

Forum: [Hack Forums](#)

Thread: [Has anyone ever programmatically accessed stored RDP windows credentials](#)

CantPackCuba - April 5, 2024, 10:46 am

Just wondering if this is even possible.

using AdysTech.CredentialManager Nuget Package i can retrieve username. Although the 2 values Password and SecurePassword seem to be blank

```
Code static void Main(string[] args)
{
    var credentials = CredentialManager.EnumerateCredentials();

    foreach (var cred in credentials)
    {
        if (cred.UserName.Contains("Administrator"))
        {
            Debug.WriteLine(cred.UserName);
            Debug.WriteLine(cred.Password);
            Debug.WriteLine(GetSecureStringAsString(cred.SecurePassword));
        }
    }

    Console.ReadLine();
}

static string GetSecureStringAsString(SecureString secureString)
{
    if (secureString == null)
        return string.Empty;

    IntPtr ptr = IntPtr.Zero;
    try
    {
        ptr =
System.Runtime.InteropServices.Marshal.SecureStringToGlobalAllocUnicode(secureString);
        return System.Runtime.InteropServices.Marshal.PtrToStringUni(ptr);
    }
    finally
    {
        System.Runtime.InteropServices.Marshal.ZeroFreeGlobalAllocUnicode(ptr);
    }
}
```

If this is possible it would make for a good stealer, Values such as ip/hostname could be found via registry :

HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default

SheldIO - April 6, 2024, 3:31 am

The password is stored in an encrypted form. The encryption method is DPAPI. Use CryptUnprotectData to decrypt.

CantPackCuba - April 6, 2024, 9:53 am

(Apr 6, 2024 03:31 AM)SheldIO Wrote: [\[CITE\]](#) The password is stored in an encrypted form. The encryption method is DPAPI. Use CryptUnprotectData to decrypt.

I have tried :(I think there is more at play here.

The only stealers i have came across that achieve this idea are injecting into mstsc.exe

SheldIO - April 6, 2024, 10:22 am

(Apr 6, 2024 09:53 AM)CantPackCuba Wrote: [\[CITE\]](#) I have tried :(I think there is more at play here.

The only stealers i have came across that achieve this idea are injecting into mstsc.exe

<https://github.com/twelvesec/passcat/blob/b446c982cf6e85fdbfedc8e953104e7302ceab01/passcat/libpasscat.cpp#L334>

You're making it too complicated))
use windows credentials

CantPackCuba - April 7, 2024, 4:53 am

(Apr 6, 2024 10:22 AM)SheldIO Wrote: [\[CITE\]](#)

<https://github.com/twelvesec/passcat/blob/b446c982cf6e85fdbfedc8e953104e7302ceab01/passcat/libpasscat.cpp#L334>

You're making it too complicated))
use windows credentials

Seems this only retrieves the generic credentials and not TERMSRV credentials, I will look through this project though thank you

```
edit : i changed this if statement in libpasscat::cat_credmanager_passwords from:
if (credentials[i]->UserName != NULL && (credentials[i]->Type == CRED_TYPE_GENERIC ||
credentials[i]->Type == CRED_TYPE_DOMAIN_VISIBLE_PASSWORD)) {
to:
if (credentials[i]->UserName != NULL || credentials[i]->Type ==
CRED_TYPE_DOMAIN_VISIBLE_PASSWORD) {
```

it now displays the TERMSRV credentials but does not seem to fetch a password. Probably because the project is from 2018

PulseLink - April 9, 2024, 11:11 am

theres some metasploit modules that can be automated using db_nmap as well as wmap -sites and then scan for vulns on a whole subnet with wmap and db_nmap.

Then use the modules given to you by vulners etc to actually exploit them. It works well scanning popular hosting subnets.