ANDY GREENBERG SECURITY 11.18.15 7:26 AM

HERE'S A SPY FIRM'S PRICE LIST FOR SECRET HACKER TECHNIQUES

GETTY IMAGES

THE TRADE IN the secret hacker techniques known as "zero day exploits" has long taken place in the dark, hidden from the companies whose software those exploits target, and from the privacy advocates who revile the practice. But one zero-day broker is taking the market for

these hacking techniques into the open, complete with a full price list.

In an unprecedented move Wednesday, the zero-day broker startup Zerodium published a price chart for different classes of digital intrusion techniques and software targets that it buys from hackers and resells in a subscription service to customers that include government agencies. The list, which details the sums it pays for attack methods that effect dozens of different applications and operating systems, represents one of the most detailed views yet into the controversial and murky market for secret hacker exploits. “The first rule of [the] 0days biz is to never discuss prices publicly,” Zerodium CEO Chaouki Bekrar wrote in a message to WIRED prior to revealing the chart. “So guess what: We’re going to publish our acquisition price list.”

An attack that can fully, remotely take over a victim’s computer through his or her Safari or Internet Explorer browser, for instance, fetches a price of as much as $50,000. For the harder target of Google Chrome, Zerodium’s price rises to $80,000. Remote exploits that entirely defeat the security of an Android or Windows Phone device go for as much as $100,000. And an iOS attack can earn a hacker half a million dollars, by far the highest price on the list.

Here’s the full price chart from Zerodium:

Zerodium's full chart of payouts it offers for different zero-day hacking techniques. Click to enlarge.

Zerodium explicitly warns sellers that any zero-day exploit Zerodium buys must be for Zerodium's eyes only; enterprising hackers can't resell it to other buyers or disclose it to the software's vendor, who might release a patch that protects users and renders the attack useless. The company stipulates that it will pay the listed prices only for "original, exclusive, and previously unreported zero-day exploits."

Zerodium, in other words, is keeping its fresh hacker techniques under wraps for its customers, which it says include "government organizations in need of specific and tailored cybersecurity capabilities," as well as corporate customers it says use the techniques for defensive purposes. Zerodium founder Bekrar says Zerodium clients pay subscription rates of at least $500,000 a year for access to its exploits. He wouldn't name any specific customers. But Bekrar's last startup, the French company Vupen, more explicitly offered its zero-day exploits to customers it described as government agencies within NATO

and “NATO ally” countries. A Freedom of Information request from the investigative news site Muckrock in 2013 showed that Vupen’s customers included the NSA.

Just what affect publicly pricing zero day exploits might have on the market for secret hacker techniques is far from clear. But it could actually encourage more hackers to sell the intrusion methods they create; Independent security researchers have long complained that the lack of public pricing in the zero-day trade makes it difficult for them to get a “fair” price, as in this 2007 paper from former NSA hacker Charlie Miller. Bekrar pitches Zerodium, which launched in July, as leveling that playing field for independent security researchers. “With Zerodium, security researchers can finally make money with their security findings and hard work,” he writes.

Publicly trading in secret intrusion techniques has also made Bekrar an easy target for criticism from both the privacy community and the software companies whose hackable flaws he exploits for a profit. Google security staffer Justin Schuh once called him an “ethically challenged opportunist.” ACLU lead technologist Chris Soghoian has labelled Bekrar’s Vupen a ““modern-day merchant of death,” selling “the bullets for cyberwar.”

Bekrar’s decision to list his exploit prices publicly, Soghoian argues, isn’t an attempt to bring more transparency to the zero-day trade so much as a savvy marketing technique. “Chaouki, with VUPEN, and now with Zerodium, has favored publicity over discretion. He wants free press in order to attract clients,” says Soghoian. Larger, more established defense contractors that sell zero-days, Soghoian adds, have no need for such stunts. “Raytheon and ManTech don’t need to publish price lists online…NSA knows the prices those firms charge.”

Bekrar didn’t respond to WIRED’s questions about why he’d chosen to publish the price list. But even if it’s intended for marketing alone, the chart may offer valuable information about the relative vulnerability of certain software. (Until now the only other such price list for zero-day exploits was an unofficial one I’d assembled after speaking with sources

in the hacking community in 2012.) Hacking techniques affecting common web publishing software like Drupal and WordPress sell for just $5,000, according to Zerodium's list. Perhaps more surprising is that an exploit affecting the anonymity-focused TorBrowser only fetches $30,000.

That revelation comes just days after Tor claimed that the FBI had paid $1 million to Carnegie Mellon University for a technique it had developed to break the anonymity protections of Tor's server-focused "hidden services" feature. It's also far less than the $110,000 the Russian government reportedly offered for a Tor-breaking technique last year. But Bekrar emphasized in an email to WIRED that Zerodium's Tor bounty was only for vulnerabilities in the TorBrowser, which is adapted from Firefox, rather than vulnerabilities in the Tor network itself, which Bekrar notes "may threaten the security and privacy of legitimate Tor users."

The high price for an iPhone or iPad attack—$500,000—still comes in at just half the reward that Zerodium offered in an open bounty last month. In what Bekrar now says was only a "limited-time deal," the company very publicly agreed to pay $1 million in late October to a team of hackers who proved that they could successfully compromise an iOS device that visited a malicious web page through its Safari or Chrome browser.

Even at that reduced price, an iOS exploit is still worth five times as much as any other technique on Zerodium's chart. Apple users may be dismayed to learn that the ability to compromise their personal device is as much a commodity as any other hacking technique. But at least it's an expensive one.

#CYBERSECURITY #HACKS AND CRACKS #NSA #ZERO DAY EXPLOIT #ZERODIUM

MORE SECURITY

CYBERSECURITY

ISIS' OPSEC Manual Reveals How It Handles Cybersecurity

18 HOURS

SECURITY

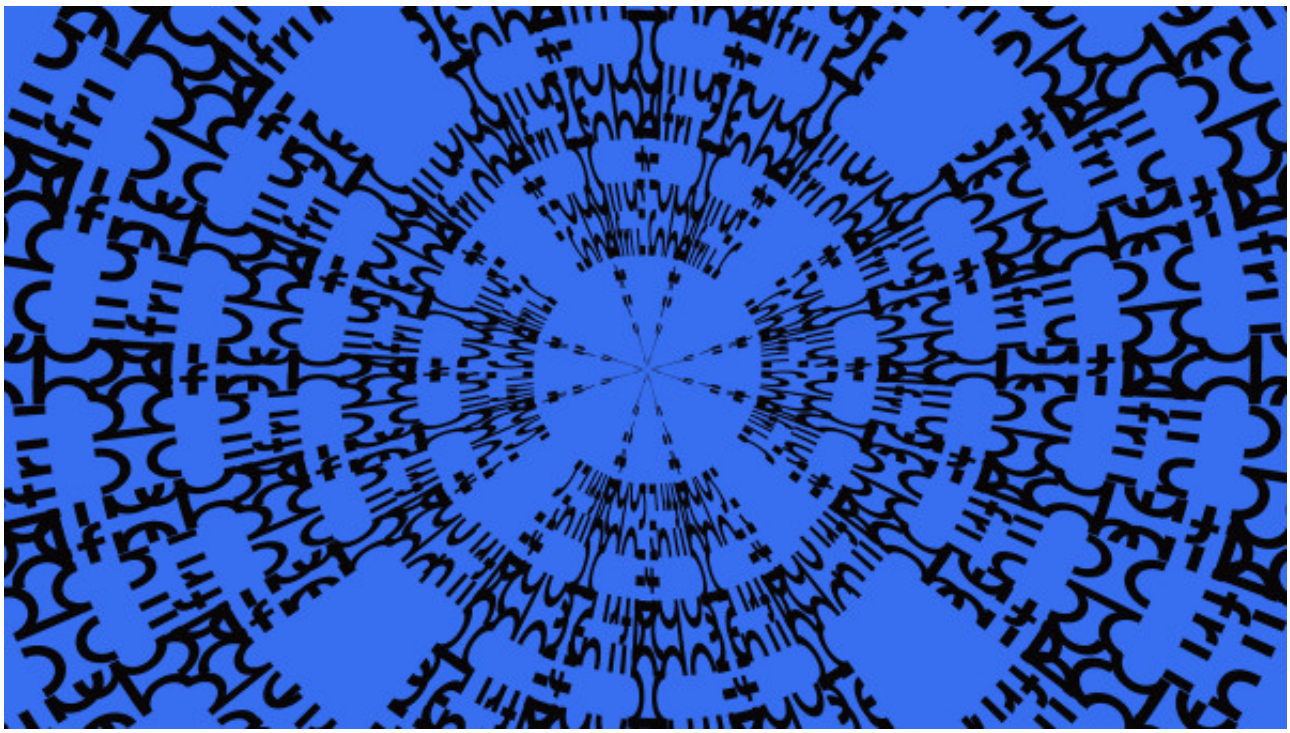
Carnegie Mellon Denies FBI Paid for Tor-Breaking Research

2 DAYS

EXPLAINED

Answers to Your Burning Questions on the Ashley Madison Hack

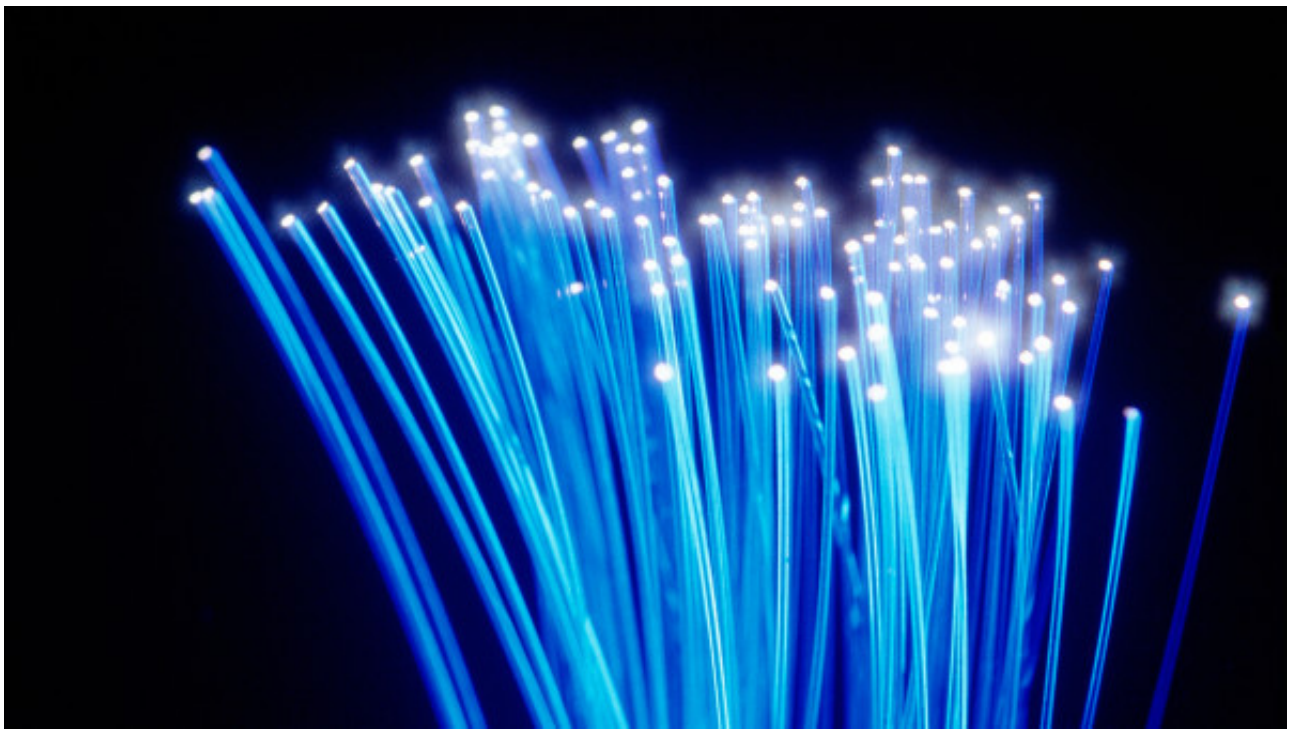
08.21.15



SECURITY

After Paris Attacks, Here's What the CIA Director Gets Wrong About Encryption

11.16.15



SECURITY THIS WEEK

Security News This Week: Someone's Cutting Fiber Optic Cables in the Bay Area

11.14.15

WE RECOMMEND

CHRISTOPHER NULL

Hello, I'm Mr. Null. My Name Makes Me Invisible to Computers

ALEX DAVIES

VW Owners Aren't Going to Like the Fixes for Their Diesels

CADE METZ

Google Is 2 Billion Lines of Code—And It's All in One Place

MICHAEL CALORE