



Ethical Hacking and Countermeasures

Version 6



Module LIX

How to Steal Passwords

WoW password stealing worm and YouTube video playing trojan

Posted on 01.02.2008



digg



reddit



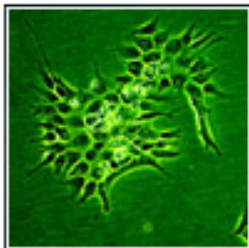
del.icio.us



stumble this!



magnolia



The list of the most active malware this week is headed by two variants of the Bagle worm. The Comet adware, which shows ads to users through banners, pop-ups, etc, comes in third place.

Regarding new strains of malware that have appeared this week, the PandaLabs report focuses on the Nabload.CXU Trojan and the Wow.SI, Lineage.HIT and Chike.B worms.

The Nabload.CXU Trojan spreads in emails with the subject "A Pessoa com o Maior Rabo do Mundo" and contains a text in Portuguese and a link to a video. However, if the user clicks the link, they will actually be downloading a copy of the Trojan onto their computers. Then, the Trojan plays a YouTube video to conceal its actions.

Also, this malicious code downloads two banker Trojans onto the computer to steal login data for accessing various banking entities' services.

Source: <http://www.net-security.org/>

Virus Stealing Bank Passwords

12 January 2008

BBC News is [reporting](#) about a stealthy Windows virus that steals login details for online bank accounts.

In the last month, the malicious program has racked up about 5,000 victims - most of whom are in Europe. Many are falling victim via booby-trapped websites that use vulnerabilities in Microsoft's browser to install the attack code.

The malicious program is a type of virus known as a rootkit and it tries to overwrite part of a computer's hard drive called the Master Boot Record (MBR). This is where a computer looks when it is switched on for information about the operating system it will be running.

Once installed the virus downloads other malicious programs, such as keyloggers, to do the work of stealing confidential information. Most of these associated programs lie in wait on a machine until its owner logs in to the online banking systems of one of more than 900 financial institutions.

Between 12 December and 7 January, iDefense detected more than 5,000 machines that had been infected with the program. Although the password-stealing programs that Mebroot installs can be found by security software, few commercial anti-virus packages currently detect its presence. Mebroot cannot be removed while a computer is running.

Source: <http://metasquad.blogspot.com/>

Copyright © by **EC-Council**

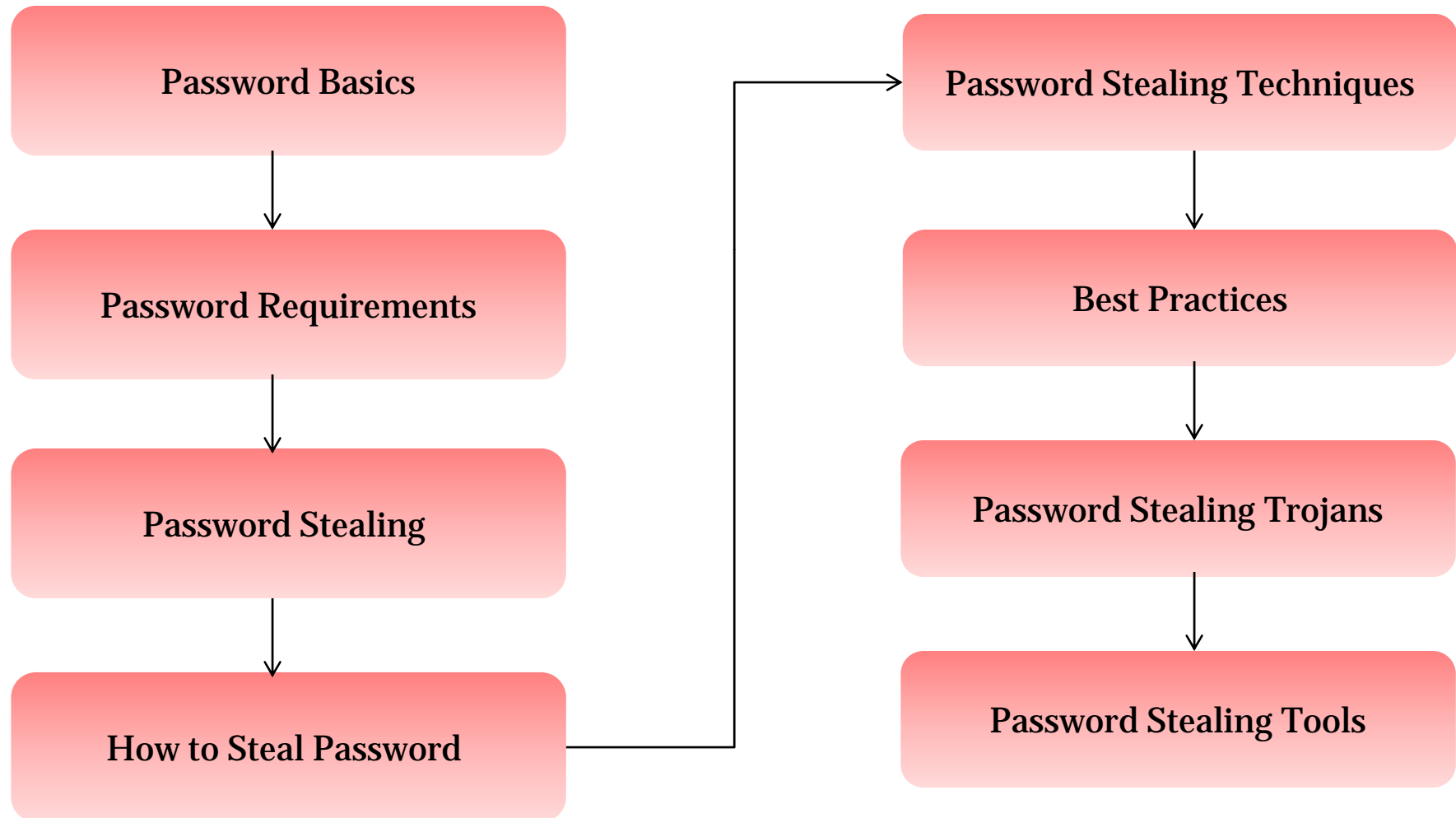
All Rights Reserved. Reproduction is Strictly Prohibited

Module Objective

This module will familiarize you with:

- Password basics
- Password Requirements
- Password Stealing
- How to Steal Password
- Password Stealing Techniques
- Best Practices
- Recommendations for Improving Password Security
- Password Stealing Trojans
- Password Stealing Tools





Password Stealing

A password is a first line of defense to systems and personal information

Password stealing is used by the hackers to exploit user credentials

It allows attackers to access personal information from the system and modify your credentials

It may cause serious data loss from the system



How to Steal Passwords

Password can be observed during entry

When password is given away voluntarily

Writing down the password somewhere and the piece of paper gets stolen

It can be guessed if it is easily guessable

It can be so short that an exhaustive search will quickly find it

Can be stolen by using password stealing tools

Can be stolen by using techniques such as Phishing and Social Engineering

When password is stored somewhere in clear text and this clear text can be copied

When password is encrypted but the encryption may be breakable

Password Stealing Techniques

Social Engineering

- Social Engineering is the human side of breaking into a corporate network to get the personal information
- An unknown person takes user credentials by using an email or by asking questions over the phone



Phishing

- Phishing is an Internet scam where the user is convinced to give valuable information
- It offers illegal websites to the users to fill their personal credentials
- It's purpose is to get access to the user's bank accounts, password, and other personal information



Password Stealing Techniques (cont'd)

Spying

- Spying refers to continuously observing a person's activities and his/her work
- It is a technique used to monitor the computer or the network and record all the user's credential on the computer or network



Guessing

- Many users choose weak passwords which are easy to guess
- It may be a word "Password", "Admin", "Passcode", or it may be a user's name, login name, their kid's name, or spouse's name, etc.

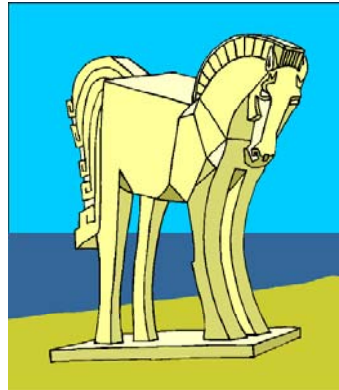


Password Stealing Techniques (cont'd)

Shoulder Surfing:

- Shoulder Surfing is done using direct observation techniques, such as looking over someone's shoulder, when they enter a password or a PIN code
- It is an effective way to get information in crowded places because it is relatively easy to stand next to someone and watch his/her activities
- It can be also done from a long distance with the help of binoculars or other vision-enhancing devices





Password Stealing Trojans

MSN Hotmail Password Stealer

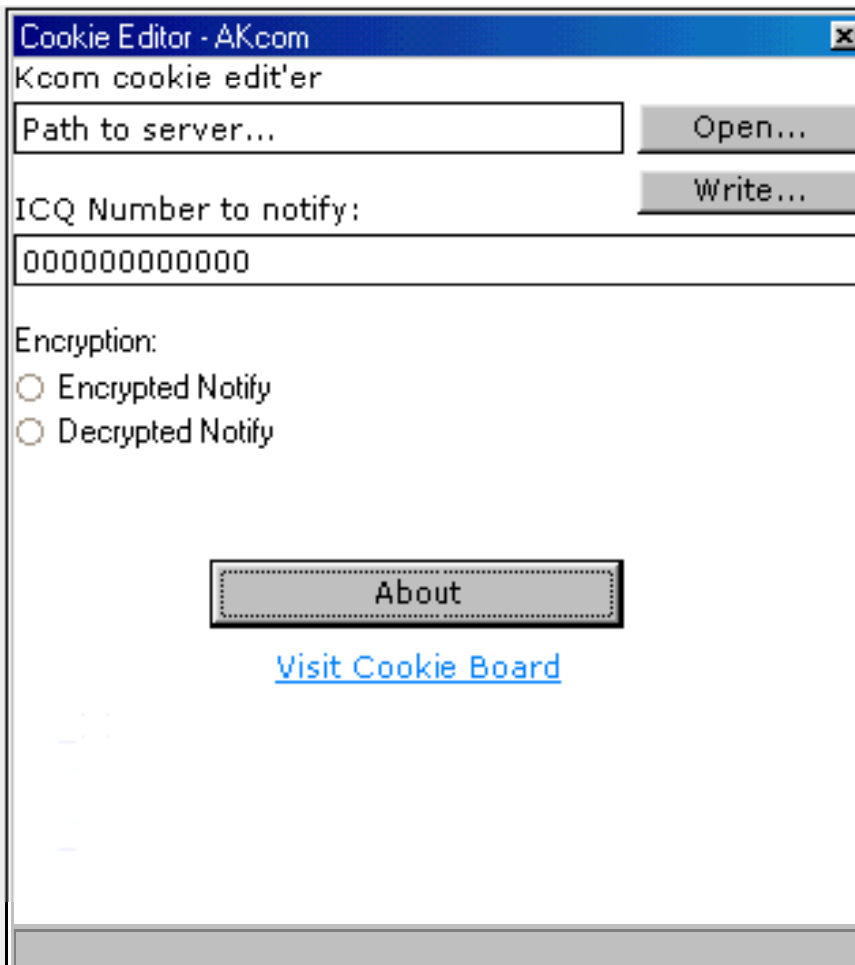
A Password Stealer is software that secretly captures passwords from the computer

It is designed to be executed and used in stealth mode, undetected by computer users and network administrators

MSN hotmail password stealer opens up the cookie in the editserver and edits away




MSN Hotmail Password Stealer: Screenshot



AOL Password Stealer

AOL Password Stealer is a email password restoration tool which restores lost forgotten passwords

AOL Connection Manager



Error, connection lost.
Please re-enter information
to sign on again:

Select Screen Name:

Password:

Select Location:

SETUP ACCESS NUMBERS HELP SIGN ON

Trojan-PSW.Win32.M2.14.a

This Trojan horses is capable of stealing various passwords

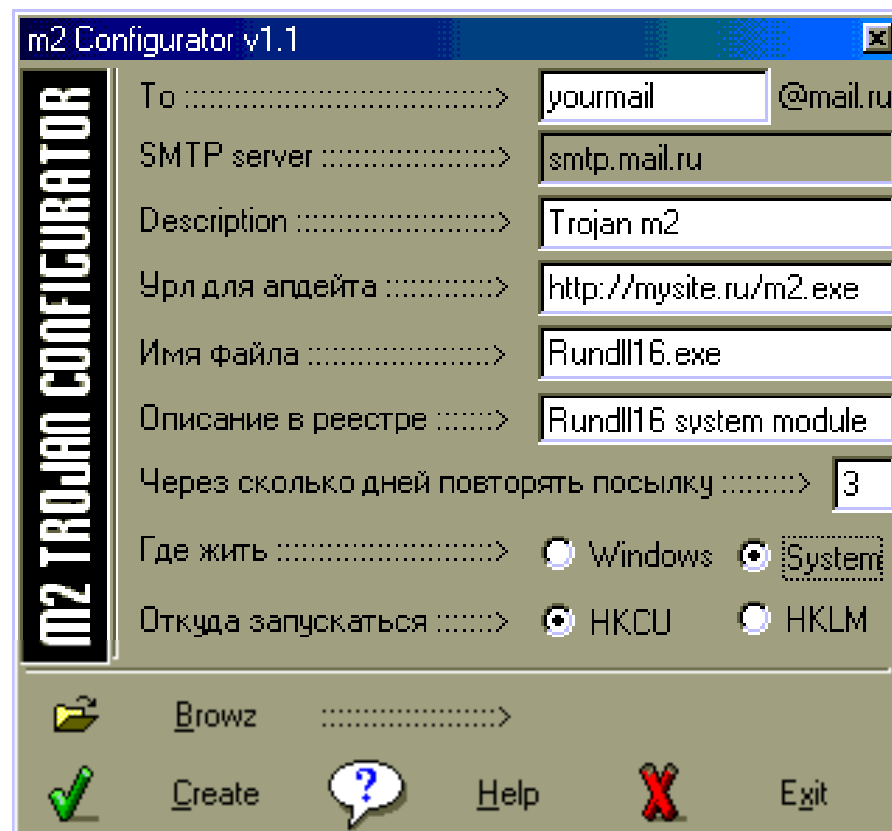
It has a program “configurer” that enables malefactors (component that controls these Trojan horses) to adjust server components according to their desire

After OS reboot, it copies itself to the %WinDir% directory, or to the directory %WinDir%\System and then it registers itself in the system registry

While running, it searches disks for files containing passwords for Windows, EDialer, and WinCommander, and also can read out a configuration for modem adjustments

It sends all collected information to a specified e-mail address in a set time interval

Trojan-PSW.Win32.M2.14.a: Screenshot



CrazyBilets is a password stealing Trojan and it spreads from a public access Web page on the narod.ru server

The web page contains:

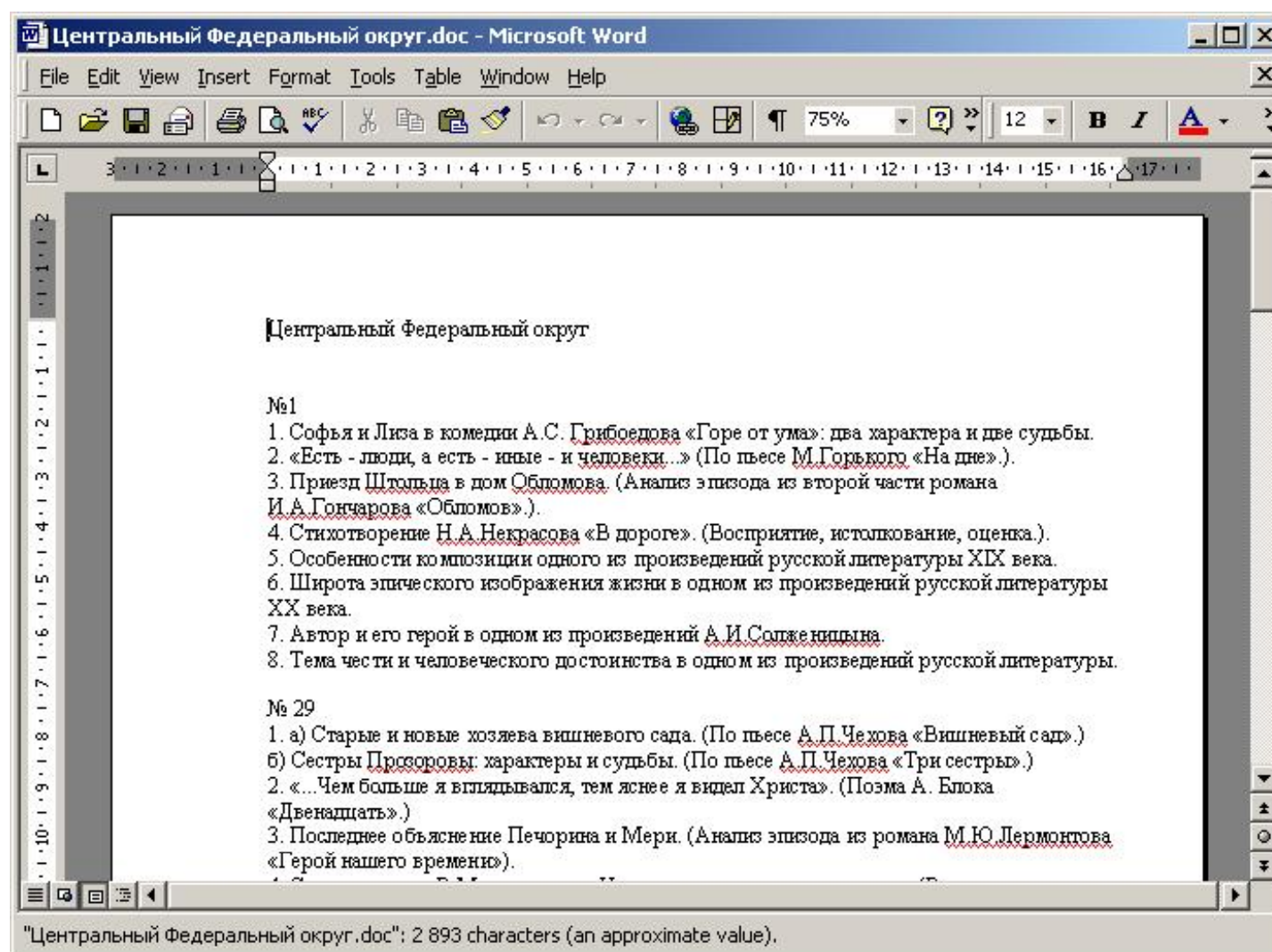
- Intermediate Examinations Test papers for mathematics and topics for compositions. Still FREE!

The file residing on the web page is a Trojan *installer*

After installing, it drops a Trojan program into the Windows directory, then extracts and creates fake examination topics

It's main purpose is to collect cached Windows passwords on victim machines and send this information to its server by direct connection to an SMTP server

CrazyBilets: Screenshot



Dipper is a Trojan which is designed to steal user passwords

This Trojan is a Windows PE EXE file

It is packed using UPX

When it runs, the user will be shown information for every remote connection in the system: user name, password, and number to be connected to



Fente Trojan is used to create other Trojan programs which steal passwords

It is a Windows PE EXE file

The user is required to enter the address where the Trojan log files should be sent

When the user clicks the left hand button, it asks by what name the Trojan which will be generated should be saved under, and then creates that Trojan

It will include the email address which was previously entered



GWGhost is a Password Stealer

Its main purpose is to capture all the masked passwords appearing on the screen

It automatically detects which window contains masked passwords, and then takes a snapshot of all text information in that window

The information will be sent to the hacker's mail-box at intervals

It can also log key strokes of applications



GWGhost: Screenshot

GWGhost v2.72 Setup

Mail Settings

Mail to: SMTP Host:

Comment: Hst.Type: ☒ SMTP ☐ MX/MTA ☐ ESMTP

Password: Confirm:

Log key strokes of the following EXEs

Misc.

Send mail every minutes

Disable in days (0=never)

☒ Log mails to ☒ Hide file

Welcome to <http://www.gwgirl.com/>

Kesk Trojan is designed to steal user passwords

It will be installed on the victim's machine by other malicious programs

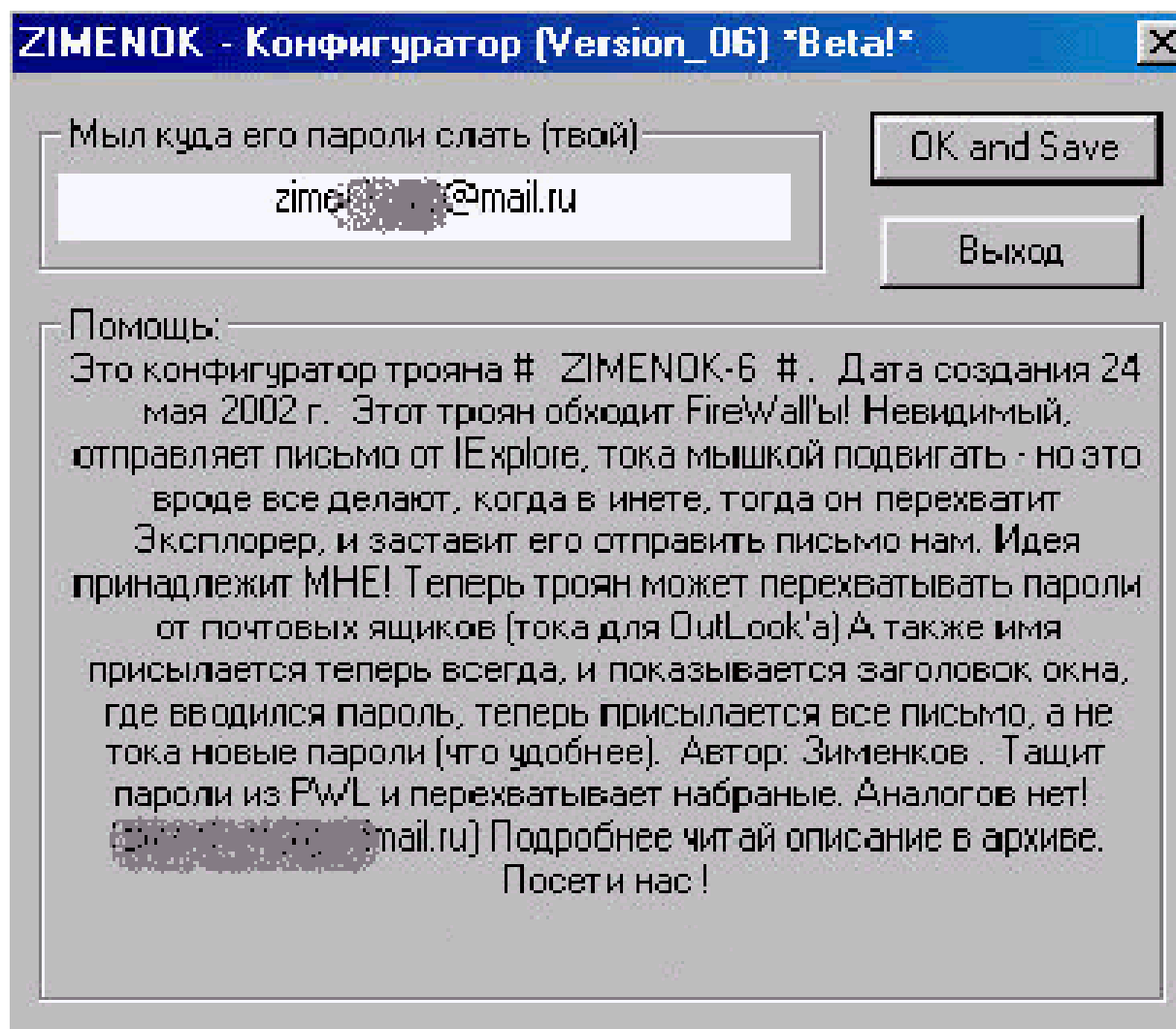
When launched, the Trojan requires the system library svrapi.dll to be present

This library contains functions for monitoring the administration of partitioned network resources

It adds the following parameters to the system registry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run] "Kernel.Tsk" = "<path to Trojan file>"

Kesk: Screenshot



MTM Recorded pwd Stealer

MTM Recorded pwd Stealer steals and sends the passwords stored on victim's computer by Internet Explorer and Outlook Express to the hacker's specified email address (must be an hotmail account)

Passwords are revealed by reading the information from the protected storage:

- Outlook Express passwords
- AutoComplete passwords in Internet Explorer
- Password-protected sites in Internet Explorer



Password Devil

Password Devil is a password stealing Trojan

It steals password from the user computer and sends it back to the server

It sends following passwords:

Outlook passwords

AutoComplete passwords in Internet Explorer

Password-protected sites in Internet Explorer

MSN Explorer Passwords

Cached Passwords (9x)



Password Devil: Screenshot

The screenshot shows the Password Devil application window with the 'SETTINGS' tab selected. The window has a title bar with a dropdown arrow, a progress bar, and standard window controls. On the left is a vertical menu with buttons: SETTINGS, FAKE ERROR, DOWNLOADER, COMPILE EXE, SMTP FINDER, and ABOUT. The main area contains the following fields and options:

- FROM: Pass Devil
- MAIL TO: Alch3mist@hotmail.com
- SMTP SERVER: mx1.hotmail.com (dropdown menu)
- ☒ SEND IE PASSES
- ☒ SEND CACHED PASSES
- ☒ MELT AFTER SEND

The screenshot shows the Password Devil application window with the 'DOWNLOAD / EXECUTE FILE' tab selected. The window has the same title bar and left menu as the previous screenshot. The main area contains the following fields and options:

- ☐ DOWNLOAD / EXECUTE FILE
- URL: http://your-site/server.exe
- SAVE AS: C:\Aut0Exec.bat



Password Stealing Tools

Password Thief

Password Thief runs hidden in the background taking note of all the passwords that have been entered

It tracks user login passwords, screen saver passwords, Internet access passwords, Microsoft Word password, or any password entered by any program

Password Thief can then show you which password was entered where



Password Thief: Screenshot



Remote Password Stealer

Remote Password Stealer is a password-logger tool to track all the password-input events in the windows system

Its purpose is to remind the forgotten-password or steal a password from a machine

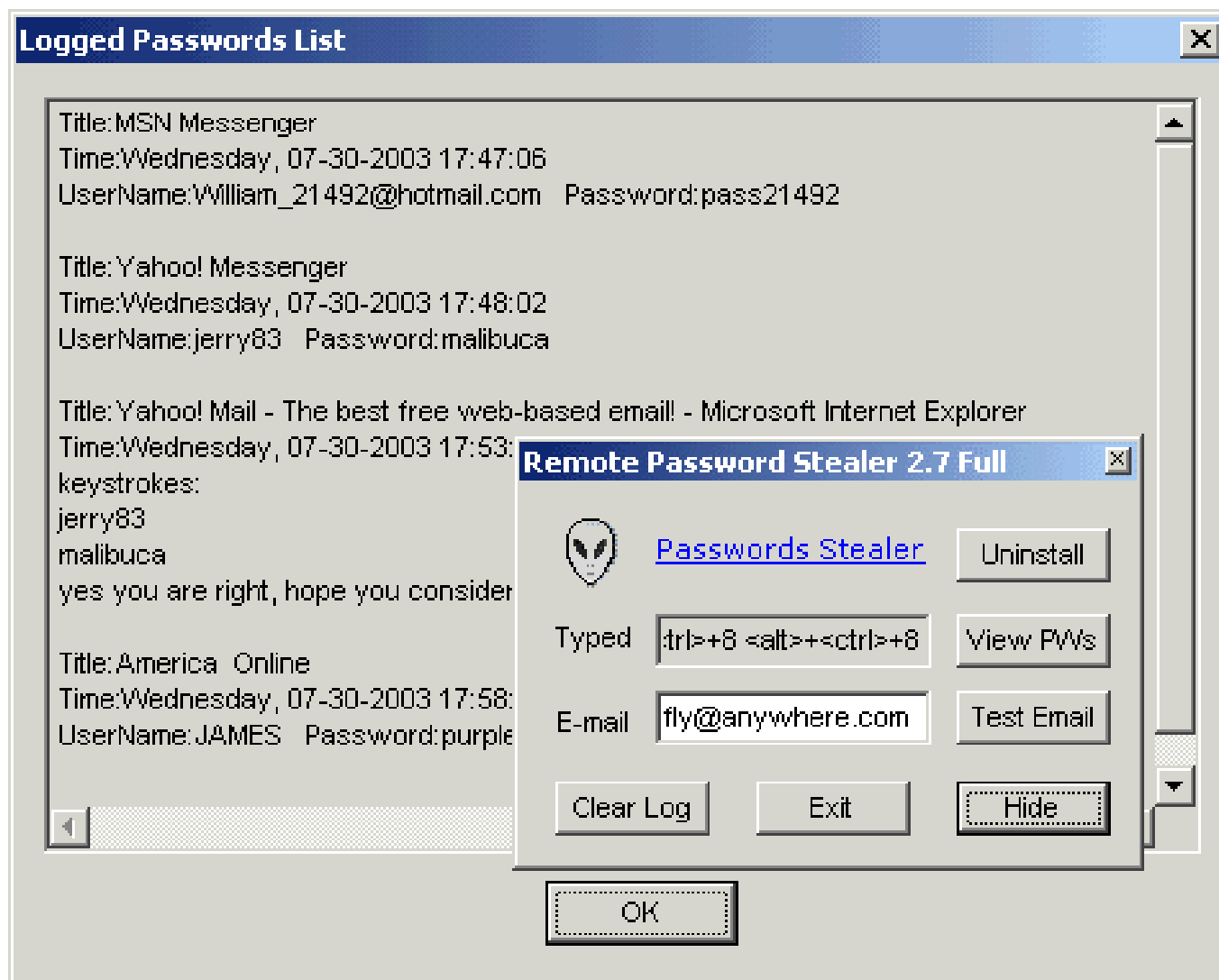
It sends the stolen passwords to hacker's e-mail address

It also steals:

- AOL password
- Yahoo password
- AIM password
- MSN password
- Email password
- FTP password
- ICQ password
- IE password
- Dial-up connection password



Remote Password Stealer: Screenshot



POP3 Email Password Finder

POP3 Email Password Finder is a tool to crack the password of an email account

It is based on dictionary-attack

By using a special dictionary, this tool can also be used for Brute-Force attack

Works with all the Windows systems to grab a POP3 email password

Features:

- Multi-threaded
- Auto-retry when connection dies
- Auto-check the result
- Username dictionary supported



POP3 Email Password Finder: Screenshot

The screenshot shows the 'POP3 Email Password Finder' application window. It features a blue title bar with standard Windows window controls. The main interface is a light yellow panel with several input fields and buttons. The 'POP3 Server' field contains 'pop.email.com'. The 'MAX Threads' is set to '1'. The 'UserName' field contains 'C:\Dictionary\UserName.txt' and the 'Password' field contains 'C:\Dictionary\Password.txt'. There are buttons for 'Username Dictionary' and 'Password Dictionary'. At the bottom, there are buttons for 'Stop', 'Help', 'Exit', and 'View Result'. A list box at the bottom displays search results, showing four entries, all with 'Result: unmatched'. The status bar at the very bottom shows 'Tasks: 5x6=30', 'Search: 9', and 'Gel: 0'.

POP3 Server:	MAX Threads:
pop.email.com	1

UserName:	Username Dictionary
C:\Dictionary\UserName.txt	

Password:	Password Dictionary
C:\Dictionary\Password.txt	

Stop

Help

Exit

View Result

Username	Password	Result
may819	password6	unmatched
geil	password1	unmatched
geil	password2	unmatched
geil	password3	unmatched

Tasks: 5x6=30 Search: 9 Gel: 0

Instant Password Finder

Instant Password Finder checks a system for possible passwords, and shows you the passwords immediately

When Windows system runs, Instant Password Finder reads the private data in current system, and extracts the username/password information for you

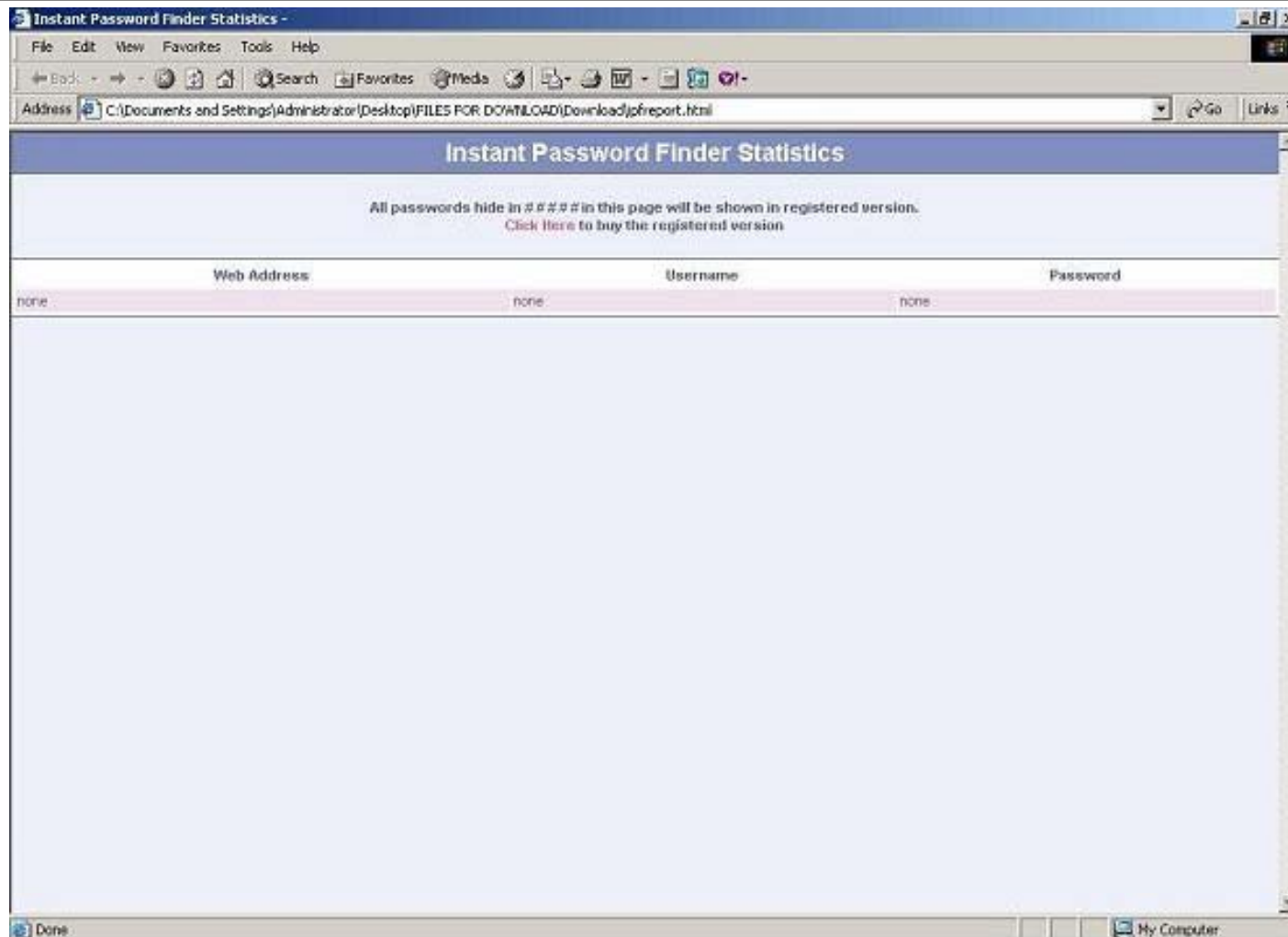
It allows you to find out hidden passwords in Windows-based system

It finds the following passwords:

- MSN Messenger password
- Windows Live Messenger password
- Hotmail password
- Yahoo password
- Outlook password
- AutoComplete passwords
- Web Site logons
- Dial-up password



Instant Password Finder: Screenshot



MessenPass is a password recovery tool

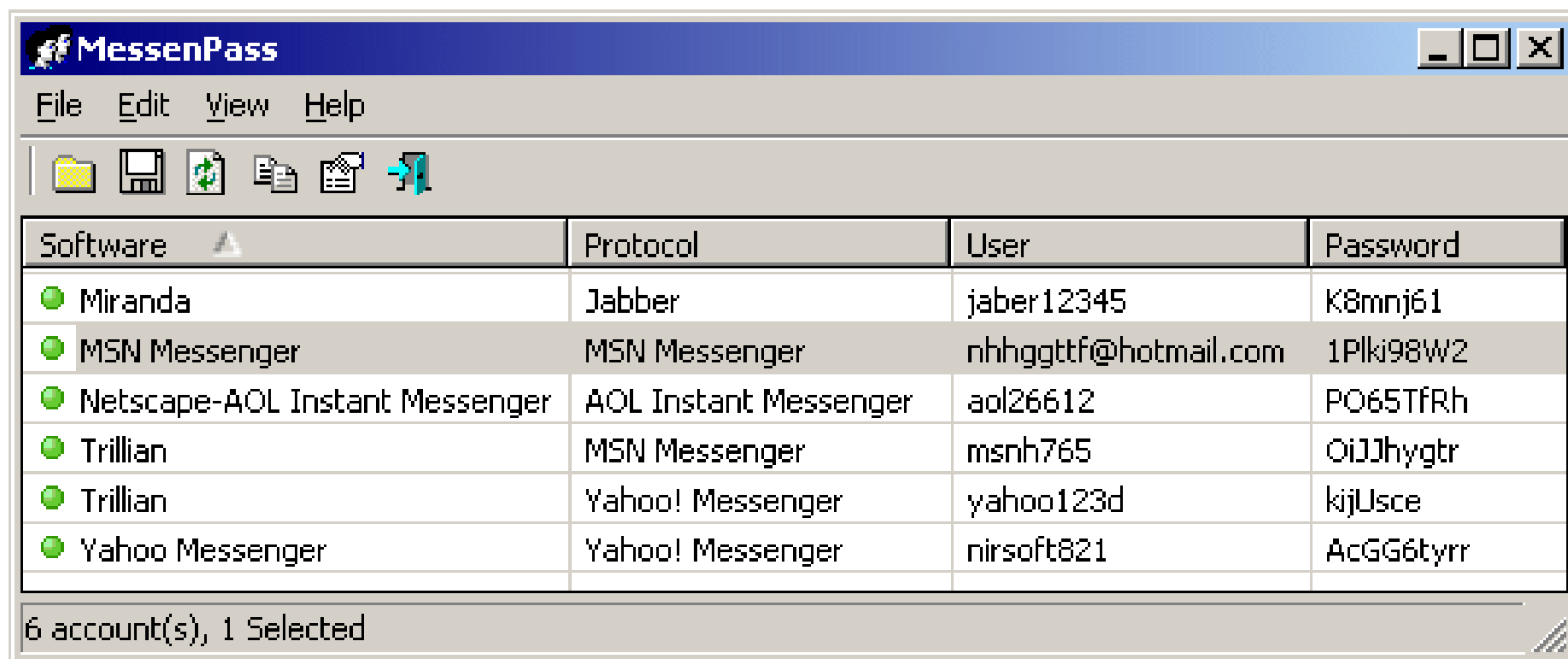
It is only used to recover the passwords for the current logged-on user on local computer

It only works if you chose to remember your password option

It reveals the password from:

- MSN Messenger
- Windows Messenger (In Windows XP)
- Windows Live Messenger (In Windows XP And Vista)
- Yahoo Messenger (Versions 5.x and 6.x)
- Google Talk
- ICQ Lite 4.x/5.x/2003
- AOL Instant Messenger v4.6 or below, AIM 6.x, and AIM Pro.
- Trillian
- Miranda

MessenPass: Screenshot



PstPassword is a small utility that recovers lost password of Outlook

It is not necessary to install MS-Outlook in your system to use this utility

It needs only the original PST file that you locked with a password

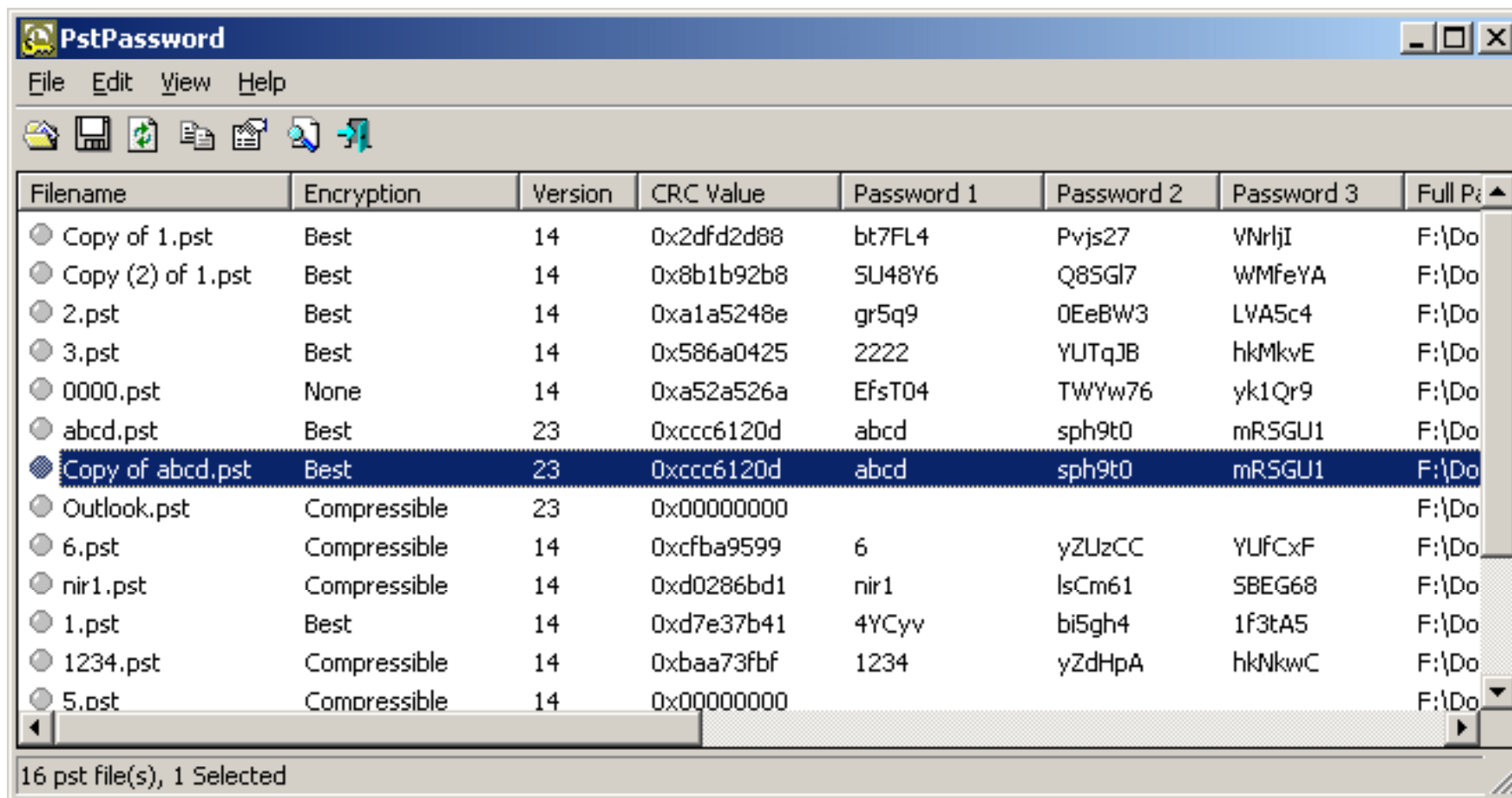
It can recover:

PST passwords of Outlook 97

Outlook 2000/XP/2003/2007



PstPassword: Screenshot



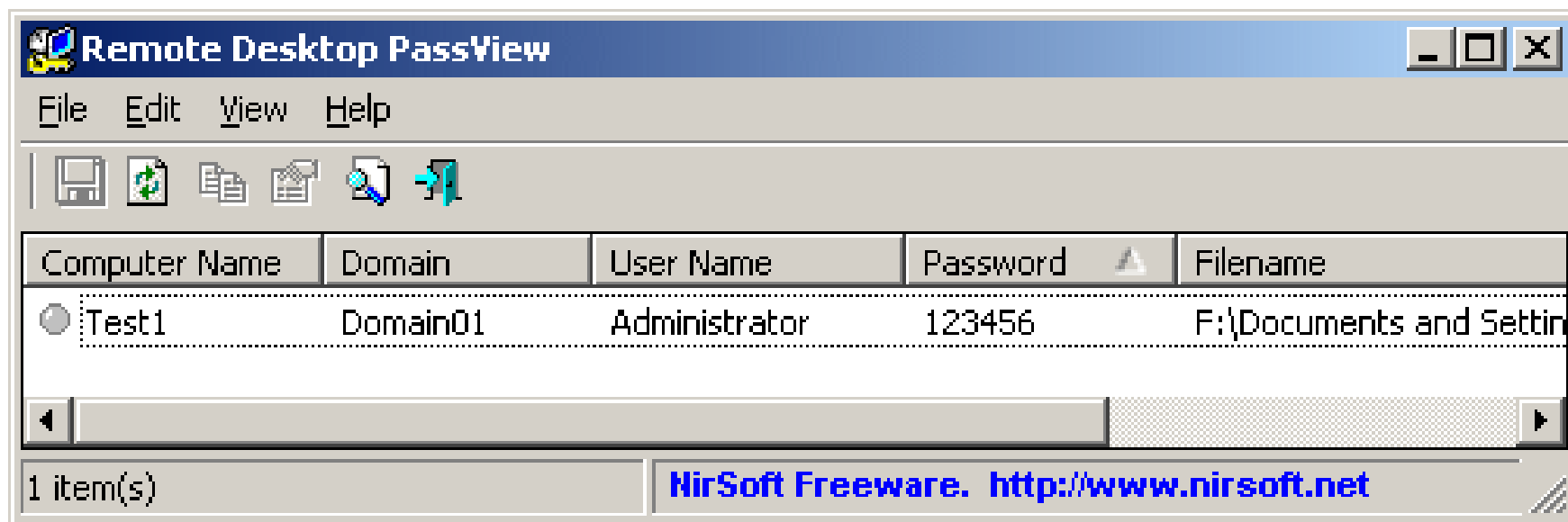
The screenshot shows the PstPassword application window. The title bar reads 'PstPassword'. The menu bar includes 'File', 'Edit', 'View', and 'Help'. Below the menu bar is a toolbar with icons for file operations. The main area is a table with the following columns: 'Filename', 'Encryption', 'Version', 'CRC Value', 'Password 1', 'Password 2', 'Password 3', and 'Full Path'. The table lists 16 PST files. The file 'Copy of abcd.pst' is selected, highlighted in blue. The status bar at the bottom indicates '16 pst file(s), 1 Selected'.

Filename	Encryption	Version	CRC Value	Password 1	Password 2	Password 3	Full Path
Copy of 1.pst	Best	14	0x2dfd2d88	bt7FL4	Pvjs27	VNrljI	F:\Do
Copy (2) of 1.pst	Best	14	0x8b1b92b8	SU48Y6	Q85GL7	WMfeYA	F:\Do
2.pst	Best	14	0xa1a5248e	gr5q9	0EeBW3	LVA5c4	F:\Do
3.pst	Best	14	0x586a0425	2222	YUTqJB	hkMkvE	F:\Do
0000.pst	None	14	0xa52a526a	EfsT04	TWYw76	yk1Qr9	F:\Do
abcd.pst	Best	23	0xccc6120d	abcd	sph9t0	mR5GU1	F:\Do
Copy of abcd.pst	Best	23	0xccc6120d	abcd	sph9t0	mR5GU1	F:\Do
Outlook.pst	Compressible	23	0x00000000				F:\Do
6.pst	Compressible	14	0xcfb9599	6	yZUzCC	YUfCxP	F:\Do
nir1.pst	Compressible	14	0xd0286bd1	nir1	lsCm61	SBEG68	F:\Do
1.pst	Best	14	0xd7e37b41	4YCyv	bi5gh4	1f3tA5	F:\Do
1234.pst	Compressible	14	0xbaa73fbf	1234	yZdHpA	hkNkwC	F:\Do
5.pst	Compressible	14	0x00000000				F:\Do

16 pst file(s), 1 Selected

Remote Desktop PassView

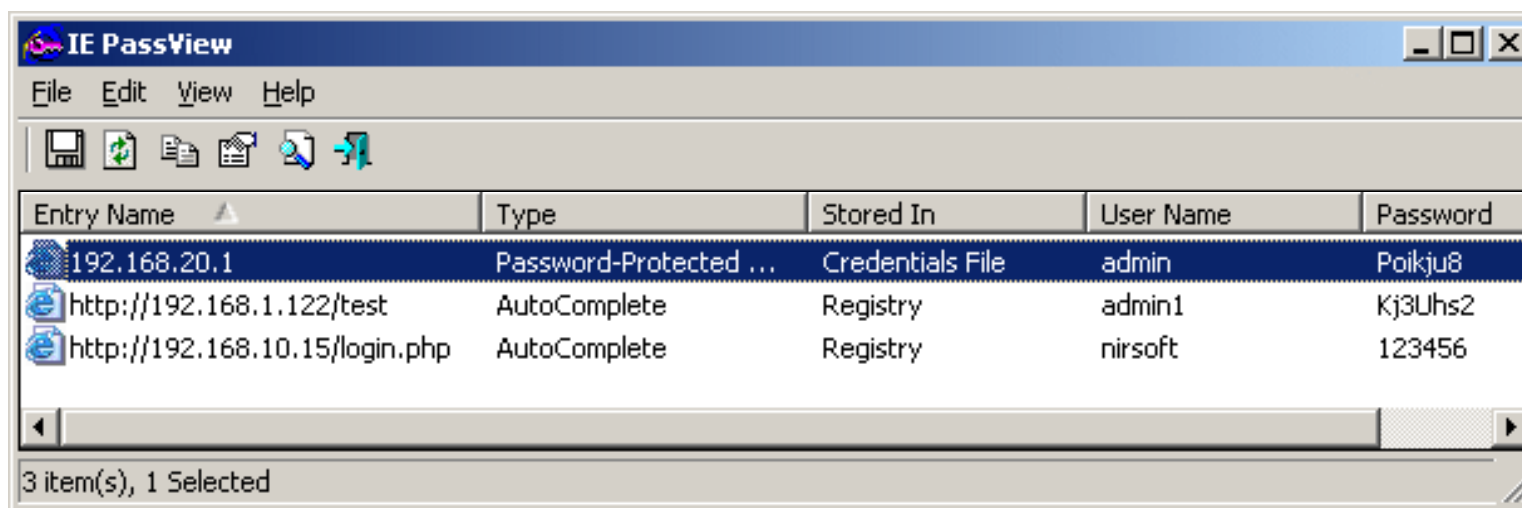
Remote Desktop PassView is a small utility that reveals the password stored by Microsoft Remote Desktop Connection utility inside the .rdp files



IE PassView is a small utility that reveals the passwords stored by Internet Explorer browser

It can recover the following passwords:

- AutoComplete Passwords
- HTTP Authentication Passwords
- FTP Passwords



Yahoo Messenger Password

Yahoo Messenger Password is a password recovery tool

It is used to recover lost or forgotten passwords for Yahoo messenger accounts

It stores login information for the current computer user

It is also used to transfer the saved password to another computer



Yahoo Messenger Password: Screenshot





Countermeasures

Recommendations for Improving Password Security

Use a strong password for root and administrator accounts

Stop unrequired and buggy services, and services not protected by a well-configured firewall

Create a schedule to change the password periodically

Use strong encryption algorithms to encrypt the password storage files such as SAM (Security Account Manager) and passwd.conf file

Use a filter that operates in real time and enforces some level of length and complexity on the passwords

Run a cracker periodically on your own password files and if it works then change the password

Best Practices

Do not use:

- Your account name or any data that appears in your record as a password
- Any word or name that appears in any dictionary
- Phrases and slang with or without space
- Alphabetic, numeric ,or keyboard sequences
- Titles of books, movies, poems, essays, songs, CDs ,or musical compositions
- Any personal information

Use the following for strong password:

- Use at least 8 characters
- Include a digit or punctuation
- Use upper and lower case separated by a non-letter non-digit
- Use different passwords on different machines
- Change password regularly and do not reuse passwords or make minor variations such as incrementing a digit

A password is the first line of defense to systems and personal information

Password Stealing is used by the hackers to exploit user credentials

Phishing is an Internet scam where the user is convinced to give valuable information

Spying refers to continuously observing a person's activities and his/her work

A Password Stealer is software that secretly captures passwords from the computer

Run a cracker periodically on your own password files and if it works then change the password

Copyright 2002 by Randy Glasbergen. www.glasbergen.com



**"I know a lot of highly-confidential company secrets,
so my boss made me get a firewall installed."**

Copyright 2004 by Randy Glasbergen.
www.glasbergen.com



**“The boss is worried about information security,
so he sends his messages one alphabet letter
at a time in random sequence.”**