fakelogonscreen

CSEC 471
By Mehul Sen

description

Created by Arris Huijgen @bitsadmin

Current Version 1.1, Last Updated 02/03/2020

Built using .NET framework which is installed by default in Windows 8, 8.1 and 10.

This tool takes advantage of the normal behavior of a Windows Lock Screen feature to phish out the victim's password.

Two Executables :

FakeLogonScreen.exe – write output to console (used for remote execution)

FakeLogonScreenToFile.exe – writes output to console as well as %LocalAppData%\Microsoft\user.db

installation and execution

1. Go to the github releases page for this tool: bitsadmin/fakelogonscreen
2. Download fakelogonscreen_trunk.zip(73.2 KB) file.
3. Unzip the tool, to get the executables.

Note: Window's Defender flags the zip file because it detects MSIL/Deismos.A!MTB. So, disabling Window's Defender or allowing the threat is required.

- The executable displays a lock screen when run, forcing the victim to enter the correct credentials to get access back to their machine.
- Validates the password against Active Directory or the local machine.
- The credentials are then saved locally or sent to a remote machine.

Note: Since, the executable is not verified, Windows also shows a warning on running the executable locally.

features

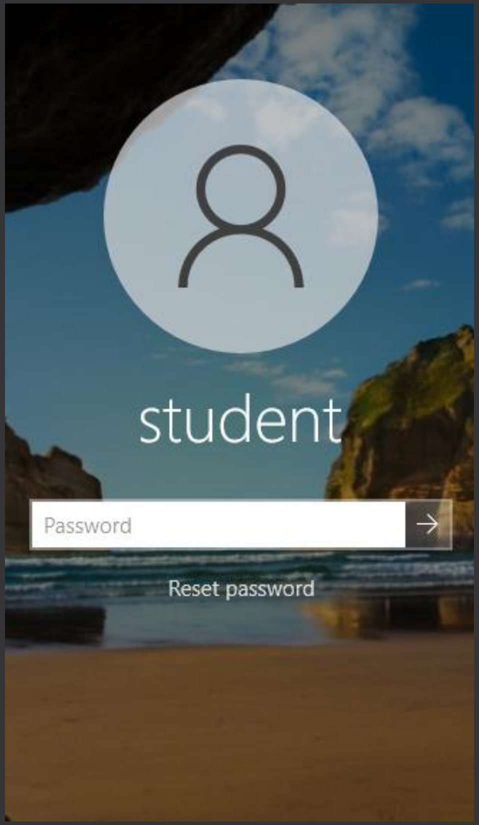
1. Minimizes all other windows, and blackens any additional displays, showing only the lock screen, it also uses the ‘Always On Top’ setting so it cannot be moved to the background
2. In case of a custom background, it displays that background instead of the default one
3. Blocks many shortcut keys to prevent circumventing the screen
4. Validates the entered password before closing the screen

demo

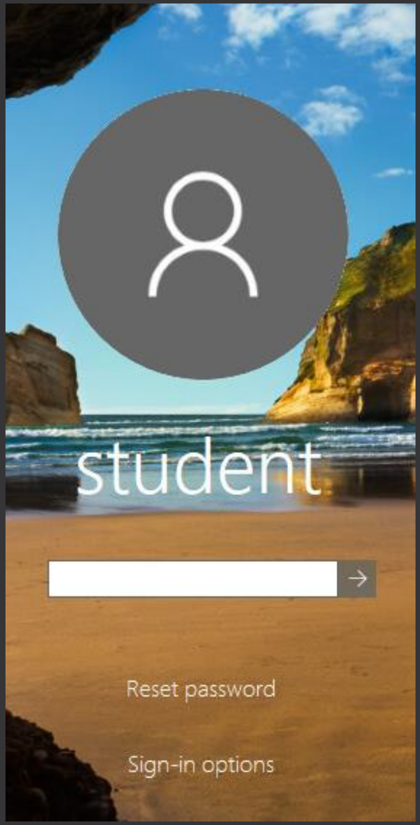
detection and bypass

There are a couple ways, we can detect whether this executable is running or not.

1. Internet, Ease of Access and Power Buttons are absent.
2. The Reset Password initially does not show up, and even after repeated failed password logging attempts, for local machines, “Sign-in options” is never present.
3. Can be bypassed using Ctrl + Alt + Delete and then opening task manager.



Windows Lock Screen



fakelogonscreen

thank you

Questions?