

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: CRWD-W03

Hacker Marketing Strategy: How Cybercriminals Promote for Press and Profit



Connect **to**
Protect

Jennifer Leggio

SVP Marketing
Digital Shadows
@mediaphyter



#RSAC

Old School Security Marketing



#RSAC



NETWORKWORLD



Complying with PCI DSS 3.0

Home > LAN & WAN

OPINION

8 Microsoft fixes coming in tomorrow's December Patch Tuesday

* Patches from MadRiva, Debian, Ubuntu * Facebook worm refuses to die * Adobe admits new PDF password protection is weaker, and other interesting reading

RELATED

Oracle emergency patch

Ending with a roar

Fast Forward to 2015



#RSAC



Scooped by Crackas with Attitude (CWA)



#RSAC

Subject: RE: CWA and FBI

Hi [REDACTED],

We wanted to flag a new development for you on the CWA story. We noticed this afternoon that several outlets, including [REDACTED] are reporting the news that CWA hacked the FBI Deputy Director. According to these reports, the hacker group approached several members of the media directly to share screen shots of the alleged hacks.

This was just confirmed by [REDACTED] whom we have been trading emails with as a part of our outreach efforts. [REDACTED] let us know that the phphax Twitter account is a troll account, and that the actor behind it shares the images posted by that account with a select handful of reporters an hour or two before they are made public.

Understanding that CWA has been independently promoting its latest claims among members of the media, we now know that some reporters may have already had access to this information. However, as a result of our outreach, we have positioned ourselves as a resource on the subject – [REDACTED] both let us know that if they cover the story, they would be interested in our insights.

As a note, we were already reaching out to [REDACTED] and will continue to follow up. We will also monitor for any additional coverage, and follow up with other reporters that are covering the story.

Best,
[REDACTED]

Hacker Group Confirmed as Source



#RSAC

MOTHERBOARD Watch Machines Discoveries Space Futures Gam

One of the members of the group, known as Cracka, told Motherboard that they have now hacked into an email account belonging to the FBI Deputy Director [Mark Giuliano](#). The hackers also boasted about it on Twitter.

anddddddd here we go again Imfao IF YOU OWN A AOL ACCOUNT YOU CAN JOIN THE GOVERNMENT RIGHT NOW!! [cracka](#) November 1, 2015

Cracka said that they got into a Comcast email that's under Giuliano's wife's name and provided a series of screenshots to prove they got access to the account. The hackers declined to reveal how they cracked the account, but said it was "easy." The screenshots, however, don't conclusively prove the hack, and Motherboard wasn't able to confirm it independently.

An FBI spokesperson declined to neither deny nor confirm that Giuliano's email got breached.

"We do not have anything to say on the matter at this time," the spokesperson Jillian Stickels said in an email.

The teenager also said they found Giuliano's cellphone in the email account's contact

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

NEWS PRODUCT REVIEWS BLOGS SC CONGRESS SC EXTRAS

SC Magazine > News > 'Crackas with Attitude' say they're at it again; claim hack of FBI deputy's email

Teri Robinson, Associate Editor
Follow @TeriRnNY

November 05, 2015

'Crackas with Attitude' say they're at it again; claim hack of FBI deputy's email

Share this article: [f](#) [t](#) [in](#) [g+](#) [v](#) [e](#) [p](#)

The teen hackers who infiltrated the email account of CIA Director John Brennan said they are prying into the accounts of other government officials, most recently claiming to hack an email account of FBI Deputy Director Mark Giuliano.

The group, which calls itself "Crackas With Attitude" and is under investigation by the FBI, has bragged about its exploits on Twitter. One member, called Cracka, sent screen shots of the alleged hack to Motherboard and claimed to have called a mobile number belonging to Giuliano and was told by a



The teen hackers who infiltrated the email account of CIA Director John Brennan claimed to have hacked an email

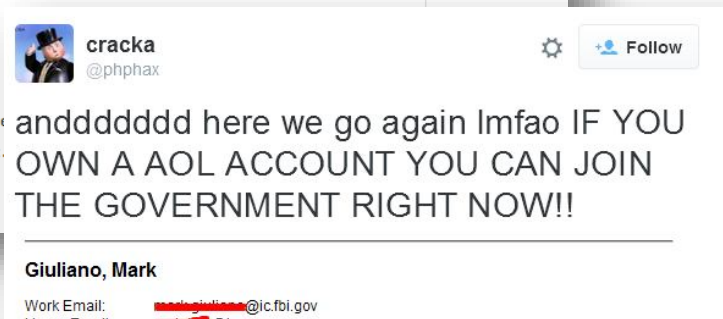
“He Went Ahead and Contacted the Media...”



#RSAC

```
0011  PASTEBIN  + new paste  trends  API  tools  faq  search...
0000
1010

and money, yet he ignored Incursio's advice.
38. (e)
39.
40. (iii)
41. You see? He claimed we joined for fame and money. But what do you know? He went ahead and contacted the media, not waiting for them to
   contact us first. And we're fame whoring? Sure, lul.
42. (e)
43.
44. (iv)
45. He claimed we were doing all of the interviews for fame. However he done the first voice interview and other typed interviews, showing we
   never was doing interviews first for "fame".
46. (e)
47.
48. (v)
49. Now Cracka tried to claim he got access by an exploit to make CWA look skilled. He gained acc
   other info he got from SE'ing his ISP with the info he got from AOL. He never used an exploit.
50. (e)
51.
```



~~Un~~common Practice



#RSAC



Brian Krebs
Krebs On Security



Steve Ragan
CSO Online

Why?



#RSAC

THE HACKER ECONOMY

Simplified Mix for Successful Business



#RSAC







Product Launch / Addressing Pain



#RSAC

HOME ESCROW LAUNDRY F.A.Q. CONTACTS

News

YOU ARE HERE: Home / News / News / New design

New design

2

Posted by admin on May 19, 2014 in News

The site was completely remade. New design and convenient forms of services.

2 Responses

Escrow & Laundry

Escrow & Laundry Escrow & Laundry New design The site was completely remade. New design and convenient forms of services. We reduced fees for our services We lowered the fee from 5% to 2%. We added a laundry service We changed the name from Escrow system to Escrow & Laundry. We added a Laundry service. Automated escrow system Today we set up a fully automated escrow system. Now your process will be processed within 6 hours. Thank you for choosing us! Opening We are pleased to announce an opening of an Escrow system & Laundry. We are ready to help you keep your money at any disputed transactions on the Tor network. Our main...[Read more](http://vur2ear4amgyacaf.onion/?p=166)

Leave a Reply


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

Name

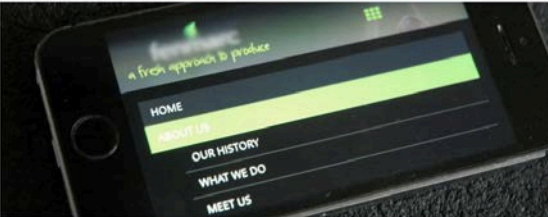
Email

Website

Comment

A fresh approach to produce

HOME ABOUT US OUR PRODUCTS NEWS JOBS CONTACT US



HOME
ABOUT US
OUR HISTORY
WHAT WE DO
MEET US

LATEST NEWS

- Vegetable & Quinoa Soup Kit Good Choice Quality Food Awards Winner November 5, 2015
- Head shave & leg waxing helps Macmillan Cancer fundraising exceed £1330 November 5, 2015
- Macmillan coffee morning September 28, 2015
- Fennmarc continues to sponsor The Harvest August 28, 2015
- Fennmarc supports sports festival July 30, 2015

New Website Launch

4 Jun | by Fennmarc | Latest News

Share this: [f](#) [t](#) [g+](#) [p](#)

Fennmarc are pleased to have launched our new website which is a fully responsive design meaning you can use it on your smartphone, tablet or PC.

We have created a website which is informative about our business and products but which also provides a good insight into the company values and how we work as a team.

The website features a jobs post device which allows us to upload information about current posts available. These are searchable between our two locations.

If you have any feedback or comments about the new website, please feel free to contact us via the [enquiry form on the contact page](#).

Thought ...Leadership?



#RSAC

WR ~ w0rm r3view

Classical Tile Journal Mosaic Slide Panel Photo Album Chronology

Move faster. Lower IT costs.
Introducing the simplest way for IT to securely deliver and manage apps and data.
[Watch Webinars Now](#)

founded in 1989 and is engaged solutions for virtualization, but organization of cloud computing hypervisor open source ... wide

Hunter Home
Login

Hunter Exploit Kit. Security Fail.
For the first time undertook to write a review about malware subjects, the author urged the package with the time, in the meantime, the network already

WhatsApp Open Security Write Up
A strange story is with the program from WhatsApp. Rugbounty kind of project is the property of FaceBook but December 11, 2014 I did not get an

The history of hacking bbc.co.uk
The story begins with the fact that my friend was gone respectable number of meathalls with uchetki on bte-exchange. As it turned out, he kept his login and

Recent searches Help **£ GBP** Log in

flights hotels car hire

Home > Blogs

Blogs

Bluewiner reinvents corporate travel spend with new online business travel service

Five New Partners Invest £128 Million in Bluewiner

ifs ProShare
Award winning employee share scheme

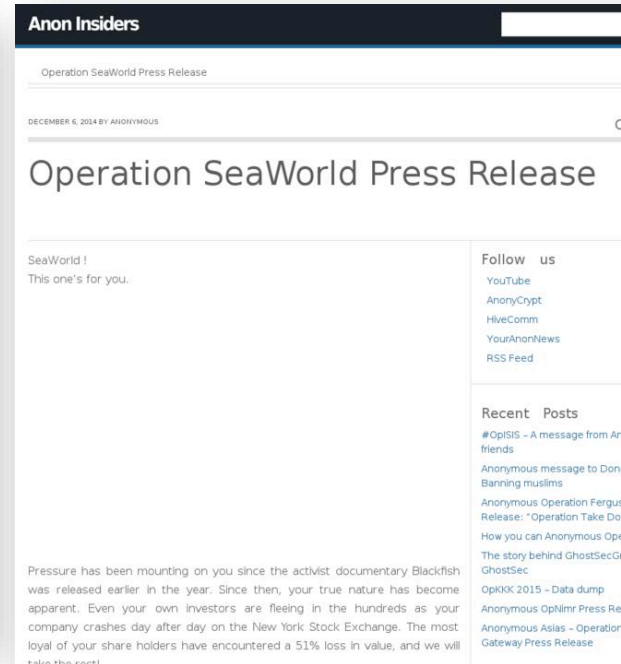
Bluewiner announced Technology Fast 50 Winner and EMEA Fast 500 winner

Bluewiner to be first metasearch with capacity to display and sell tickets using the NDC standard

Gareth wins prestigious WTM World Travel Leaders Award

Alexa, find me a flight through Bluewiner

Press Releases – Common for Hacktivists



“Evolution” of the PR Rep

#RSAC



moneymoney2020 2014-06-18 16:10:06 #1

Member
Registered: 2014-01-25
Posts: 204

Vendor "bannedbooks" is scammer.. Here is the story

Bought his listing for Evo lottery to double you bitcoin. Rules were.. if you have last 3 evo order number ODD or EVEN or if u have 3 of kind in your order number. You Win, if not you lose.. when some one win he will cancel the order and send the winning to your btc address with proof from block-chain.

So i played for 0.005 i lose. and i release the escrow. Few days later i played again for 0.02 and i win. I had 3 ODD number. So its time to pay up. This is what i get from him.

bannedbooks
Look man, this is en
your additional 0.02

With some link to li
Me----> common m
be fair and pay up..

bannedbooks
No can do man, eve
He spouse to declin
Report Him to admin

Offline

Public Relations

Hold up. Evolution doesn't even allow lotteries to begin with Mainly due to them being too

Last edited by Scattermind (2014-05-18 16:37:57)

Evolution's PR Rep. Boogie Contact Information: BoogieEvoPR@lelantos.org
PGP key: <http://pastebin.com/jw0Z4usm>

From: lol
Registered: 2014-01-14
Posts: 2,251

Scattermind 2014-06-18 16:37:20 #2

Public Relations

Hold up. Evolution doesn't even allow lotteries to begin with Mainly due to them being too easy to abuse.

Last edited by Scattermind (2014-05-18 16:37:57)

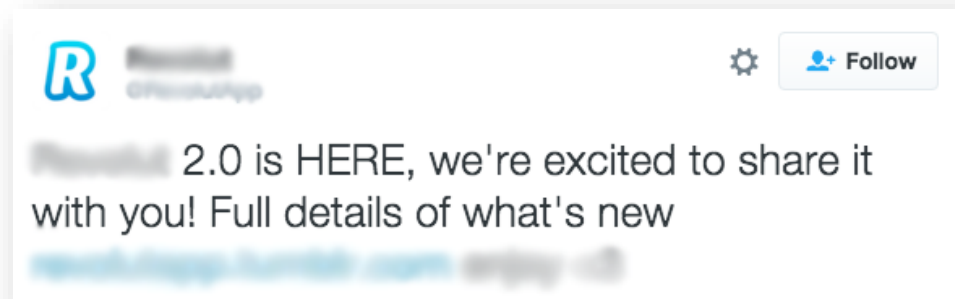
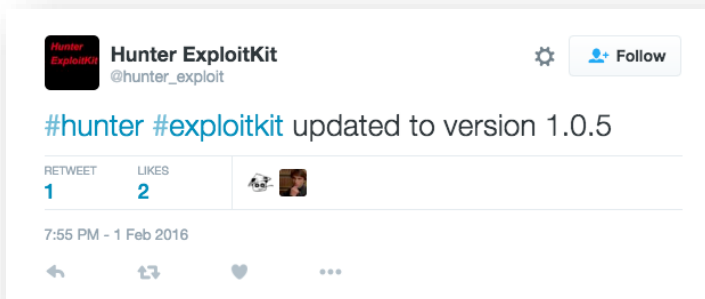
Evolution's PR Rep. Boogie Contact Information: BoogieEvoPR@lelantos.org
PGP key: <http://pastebin.com/jw0Z4usm>

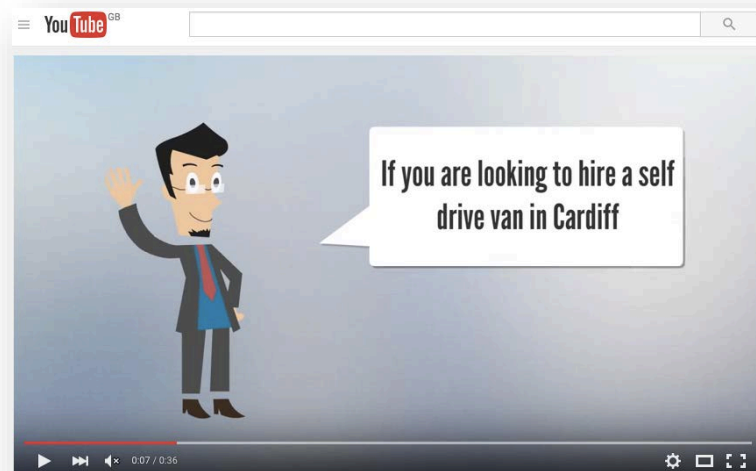
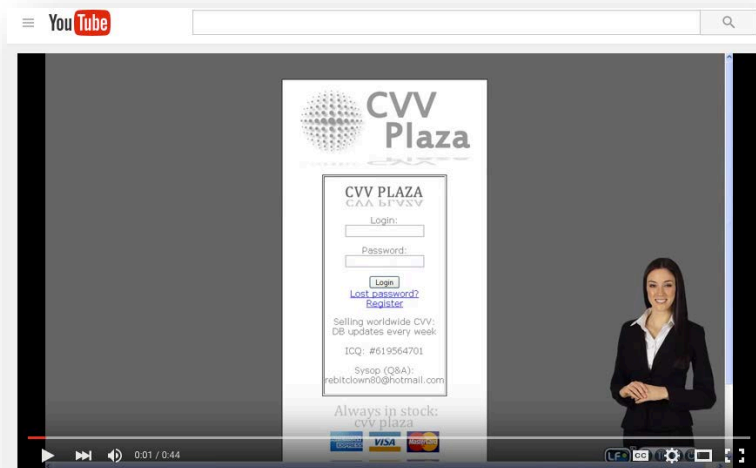
From: lol
Registered: 2014-01-14
Posts: 2,251

Social Media (in this case, Twitter)



#RSAC





Scamming the Scammers



#RSAC

Name	Price	V
10 000 Real Europe High Retention Youtube views Buy Youtube Views From The Most Trusted Social Media Supplier on deep web. Increase views on youtube. Get more YouTube views easily and safely with our service. We've helped promote over 100,000 v ...	0.36929226 BTC	
Facebook Services - 2 000 Real Facebook Likes (Web Page) Better marketing of your brand - This campaign brings with it the possibility of marketing your products worldwide. The best part is that you do not have to increase your spend on advertisements, mar ...	0.52135378 BTC	

Giveaways and Incentives



#RSAC

and Vendor Reviews » ### Anon sim card / Anon credit card FREE SAM

2015-05-20 09:25:10

Anon sim card / Anon credit card

Note: I offer 5 FREE sample off sim card for first client.

[] Anon Sim Card

Anon sim card with 5k credit charged. i can charge it more for you PM me)
6 month expire date, after you have to clear it.
You can charged it by credit card on clear net.

[] Anon credit card

<http://nucleuspf3zq7o6.onion/item/6beb-dfc9ab9efa>
Anon physical credit card with IBAN and pin.

You can use it in ATM or in store.
You can charged it by credit card or IBAN on clear net. Or i can charged it fo
Work great with paypal.

No registration:

- you can charge it 2500k per year
- you can withdraw 250k per year
- you can shop 1000k per day

After registration:

- you can charge 5000k per month
- you can withdraw 500k per day, 4000k per month.
- you can shop 2500k per day

I can do the registration for you, PM me

Special Offers

Try three of our **[REDACTED]**
must-have products free*
when you spend £40+

Includes:

- High Impact mascara 4ml
- Moisture Surge Extended Thirst Relief 15ml
- Smart Custom Serum 10ml

Enter code: **MUSTHAVE**

SHOP NOW



Or Your Money Back



#RSAC

This is a limited offer for a pack of 5 VISA CCN's/CVV's for the digital carder. When I pulled these from work they didnt have full DOX info attached, so there are no account numbers or passwords like with my other offers.

These include

- Name on Card
- Card Number
- CVV
- Expiration Date

These are dual-linked cards, meaning one card can access both debit accounts + a line of credit.

Get them while they last, only 4 packs available, Only \$10 - Thats just \$2.00 a card!!!

Please include your public PGP key with order so I can encrypt the data before sending it to you.

I OFFER A FULL REPLACEMENT GUARANTEE. IF FOR ANY REASON A CARD COMES BACK DECLINED LET ME KNOW WITHIN 48 HOURS OF PURCHASE AND I WILL GLADLY REPLACE IT! These are 100% guaranteed to work because I get them straight from the source where I work, and before I send them to you, there is no reason for anyone to suspect they are stolen. This is also why Im able to offer these so cheap, no middleman.

You might ask why Id rather sell these for pennies instead of carding and cashing them out myself - the answer is simple - Im too chickenshit. Im the first person scrutinized when these come up stolen, and if I was cashing them out instead of selling them I would be easy to catch, meaning Id lose my job, my home, my wife, and my children. Thats just entirely too much risk for me. But for you, the risk is minimal, since you are not attached to any businesses with access to these, or the cardholders themselves.

FLORIST'S GUARANTEE

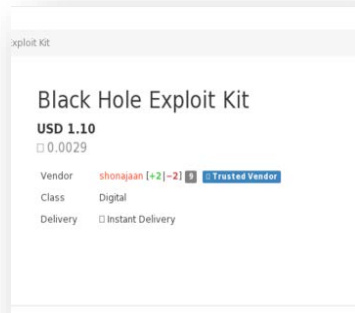
Florist and Greenhouses - Our Guarantee



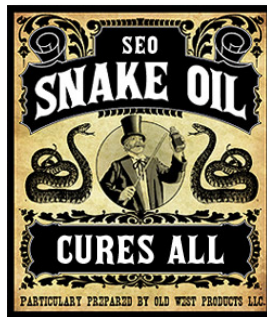
Our Promise: If you are not completely satisfied with any product we deliver, we will be more than happy to help resolve any problem. We guarantee freshness for a complete seven days.

Please notify us within 48 hours of delivery of your dissatisfaction and we will be happy to issue a complete refund, or if you wish, a replacement of the item delivered. If you notify us after 48 hours of delivery, we can send a replacement of your order and will pick up the original delivery. Please note, our guarantee extends to both the deliveries we make, and orders that may be called to our affiliate Florists.

Why Hackers Market



+



+



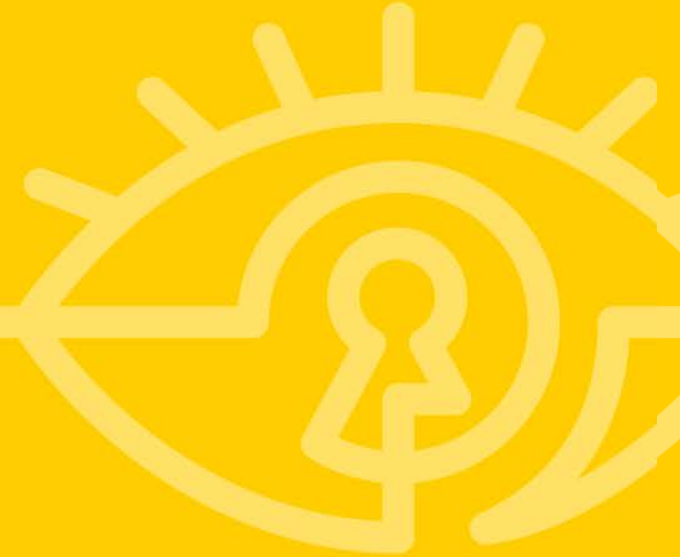
=



So What?



- Vendor mission is to protect and profit
- Attacker mission is to profit – at all costs
- Success of the missions is predicated on ability to market and sell
- Marketing can negate OPSEC – providing more insight into offerings and motives
- Vendor *marketers* must now also outsmart attackers
- The rules will never apply



Thank You.

jennifer@digitalshadows.com
@mediaphyter