

Forum:[Hack Forums](#)

Thread: [Locations Of All Saved Password In Computer](#)

supersurfer - December 11, 2010, 9:44 pm

All Saved Password Locations.

NOTE: I know this is ripped/leeches, but I really thought this forum could use this type of information.

Quote: Credits to <http://leetcoders.org/showthread.php?tid=1668>

Google Chrome:

Chrome Passwords are stored in a SQLite file the sites name and sites username is in clear text but the password is seeded in a Triple DES algorithm. The file is called Web Data and is stored in the following location

XP - C:\Documents and Settings\Username\Local Settings\Application Data\Google\Chrome\User Data\Default

Vista - C:\Users\Username\AppData\Local\Google\Chrome\User Data\Default

Trillian:

Note- I have just realised the new version of trillian the passwords made be stored/encrypted differently

Trillian Passwords are stored in .ini files the first character of the password is encrypted with XOR with the key 243 then the password is converted into hex. The file is based on what the password is for so if it was icq it would be icq.ini (for new versions I think they are all stored in a file called accounts.ini or something similar if you open it up with notepad you will see all the data + the encrypted password). The files are stored in the following location:

XP (old version) - C:\Program Files\Trillian\users\

XP (new version) - C:\Documents and Settings\Username\Local Settings\Application Data\Trillian\user\global - I am not sure on exact but it is somewhere their

Vista (old version)- C:\Program Files\Trillian\users\

Vista (new version)- C:\Users\Username\AppData\Roaming\Trillian\user\global

MSN /Windows Live Messenger:

MSN Messenger version 7.x: The passwords are stored under
HKEY_CURRENT_USER\Software\Microsoft\IdentityCRL\Creds\[Account Name]

Windows Live Messenger version 8.x/9.x: The passwords are stored in the Credentials file, with entry name begins with "WindowsLive:name=". They a set of Win API functions (Credential API's) to store its' security data (Credentials). These functions store user information, such as names and passwords for the accounts (Windows Live ID credentials). Windows Live ID Credential records are controlled by the operating system for each user and for each session. They are attached to the "target name" and "type". If you are familiar with SQL you can think of target name and type as the primary key. Table below lists most frequently used fields in Windows Live ID Credential records.

Paltalk:

Paltalk Passwords are using the same password encryption algorithm. Paltalk passwords are stored in the registry. To encrypt the new password Paltalk looks at the serial number of the disk C:\ and performs a mix with the Nickname. The resulting string is then mixed again with the password and some other constants. The final string is then encoded and written to the registry.

AIM, ICQ and Yahoo Messenger passwords that are stored by Paltalk are encoded by BASE64 algorithm.

The passwords are stored in the Registry, under
HKEY_CURRENT_USER\Software\Paltalk\[Account Name]

Google Talk:

Google Talk passwords are encoded/decoded using Crypto API. Encrypted Gmail passwords are stored by Google Talk in the registry under HKEY_CURRENT_USER\Software\Google\Google Talk\Accounts\[Account Name]

Firefox:

The passwords are stored in one of the following filenames: signons.txt, signons2.txt, and signons3.txt (depends on Firefox version)

These password files are located inside the profile folder of Firefox, in [Windows Profile]\Application Data\Mozilla\Firefox\Profiles\[Profile Name]

Also, key3.db, located in the same folder, is used for encryption/decription of the passwords.

Yahoo Messenger 6.x:

The password is stored in the Registry, under HKEY_CURRENT_USER\Software\Yahoo\Pager ("EOptions string" value)

Yahoo Messenger 7.5 or later:

The password is stored in the Registry, under HKEY_CURRENT_USER\Software\Yahoo\Pager – "ETS" value.

The value stored in "ETS" value cannot be recovered back to the original password.

AIM:

AIM uses Blowfish and base64 algorithms to encrypt the AIM passwords.

448-bit keyword is used to encrypt the password with Blowfish. The encrypted string is then encoded using base64. The passwords are stored in the Registry, under
HKEY_CURRENT_USER\Software\America Online\AIM6\Passwords

No Ip (easy to make in vb.net):

Passwords encoded with Base64 you can find the account information in the following locations

HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks\DUC\", "Password"
HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerk\SDUC\", "Checked"
HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks\DUC\", "Username"
KEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks\DUC\", "ProxyUsername"
HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks\DUC\", "ProxyPassword"
HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks\DUC\", "Hosts"

Filezilla:

Passwords are stored in a .xml file located in Filezilla on appdata their is sources for this

Internet Explorer 4.00 – 6.00:

The passwords are stored in a secret location in the Registry known as the "Protected Storage".

The base key of the Protected Storage is located under the following key:

"HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider".

You can browse the above key in the Registry Editor (RegEdit), but you won't be able to watch the passwords, because they are encrypted.

Also, this key cannot easily moved from one computer to another, like you do with regular Registry keys.

Internet Explorer 7.00 – 8.00:

The new versions of Internet Explorer stores the passwords in 2 different locations.

AutoComplete passwords are stored in the Registry under

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2.

HTTP Authentication passwords are stored in the Credentials file under Documents and Settings\Application Data\Microsoft\Credentials , together with login passwords of LAN computers and other passwords.

Opera:

The passwords are stored in wand.dat filename, located under [Windows Profile]\Application Data\Opera\Opera\profile

Outlook Express (All Versions):

The POP3/SMTP/IMAP passwords Outlook Express are also stored in the Protected Storage, like the passwords of old versions of Internet Explorer.

Outlook 98/2000:

Old versions of Outlook stored the POP3/SMTP/IMAP passwords in the Protected Storage, like the passwords of old versions of Internet Explorer.

Outlook 2002-2008:

All new versions of Outlook store the passwords in the same Registry key of the account settings.

The accounts are stored in the Registry under HKEY_CURRENT_USER\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\[Profile Name]\9375CFF0413111d3B88A00104B2A6676\[Account Index]

If you use Outlook to connect an account on Exchange server, the password is stored in the Credentials file, together with login passwords of LAN computers.

ThunderBird:

The password file is located under [Windows Profile]\Application Data\Thunderbird\Profiles\[Profile Name]

You should search a filename with .s extension.

Digsby:

The main password of Digsby is stored in [Windows Profile]\Application Data\Digsby\digsby.dat

All other passwords are stored in Digsby servers.

Well thats all the one's i no of, if you have any feel free to post them

??h™ - December 11, 2010, 9:56 pm

Nice share. This will help people coding stealers. :)

MoonWoLF - December 12, 2010, 12:25 am

Thanks for this Supersufer. It will help a lot of Vb Coders ...

supersurfer - December 12, 2010, 1:01 am

yeh.. but since am a RATER.. and can edit registry in vic pc.. its too helpful for me..

Fallenbot - December 12, 2010, 1:35 am

Already posted mate. Please use the search button next time,thank you.

adampelletgun - December 12, 2010, 1:45 am

Not really a hacking tool

But looks interesting

Thanks for the post

Not really a hacking tool

But looks interesting

Thanks for the post

Em re - December 12, 2010, 2:15 am

Nice detailed tutorial mate.

Thanks. /

Maxie - December 12, 2010, 2:24 am

Bookmarked :D. Really useful mate :).

supersurfer - December 12, 2010, 9:29 am

thanks everyone.. i didn't found this.. thats why posted..

The Unknown - December 12, 2010, 9:52 am

awesome man , now we can code an iStealer , great job , 10x

Siltho - December 12, 2010, 9:59 am

Files not found on Firefox 4.0 Beta 6, only signons.sqlite, which I am too lazy to open myself.

supersurfer - December 12, 2010, 10:49 pm

(Dec 12, 2010 10:59 AM)Siltho Wrote: [\[CITE\]](#) Files not found on Firefox 4.0 Beta 6, only signons.sqlite, which I am too lazy to open myself.

try opening this file with NotePad++ you can find the site and UN and Pass but the UN and pass are encrypted..

sheikh_shahzeb - December 13, 2010, 1:01 am

cool sharing

sharing is caring :)

SIM-135152 - December 13, 2010, 1:06 am

thanks for this great share this will more people and me too

i bookmarked

thanks

Damion774 - December 13, 2010, 4:38 am

Perfect for Stealing :) Well done :D

Codeine - *December 13, 2010, 5:15 am*

Already knew a few of these, but thanks for sharing the rest.

MCart - *December 13, 2010, 6:13 am*

Thanks for this post. It will help me to code a stealer. :)