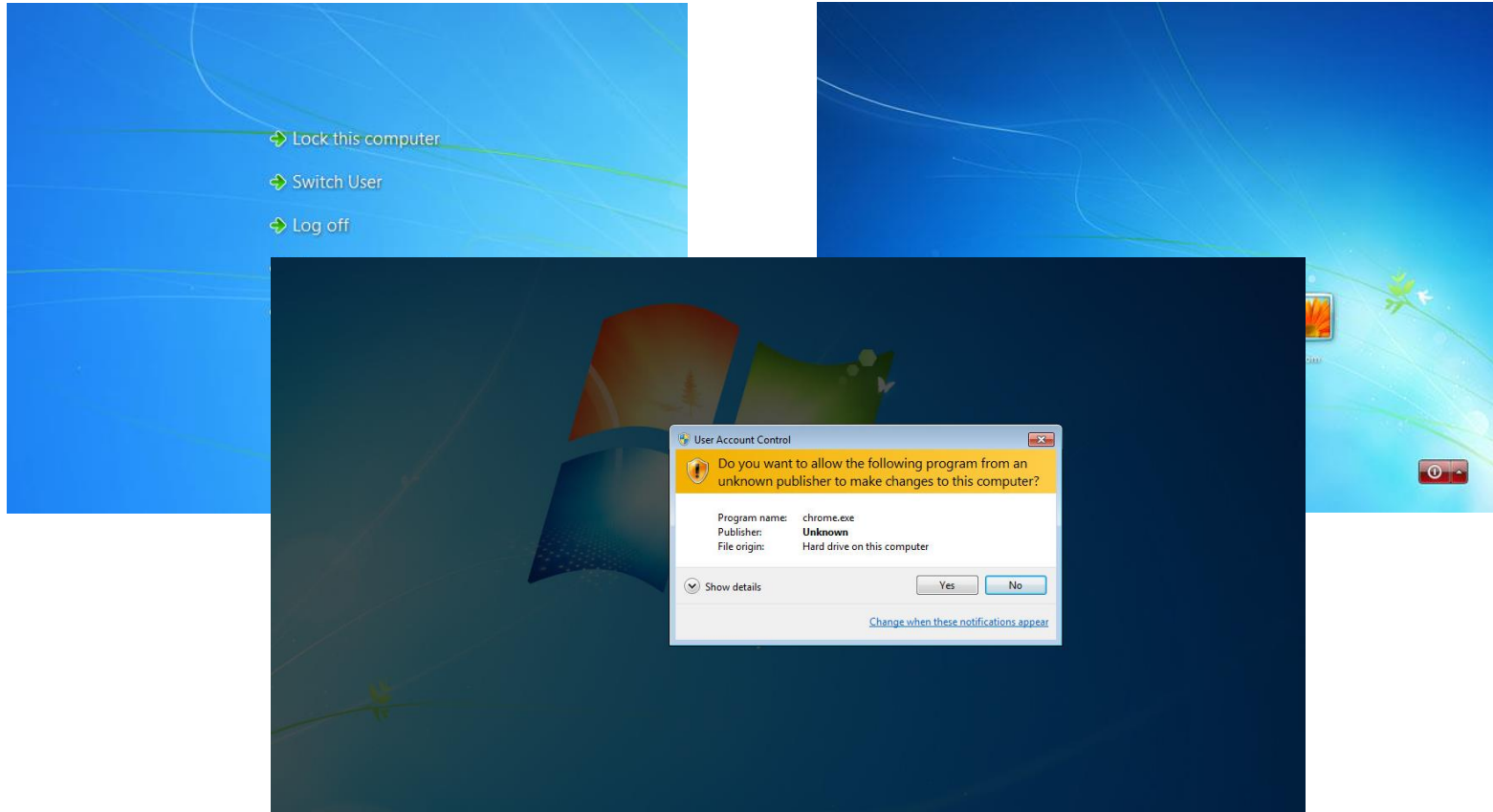
- A desktop is a logical display surface that contains UI objects such as windows, menus and hooks.
- Used as a container to create and manage windows.
- Associated with a thread.
- By default, there are few interactive desktops on windows:
 - The default desktop: \Sessions\1\Windows\WinSta0\Default
 - The Winlogon secure desktop: \Sessions\1\Windows\WinSta0\Winlogon
 - And more...
- There can be only one interactive desktop at a time.



The screenshot shows the Windows Task Manager interface. At the top, two processes are listed: 'conhost.exe' (PID 12988, CPU < 0.01, Console Window Host, Microsoft Corporation) and 'winlogon.exe' (PID 616, Windows Logon Application, Microsoft Corporation). Below this, a table lists desktops:

Type	Name
ALPC Port	\RPC Control\WMsgKRpc0323181
Desktop	\Winlogon
Desktop	\Disconnect
Desktop	\Default
Directory	\KnownDlls

Winlogon Secure Desktop Examples



Multiple Desktops

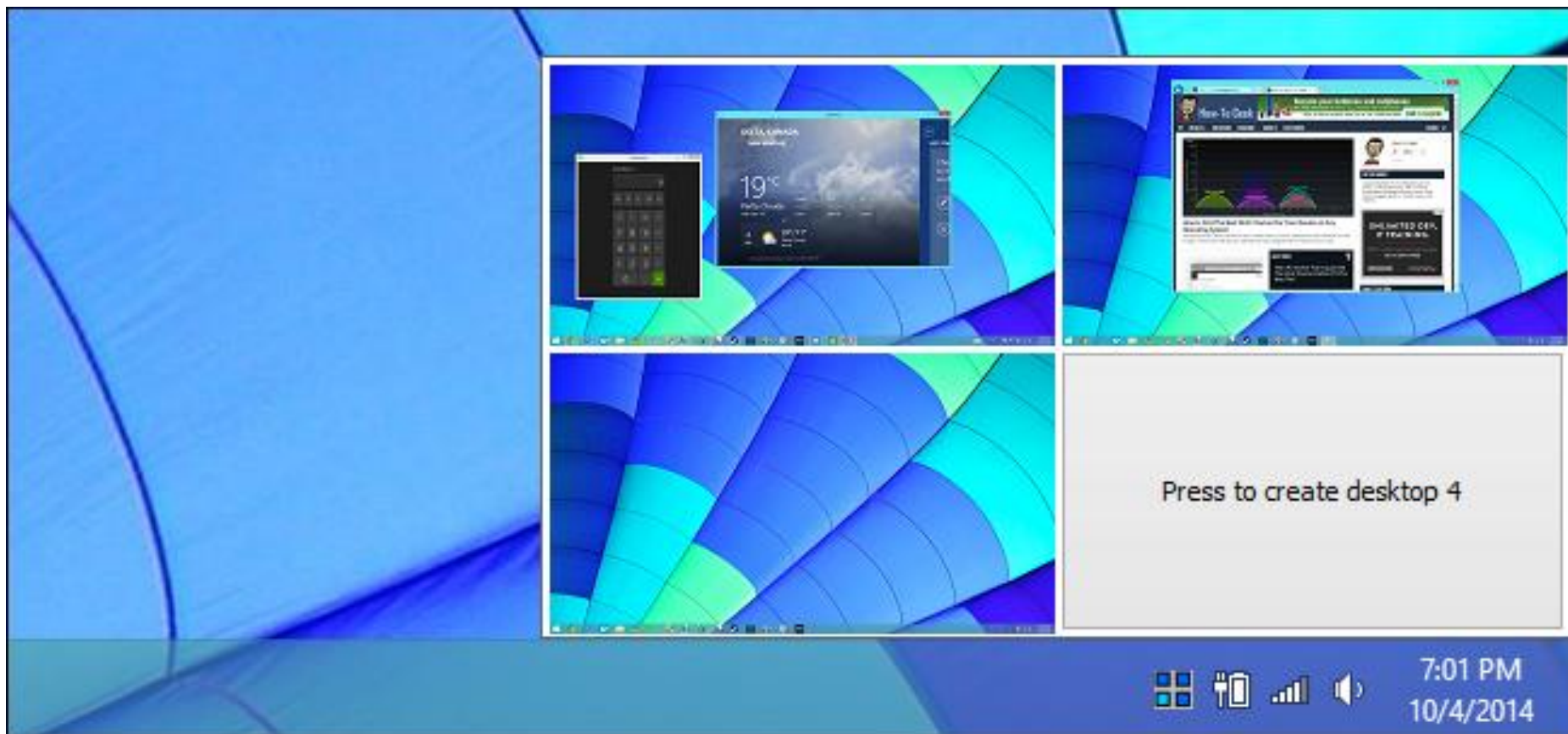
- Supported by Windows API since Windows 2000.

```
HDESK WINAPI CreateDesktop(  
    _In_      LPCTSTR          lpszDesktop,  
    _Reserved_ LPCTSTR          lpszDevice,  
    _Reserved_ DEVMODE         *pDevmode,  
    _In_      DWORD            dwFlags,  
    _In_      ACCESS_MASK      dwDesiredAccess,  
    _In_opt_  LPSECURITY_ATTRIBUTES lpsa  
);
```

- Have many legitimate uses:
 - Security applications
 - Multiple desktops
 - Windows logon/logoff screens
 - UAC
 - Ctrl + Alt + Del screen
 - Screensavers



Desktops



Association to Desktops under the hood

- When a program calls a USER32 or GDI32 function, a window station is assigned to the calling process and a desktop is assigned to the calling thread according to the following rules:
 - As specified using the SetThreadDesktop() / SetProcessWindowStation() APIs.
 - Inherited from the parent process.
 - As specified in the STARTUPINFO structure.
 - The calling thread connects to the “\Default” Desktop.

```
BOOL WINAPI CreateProcess(  
    _In_opt_ LPCTSTR lpApplicationName,  
    _Inout_opt_ LPTSTR lpCommandLine,  
    _In_opt_ LPSECURITY_ATTRIBUTES lpProcessAttributes,  
    _In_opt_ LPSECURITY_ATTRIBUTES lpThreadAttributes,  
    _In_ BOOL bInheritHandles,  
    _In_ DWORD dwCreationFlags,  
    _In_opt_ LPVOID lpEnvironment,  
    _In_opt_ LPCTSTR lpCurrentDirectory,  
    In_ LPSTARTUPINFO lpStartupInfo,  
    _Out_ LPPROCESS_INFORMATION lpProcessInformation  
);
```

```
typedef struct _STARTUPINFO {  
    DWORD cb;  
    LPTSTR lpReserved;  
    LPTSTR lpDesktop;  
    LPTSTR lpTitle;  
    DWORD dwX;  
    DWORD dwY;  
    DWORD dwXSize;  
    DWORD dwYSize;
```

Part 2 – Financial Malware and hVNC



About financial malware

Digital Banking

ご契約番号

(半角数字)

IBログイン
パスワード

(半角英数字・記号4～16桁)



ソフトウェアキーボードで入力

ご契約番号・IBログインパスワードとは

ログイン

Digital banking Credit card ser

Welcome to Digital Ban

Customer number

> [Forgotten any of your log in details?](#)

This is your date of birth (ddmmyy) followed by your unique number which identifies you to the bank.

Remember me. We don't recommend storing data on a shared computer.

> [Tell me more about this feature](#)

Log in

כניסה לחשבון

קוד משתמש

סיימה

כניסה

נחסמה / שכחת סיימתך?

Credential theft techniques

- Web Injections
- Form Grabbing
- Cookie Grabbing
- KeyLogging (kernel mode \ user mode)
- SSL Proxy (with certificate installation)
- DNS Pharming
- Redirects



Web Injections



One account. All of Google.

Sign in to continue to Gmail

←

EMBogachev@gmail.com

Password

Google will never ask for your grandmother's preferences!

Sign in

Stay signed in [Forgot password?](#)



One account. All of Google.

Sign in to continue to Gmail

←

EMBogachev@gmail.com

Password

Grandmother's Favorite Pet

Google will never ask for your favorite pizza!

Sign in

Financial Malware and hVNC

- Introduced to the world by the infamous Zeus malware.
- Allows the attacker to use the exact same machine as the victim.
- hVNC alone is usually not enough to commit a fraudulent transaction.
- Most modern financial malware have an embedded hVNC module (Zeus, Gozi, Dridex and more).



hVNC Evolution



Password validation

Keyloggers/Form grabbers



IP/Geo-location validation

SOCKS Proxy Server

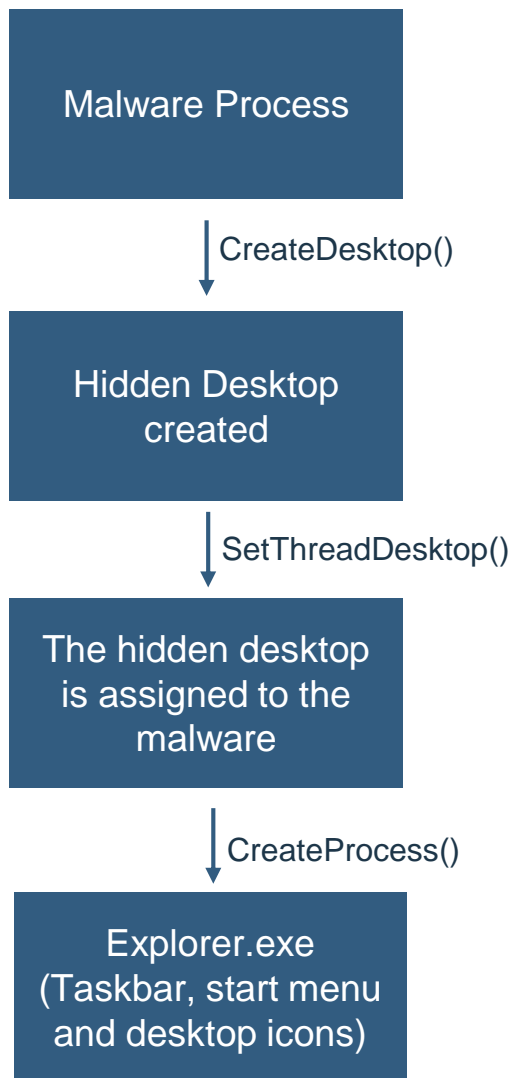


Browser/System fingerprint

hVNC

hVNC

- Has same capabilities like regular VNC.
- Hidden (runs on a different desktop).
- Cannot see the user's desktop and can't be seen by the user.
- Makes sure the SwitchDesktop API is never called.
- Has the same browser-system fingerprint as the user.
- Uses BackConnect – the server sends the first connection request to the client.
- Slightly modified RFB protocol to authenticate the malware.
- Must implement all the user interaction by itself (Windows supports only a single interactive desktop at a time).
- Can be used to log in to active web-sessions (shopping websites, Facebook, Gmail).



Part 3 – Gozi ISFB hVNC case study



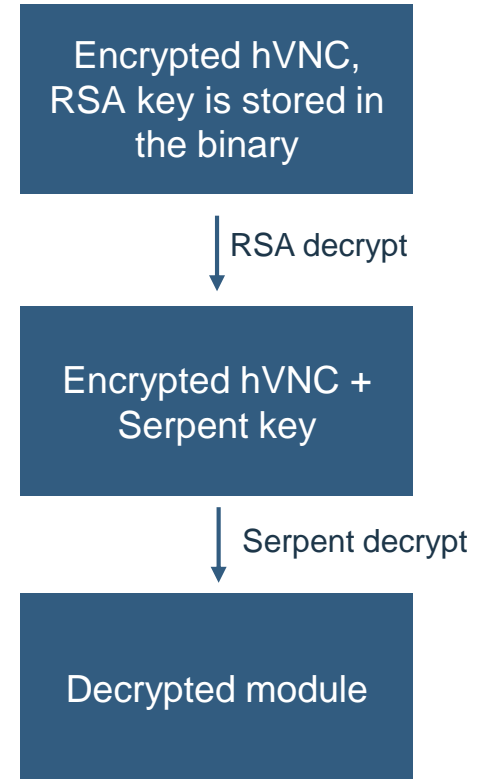
Gozi ISFB

- One of the most widespread financial malwares.
- One of the best hVNC modules found in the wild.
- Based on the hVNC code of Zeus.
- Has debug versions – `fd36d1e2be1f0079c7cb66288778ffa9`.
- Became an open source malware when an unknown player leaked it's code (the hVNC module is missing from the source code).



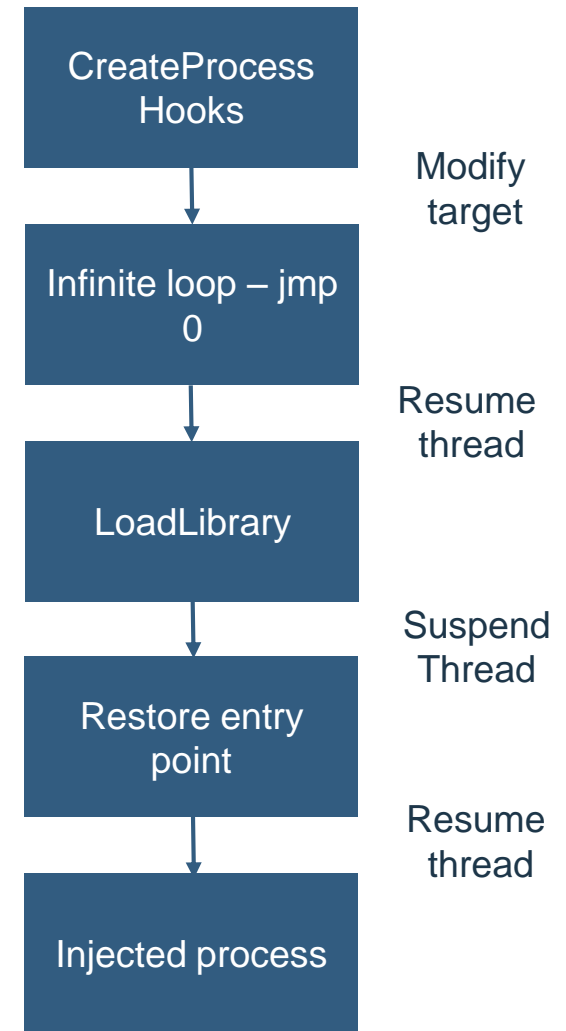
Finding and Decrypting Gozi's hVNC Module

- The hVNC module is downloaded from a remote server.
- The module is encrypted with two layers of encryption:
 - Serpent cipher with a randomly generated key (appended to the encrypted module).
 - The Serpent encrypted hVNC module and the Serpent key are encrypted again using an RSA cipher.



Gozi's hVNC injection to processes

- The code injection technique is the same one the Gozi malware uses.



hVNC Server Authentication

- Most hVNC modules send a unique identifier of the malware to the hVNC client in order to authenticate it.
- A regular VNC client will not work out of the box, it has to be reversed and patched.

```
0000 00 50 56 a2 20 65 00 50 56 8e a4 3a 08 00 45 00 .PV. e.P V...E.
0010 00 60 57 70 40 00 80 06 00 00 c0 a8 14 46 c0 a8 .`wp@... ..F..
0020 14 40 c2 b3 01 bb 3b 6d 5f 42 81 8b f0 00 50 18 .@....;m _B....P.
0030 01 00 aa 29 00 00 34 36 39 45 45 42 45 45 2d 34 ...)..46 9EEBEE-4
0040 46 32 38 2d 44 43 30 36 2d 31 42 42 45 2d 30 35 F28-DC06 -1BBE-05
0050 41 30 33 36 36 41 31 33 31 34 2d 30 32 00 00 00 A0366A13 14-02...
0060 00 00 00 00 00 00 00 00 00 00 ab f4 57 30 .....W0
```

- After the authentication phase is over, the regular RFB protocol is initiated.

```
0000 00 50 56 a2 20 65 00 50 56 8e a4 3a 08 00 45 00 .PV. e.P V...E.
0010 00 34 59 8f 40 00 80 06 00 00 c0 a8 14 46 c0 a8 .4Y.@... ..F..
0020 14 40 c3 06 01 bb 9f 82 8a 70 54 a7 b8 eb 50 18 .@..... .pT...P.
0030 01 00 a9 fd 00 00 52 46 42 20 30 30 33 2e 30 30 .....RF B 003.00
0040 38 0a 8.
```

Browser manipulation

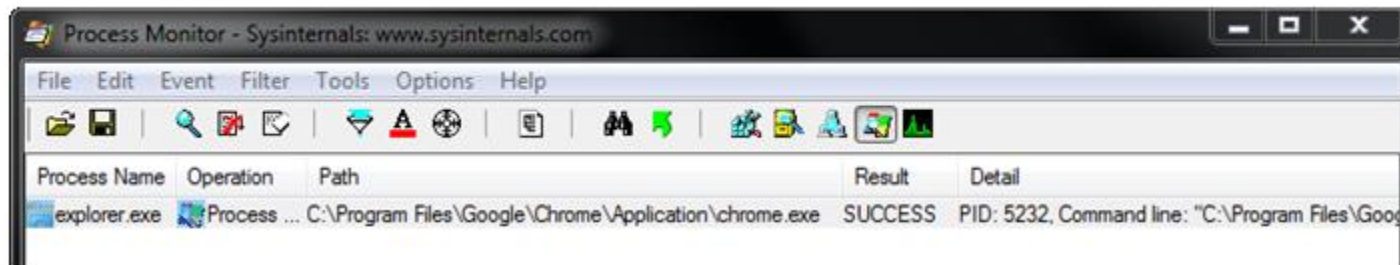
- Has code to deal with every common browser (IE, Chrome, Firefox, Opera).
- One cannot open the same browser in two separate desktop under the same user profile.



Browser manipulation - Chrome

- For Chrome, hVNC copies the whole user profile (user data folder) to a different location and setting it as the user data directory for the new browser process.

explorer.exe	ReadFile	C:\Users\tom\AppData\Local\Google\Chrome\User Data\Certificate Transparency\289\manifest.fingerprint
explorer.exe	WriteFile	C:\Users\tom\AppData\Local\Temp\{FB68EAC9-1E4A-E5AA-005F-32E93403862D}_CR\Certificate Transparency\289\manifest.fingerprint
explorer.exe	ReadFile	C:\Users\tom\AppData\Local\Google\Chrome\User Data\Certificate Transparency\289\manifest.fingerprint
explorer.exe	ReadFile	C:\Users\tom\AppData\Local\Google\Chrome\User Data\Certificate Transparency\289\manifest.json
explorer.exe	WriteFile	C:\Users\tom\AppData\Local\Temp\{FB68EAC9-1E4A-E5AA-005F-32E93403862D}_CR\Certificate Transparency\289\manifest.json
explorer.exe	ReadFile	C:\Users\tom\AppData\Local\Google\Chrome\User Data\Certificate Transparency\289\manifest.json



PID: 5232

Command line: "C:\Program Files\Google\Chrome\Application\chrome.exe" -user-data-dir="C:\Users\tom\AppData\Local\Temp\{FB68EAC9-1E4A-E5AA-005F-32E93403862D}_CR" -no-sandbox -allow-no-sandbox-job -disable-3d-apis -disable-accelerated-layers -disable-accelerated-plugins -disable-audio -disable-gpu -disable-d3d11 -disable-accelerated-2d-canvas -disable-deadline-scheduling -disable-ui-deadline-scheduling -aura-no-shadows

Browser manipulation - Chrome

- The browser might render pages using the graphics card (GPU).
- The browser uses a sandbox that might not play well with hVNC module.

```
aNoSandboxAllow:                                ; DATA XREF: set_chrome_cmdline_args+6A↑o
text "UTF-16LE", ' --no-sandbox --allow-no-sandbox-job --disable-3d-a'
text "UTF-16LE", 'pis --disable-accelerated-layers --disable-accelera'
text "UTF-16LE", 'ted-plugins --disable-audio --disable-gpu --disable'
text "UTF-16LE", '-d3d11 --disable-accelerated-2d-canvas --disable-de'
text "UTF-16LE", 'adline-scheduling --disable-ui-deadline-scheduling '
text "UTF-16LE", '--aura-no-shadows',0
```

Browser manipulation – Internet Explorer

- hVNC doesn't want to allow IE to merge different frames into the same process.

```
text "UTF-16LE", '-nomerge -noframemerging',0
```

- Virtual registry hooks
 - Hook registry query functions to change settings only in the hVNC session without any permanent changes.
- IE settings
 - Alter many IE settings virtually: protected mode for internet zones, enhanced protected mode and more.
- UAC adjustments:
 - When UAC is on and off, IE uses different location to load session cookies.

System manipulation

- Virtual registry hooks for changing system settings:
 - Disable visual effects [Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects]
 - Disable active desktop [Software\Microsoft\Windows\CurrentVersion\Policies]
 - Removes wallpaper [Software\Microsoft\Internet Explorer\Desktop\General]
- Hook window events:
 - EVENT_OBJECT_CREATE
 - EVENT_OBJECT_HIDE
 - EVENT_OBJECT_SHOW
 - EVENT_OBJECT_DESTROY
 - EVENT_OBJECT_LOCATIONCHANGE
 - etc.
- Virtual keyboard and mouse (PostMessage to the topmost window).
- Virtual Clipboard.
- Screenshots (Using BitBlt and PrintWindow APIs).

Taking the “h” off

- We are able to watch fraudsters in action with two easy steps.
- Open a handle by using the OpenDesktop API.
- Switch to the fraudster’s desktop using the SwitchDesktop API.

```
hvinc_handle = OpenDesktopA(hvinc_desktop_name, NULL, FALSE, GENERIC_ALL);  
SwitchDesktop(hvinc_handle);
```

Piecing the Puzzle

- Obtain and decrypt the hVNC module.
- Inject the hVNC module into explorer.exe the same way Gozi does.
- Direct the hVNC module to communicate with our machine instead of the one originally hardcoded into the binary.
- Overcome the protocol differences between Gozi's hVNC and the standard RFB.



Demo

Server (Victim)

- Manually inject the Gozi hVNC module and make it run from explorer.exe.
- Make it connect to our VNC client by replacing the IP address.
- Establish a connection and bypass the bot identifier authentication.

Client (Attacker)

- Set up a VNC client in listening mode.
- Wait for an RFB connection from the server and obtain control over the victim's machine.



IOCs

- Second explorer.exe holding a handle to an unknown desktop (Not the default one).
- Usually has ctfmon.exe automatically running under it (text input services support).
- Has processes running under it that you don't see their windows, such as a browser.

winlogon.exe		2,060 K	5,184 K
explorer.exe	1.43	34,500 K	49,628 K
explorer.exe	1.18	24,972 K	38,316 K
ctfmon.exe		9,660 K	3,676 K
calc.exe	1.10	13,844 K	9,716 K
ieexplore.exe	0.62	13,388 K	17,028 K
ieexplore.exe	1.33	21,132 K	25,320 K
procexp.exe	3.05	15,328 K	23,808 K
vmtoolsd.exe	0.05	5,200 K	11,072 K

Type	Name
ALPC Port	\RPC Control\OLE287ED3F73B874792A3544C655C11
Desktop	\Default
Desktop	\{2FA91BB8-C244-39BD-44D3-167DB88B7AA01}

winlogon.exe		2,060 K	5,184 K
explorer.exe	1.42	34,432 K	49,628 K
explorer.exe	1.24	24,976 K	38,316 K
ctfmon.exe		9,660 K	3,676 K
calc.exe	1.33	13,844 K	9,716 K
ieexplore.exe	0.61	13,592 K	17,068 K
ieexplore.exe	1.25	20,988 K	25,384 K
procexp.exe	2.42	15,200 K	23,608 K
vmtoolsd.exe	0.02	5,184 K	11,056 K

Type	Name
ALPC Port	\RPC Control\OLE1F518E353C8C4F5894A4C446CD9F
Desktop	\{2FA91BB8-C244-39BD-44D3-167DB88B7AA01}
Desktop	\{2FA91BB8-C244-39BD-44D3-167DB88B7AA01}

Conclusions

- The hVNC code is extremely complicated.
- It is one of the top tools in the financial malware toolkit.
- It uses many cool tricks and manipulations in order to achieve its purpose.
- Although not new, it is still popular and common in online banking fraud today.




Questions?





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.