T1056.002 - GUI Input Capture

Description from ATT&CK

> Adversaries may mimic common operating system GUI components to prompt users for credentials with a seemingly legitimate prompt. When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task (ex: [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002)).
> Adversaries may mimic this functionality to prompt users for credentials with a seemingly legitimate prompt for a number of reasons that mimic normal usage, such as a fake installer requiring additional access or a fake malware removal suite.(Citation: OSX Malware Exploits MacKeeper) This type of prompt can be used to collect credentials via various languages such as AppleScript(Citation: LogRhythm Do You Trust Oct 2014)(Citation: OSX Keydnap malware) (Citation: Spoofing credential dialogs) and PowerShell.(Citation: LogRhythm Do You Trust Oct 2014)(Citation: Enigma Phishing for Credentials Jan 2015)(Citation: Spoofing credential dialogs)
> On Linux systems adversaries may launch dialog boxes prompting users for credentials from malicious shell scripts or the command line (i.e. Unix Shell).(Citation: Spoofing credential dialogs)

Atomic Tests

Atomic Test #1 - AppleScript - Prompt User for Password

Prompt User for Password (Local Phishing) Reference:
http://fuzzynop.blogspot.com/2014/10/osascript-for-local-phishing.html

Supported Platforms: macOS

auto_generated_guid: 76628574-0bc1-4646-8fe2-8f4427b47d15

Attack Commands: Run with `bash`!

```
osascript -e 'tell app "System Preferences" to activate' -e 'tell app "System Pref
```

Atomic Test #2 - PowerShell - Prompt User for Password

Prompt User for Password (Local Phishing) as seen in Stitch RAT. Upon execution, a window will appear for the user to enter their credentials.

Reference: https://github.com/nathanlopez/Stitch/blob/master/PyLib/askpass.py

Supported Platforms: Windows

auto_generated_guid: 2b162bfd-0928-4d4c-9ec3-4d9f88374b52

Attack Commands: Run with `powershell`!

```
# Creates GUI to prompt for password. Expect long pause before prompt is available
$cred = $host.UI.PromptForCredential('Windows Security Update', '',[Environment]::U
```

```
# Using write-warning to allow message to show on console as echo and other simila
write-warning $cred.GetNetworkCredential().Password
```