Threatpost | The first stop for security news

- Categories
  - Category List
    - Apple
    - Cloud Security
    - Compliance
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Microsoft
    - Mobile Security
    - Privacy
    - Ransomware
  - Category List
    - SAS
    - SMB Security
    - Social Engineering
    - Virtualization
    - Vulnerabilities
    - Web Security
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - Additional Categories
    - Slideshows
  - The Kaspersky Lab News Service
- Featured
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - The Kaspersky Lab News Service

Featured Posts

All
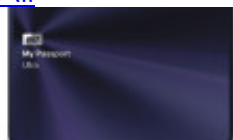
Academics Find Critical Flaws in Self-Encrypting···

Apple to Remove 256 iOS Apps···

Facebook Notifying Users of Targeted, Nation-State···

- Podcasts

Latest Podcasts

All

[Threatpost News Wrap, October 23, 2015](#)

[Juan Andres Guerrero-Saade on the Dangers···](#)

[Threatpost News Wrap, October 16, 2015](#)

[Cesar Cerrudo on Securing Smart Cities](#)

[Threatpost News Wrap, October 12, 2015](#)

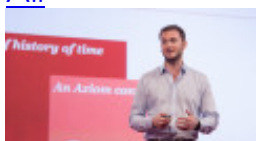[Martijn Grooten on the Highlights of···](#)

Recommended

- [Robert Hansen on Aviator, Search Revenue and the $250,000 Security Guarantee](#)
- [Threatpost News Wrap, February 21, 2014](#)
- [How I Got Here: Jeremiah Grossman](#)
- [Chris Soghoian on the NSA Surveillance and Government Hacking](#)
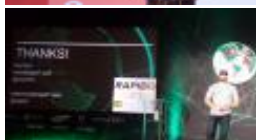
[The Kaspersky Lab Security News Service](#)

- [Videos](#)

Latest Videos
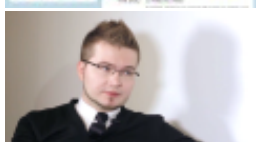
[All](#)

[Kris McConkey on Hacker OpSec Failures](#)

[Trey Ford on Mapping the Internet···](#)

[Christofer Hoff on Mixed Martial Arts,···](#)

[Twitter Security and Privacy Settings You···](#)

[The Biggest Security Stories of 2013](#)

[Jeff Forristal on the Android Master-Key…](#)

Recommended

- - [Twitter Security and Privacy Settings You Need to Know](#)
  - [Lock Screen Bypass Flaw Found in Samsung Androids](#)
  - [Facebook Patches OAuth Authentication Vulnerability](#)
  - [Video: Locking Down iOS](#)
[The Kaspersky Lab Security News Service](#)

[Search]

- [Twitter](#)
- [Facebook](#)
- [Google](#)
- [LinkedIn](#)
- [YouTube](#)
- [RSS](#)

10/27/15 5:14
Adobe updated Shockwave this morning and fixed a critical vulnerability -
https://t.co/05LzJliC2U

- 🇬🇧
- 🇷🇺

[Welcome](#) > [Blog Home](#)>[Government](#) > VUPEN Founder Launches New Zero-Day Acquisition Firm Zerodium

| 🐦 0 | f 0 | G+ 0 | in 82 | 🔴0 | 💬 1 |

VUPEN Founder Launches New Zero-Day Acquisition Firm

Zerodium

[Follow @dennisf] by [Dennis Fisher]   July 24, 2015 , 9:46 am

UPDATE–In the weeks since the [Hacking Team breach], the spotlight has shone squarely on the small and often shadowy companies that are in the business of buying and selling exploits and vulnerabilities. One such company, Netragard, this week decided to [get out of that business] after its dealings with Hacking Team were exposed. But now there's a new entrant in the field, Zerodium, and there are some familiar names behind it.

The company was launched by Chaouki Bekrar, founder of [VUPEN], a vulnerability and exploit broker that often is at the center of discussions about the legality and ethics of such businesses. VUPEN is one of the rare companies in that field that does all of its own research and development; it does not buy vulnerabilities or exploits from outside sources. But now, at a time when there has never been more attention from lawmakers, media, and governments, Bekrar has created a new venture that will wade fully into the purchase of bugs and exploits.

Related Posts

[Attackers Targeting Unpatched Joomla Sites Through SQL Injection Vulnerability]

October 27, 2015 , 1:43 pm

[Yahoo Hires Bob Lord as its CISO]

October 26, 2015 , 12:16 pm

[NSA's Divorce from ECC Causing Crypto Hand-Wringing]

October 23, 2015 , 3:55 pm

Zerodium plans to focus exclusively on buying high-risk vulnerabilities, leaving aside the lower end of the spectrum. The company will use the vulnerabilities it acquires to make up a feed of vulnerabilities, exploits, and defensive measures, that it provides to customers.

"ZERODIUM pays premium rewards to security researchers to acquire their zero-day discoveries and exploits affecting widely used operating systems, software, and/or devices. While the majority of existing bug bounty programs may accept almost any kind of vulnerabilities and PoCs but pay low rewards, at ZERODIUM we only focus on high-risk vulnerabilities with fully functional and reliable exploits, and we pay higher rewards," the company's [site] says.

Zerodium will be looking for vulnerabilities and exploits for the most commonly used platforms and applications, including Windows, OS X, and Linux; the four major browsers; Flash and Reader; Microsoft Office; Android, iOS, BlackBerry, and Windows Phone; and the major Web and mail servers. What the company is not interested in buying are partially working exploits or vulnerabilities in Web services such as Google or Twitter.

"ZERODIUM does not acquire theoretically exploitable or non-exploitable vulnerabilities. We only acquire zero-day vulnerabilities with a fully functional exploit whether including only one stage or multiple stages e.g. browser exploits with or without a sandbox bypass/escape are both eligible," the company says.

The company says it will pay premium prices for the bugs and exploits it's seeking and will not buy from researchers who live in countries that are sanctioned by the United

Nations or United States. Zerodium does not specify what kind of companies or organizations it will sell its service to, but Bekrar always has said that VUPEN only sells its exploits to law enforcement agencies and government customers in non-sanctioned countries.

"We only sell to democracies. We respect international regulations, of course, and we only sell to trusted countries and trusted democracies," Bekrar said in an interview with Threatpost in 2012. "We do not sell to oppressive countries."

VUPEN runs a subscription service that supplies customers with vulnerability data and exploits for zero days and other bugs. The company's customers have included the NSA.

The demand for high-end vulnerabilities and exploits is showing no signs of waning. Intelligence agencies, law enforcement organizations and many other government agencies in countries around the world are expanding their offensive security capabilities and a key ingredient in how these teams operate is the use of zero days. Exploits for undisclosed vulnerabilities often are used to compromise target systems as part of law enforcement investigations and intelligence operations, a controversial practice that has become even more so in the wake of the Hacking Team breach three weeks ago.

This story was updated on July 24 to correct that Zerodium was launched by Bekrar, not VUPEN

About Dennis Fisher

Dennis Fisher is a journalist with more than 13 years of experience covering information security.

View all posts by Dennis Fisher →

Latest Tweet from: Dennis Fisher

DennisF
@DennisF

[Follow]

@suburbsec I'm here for ya

11:33 PM - 22 Oct 2015

🐦 0   f 0   G+ 0   in 82   🔴 0   💬 1

Categories: Government, Malware, Vulnerabilities, Web Security

Comment (1)

1. *Rob Shein* July 24, 2015 @ 1:49 pm
   1

   It's curious that in their press release they say will only sell to LEO and government

in "non-sanctioned countries" but Bekrar says that they only sell to "democracies." The latter is a subset of the former, and the difference between the two is significant. Most of the countries over which Hacking Team received criticism were non-sanctioned, but none of them were democracies.

[Reply](#) ↓

Leave A Comment

Your email address will not be published. Required fields are marked *

Name

Email

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

I'm not a robot
reCAPTCHA
Privacy - Terms

Post Comment

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

Recommended Reads

🐦 0   f 29   G+ 0   in 0   🔴0   💬 0

October 27, 2015 , 1:43 pm
Categories: [Vulnerabilities](#), [Web Security](#)

[Attackers Targeting Unpatched Joomla Sites Through SQL Injection Vulnerability](#)

by [Chris Brook](#)

Attackers have been carrying out attacks on sites running old, unpatched versions of Joomla following the disclosure of a critical SQL injection vulnerability in the software last week

Read more...

Twitter	Facebook	Google+	LinkedIn	Reddit	Comments
0	24	4	25	1	0
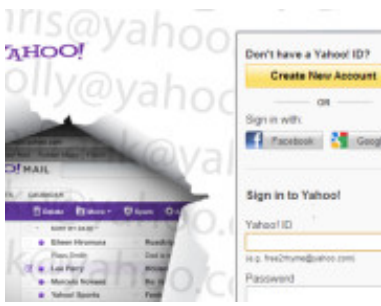
October 26, 2015 , 12:16 pm
Categories: Compliance, Privacy, Web Security

Yahoo Hires Bob Lord as its CISO

by Michael Mimoso

Yahoo has hired former Twitter and Rapid7 security executive Bob Lord as its new CISO, taking over for Alex Stamos, who this summer left Yahoo for Facebook.

Read more...

Twitter	Facebook	Google+	LinkedIn	Reddit	Comments
0	74	46	163	61	0

October 23, 2015 , 3:55 pm
Categories: Cryptography, Government, Privacy, Vulnerabilities, Web Security

NSA’s Divorce from ECC Causing Crypto Hand-Wringing

by Michael Mimoso

The NSA is moving away from Elliptic Curve Cryptography, and cryptographers aren’t buying their reasoning that advances in post quantum computing put ECC in jeopardy.

Read more...

Top Stories

NSA’s Divorce from ECC Causing Crypto Hand-Wringing

October 23, 2015 , 3:55 pm

Disclosed Netgear Router Vulnerability Under Attack

October 8, 2015 , 1:29 pm

[Targeted Attack Exposes OWA Weakness](#)

October 6, 2015 , 10:54 am

[European Aviation Agency Warns of Aircraft Hacking](#)

October 9, 2015 , 11:30 am

[New Android Ransomware Communicates over XMPP](#)

September 3, 2015 , 10:50 am

[New Versions of Carbanak Banking Malware Seen Hitting Targets in U.S. and Europe](#)

September 3, 2015 , 8:57 am

[JavaScript DDoS Attack Peaks at 275,000 Requests-Per-Second](#)

September 28, 2015 , 12:24 pm

[WordPress Jetpack Plugin Patched Against Stored XSS Vulnerability](#)

October 2, 2015 , 9:20 am

[Experian Breach Spills Data on 15 Million T-Mobile Customers](#)

October 2, 2015 , 9:43 am

[NY Health Provider Excellus Discloses Data Breach Dating to 2013](#)

September 10, 2015 , 9:09 am

The Final Say

From Kaspersky Blogs

[On the Avatar set – in China....](#)

Believe me – in China there's plenty to look at. I gave myself a present for my for 50th B-Day and spent a few days there recently. Get ready to say 'wow!' when you see some of the ...

[Read more…](#)

On the trail of Stagefright 2...

In early October, it was announced that a critical vulnerability had been found in the libutils library. Although exploits for newly discovered vulnerabilities take a while to appear 'in the wild', we...

Read more…

Mission: Hacking Grandma. Level: piece of cake

Do you think that you have nothing to hack whatsoever? Bad news, guys: everyone has something hackable!

Read more…

33% of financial organizations prefer react, not p...

The latest research by Kaspersky Lab and B2B International shows that 33% of financial services organizations don't offer customers a secure channel for all of their online payments, despite the fact ...

Read more…

[The story of Maurizio Abba...](#)

The story of Maurizio Abba, who hasn't saved the world yet, but is saving it little by little every day. This is a highly regular and ordinary story. No, no, our hero is a good guy and an excell...

[Read more…](#)

[Threatpost | The first stop for security news](#) The Kaspersky Lab Security News Service Categories[Apple](#) | [Black Hat](#) | [Cloud Security](#) | [Compliance](#) | [Critical Infrastructure](#) | [Cryptography](#) | [Data Breaches](#) | [Featured](#) | [Featured Podcast](#) | [Featured Video](#) | [Google](#) | [Government](#) | [Hacks](#) | [How I Got Here](#) | [Malware](#) | [Microsoft](#) | [Mobile Security](#) | [Podcasts](#) | [Privacy](#) | [Ransomware](#) | [Scams](#) | [Security Analyst Summit](#) | [Slideshow](#) | [SMB Security](#) | [Social Engineering](#) | [Uncategorized](#) | [Videos](#) | [Virtualization](#) | [Vulnerabilities](#) | [Web Security](#)

- [RSS Feeds](#)
- [Home](#)
- [About Us](#)
- [Contact Us](#)

Authors

[Michael Mimoso](#)
[Christopher Brook](#)