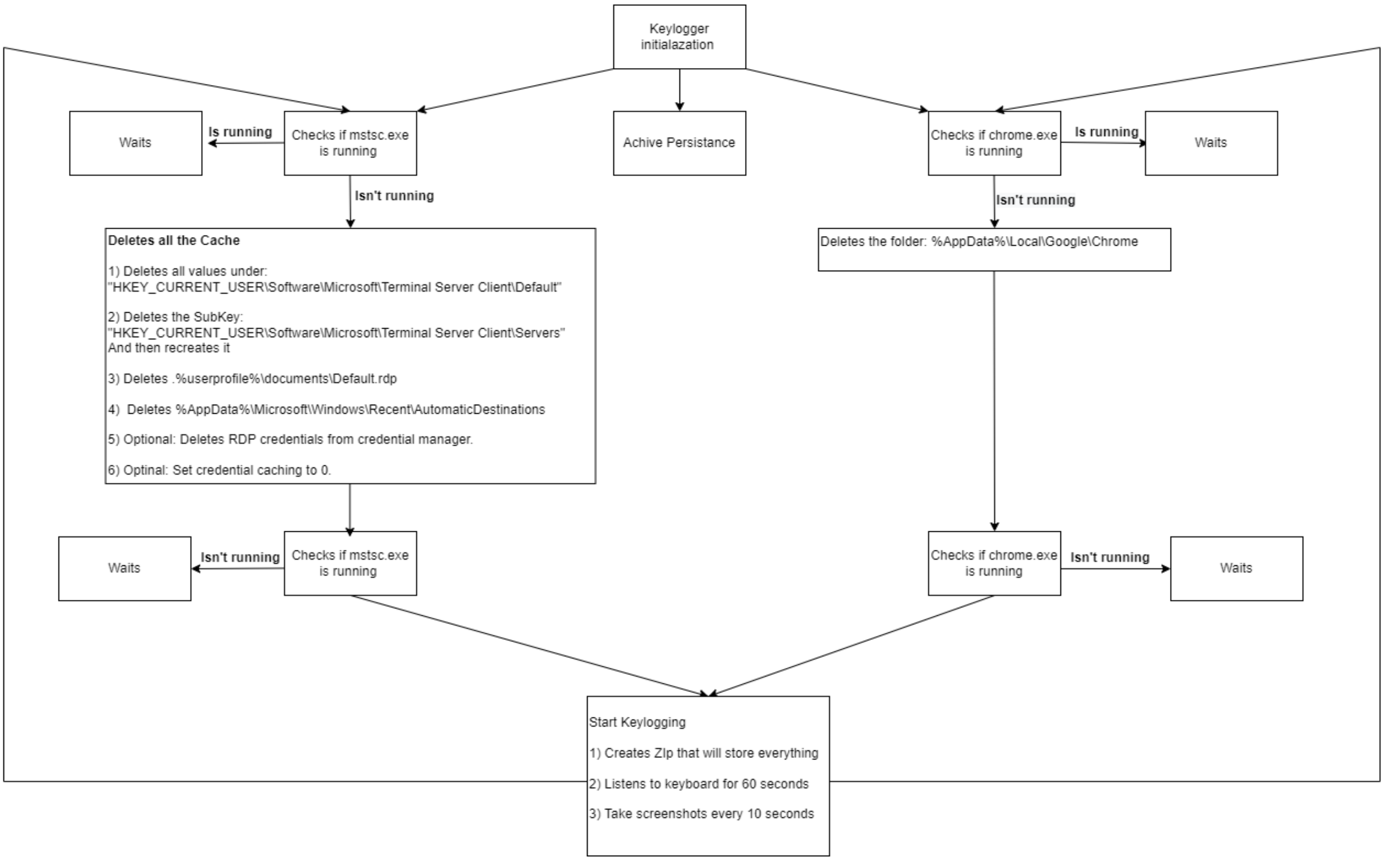
S&S Keylogger

Creating a simple keylogger with python can be done with 5 lines of code….
But creating a **S**mart **&** **S**tealthy keylogger that can almost guarantee you passwords with little to none un-needed characters, is a whole different ball game.

The S&S Keylogger provides the attacker with a Zip file that holds screenshots and .txt files containing keyboard inputs of key moments. The files are named after the time and date they were created, thus the attacker can build a timeline.
On top of that, it achieves persistence and creates no child processes.

S&S Keylogger workflow (on a high level):

[+] The malware first takes persistence, then the circular behavior begins.
[+] After achieving a foothold in the system, it checks if the chrome or RDP processes are running. If one of them is not in use, the Keylogger will delete its cache so the user will have to authenticate next time.
[+] Now the malware will monitor the running processes. The moment chrome.exe or mstsc.exe are executed the Keylogger will start listening to the keyboard inputs and will take screenshots.
[+] The keyboard inputs and the screenshots file names, will be saved as the time they were taken, so the attacker can access the needed .txt files after looking at the corresponding .png files
[+] all the .txt and .png files will be moved to a zip file.



Deletes all the Cache

1) Deletes all values under:
"HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default"

2) Deletes the SubKey:
"HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
And then recreates it

3) Deletes .%userprofile%\documents\Default.rdp

4) Deletes %AppData%\Microsoft\Windows\Recent\AutomaticDestinations

5) Optional: Deletes RDP credentials from credential manager.

6) Optinal: Set credential caching to 0.

Deletes the folder: %AppData%\Local\Google\Chrome

Start Keylogging

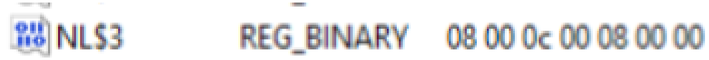
1) Creates Zip that will store everything

2) Listens to keyboard for 60 seconds

3) Take screenshots every 10 seconds

Deleting the RDP cache and credentials:
Clearing the RDP cache and saved credentials is a 4 step process with an optional 5th and 6th, which are commented out with a small explanation in the script.

Step 1 (optional) – Disabling credential caching.
Windows can cache up to 50 credentials locally, for local and remote authentication. These will be used if the machine is part of a domain and can't access the DC.
The cached credentials are encrypted and saved in base 16 format as registry data of the registry value's NL$x under the registry subkey HKEY_LOCAL_MACHINE\Security\Cache



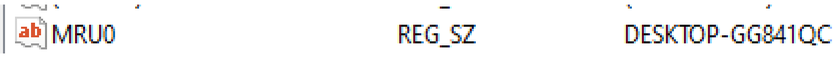
NL$3 REG_BINARY 08 00 0c 00 08 00 00

Why caching credentials is so dangerous? Mimikatz and other attack tools often target this registry key to retrieve the cached encrypted passwords and crack them offline.
How come this part is optional? First, it's unlikely that the machine won't be able to access the AD exactly when the keylogger is running and exactly when user tries use RDP. But the real reason is because of a widely used GPO.
Microsoft best practices are to set the GPO Interactive Logon: Number of previous logons to cache to 0.
This changes the data of the value CachedLogonsCount under the subkey HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon to 0, thus disables credential caching.

Step 2 (optional) – Deleting the saved credentials.
First, lets understand the flow.
When using RDP a user may check the option of Remember Me which will store the credentials for the future.
Those credentials are saved in the credential manager, and will automatically be used next time.
So how come that the only part that refers to saved credentials as a whole is optional? Well, in Domain environments IT usually enables the following GPO as best practice:

Network access: Do not allow storage of passwords and credentials for network authentication
Which disables saving credentials for all network based authentications in the credential manager.

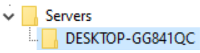
Step 3 – Clearing the values under "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default"
This key is used to cache the identity of the last 10 destinations machines that were accessed by this asset with RDP.
The values under this key are named MRU{number}, when MRU0 is the latest connection and MRU9 is the oldest one.
The MRU values hold a string type (REG_SZ) registry data which can contain one of 3 parameters that represent the destination machine: IP, FQDN, Hostname.



MRU0 REG_SZ DESKTOP-GG841QC

We must delete all the MRU values.

Step 4 - Deleting and recreating the "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers".
The \Servers key contains a subkey, for each destination machine our asset accessed with RDP ever.
The subkey is called after the IP/Hostame of the destination host.

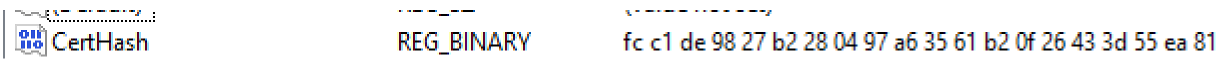


Servers
DESKTOP-GG841QC

This subkey will contain 2-3 values.
The default "(Default)" value will be empty
Then "UsernameHint" will contain the username we used to access the destination machine.

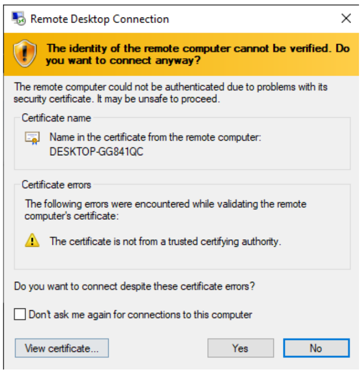
UsernameHint REG_SZ aaa

When the system auto-fills the username in the RDP box it may take the value from here .
Another important value that it may contain is the CertHash.
This value contains the RDP server SSL certificate thumbprint.



```
CertHash                REG_BINARY        fc c1 de 98 27 b2 28 04 97 a6 35 61 b2 0f 26 43 3d 55 ea 81
```

Important to know that this value will only be created if the user checks the "Don’t aske me for…" check box



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
DESKTOP-GG841QC

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

⚠ The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

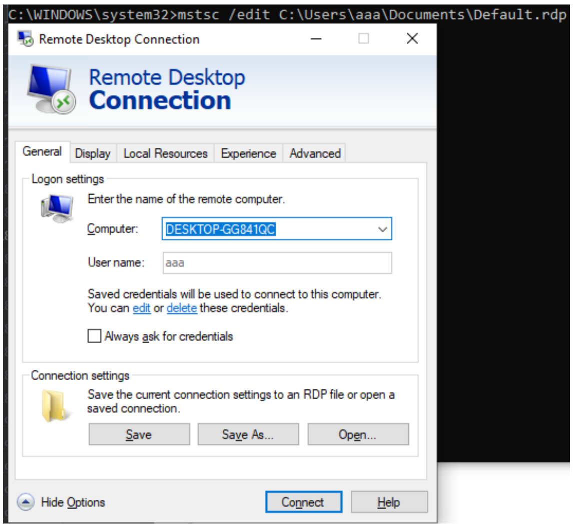
□ Don't ask me again for connections to this computer

Step 5 – deleting the Default.rdp file.

Under the documents folder there is a hidden file called "Default.rdp". This file is called " Connection File" by Microsoft.

The file contains ALL the settings of your latest RDP session and is the first place mstsc.exe goes when is executed.

We can see a proof for what exactly this file is in the bellow screenshot



```
C:\WINDOWS\system32>mstsc /edit C:\Users\aaa\Documents\Default.rdp
```

Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: DESKTOP-GG841QC

User name: aaa

Saved credentials will be used to connect to this computer. You can edit or delete these credentials.

□ Always ask for credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

If you have never made an RDP connection, this file will still be there but with a size of 0KB.

Step 6 – Deleting the jump lists.

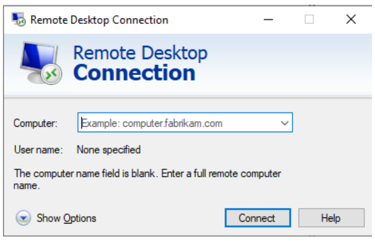
This part is the least important one as it isn't crucial for deleting the Cache or credentials, but just deletes some visual entrees… On top of that, this doesn't always work as the machine may recreate some lines of the jump list immediately after the deletion. This part can be deleted from the code if wanted.

In Windows 7, Microsoft introduced the Jump list feature. The Jump List allows you to right-click an application icon pinned to your taskbar and quickly access recent, pinned, or frequently-accessed files or in our case recent connections. Windows creates AUTOMATICDESTINATIONS-MS files when you use certain apps. These files contain information, that allows the system to open items from an application's Jump List. For example, if you use Microsoft Word to create and save a new Word document, Windows may create an AUTOMATICDESTINATIONS-MS file that is used to show the new document in the Recent section of Word's Jump List.

AUTOMATICDESTINATIONS-MS files are stored in a hidden folder
"Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations"
which I was able to find only using "Everything search tool".

Deleting this folder may delete the GUI entrees that represent RDP history.

If all of the above steps above are done, next time the user will try to access the remote machine via RDP he will face



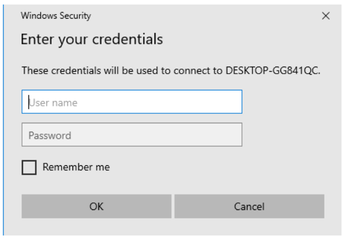
Remote Desktop Connection

Remote Desktop
Connection

Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.



Windows Security

Enter your credentials

These credentials will be used to connect to DESKTOP-GG841QC.

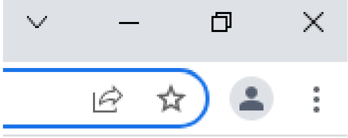
User name

Password

□ Remember me

while we are logging and screenshotting every move.

Deleting chrome cache and credentials:
This is a much easier task as it only requires one folder deletion.
Once we see that no chrome.exe process is running, we will delete AppData\Local\Google\Chrome.
This folder holds ALL the credentials, cache, etc' of our user in chrome. Next time the user will open chrome he won't be signed



and he will have to type his credentials when accessing everything.

Persistence:
The persistence is a scheduled task with a name which I saw numerous times on a wide variety of customers at my job as a SOC Tier-3 Analyst.

I've decided to let the attacker choose how he wants to get the Zip file, and didn't add this part to the code.
My advice is with one of: the socket library, SFTP server, SMTP library as port 25 will always be available.