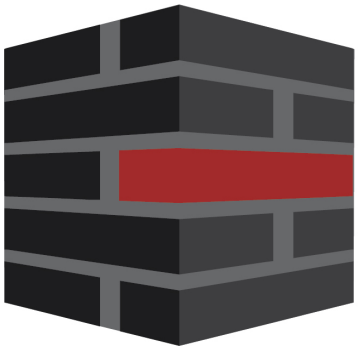

REDSTONE

SECURITY OPERATIONS

If They Can Do It, You Should Know It!

APPLE ICLOUD AUTHORIZATION BYPASS

VULNERABILITY REPORT

8 OCT, 2022

Table of Contents

Summary

An authorization bypass vulnerability exists in Apple iCloud whereby a sophisticated attacker with physical access to a target Apple computer, such as a MacBook, can gain full, persistent and undetectable access to the victim's iCloud account.

By creating a copy of the victim computer's EFI firmware, an attacker can create a clone of the device including the System Serial Number (SSN) and secret key material stored in firmware used to uniquely identify the system within the AppleID/iCloud ecosystem.

Once the device has been cloned, the attacker has full control of the iCloud account data including Keychain data, giving the attacker access to non-apple assets such as websites where the victim user has saved credentials in the browser.

The cloned device does not appear in the iCloud or AppleID device list, apart from the legitimate device. Importantly, in some circumstances the level of access persists ***even after*** an AppleID/iCloud password change, including a password change that forces the signout of other devices. If the password change is initiated on the target device which was cloned, the access tokens are not refreshed and the attacker maintains access.

Technical Requirements

The attack is possible with the following technical requirements:

- Physical access to the target computer
- Ability to read the EFI Firmware
  - Reboot into USB live system with flash reading software
  - Using EEPROM Flash reader connected to the SPI chip
  - Using Apple proprietary and controlled flash software
- Knowledge of the target iCloud username:password
  - Credential theft
  - Credential reuse (of compromised credentials)
  - Social Engineering
- Ability to accept initial Apple 2FA push (if 2FA is enabled) for FaceTime
  - Access to victim laptop
  - Cloned iPhone
  - Social engineering scenarios

Finding Detail

The research team found that it is possible to clone a MacBook laptop and gain access to a target AppleID/iCloud account by overwriting elements of the EFI Firmware of an attacker controlled device. The assessment team acquired two MacBook Pro 15" Mid 2012 laptops and two iPhone 6s handsets from eBay for this test. The team noted the serial numbers of the devices and designated one laptop to be the victim, and one laptop to be the attacker as shown below.

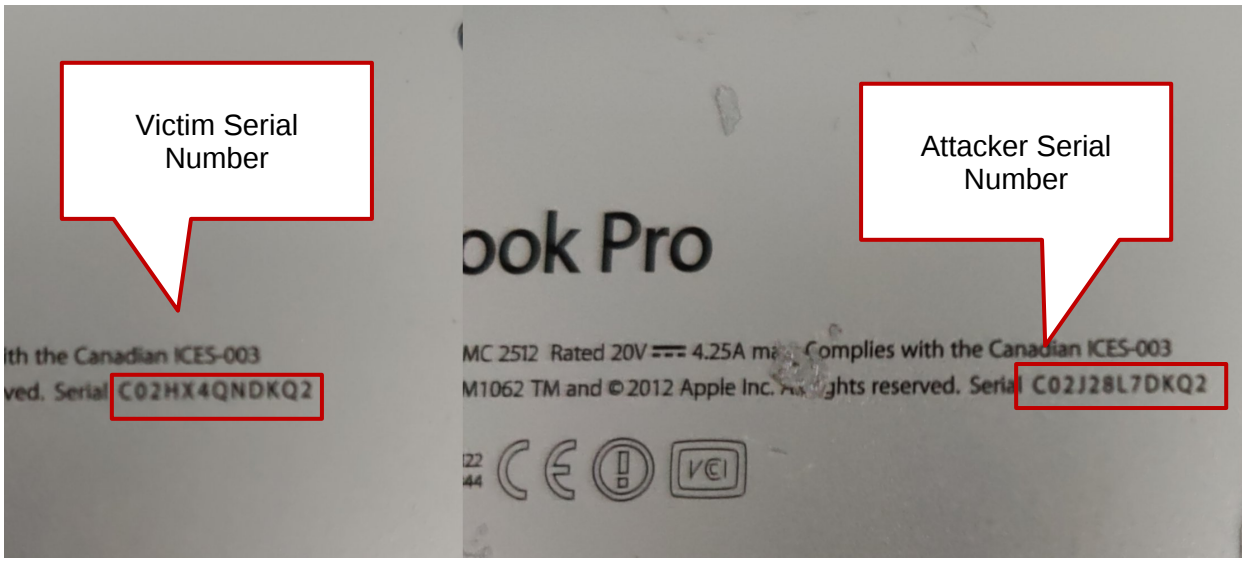

Figure 1 – System Serial Numbers

The team then created an iCloud account, `test.victim@icloud.com,` from the iPhone and associated the Victim MacBook as a trusted device, enabling full data sync as is typical for Apple users, as shown below.

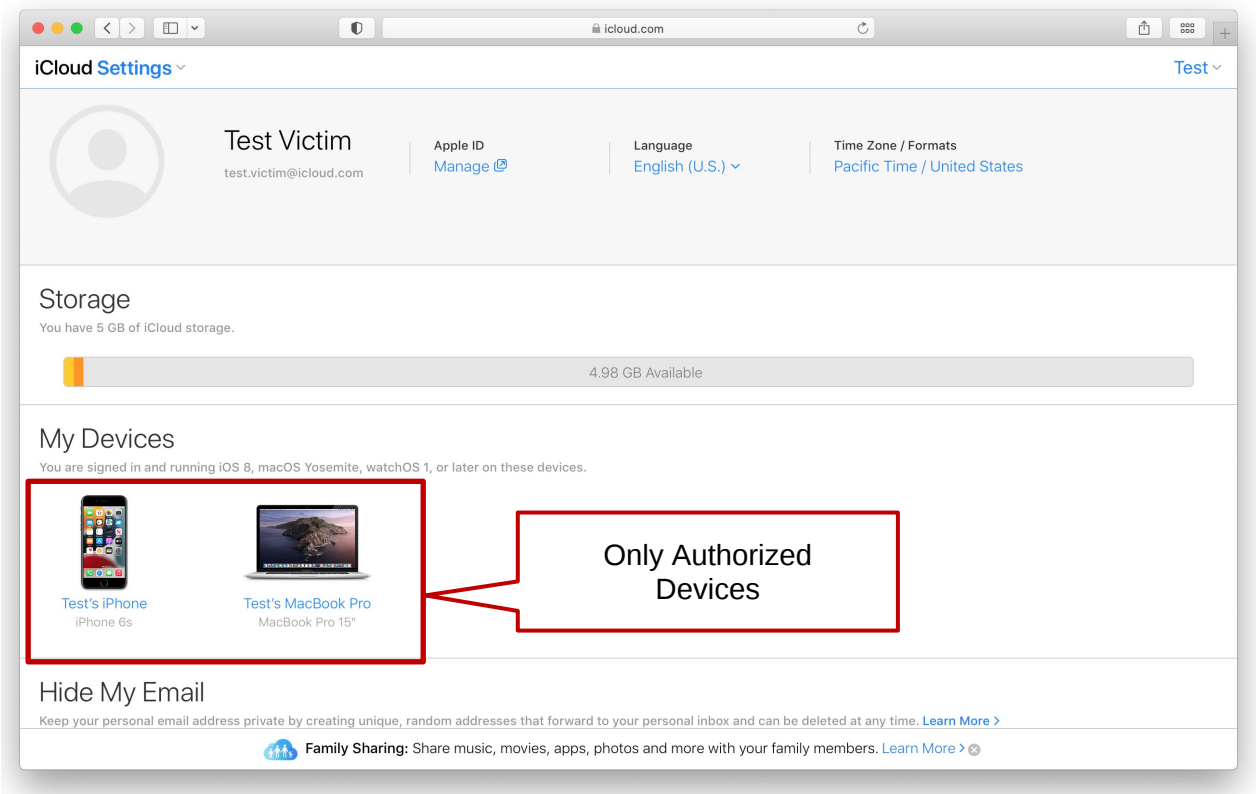

Figure2 – Victim iCloud account

The team then used a live boot distribution of Kali Linux on a USB flash drive to create a copy of the EFI firmware as shown in the following figure.

```
┌──(kali㉿kali)-[~]
└─$ sudo flashrom -p internal -r victim_efi.bin
flashrom v1.2 on Linux 5.18.0-kali5-amd64 (x86_64)
flashrom is free software, get the source code at https://flashrom.org

Using clock_gettime for delay loops (clk_id: 1, resolution: 1ns).
No DMI table found.
Found chipset "Intel HM77".
Enabling flash write... SPI Configuration is locked down.
PR0: Warning: 0x00190000-0x0066ffff is read-only.
PR1: Warning: 0x00692000-0x01ffffff is read-only.
At least some flash regions are write protected. For write operations,
you should use a flash layout and include only writable regions. See
manpage for more details.
OK.

…omitted for brevity…

Reading flash... done.
```

Figure 3: - Reading Flash Image

With the EFI binary image successfully copied, the team next used an in expensive EEPROM programmer to write that flash image to the SPI_FLASH chip of the attackers laptop as shown below.

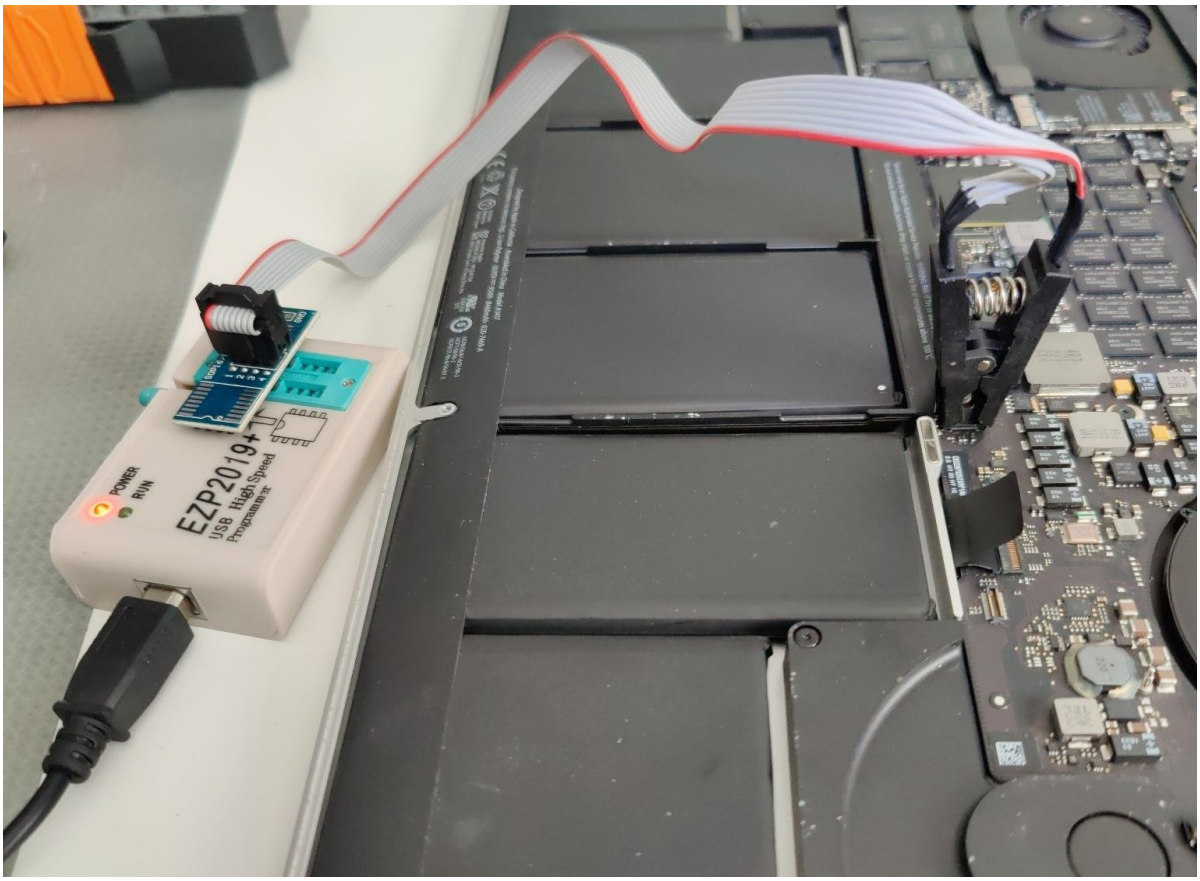

Figure 4: Writing Flash Image

Once the EFI Flash image was written to the attacking laptop, this MacBook effectively became a clone of the victim device. Both laptops appear to have the same system serial number as shown in the following image.

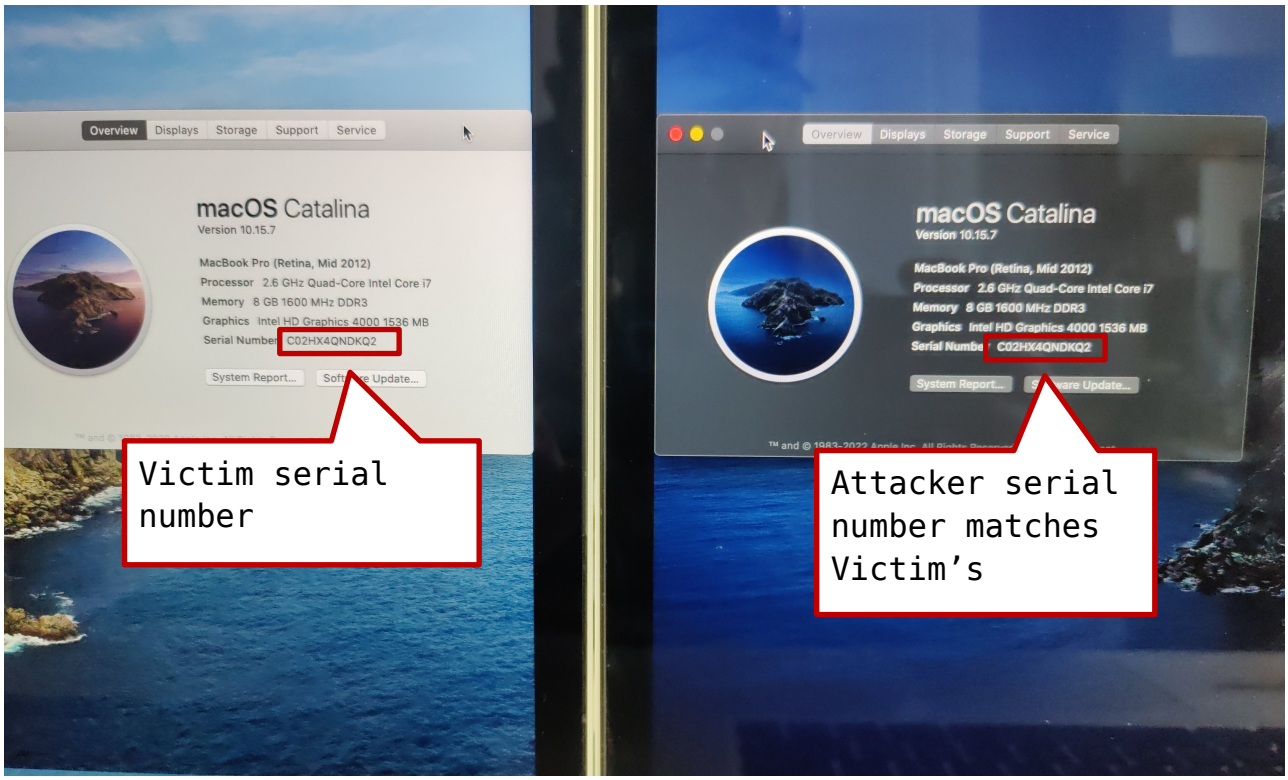

Figure13 – Attacker SN matches that of Victim SN

As demonstrated above, after the cloning attack, the OS-reported System Serial Number (SSN) of the Attacker laptop matched that of the Victim laptop.

The team verified that no additional devices were apparent in the Trusted Devices section of the AppleID portal, as shown below.

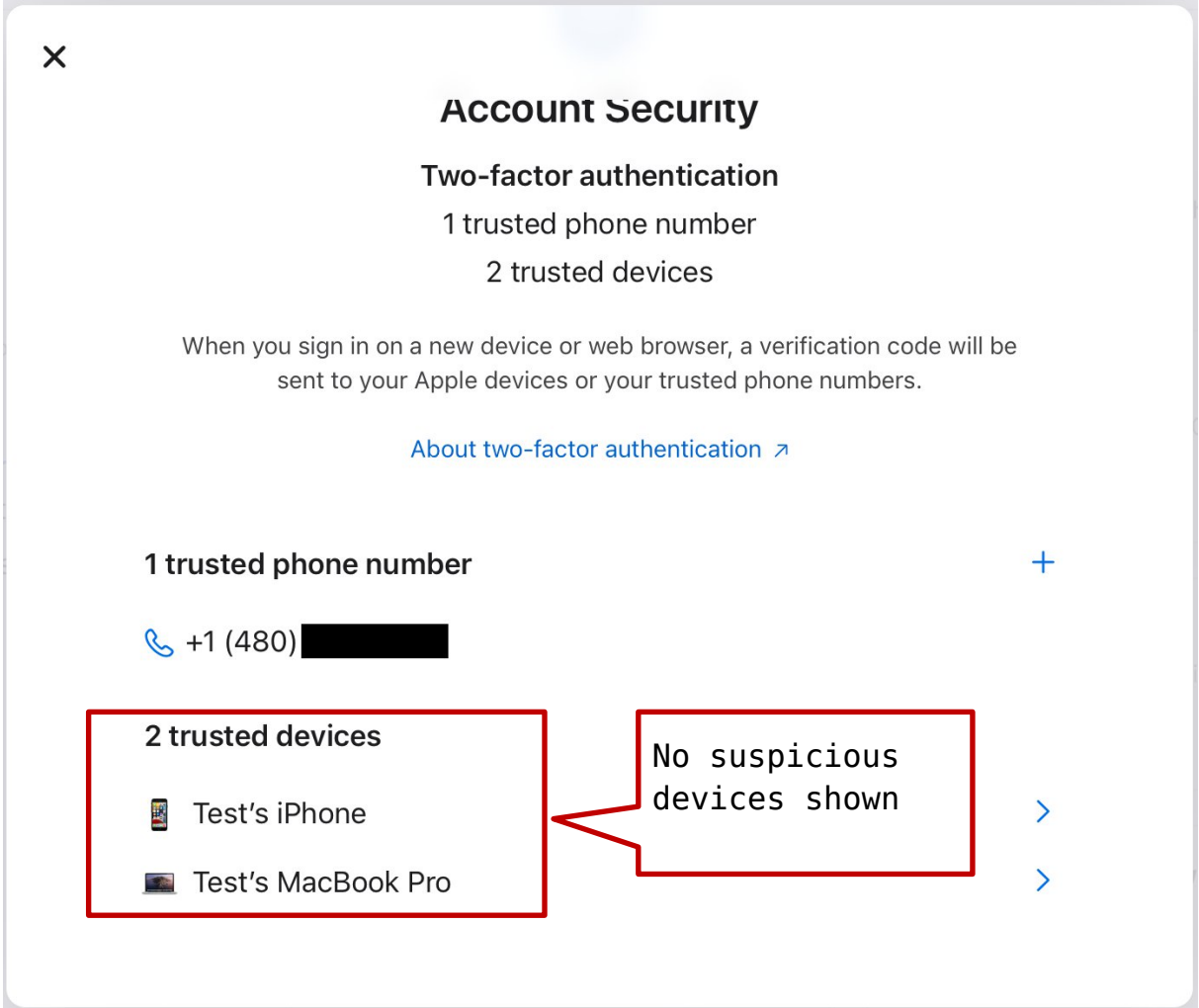

Figure14 – Trusted devices of AppleID Portal after attack

This attack, and the cloned device, is undetectable to the user. By all appearances, only known and trusted devices are connected to the iCloud and AppleID accounts of the victim.

All iCloud content was immediately available to the attacker since the content was Synchronized from iCloud. New messages and notes were populated in real time, giving the attacker unprecedented access to confidential information, as shown below.

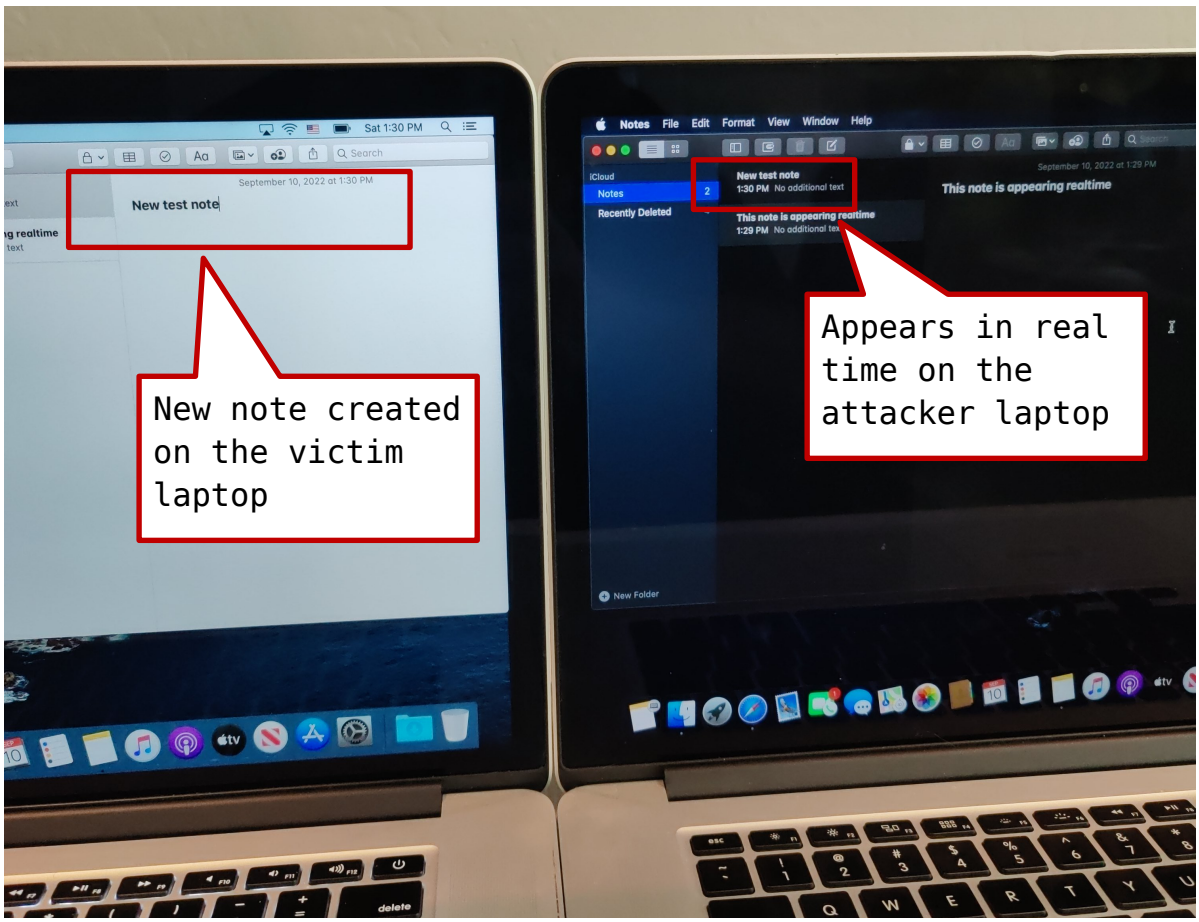

Figure15 – Real-time sync of Notes to Attacker laptop

In the example above, notes were created on the Victim laptop using the Notes app and were immediately synchronized to the Attacker laptop in real time.

The team then tested the behavior of calling the iPhone. As is shown below, the Attacker laptop sees the metadata of the call and can answer the call if desired.

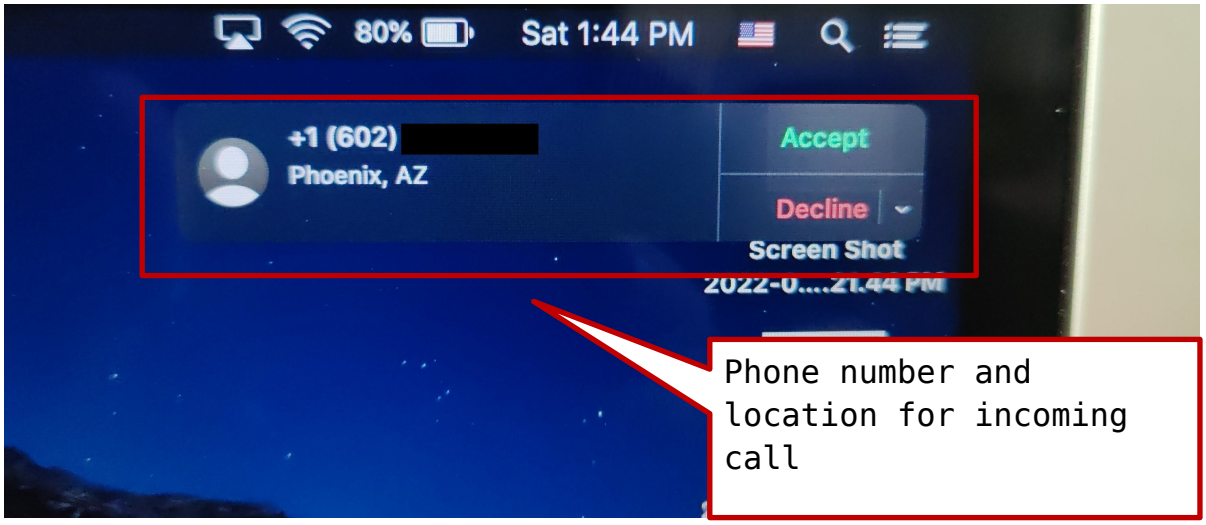

Figure16 – Incoming phone call shown on Attacker laptop

Incoming phone call metadata is known to the attacker, including exact time, location and identity of the caller, giving the attacker a highly detailed profile of life for the victim.

Disturbingly, this attack persists across password changes. The team changed the password from the Victim laptop and selected the option "sign-out of all connected devices," but new content was still streamed to the Attacker device.

An attack of this nature will grant the attacker access to the following:

- Full access to all documents stored in iCloud, including the ability to change, modify and delete documents
- Full access to all pictures stored in iCloud, including the ability to change, modify and delete pictures
- Full access to iMessage conversations, including message content as well as metadata concerning who and when conversations took place. In the case of iPhone cloning, this would also include the ability to delete conversation history
- The ability to send iMessage and SMS messages which appear to originate from the victim
- Full access to FaceTime conversation metadata, including times and participants of the FaceTime calls
- Full access to call history metadata, including specific times and participants of phone conversations
- Real-time access to phone calls, including the ability to see and answer incoming phone calls
- Full access to the Apple Keychain, including access to other stored passwords such as online services and WiFi networks
- Full access to "Find My" features of iCloud, including the ability to positively identify the location of a specific device with 1 meter resolution
- Full access to other stored information including Schedule Reminders, Notes, email, location history, etc