

Malware Challenge 2008

Nelson B Santos

nbsantos@gmail.com

Describe your malware lab.

Environment:

- Virtual Machine with Host-Only NIC running on VMWare Workstation 6.5;
- The virtual machine is running Windows XP SP3 with all Microsoft patches (as of 10/23);

Tools:

- Sysinternals: Strings, TCPView, ProcExp, FileMon, RegMon, AutoRuns;
- HxD (Hex Editor);
- Beware IRCd (running on the host);
- OllyDbg 1.10 and IdaPro 4.9;
- UPX Packer 3.03
- Wireshark

What information can you gather about the malware without executing it?

Running Strings on the file revealed no meaningful information except for a few DLLs. With that information it seemed obvious the malware had been obfuscated.

At first the file's header did not seem to have any relevant information regarding what, if any, packer was used. A closer look did reveal some information that was later used to unpack the malware (next question).

After unpacking the malware many interesting strings were found. A few are shown below:

- Crxbot Alias REalmbot -by Lindem-
- testirc1.sh1xy2bg.NET
- Winsec32.exe
- <http://www.W32-gen.us>
- Software\Microsoft\Windows\CurrentVersion\Run
- <http://www.Nivdav.net/Winsec32.exe>

Besides those strings, I also found many IRC commands; what seemed like responses to commands (starting with “[REALMBOT]”); some other strings that seemed like C&C commands (“pingflood”, “advscan”, “ddos.random”); some HTML code was also found.

Is the malware packed? If so, how did you determine what it was?

Yes. By looking at the file header using a hex editor I was able to find a few strings that looked suspicious. The strings were: ABC0, ABC1, ABC2 and ABC!

A file that has been packed with UPX has the following strings on its header: UPX0, UPX1, UPX2 and UPX!

Simply running UPX on the file returned an error suggesting the file had been further obfuscated or another packer was used.

I then changed the malware header to match a UPX packed header (replaced the ABCs with UPXs) and reran UPX. This time the unpacking was successful (beats the hell out of letting the file unpack itself and then stop execution :-D).

Describe the malware's 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?

The malware makes an exact copy of itself (same MD5) and places it on C:\WINDOWS\Winsec32.exe. This is flagged as a hidden system file.

The malware seems to access many registry keys. Some of them are Internet Settings keys, some WinSock2 parameter keys, etc.

It also creates entries on “Software\Microsoft\Windows\CurrentVersion\Run” and “Software\Microsoft\Windows\CurrentVersion\RunServices”. This is how it auto-starts. It tries to connect to an IRC server. Although I did find more URLs among the file’s strings I could not see any other connection attempts. Maybe it requires special commands to be sent to the malware.

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.

The malware tries to connect to a IRC server on “testirc1.sh1xy2bg.net”. It creates a channel called “#challenge” and changes its subject to “.asc vnc 100 0 0 -r -b”. This gave me the idea that it might receive commands thru topic changes. There are references on the strings to PRIVMSGs too.

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.

I was able to set an IRC server and change the hosts file to point to it. I then tried many combinations of setups (letting the malware create the channel and joining after, creating the channel myself and joining after, etc). As stated before I found many commands that look like C&C commands. I tried to send MSGs, PRIVMSGs and TOPIC changes to the malware but I received no response. I also tried to “login” to it but was again unsuccessful.

One interesting thing that happened was that if I kicked the malware out of the channel after he had changed the topic to “.asc vnc 100 0 0 -r -b” it would rejoin the channel and started trying to connect to random servers on the same subnet on port 5900 (VNC).

I tried many combinations of topics using the strings found on the file but the malware did not respond to any.

How would you classify this malware? Why?

After looking at the dynamic behavior of the malware I would say it is a trojan horse/bot. After infecting a machine it would allow an attacker to control the machine remotely using IRC.

What do you think the purpose of this malware is?

I believe the main purpose is to steal passwords and serve as an attack platform for the attacker. Some of the strings on the file (e-gold, PayPal, MercadoLivre Brasil) seem to confirm this.

I did not find any mail functionality so I doubt it serves as a spamming platform.

Bonus questions: (These questions are not required to be answered but could be used to break a tie for prizes.)

Is it possible to find the malware's source code? If so, how did you do it?

Yes. One of the strings on the file was "Crxbot Alias REalmbot -by Lindem-". I then searched for "CRX RealmBot" and found the source code on [http://darksun.ws/download/bots/Crx-realmbot.VNC.exploit.and.RFI-\(rfi.not.tested\).rar](http://darksun.ws/download/bots/Crx-realmbot.VNC.exploit.and.RFI-(rfi.not.tested).rar)

How would you write a custom detection and removal tool to determine if the malware is present on the system and remove it?

Detection: I would first search for the Winsec32.exe process, then search for a reference to that process on the registry and then search for the file it self.

The following VBScript code removes the malware:

```
On Error Resume Next
```

```
const HKEY_LOCAL_MACHINE = &H80000002
strComputer = "."
file = "c:\WINDOWS\Winsec32.exe"
```

```
'-----
```

```
Set objWMIService = GetObject("winmgmts:{impersonationLevel=impersonate}!/" & strComputer)
```

```
Set colProcessList = objWMIService.ExecQuery ("Select * from Win32_Process Where Name = 'winsec32.exe'")
```

```
For Each Proc in colProcessList
```

```
    Proc.Terminate()
```

```
Next
```

```
'-----  
Set fs = CreateObject("Scripting.FileSystemObject")  
Set f = fs.GetFile(file)
```

```
f.attributes = 0
```

```
'Don't ask... it was trying to delete the file before the attribute change were committed.  
wscript.sleep 1000
```

```
fs.DeleteFile(file)
```

```
'-----  
Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" &  
strComputer & "\root\default:StdRegProv")
```

```
strRunKey = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"  
strRunValue = "Microsoft Svchost local services"
```

```
strRunServicesKey = "SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices"  
strRunServicesValue = "Microsoft Svchost local services"
```

```
oReg.DeleteValue HKEY_LOCAL_MACHINE, strRunKey, strRunValue  
oReg.DeleteValue HKEY_LOCAL_MACHINE, strRunServicesKey,  
strRunServicesValue
```