

Describe your malware lab

I've tried the malware on Windows XP SP2 not patched with latest patch, and where there was installed the following softwares:

- Comodo Personal Firewall (Firewall + Defense+),
- Ati Driver
- Realtek audio driver
- Mozilla Firefox
- TrendNet wireless adapter driver
- Winrar

The system was installed on an AMD Athlon 64 3200+, 1 GB RAM, 80 GB HD.

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

I can get the following information:

- MD5: 59a95f668e1bd00f30fe8c99af675691
- SHA1: 2d1c8898ccc33c58c552f7a7091b165088c180d5
- SHA256: ab8462fac7a54b96ec59f32464cb6fa68e04f59c7f563e7f348db541f1dd198b
- SHA512: 4f68f14783442e4ec8cd0ba9427204f9fa9e3609245713fb79035e5b5ed5eea44d03df09a83e0c9fd756e4be53a3edc98fdf27d73131a40a97773a7303058a8d

What kind of file is it? Probably it is a **Win32 EXE Yoda's Crypter**.

Its file size is of 75 264 bytes.

It is packed with UPX.

Is the malware packed?

Yes, it is packed with UPX 0.89.6 - 1.02 / 1.05 - 1.24, I got this information with PEiD 0.94.

Describe the malware's behaviour

After executing malware.exe, it creates the file Winsec32.exe with the attributes system, hidden, only read. This file is the same of malware.exe, just copied in C:\WINDOWS and renamed.



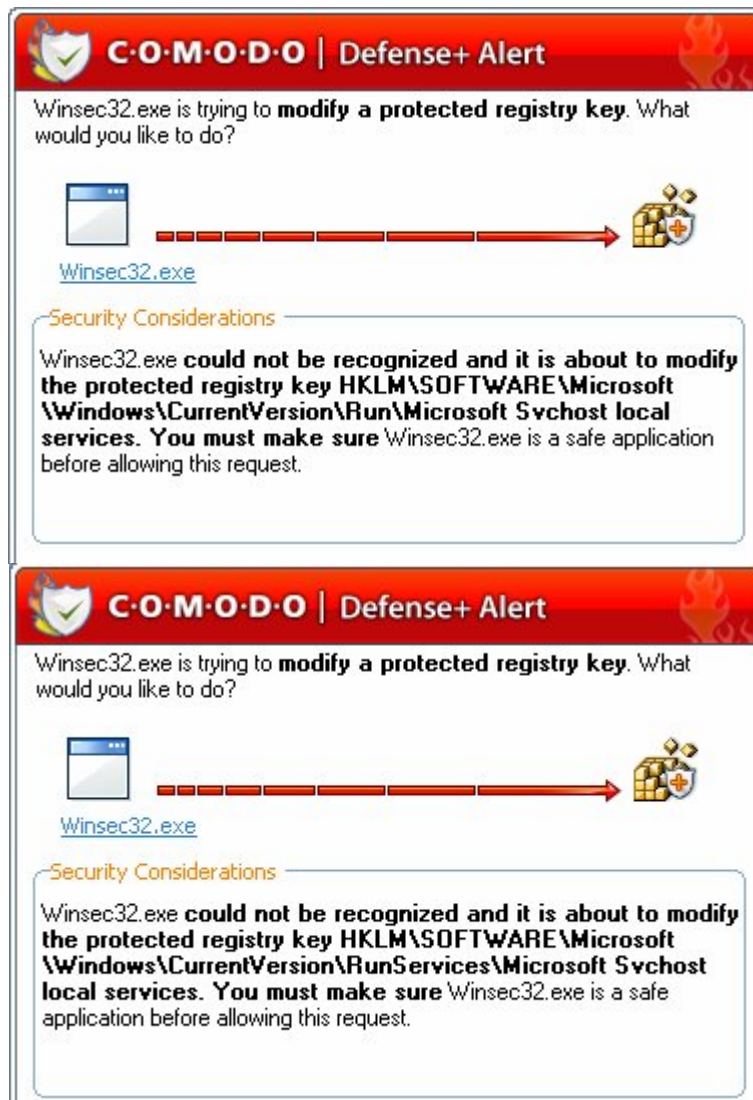
Winsec32.exe creates the following keys/values in the system:

- HKU\S-1-5-21-57989841-152049171-725345543-1003\Software\Microsoft\OLE\Microsoft Svchost local services: "Winsec32.exe"

- HKEY_CURRENT_USER\Software\Microsoft\OLE\Microsoft Svchost local services: “Winsec32.exe”
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Svchost local services: “Winsec32.exe”
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Svchost local services: “Winsec32.exe”

It edits this:

- HKLM\SOFTWARE\Microsoft\ESSENT\Process\ipconfig\DEBUG\Trace Level: “”



It also establish a connection with the IP address 77.67.20.164, and open the ports 1092, 1093, 1094, 1095.

TCP	megalab:ingres lock	77.67.20.164:http	ESTABLISHED
TCP	megalab:1552	77.67.20.164:http	TIME_WAIT
TCP	megalab:1555	77.67.20.164:http	TIME_WAIT

It autostart by the following registry values:

- HKU\S-1-5-21-57989841-152049171-725345543-1003\Software\Microsoft\OLE\Microsoft Svchost local services: “Winsec32.exe”

- HKEY_CURRENT_USER\Software\Microsoft\OLE\Microsoft Svchost local services: “Winsec32.exe”
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Svchost local services: “Winsec32.exe”
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Svchost local services: “Winsec32.exe”

What type of command and control server does the malware use?

It sends/receives these commands:

```
NICK USA[XP]9277007
USER fnxveqpd 0 0 :USA[XP]9277007
USERHOST USA[XP]9277007
MODE USA[XP]9277007 +i-x+s
JOIN #challenge happy12
NOTICE USA[XP]9277007 :.VERSION http://www.W32-gen.us (-National Virus Site-).
NOTICE #challenge :USA[XP]9277007 has just versioned me.
PRIVMSG #challenge :RealmBoT (irc.p.l.g) .... Status: Ready. Bot Uptime: 0d 0h 0m.
PRIVMSG #challenge :RealmBoT (irc.p.l.g) .... Bot ID: 1.
PRIVMSG #challenge :RealmBoT (portscan.p.l.g) .... Exploit Statistics: VNC: 0, Total: 0 in 0d 0h 0m.
PRIVMSG #challenge :RealmBoT (irc.p.l.g) .... Uptime: 0d 0h 35m.
PRIVMSG #challenge :[REALMBOT] : Failed to start scan, port is invalid.
NICK USA[XP]6071111
USER wycbtzuvy 0 0 :USA[XP]6071111
USERHOST USA[XP]6071111
MODE USA[XP]6071111 +i-x+s
NICK USA[XP]7100383
USER wycbtzuvy 0 0 :USA[XP]7100383
USERHOST USA[XP]7100383
MODE USA[XP]7100383 +i-x+s
NICK USA[XP]0098537
USER vwtqvmfr 0 0 :USA[XP]0098537
USERHOST USA[XP]0098537
MODE USA[XP]0098537 +i-x+s
```

It try to connect to <http://testirc1.sh1xy2bg.net/>.

What commands are present within the malware and what do they do?

It try to spread itself on shared folders like ADMIN\$, C\$, D\$, IPC\$; using a dictionary attack to access to the folders.

How would you classify this malware?

This malware is, in my opinion, a worm and a backdoor.

What do you think the purpose of this malware is?

The purpose of the malware is to infect more computers, and give access to the system to a remote server.

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

This tool has to verify if there is a process Winsec32.exe, if so, kill it, and delete %System%\Winsec32.exe with related registry values.