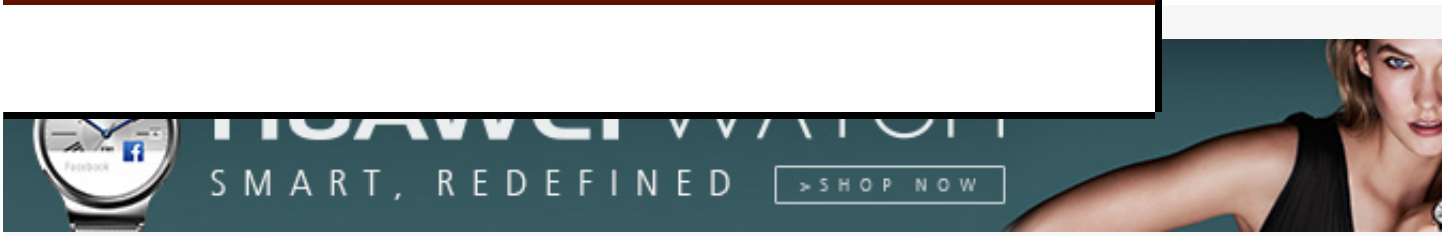
WIRED SUBSCRIBE




ANDY GREENBERG SECURITY 09.21.15 10:49 AM

# SPY AGENCY CONTRACTOR PUTS OUT A $1M BOUNTY FOR AN IPHONE HACK

SCOTT DADICH/WIRED

AS LONG AS hackers have sold their secret hacking techniques known as zero-day exploits to government spies, they've generally kept that trade in the shadows. Today it's come into the spotlight with the biggest bounty ever publicly offered for a single such exploit: $1 million for a technique that can break into an iPhone or iPad running Apple's freshly released iOS 9.

On Monday, a new security industry firm known as Zerodium announced that it will pay that seven-figure sum to anyone who gives the company a hacking technique that can take over an iOS device remotely, via a web page the victim visits, a vulnerable app on the victim's device, or by text message. The company says it's willing to pay the bounty multiple times, though it may cap the payouts at $3 million.

"Due to the increasing number of security improvements and the effectiveness of exploit mitigations in place, Apple's iOS is currently the most secure mobile OS," reads the statement on Zerodium's website announcing the bounty. "But don't be fooled, secure does not mean unbreakable, it just means that iOS has currently the highest cost and complexity of vulnerability exploitation and here's where the Million Dollar iOS 9 Bug Bounty comes into play."

Zerodium founder Chaouki Bekrar has long been one of the few public faces of the zero-day industry; In addition to his new startup Zerodium, which launched in July, he's also the founder of the more established French hacking firm Vupen, which has been unusually open about the fact that it develops intrusion techniques for popular software and sells them to government agencies around the world. With the new company and his flashy iOS bounty, Bekrar is expanding from merely creating zero-days to brokering them, too, as a kind of hacker middleman.

"Zerodium's main goal is to capture the most advanced zero-day exploits and the highest risk vulnerabilities which are discovered, held, or sometimes stockpiled by talented researchers around the globe," he wrote to WIRED in an email.

Bekrar has made no apologies for the fact that his business thrives on digital insecurity. Rather than report vulnerabilities in software to the companies that make it to help fix hackable bugs, Vupen develops hacking techniques based on those bugs and typically sells them to multiple government customers. His iOS bounty is no different: The terms of the offer include the demand that the bug not be reported to Apple or publicly disclosed, the better to allow Zerodium's customers to use the technique in secret. Apple didn't immediately respond to a

request for comment.

Bekrar's past customers for such undisclosed hacking techniques have included the NSA as well as other NATO countries and "NATO partners" that Bekrar declines to name. Bekrar declined to identify any of Zerodium's potential customers, but the company's website describes them as "major corporations in defense, technology, and finance, in need of advanced zero-day protection, as well as government organizations in need of specific and tailored cybersecurity capabilities."[1]

But even Bekrar has admitted that he doesn't always know where Vupen's hacking tools have ended up, or how a customer agency uses or shares them. "We do the best we can to ensure it won't go outside that agency," Bekrar told me in 2012. "But if you sell weapons to someone, there's no way to ensure that they won't sell to another agency."

Privacy and security advocates put it more simply: ACLU lead technologist Chris Soghoian has called Bekrar a "modern-day merchant of death," selling "the bullets for cyberwar." After a sale, Soghoian argues, Vupen turns a blind eye to where its exploits end up and whether repressive regimes might be using them to spy on citizens. "Vupen doesn't know how their exploits are used, and they probably don't want to know," Soghoian told me in 2012. "As long as the check clears." After Bekrar refused to share a Chrome hacking technique with Google, Google security staffer Justin Schuh called him an "ethically challenged opportunist."

In fact, the controversial treaty known as the Wassenaar Arrangement, which would regulate the spread of zero-day exploits between countries, is widely seen as a reaction to firms like Vupen that trade in such digital intrusion tools. But Bekrar doesn't see Wassenaar as a serious obstacle to his new business, and points out that the arrangement has yet to be implemented in the United States. "We will comply with applicable regulations as any cybersecurity company," Bekrar says. "Wassenaar adds a layer of paperwork but does not aim to prevent companies from conducting their businesses."

But Zerodium certainly isn't the only willing buyer for an iOS exploit. For discreet government customers, an iPhone hacking technique has long been a rare and expensive prize due to Apple's tight security measures. In the eight years since the iPhone's launch, an iOS hack has almost never been seen outside of a controlled demonstration. (Last week was a rare exception, when malicious apps penetrated Apple's app store targeting Chinese users.)

When I assembled a price list for secret software exploits in 2012 based on talking to players in the zero-day trade, an iOS exploit sold for $250,000, far more than the mere $60,000 for an Android hack. The next year, the *New York Times* reported that an iPhone zero-day sold for $500,000.

Zerodium's unprecedented bounty may show just how difficult it's become to penetrate Apple's increasing layers of security. But with a million dollars on the table, expect a new wave of hackers to try.

[1]*Correction 9/21/2015 11am EST: An earlier version of the story stated that Zerodium sold only to government agencies, when in fact its website also states that it sells to corporate customers.*

#APPLE #BEKRAR #BOUNTY #IOS 9 #VUPEN #ZERO-DAY #ZERODIUM

VIEW COMMENTS

SPONSORED STORIES

WEBIOT
13 Little Known Free Programs Any LifeHacker Must Try

22 WORDS

25 Crazy Building Designs You Won't Believe are Real

GUARDIAN

Creating a sustainable coffee industry in South Sudan

TRADEGOOD

Difference between OEM and ODM

LEXUS

Intersect by Lexus: Inside the world of Tokyo's new creative space

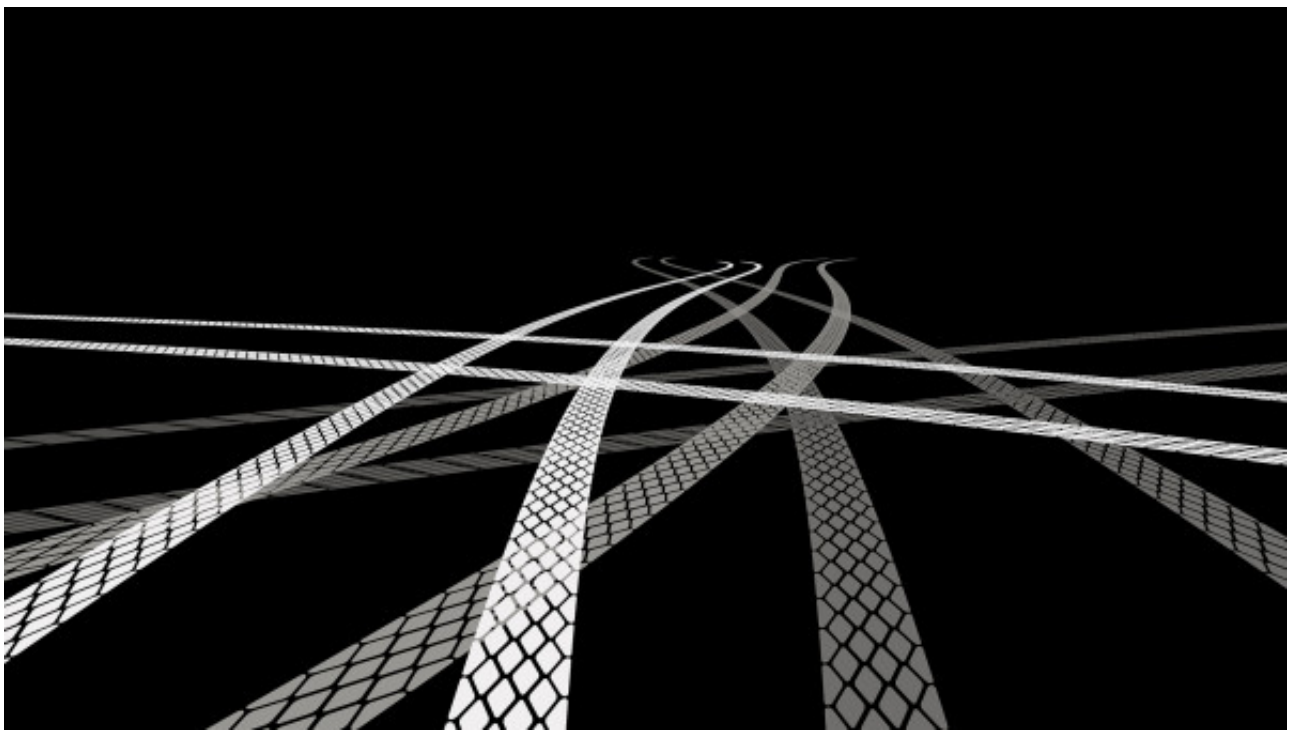
POWERED BY OUTBRAIN

# MORE SECURITY

SURVEILLANCE

## CISA Security Bill Passes Senate With Privacy Flaws Unfixed

6 HOURS



SECURITY

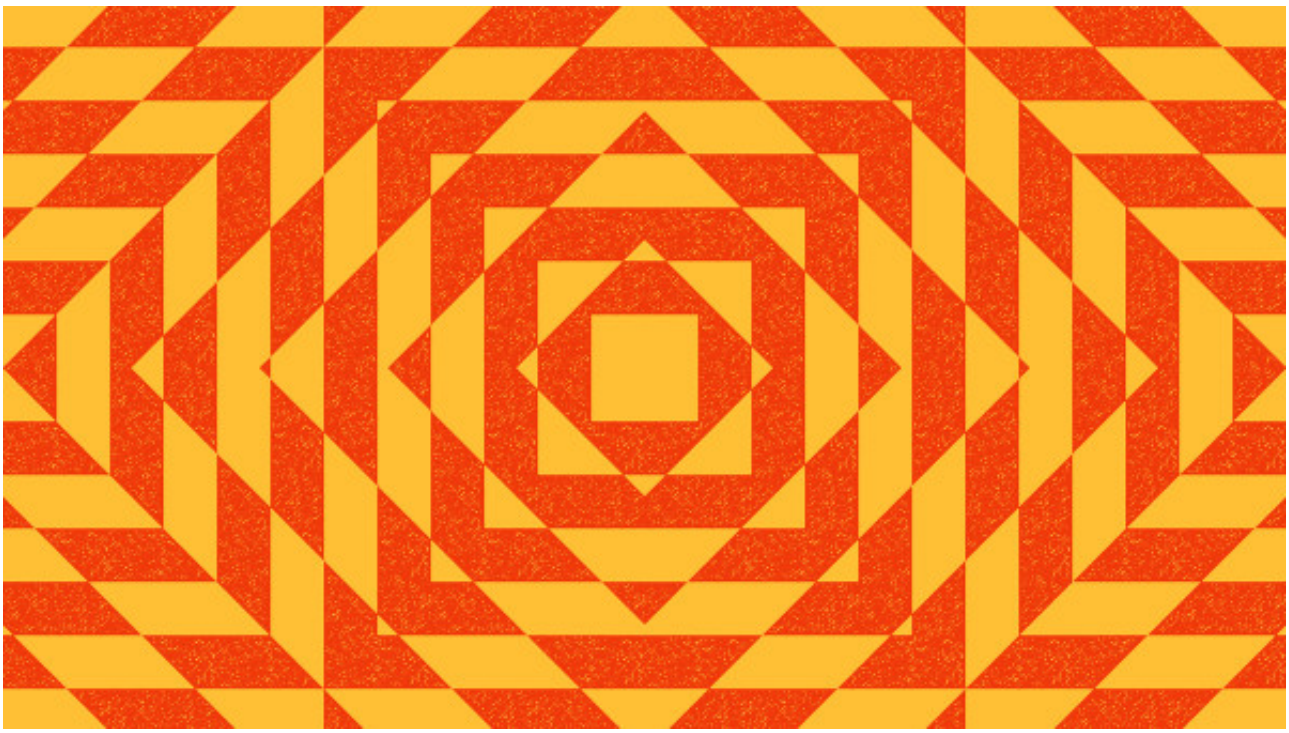
## Cars That Talk to Each Other Are Much Easier to Spy On

13 HOURS

EXPLAINED

## Answers to Your Burning Questions on the Ashley Madison Hack

08.21.15



SECURITY THIS WEEK

## Security This Week: Apparently China Is Still Hacking US Companies

10.24.15

FROM THE EDITORS

**David Pogue Gets Car Hacking Dangerously Wrong**

10.22.15

# WE RECOMMEND

JORDAN CRUCCHIOLA

The Age of the Messed Up Child Star Is Over

CADE METZ

The Porn Business Isn't Anything Like You Think It Is

JULIA GREENBERG

Star Wars Ticket Sale Shows Disney Can Do Whatever It Wants

JAKE MUNCY
Metal Gear Creator Hideo Kojima Has Finally Left Konami

AFAR
12 Experiences You'll Love in Hong Kong

POWERED BY OUTBRAIN

# FOLLOW US ON TWITTER

2 MINS
(PHOTOS) The brilliant neon shops that lure Mecca's pilgrims wrd.cm/1Q68wIY

FOLLOW

WIRED

SUBSCRIBE

ADVERTISE | SITE MAP

| | |
|---|---|
| PRESS CENTER | FAQ |
| CUSTOMER CARE | CONTACT US |
| NEWSLETTER | WIRED STAFF |
| JOBS | RSS |

Use of this site constitutes acceptance of our user agreement (effective 3/21/12) and privacy policy (effective 3/21/12). Your California privacy rights. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.