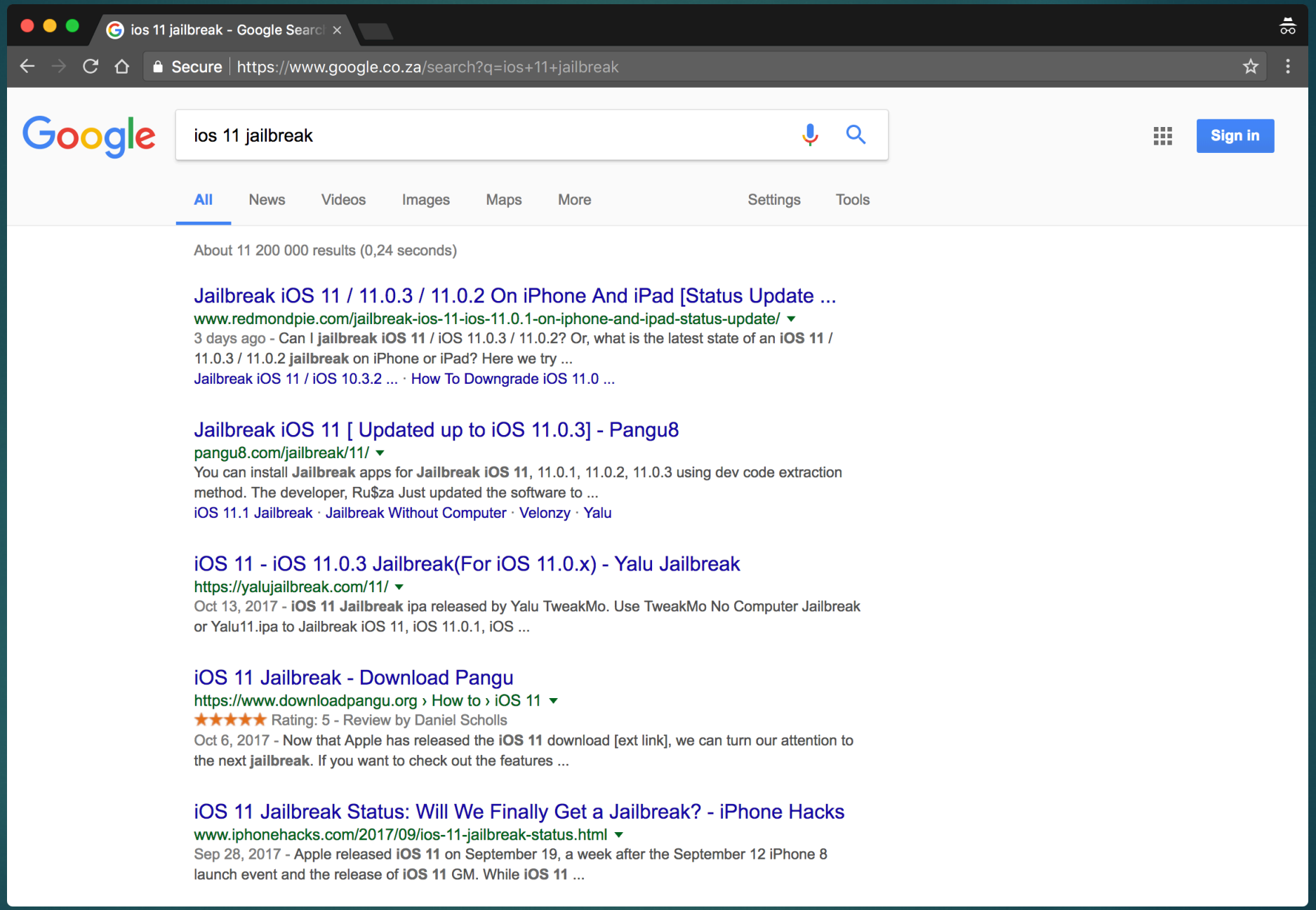
objection

RUNTIME MOBILE EXPLORATION

0xcon 2017

@leonjza

@sensepost


ios 11 jailbreak - Google Searc
Secure https://www.google.co.za/search?q=ios+11+jailbreak
Google
ios 11 jailbreak
Sign in
All News Videos Images Maps More Settings Tools
About 11 200 000 results (0,24 seconds)
Jailbreak iOS 11 / 11.0.3 / 11.0.2 On iPhone And iPad [Status Update ...
www.redmondpie.com/jailbreak-ios-11-ios-11.0.1-on-iphone-and-ipad-status-update/
3 days ago - Can I jailbreak iOS 11 / iOS 11.0.3 / 11.0.2? Or, what is the latest state of an iOS 11 / 11.0.3 / 11.0.2 jailbreak on iPhone or iPad? Here we try ...
Jailbreak iOS 11 / iOS 10.3.2 ... · How To Downgrade iOS 11.0 ...
Jailbreak iOS 11 [Updated up to iOS 11.0.3] - Pangu8
pangu8.com/jailbreak/11/
You can install Jailbreak apps for Jailbreak iOS 11, 11.0.1, 11.0.2, 11.0.3 using dev code extraction method. The developer, Ru$za Just updated the software to ...
iOS 11.1 Jailbreak · Jailbreak Without Computer · Velonzy · Yalu
iOS 11 - iOS 11.0.3 Jailbreak(For iOS 11.0.x) - Yalu Jailbreak
https://yalujailbreak.com/11/
Oct 13, 2017 - iOS 11 Jailbreak ipa released by Yalu TweakMo. Use TweakMo No Computer Jailbreak or Yalu11.ipa to Jailbreak iOS 11, iOS 11.0.1, iOS ...
iOS 11 Jailbreak - Download Pangu
https://www.downloadpangu.org › How to › iOS 11
★★★★★ Rating: 5 - Review by Daniel Scholls
Oct 6, 2017 - Now that Apple has released the iOS 11 download [ext link], we can turn our attention to the next jailbreak. If you want to check out the features ...
iOS 11 Jailbreak Status: Will We Finally Get a Jailbreak? - iPhone Hacks
www.iphonehacks.com/2017/09/ios-11-jailbreak-status.html
Sep 28, 2017 - Apple released iOS 11 on September 19, a week after the September 12 iPhone 8 launch event and the release of iOS 11 GM. While iOS 11 ...

meh.

frida

- Ole André Vadla Ravnås (@oleavr)
- dynamic instrumentation toolkit
- injects chrome v8 (or duktape) into process
- instrumentation done using JavaScript

- **basically magic (no really.)**

‘embedded mode’

(recently added fully autonomous mode)

demo

(native function hooking)

objective-c

(and java)

```objc
@implementation JailbreakDetection

+(BOOL) isJailbroken {

  NSFileManager *fm = [NSFileManager defaultManager];

  if ([fm fileExistsAtPath:@"/bin/bash"]) {
    return YES;
  }

  return NO;
}

@end
```

```
var JailbreakDetection = ObjC.classes.JailbreakDetection;

Interceptor.attach(
  JailbreakDetection.isJailbroken.implementation, {

    onEnter: function (args) {

      //
    },

    onLeave: function (retval) {

      retval.replace(0x0);
    }
});
```

demo

(jailbreak detection simulation/bypass)

lets... inject arbitrary code

demo

(nsuserdefaults extraction)

bundled it up, and called it…

objection

(object)inject(ion)

internals

- python3, installable with pip3
- bundles ios and android hooks
- 'compiles' hooks with Jinja2
- can import arbitrary Frida scripts

- do **not** need a jailbroken / rooted device

thanks! 🎉

bernard-wagner
5 commits 327 ++ 30 --

hypn0s
2 commits 49 ++ 7 --

FlavSec
2 commits 64 ++ 41 --

BlackAp3rture
1 commit 51 ++ 0 --

ropnop
1 commit 1 ++ 1 --

colman-mbuya
1 commit 1 ++ 1 --

juanriaza
1 commit 6 ++ 3 --

melvinsh
1 commit 5 ++ 3 --

demo

(exploring the filesystem)

demo

(ssl pinning bypass)

demo

(class method monitoring)

and lots more!

- dump process/module memory
- interact with iOS keychain
- bypass touchid*
- monitor iOS pasteboard
- extract iOS binary cookies

questions?

https://github.com/sensepost/objection

@leonjza / @sensepost