

Automatic Sinowal Extraction

Automatic Sinowal Extraction	1
1. Use Clean VMware	2
2. Install Sysinternals Autlogon	2
3. Extract the Files	2
4. Copy Sinowal Infectors	2
5. Execute Automatic-Sinowal.cmd	2

Eigene Dateien

Utils

Arbeitsplatz

Netzwerkumgebung

Internet Explorer

Bginfo.exe

Papierkorb

SysAnalyzer

TrueCrypt

1. Use Clean VMware

With clean Windows XP.
We will put stuff on desktop then.



IDA Pro Advanced
(32-bit)

OS Version:
Service Pack:
System Type:
User Name:
Volumes:

Windows XP
Service Pack 2
Workstation
Administrator
C:\ 3.99 GB NTFS

Eigene Dateien

Utils

Arbeitsplatz

Netzwerkumgebung

Internet Explorer

Bginfo.exe

Papierkorb

SysAnalyzer

TrueCrypt

Autologon.exe

2. Install Sysinternals Autologon

<http://download.sysinternals.com/Files/Autologon.zip>: We need it for later automatic extraction (Stoned Bootkit needs restarts to become active).



IDA Pro Advanced
(32-bit)

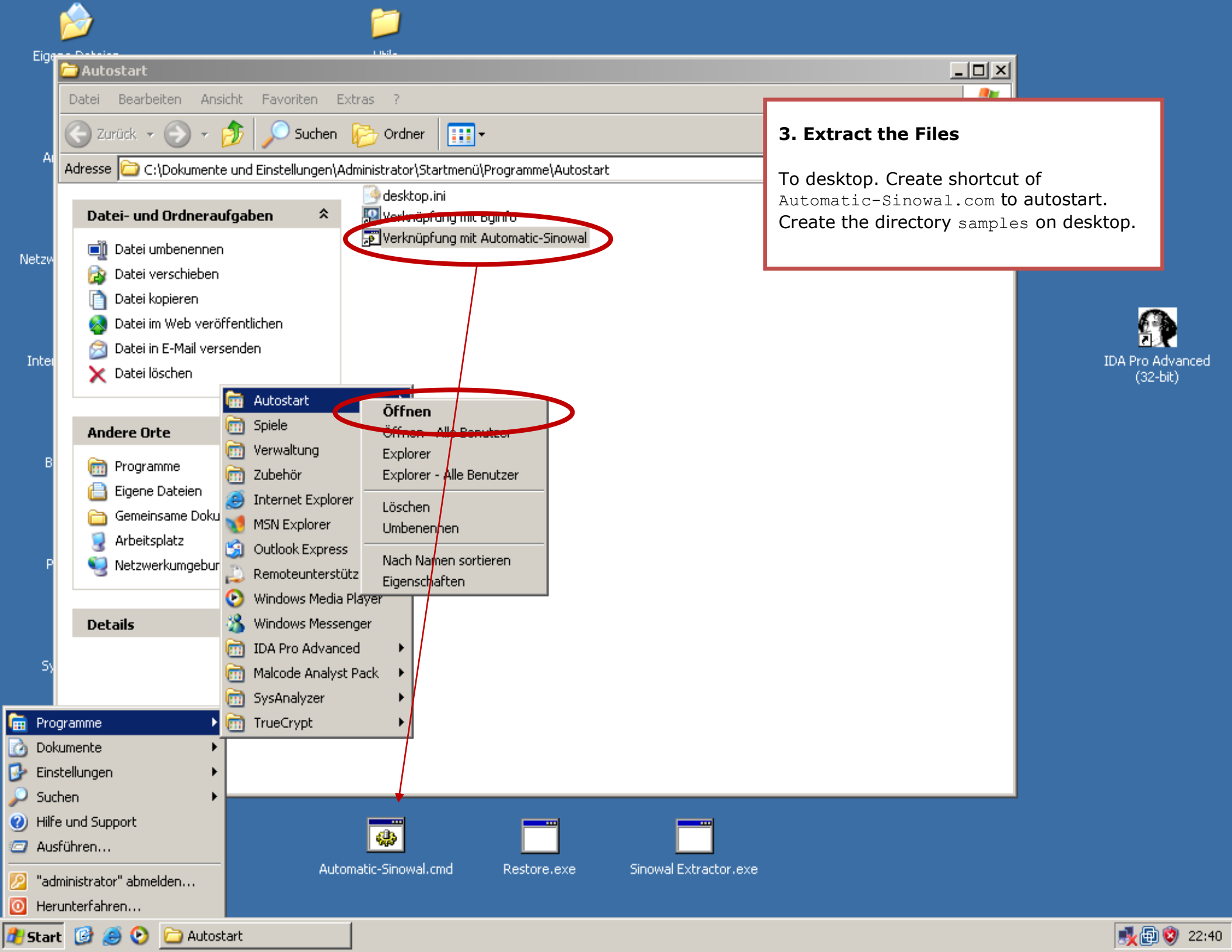
OS
S
U
V

Autologon - Sysinternals [X]

Username:	<input type="text" value="administrator"/>	<input type="button" value="Enable"/>
Domain:	<input type="text" value="ANTITROJAN"/>	<input type="button" value="Disable"/>
Password:	<input type="password" value=" "/>	<input type="button" value="About"/>

3. Extract the Files

To desktop. Create shortcut of Automatic-Sinowal.com to autostart. Create the directory samples on desktop.



Eigene Dateien

Utils

Arbeitsplatz

Netzwerkumgebung

Internet Explorer

Bginfo.exe

Papierkorb

SysAnalyzer

TrueCrypt

Autologon.exe

Automatic-Sinowal.cmd

Restore.exe

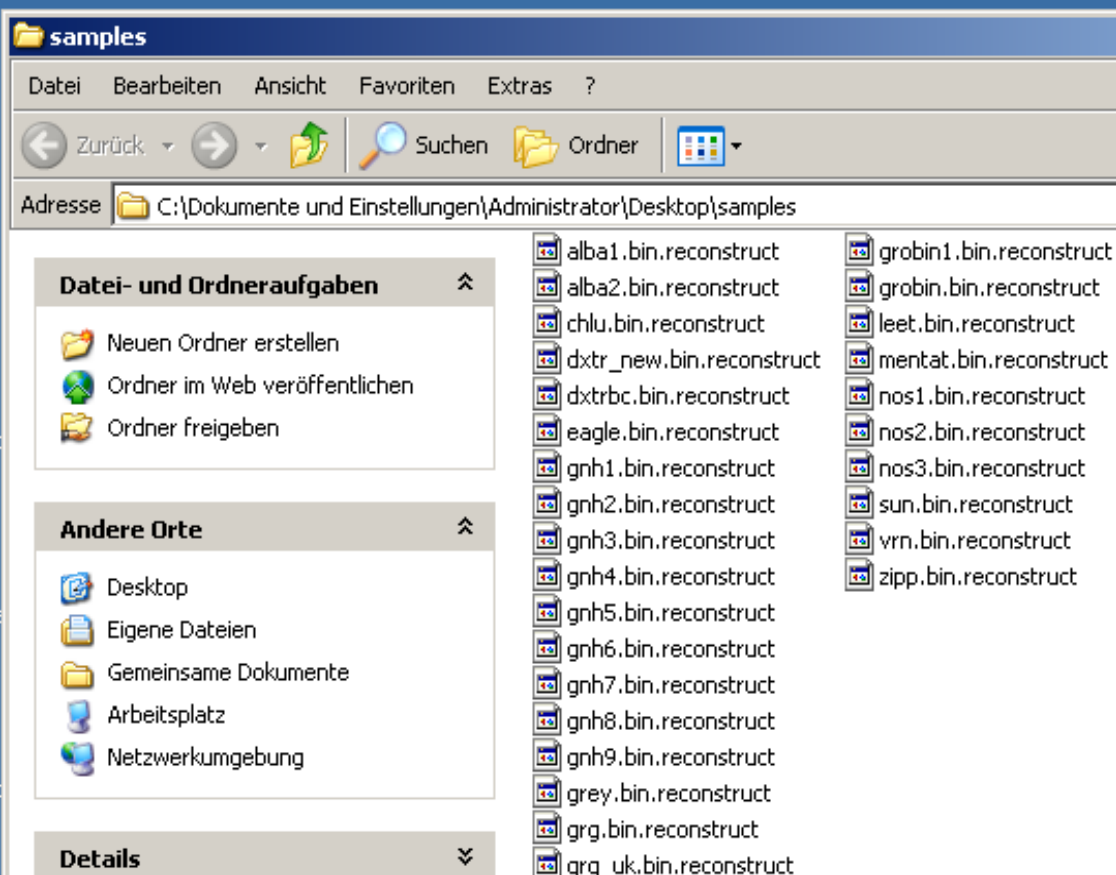
Sinowal Extractor.exe

samples

IDA Pro Advanced
(32-bit)

4. Copy Sinowal Infectors

Which you have directly downloaded from Sinowal server, copy them into samples.



Eigene Dateien

Arbeitsplatz

Netzwerkumgebung

Internet Explorer

Bginfo.exe

Papierkorb

SysAnalyzer

TrueCrypt

Autologon.exe

Analysis of
alba1.bin.reconstruct

Utils

C:\WINDOWS\system32\cmd.exe

Das System kann die angegebene Datei nicht finden.
alba1.bin.reconstruct

Sinowal Extractor
Version A Jun 8 2009
(C) 2009 Peter Kleissner


Started with Process ID 892,
Found unpartitioned space at :

Entering check-loop:
* Extracted Sinowal Master Boot
* Extracted Unpartitioned Space
* Found Kernel driver at sector
* Extracted Kernel Driver successfully

Clean-up:
* Terminated Sinowal Process
* Restored original MBR and boot sector

Sinowal Bootkit extracted successfully.
Exited successfully.
Drücken Sie eine beliebige Taste . . . _

System herunterfahren

 Das System wird heruntergefahren. Speichern Sie alle Daten, und melden Sie sich ab. Alle Änderungen, die nicht gespeichert werden, gehen verloren. Das Herunterfahren wurde von ANTITROJAN\Administrator ausgelöst.

Zeit bis zum Herunterfahren: 00:00:03

Meldung

5. Execute Automatic-Sinowal.cmd

It will do everything automatically.
Just enjoy!
Don't wonder your system will restart automatically.


IDA Pro Advanced
(32-bit)

Automatic-Sinowal.cmd

Restore.exe

Sinowal Extractor.exe

samples

Your system will restart as many times as many files you have in the directories `\samples\`. You can put Sinowal Infectors or Sinowal Packed Drivers in the samples folder. The extracted files for each file will land on `Analysis of [Filename]` on desktop. You are probably most interested in the `Unpacked Sinowal Driver.sys` file.

When finished, it will display **Your PC is now Stoned!** ..again and pause (in console).

Issue 1: Sinowal Extractor hangs

It was reported that Sinowal Extractor hangs on writing out the bootkit. If you experience that, please drop me a mail together with the `Extraction Log.txt` from the `Analysis..` directory and tell me your configuration (how many partitions, what OS you use).

Issue 2: Windows XP is currently only supported!