Transferring files on isolated remote desktop environments using windows messages

Hernan Ochoa
hernan@ampliasecurity.com

September, 2010

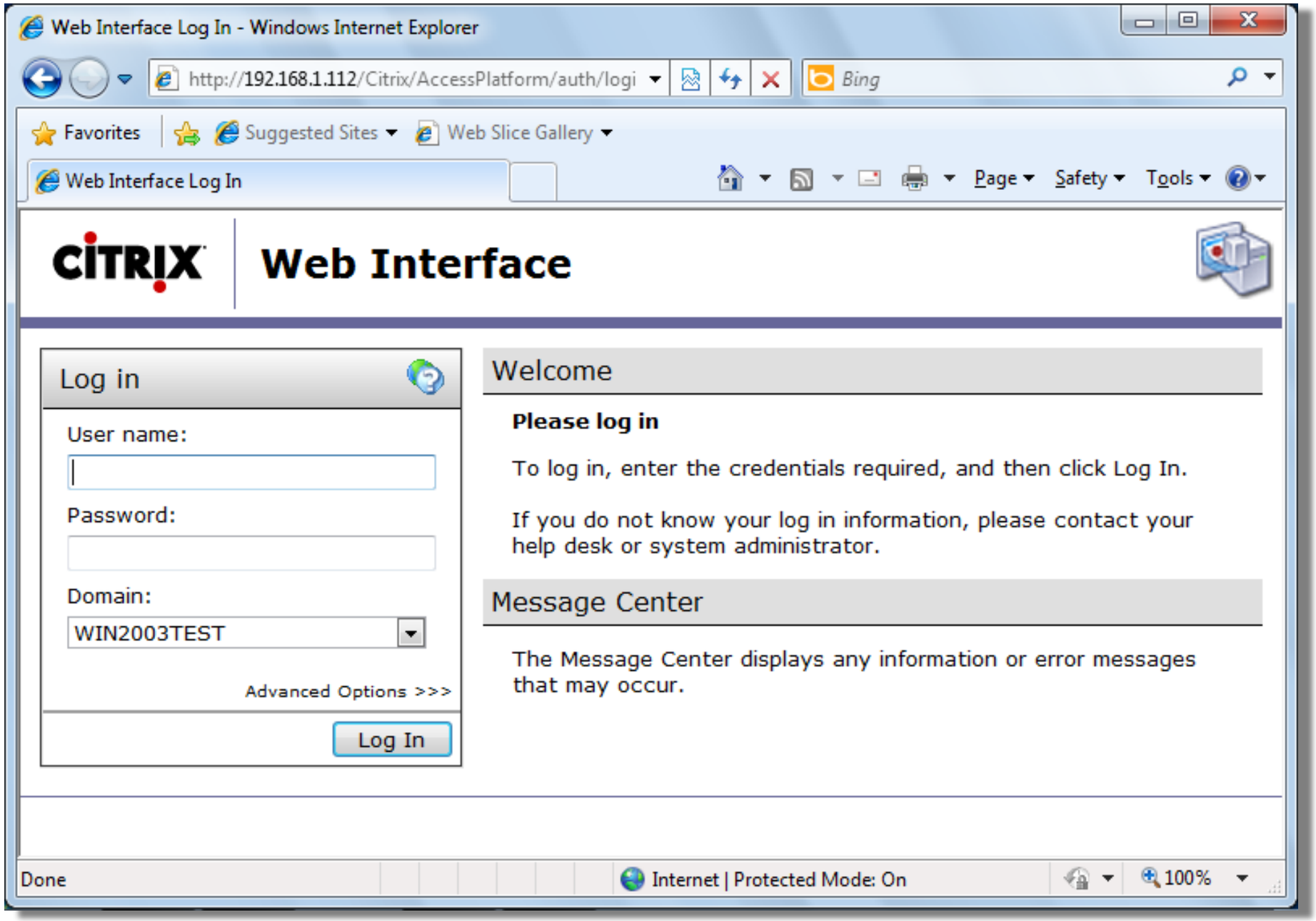
This presentation is about:

- Post-exploitation 'technique' to upload & download files on isolated remote desktop environments
  - ➡ Test case: *Citrix*

- GUI Transfer Toolkit v1.0 (GTT)

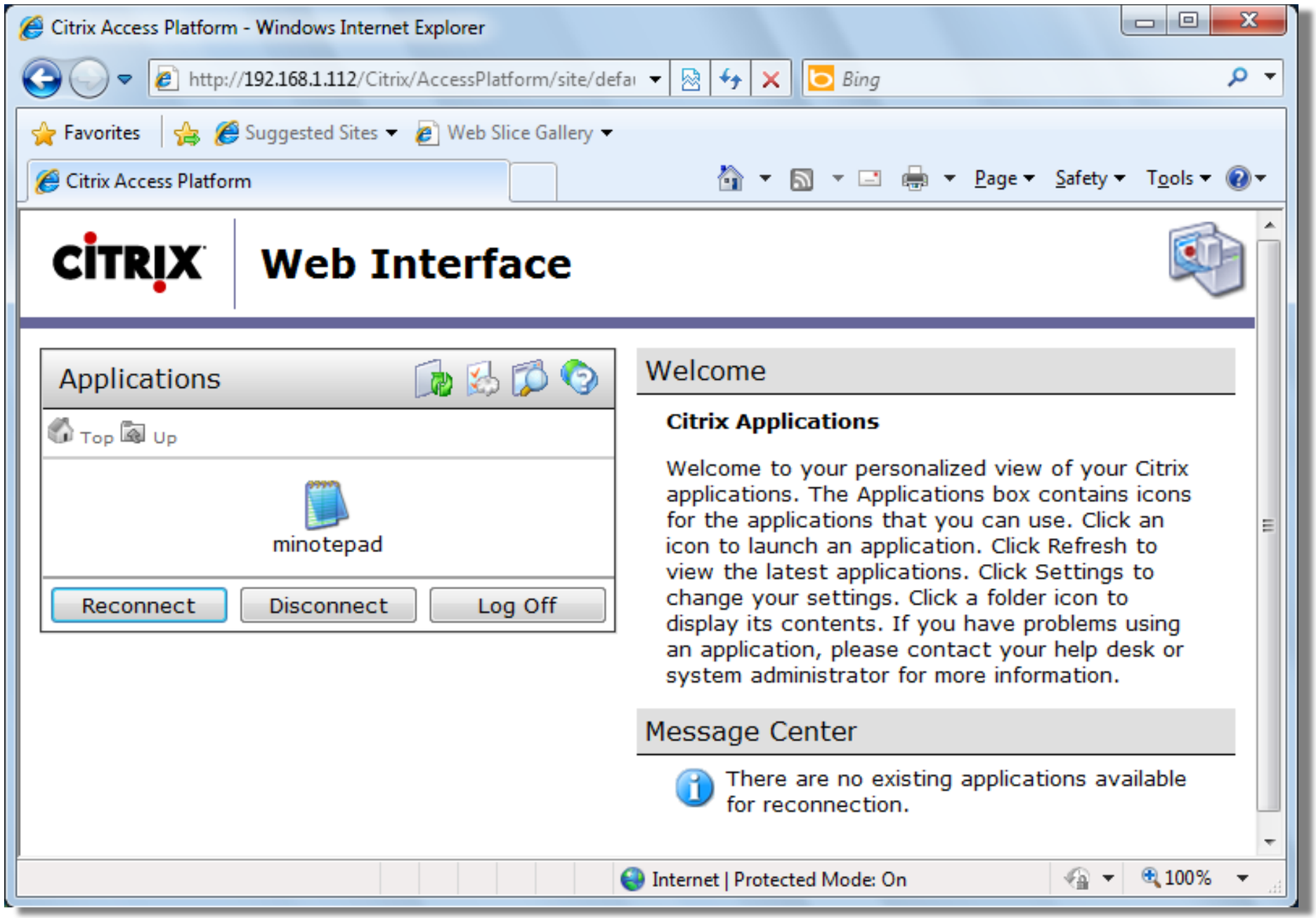
Scenario

- You found a MS RDP / Citrix server during a pentest



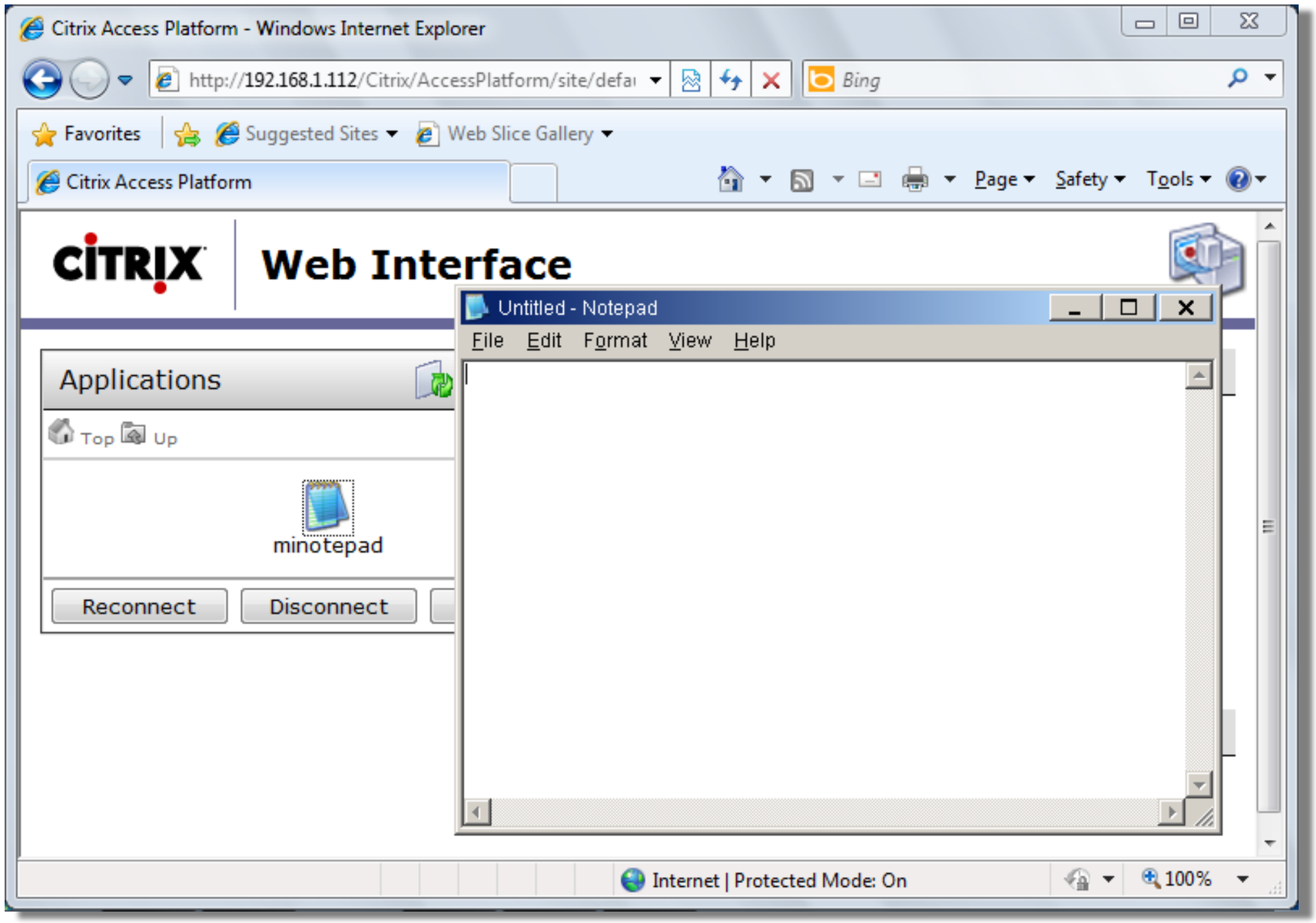
Scenario

- You gained access and can execute available apps



Scenario

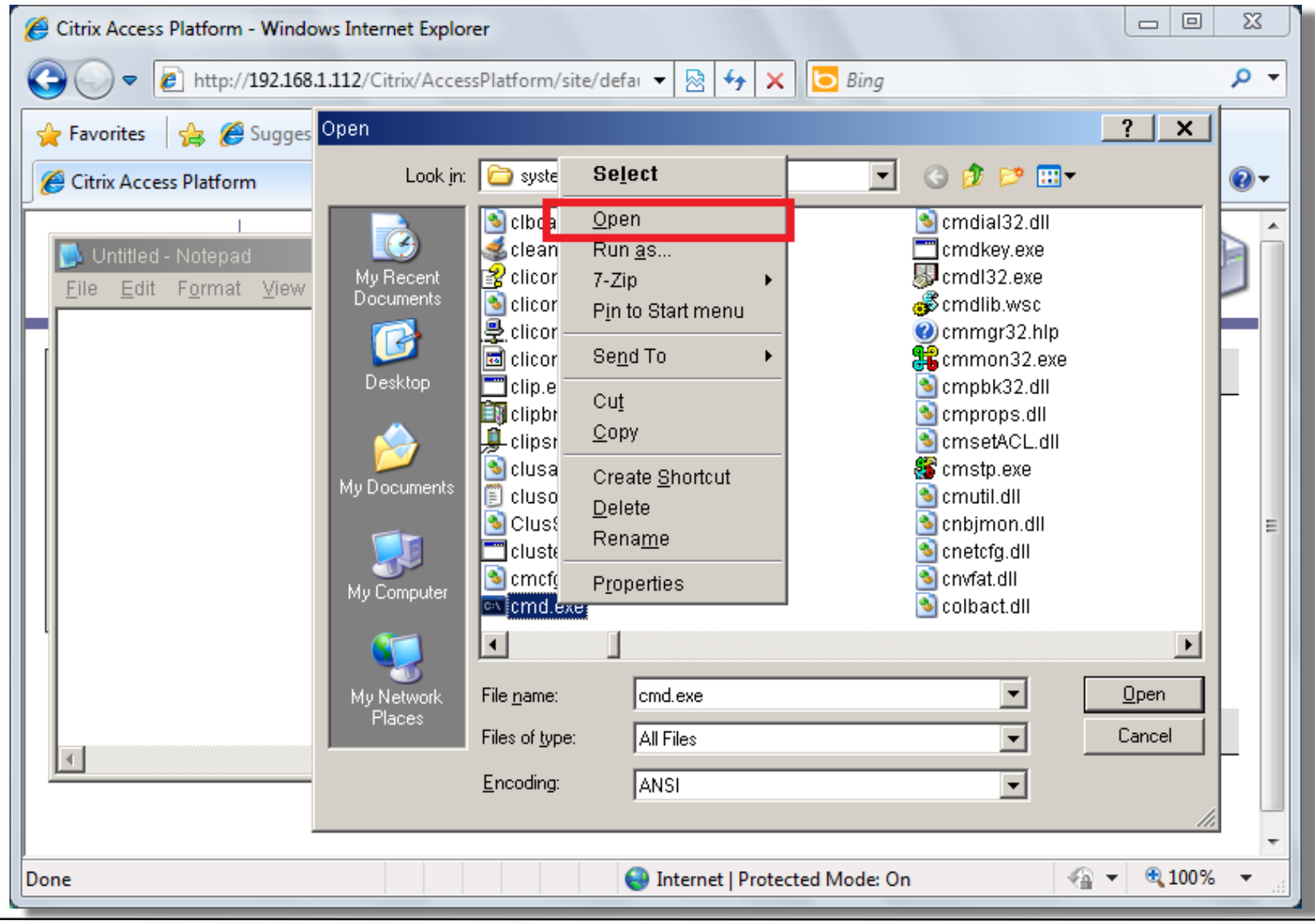
- In this example, you can run Notepad



Scenario

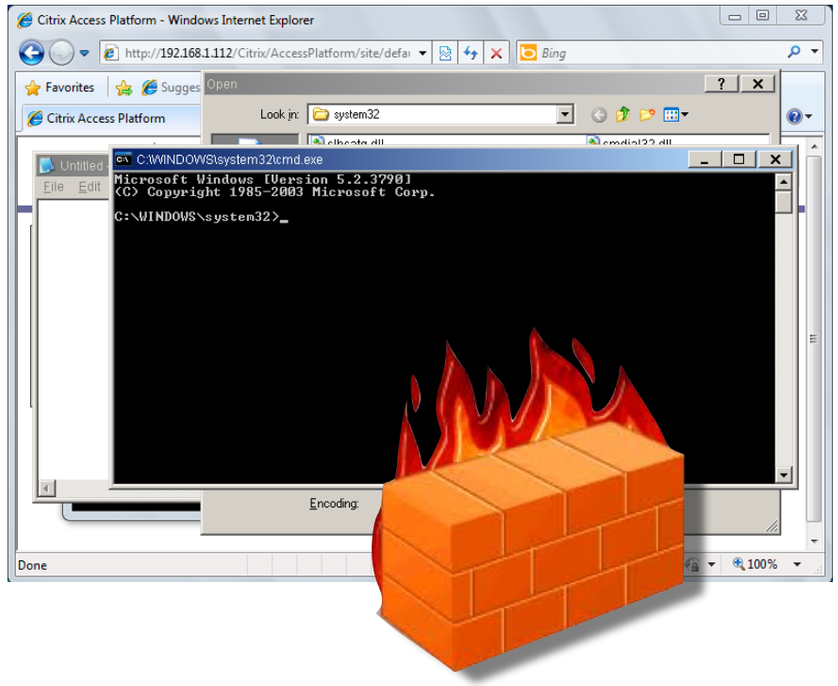
- Now you get shell to exec arbitrary cmds
- Many ways to do it...

➡ e.g.: Help system, file open/save dialogs, menu bar, print menus, hot-keys, etc.



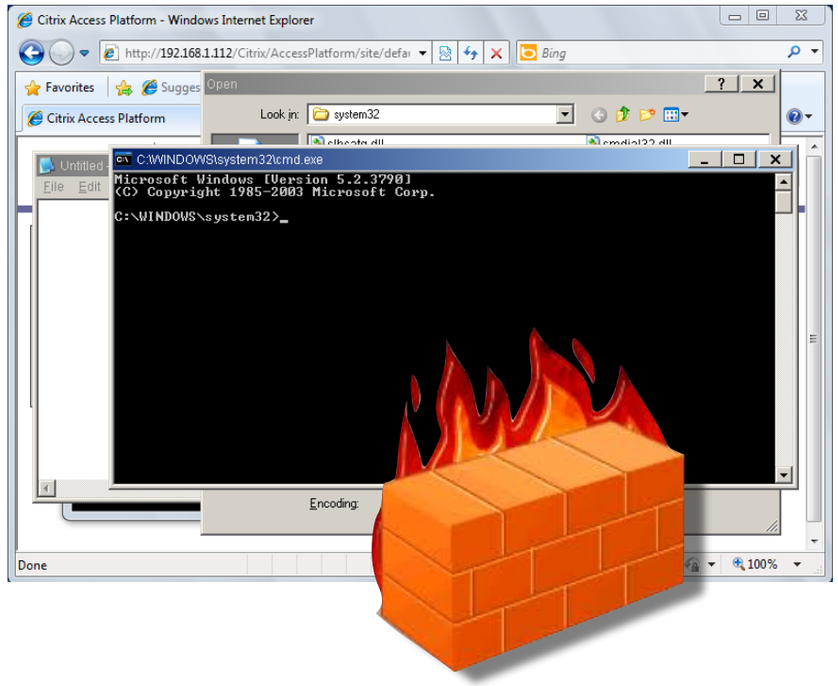
Scenario: the problem

- How to upload/download files from the isolated server?
  - No clipboard functionality available
    - no cut&paste, or binary transfers using clipboard
  - No 'client drive mapping'
  - No Internet access
    - No outgoing/incoming network traffic whatsoever



Scenario: the problem

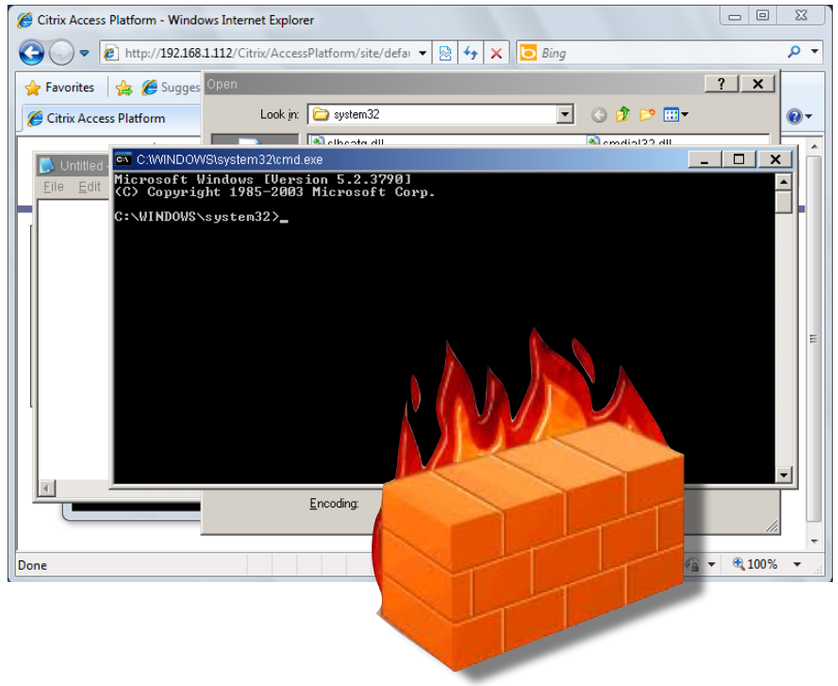
- How to upload/download files from the isolated server?
  - No clipboard functionality available
    - no cut&paste, or binary transfers using clipboard
  - No 'client drive mapping'
  - No Internet access
    - No outgoing/incoming network traffic whatsoever



- Only link with remote server is the GUI...

Scenario: the problem

- How to upload/download files from the isolated server?
  - No clipboard functionality available
    - no cut&paste, or binary transfers using clipboard
  - No 'client drive mapping'
  - No Internet access
    - No outgoing/incoming network traffic whatsoever



- Only link with remote server is the GUI...
  - ➡ Let's use that!...

The GUI: a two-way communication channel

cmd.exe

notepad.exe

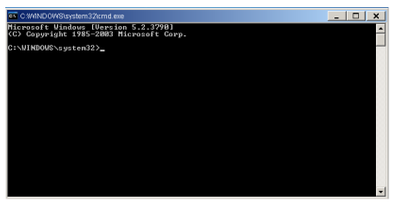
Remote desktop server (e.g.: Citrix server)

Server

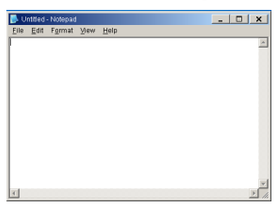
User input

GUI 'Changes'

'View' of cmd.exe



'View' of notepad.exe



User input

Remote desktop client (e.g.: Citrix client)

Workstation

The GUI: a two-way communication channel

cmd.exe

notepad.exe

Remote desktop server (e.g.: Citrix server)

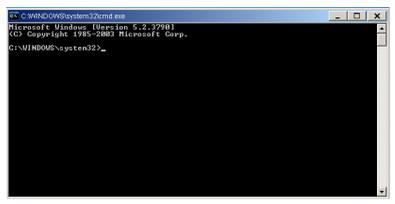
Server

'Send'/'Upload' channel

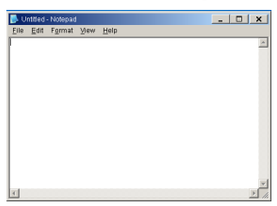
User input

GUI 'Changes'

'View' of cmd.exe



'View' of notepad.exe



User input

Remote desktop client (e.g.: Citrix client)

Workstation

The GUI: a two-way communication channel

cmd.exe

notepad.exe

Remote desktop server (e.g.: Citrix server)

Server

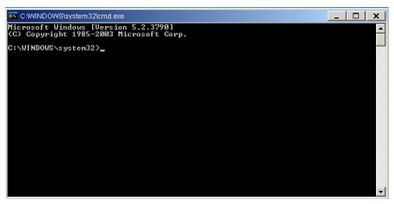
‘Send’/‘Upload’ channel

User input

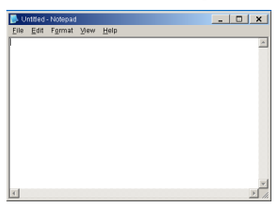
GUI ‘Changes’

‘Receive’/‘Download’ channel

‘View’ of cmd.exe



‘View’ of notepad.exe



User input

Remote desktop client (e.g.: Citrix client)

Workstation

The GUI: a two-way communication channel

cmd.exe

notepad.exe

Remote desktop server (e.g.: Citrix server)

Server

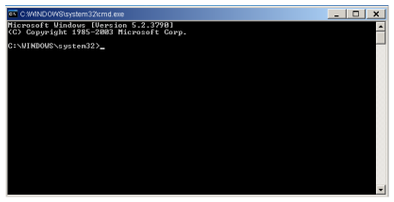
‘Send’/‘Upload’ channel
- mimic/automate user input

User input

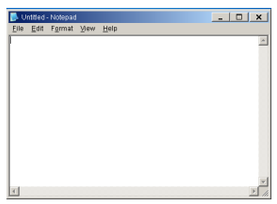
GUI ‘Changes’

‘Receive’/‘Download’ channel

‘View’ of cmd.exe



‘View’ of notepad.exe



User input

Remote desktop client (e.g.: Citrix client)

Workstation

The GUI: a two-way communication channel

cmd.exe

notepad.exe

Remote desktop server (e.g.: Citrix server)

Server

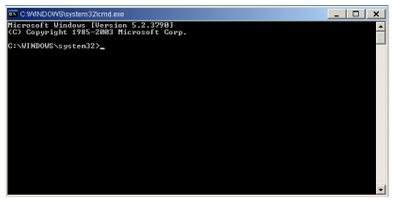
‘Send’/‘Upload’ channel
- mimic/automate user input

User input

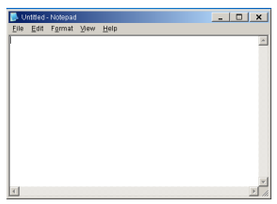
GUI ‘Changes’

‘Receive’/‘Download’ channel
- Detect changes in the GUI

‘View’ of cmd.exe



‘View’ of notepad.exe



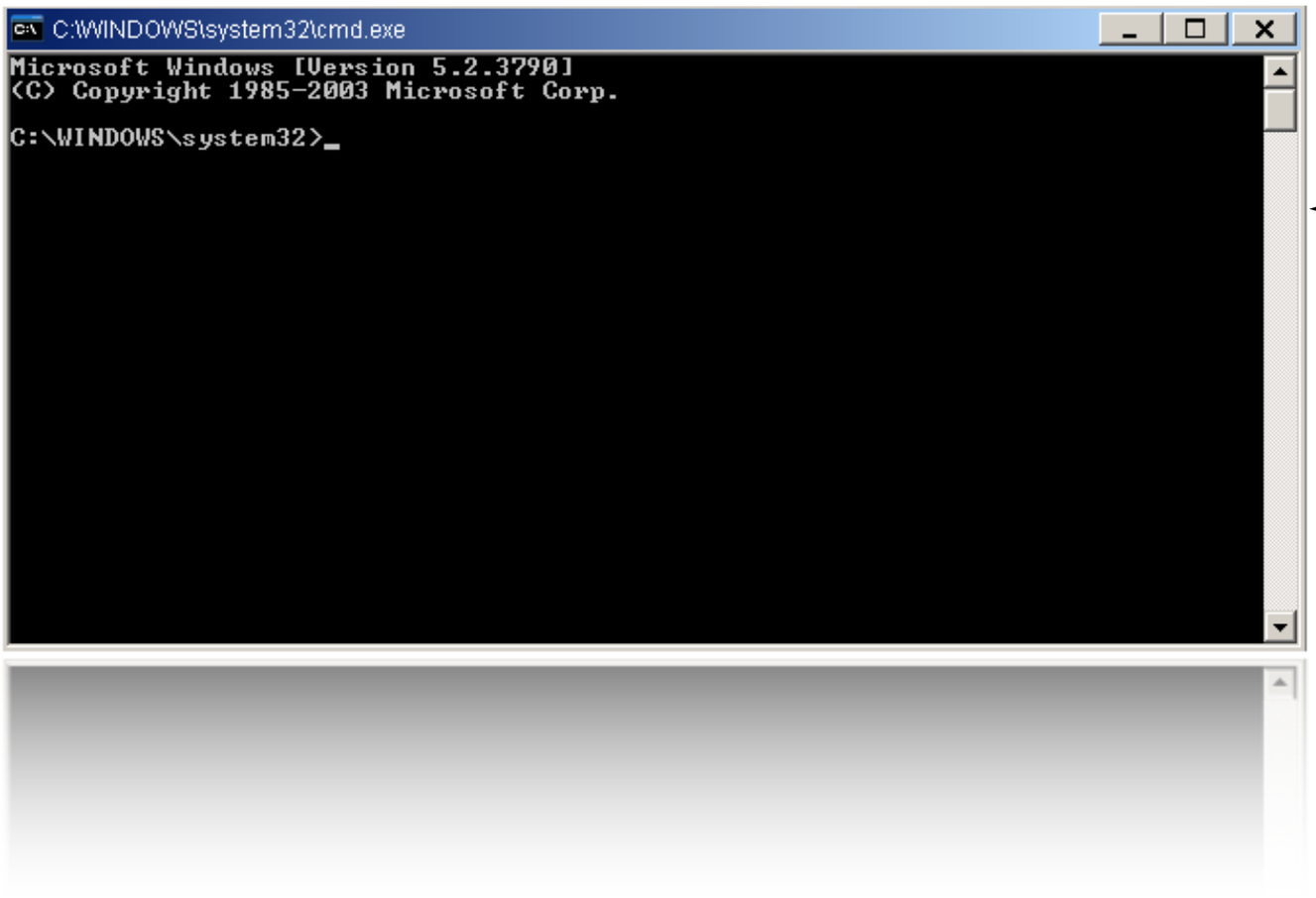
User input

Remote desktop client (e.g.: Citrix client)

Workstation

‘Send’/‘Upload’ channel

- mimic/automate user input



message loop

```
while(GetMessage(&Msg, NULL, 0, 0) > 0)
{
    TranslateMessage(&Msg);
    DispatchMessage(&Msg);
}
```

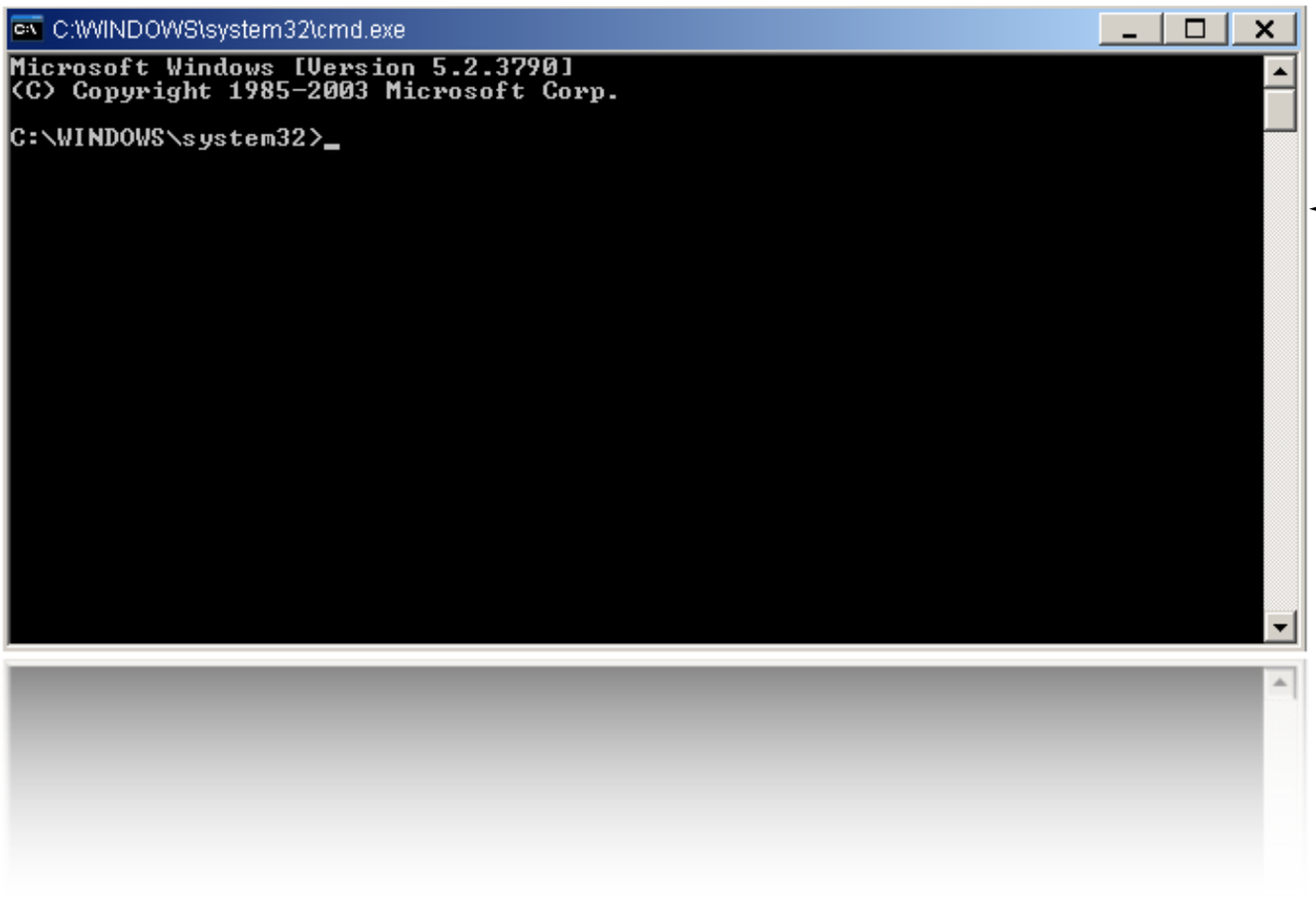
User input

Send/PostMessage(*HWND hWnd, UINT Msg, WPARAM wParam, LPARAM lParam*)

MyProcess.exe

‘Send’/‘Upload’ channel

- mimic/automate user input



message loop

```
while(GetMessage(&Msg, NULL, 0, 0) > 0)
{
    TranslateMessage(&Msg);
    DispatchMessage(&Msg);
}
```

User input

Send/PostMessage(hCmdWnd, ***WM_CHAR***, *char_code (e.g.:‘A’)*, *repeat count_&_others*)

MyProcess.exe

GUI Transfer Toolkit (GTT)

- **gtt_upload_citrix**
  - Mimics/automates user input using WIN32 API
    - E.g.: *SendMessage(hwnd,WM_CHAR, keycode, flags)*
    - Uploads 1 byte 'at a time' (per 'message sent')
    - Can upload ascii & binary files
  - Four 'modes':
    - 'plaintext' mode: sends ASCII data
    - 'copy con' mode: same as 'plaintext' but creates file
    - 'base64' mode: uploads base64-encoded binary data
    - 'debug.com' mode: uploads binary data using debug.com (hexa)
      - ➡ debug.com/exe is everywhere

GUI Transfer Toolkit (GTT)

- With **gtt_upload_citrix** we can upload files now

Send/PostMessage(hCmdWnd, ***WM_CHAR***, *char_code (e.g.:'A')*, *repeat count_&_others*)

MyProcess.exe

1-byte at a time

...but we want to do it faster..

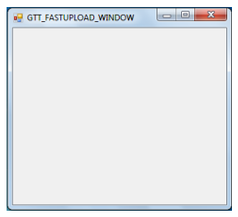
gtt_fastupload_server_citrix.exe

Remote desktop server (e.g.: Citrix server)

Server

WM_AMSG, *4-bytes*, *4-bytes*

'View' of gtt_fastupload_server_citrix.exe



Send/PostMessage(hWnd, ***WM_AMSG***, *4-bytes*, *4-bytes*)

Remote desktop client (e.g.: Citrix client)

Workstation

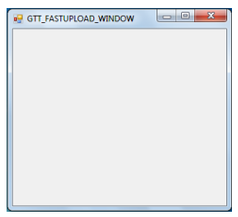
gtt_fastupload_server_citrix.exe

Remote desktop server (e.g.: Citrix server)

Server

WM_AMSG, *4-bytes*, *4-bytes*

'View' of gtt_fastupload_server_citrix.exe



Send/PostMessage(hWnd, ***WM_AMSG***, *4-bytes*, *4-bytes*)

Remote desktop client (e.g.: Citrix client)

Workstation

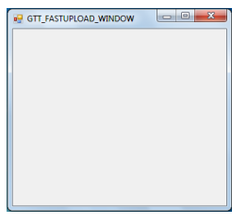
gtt_fastupload_server_citrix.exe

Remote desktop server (e.g.: Citrix server)

Server

WM_AMSG, *4-bytes*, *4-bytes*

'View' of gtt_fastupload_server_citrix.exe



Send/PostMessage(hWnd, ***WM_AMSG***, *4-bytes*, *4-bytes*)

Remote desktop client (e.g.: Citrix client)

Workstation

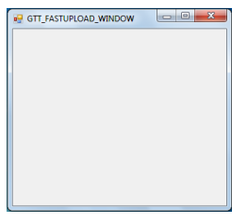
gtt_fastupload_server_citrix.exe

Remote desktop server (e.g.: Citrix server)

Server

WM_AMSG, *4-bytes*, *4-bytes*

'View' of gtt_fastupload_server_citrix.exe



Send/PostMessage(hWnd,
WM_AMSG, *4-bytes*, *4-bytes*)

Remote desktop client (e.g.: Citrix client)

Workstation

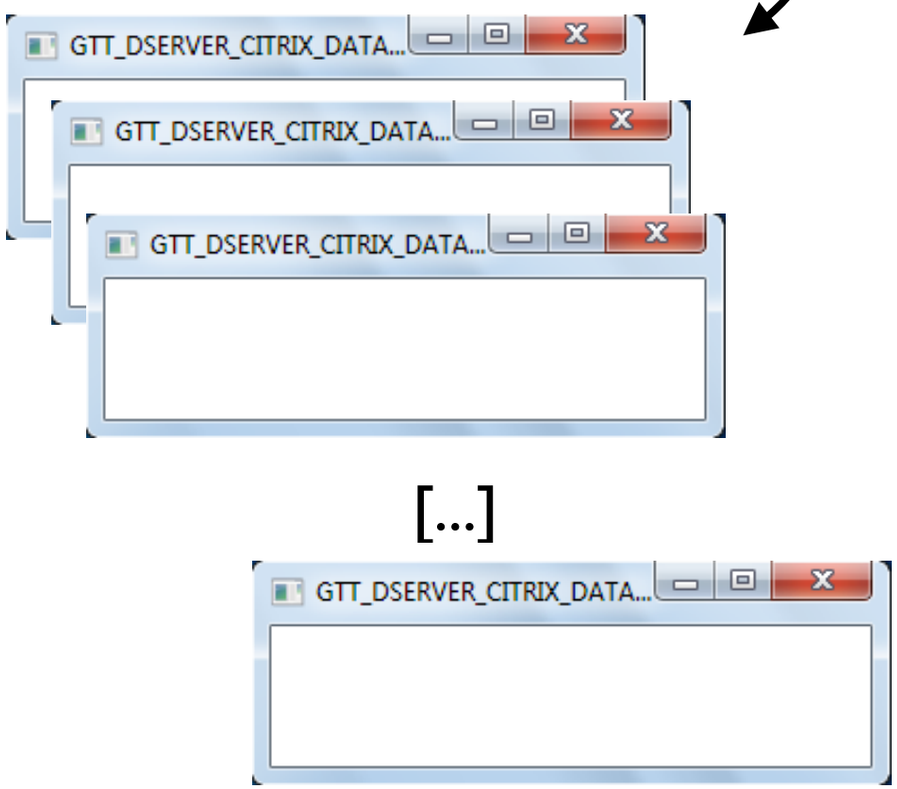
GUI Transfer Toolkit (GTT)

- **gtt_fastupload_citrix**
  - Uploads 8 bytes at a time (per 'message sent') instead of 1
    - Uses 'special' windows message that is sent to server without 'filtering'
      - e.g.: *SendMessage(hwnd,* ***WM_MYMSG****,* ***4-bytes****,* ***4-bytes****)*
    - Only message found with this characteristics out of 2^32 possible messages
  - Client/server
  - Faster uploads
  - ASCII & binary files (no base64-encoding needed)

‘Receive’/‘Download’ channel

- Detect changes in the GUI

bytes of file.exe are ‘translated’
to (x,y) coordinates



gtt_fastdserver_citrix.exe

hwnd = FindWindow(*CLTRWND*)
(x,y) = GetWindowRect(*hwnd*)

Filesize = *(x,y)*

While FileSize > 0:
    hwnd = FindWindow(*DataWnd*)
    (x,y) = GetWindowRect(*hwnd*)
    WriteToFile(*x,y*)
    FileSize -= 2

gtt_fastdclient_citrix.exe

Server

Workstation

‘Receive’/‘Download’ channel

- Detect changes in the GUI

File.exe: 10,20,40,F4 [..]

File.exe:

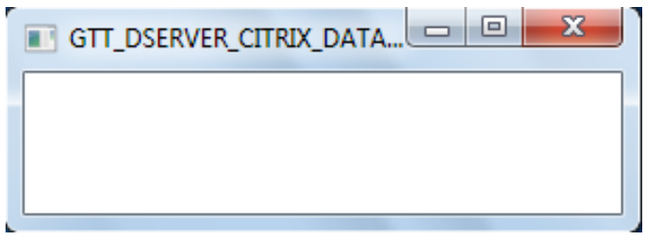
Server

Workstation

‘Receive’/‘Download’ channel

- Detect changes in the GUI

File.exe: 10,20,40,F4 [..]



(10,20)

File.exe:

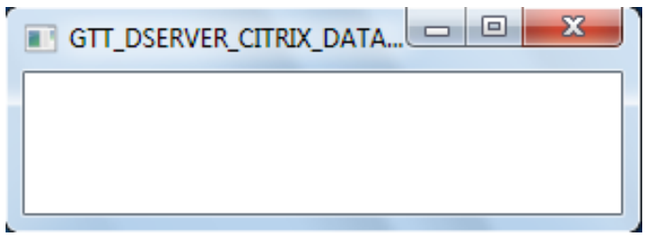
Server

Workstation

‘Receive’/‘Download’ channel

- Detect changes in the GUI

File.exe: 10,20,40,F4 [..]



(10,20)

hwnd = FindWindow(*DataWnd2*)

(10,20) = GetWindowRect(*hwnd*)

File.exe:

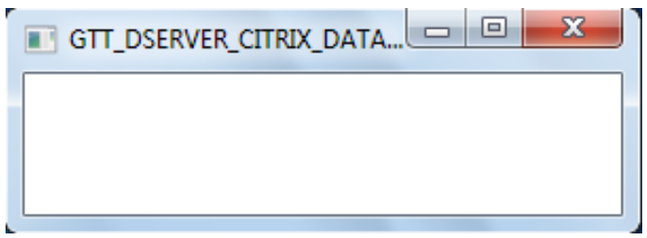
Server

Workstation

‘Receive’/‘Download’ channel

- Detect changes in the GUI

File.exe: 10,20,40,F4 [..]



(10,20)

hwnd = FindWindow(*DataWnd2*)

(10,20) = GetWindowRect(*hwnd*)

WriteToFile(*10,20*)

File.exe:
10,20

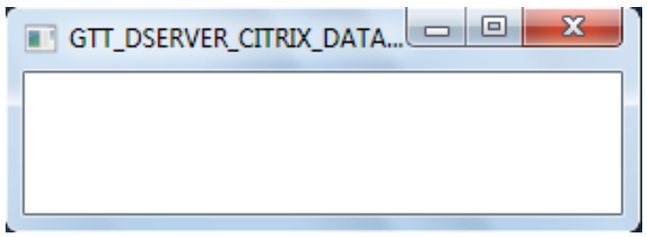
Server

Workstation

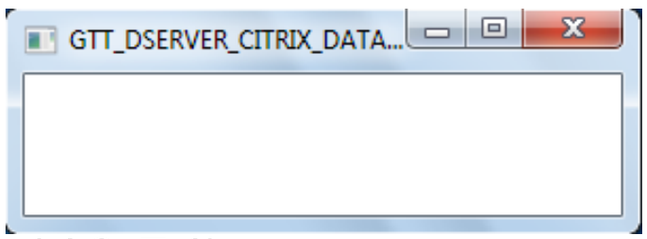
‘Receive’/‘Download’ channel

- Detect changes in the GUI

File.exe: 10,20,40,F4 [..]



(10,20)



(40,F4)

hwnd = FindWindow(*DataWnd2*)

(10,20) = GetWindowRect(*hwnd*)

WriteToFile(*10,20*)

File.exe:
10,20

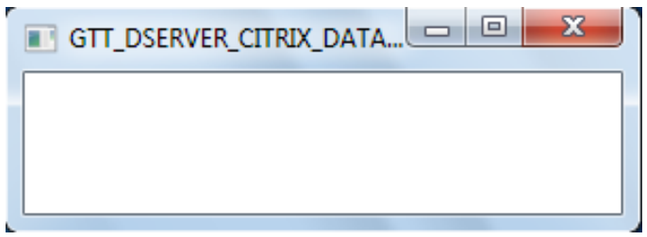
Server

Workstation

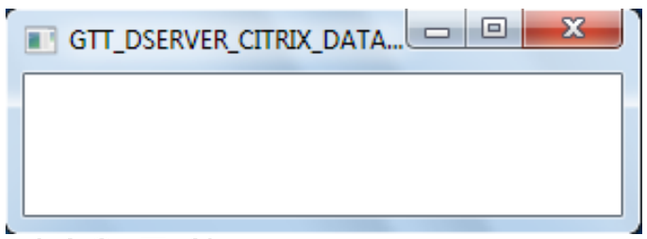
‘Receive’/‘Download’ channel

- Detect changes in the GUI

File.exe: 10,20,40,F4 [..]



(10,20)



(40,F4)

hwnd = FindWindow(*DataWnd2*)

(10,20) = GetWindowRect(*hwnd*)

WriteToFile(*10,20*)

hwnd = FindWindow(*DataWnd3*)

(40,F4) = GetWindowRect(*hwnd*)

File.exe:
10,20

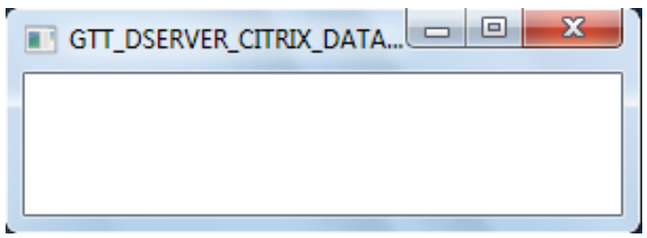
Server

Workstation

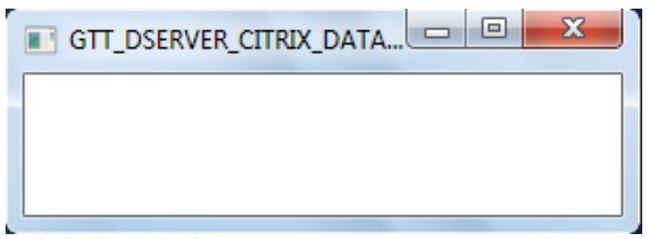
‘Receive’/‘Download’ channel

- Detect changes in the GUI

File.exe: *10,20,40,F4* *[..]*



(10,20)



(40,F4)

hwnd = FindWindow(*DataWnd2*)

(10,20) = GetWindowRect(*hwnd*)

WriteToFile(*10,20*)

hwnd = FindWindow(*DataWnd3*)

(40,F4) = GetWindowRect(*hwnd*)

WriteToFile(*40,F4*)

File.exe:

10,20,40,F4

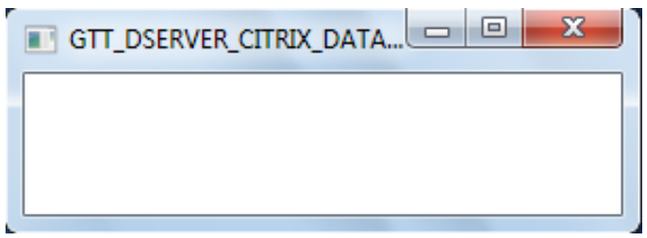
Server

Workstation

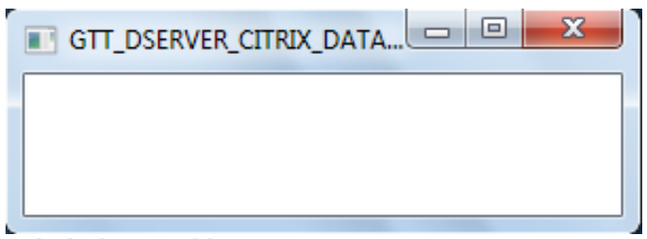
‘Receive’/‘Download’ channel

- Detect changes in the GUI

File.exe: 10,20,40,F4 [..]



(10,20)



(40,F4)

[..]

hwnd = FindWindow(*DataWnd2*)

(10,20) = GetWindowRect(*hwnd*)

WriteToFile(*10,20*)

hwnd = FindWindow(*DataWnd3*)

(40,F4) = GetWindowRect(*hwnd*)

WriteToFile(*40,F4*)

[..]

File.exe:

10,20,40,F4 [..]

Server

Workstation

GUI Transfer Toolkit (GTT)

- **gtt_fastdownload_citrix**
  - Client/server
  - Downloads binary & ascii files
  - Server creates 10 windows
  - Download loop:
    - Server sets (x,y) of windows with bytes from file to transfer
    - Client tracks (x,y) coordinates of windows
    - Client saves new (x,y) as bytes to file
  - Downloads 20 bytes ‘at a time’ (per ‘delay unit’...)
    - 2 bytes per window (x,y)

Future Work

- Support for MS RDP and other platforms (e.g.: xserver)
- Improve speed
- 'Delay' auto-sensing
- Built-in compression
- Experiment with other implementations of same idea
  - e.g.: use pixels/images instead of (x,y) coordinates
  - e.g.: grab (x,y) and also size (x2,y2)
  - etc.
- Implement tcp/socks proxy
- Use Citrix Protocol
  - Better results? but current implementation is super simple

Conclusions

- Even when explicitly disabled through different measures
  - ➡ data/file transfers are possible on isolated remote desktop environments
  - ➡ GUI provides implicit bidirectional channel for data transfer

- The GUI Transfer Toolkit (GTT) is an implementation of this concept

- Don’t trust isolation lightly
  - ➡ perform thorough assessment of your environment

Thank you!

- Hernan Ochoa (hernan@ampliasecurity.com)
- www.twitter.com/hernano