

The trade in security exploits: Free speech or weapons in need of regulation?

Christopher Soghoian

Presentation to VB2012, Sept 26, 2012





First: a disclaimer

These opinions are my own, and do not reflect the official position of the ACLU.

(I've only been there 3 weeks)



The Legitimate Vulnerability Market

Inside the Secretive World of 0-day Exploit Sales

Charlie Miller, PhD, CISSP
Independent Security Evaluators
www.securityevaluators.com

May 6, 2007

3-7615/360

282643


Date September 08, 2006

Pay Amount ***\$50,000.00***

Pay ****FIFTY THOUSAND AND XX / 100 DOLLAR****

To The Order of CHARLES MILLER

Authorized Signature




“The government official said he was not allowed to name a price, but that I should make an offer.

And when I [set a price of \$80k], he said OK, and I thought, 'Oh man, I could have gotten a lot more.

”

- Charlie Miller, Interview with SecurityFocus,
2007





“I don't think it fair that researchers don't have the information and contacts they need to sell their research.”

- Charlie Miller, Interview with SecurityFocus, 2007

“Legit” bug sale options in ‘99: Vendor bounties



\$500



\$500-1337

“Legit” bug sale options in ‘99: subscription services



\$500 – \$20,000




Community debate:

Responsible disclosure vs. full disclosure



Alex Sotirov and Dino Dai Zovi, CanSecWest,
2009



“Vendors have been getting a freebie for a while, why would I want to sit down and volunteer to find a bug in someone’s browser when it’s a nice, sunny day outside?”

- Dino Dai Zovi, Interview with SC Magazine, 2009



ENDGAME

Aaron,

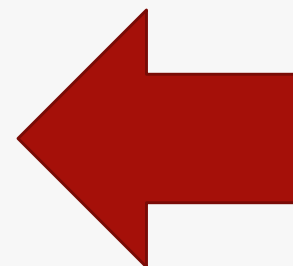
Chris wanted me to pass this along. We've been very careful NOT to have public face on our company. Please ensure Palantir and your other partners understand we're purposefully trying to maintain a very low profile. Chris is very cautious based on feedback we've received from our government clients. If you want to reconsider working with us based on this, we fully understand.

I'll see you at 1300 today. Thanks

John

Please let HBgary know we don't ever want to see our name in a press release.

--
Chris Rouland
chris@endgames.us



Subscriptions – Tier 1



Maui

- Original vulnerability research – General, Indigenous and Directed
- Exploit toolkit development
- Productization

Cayman

- Global Internet vulnerability analytics
- Infection status
- Multi-feed correlation

Corsica

- Application-layer, global vulnerability assessment
- Zero-day and public vulnerability correlation



What was “No More Free Bugs” really about?

**Google and Microsoft will never be able to
outbid the US Government.**




Fast forward: 2012

'0-day exploit middlemen are cowboys, ticking bomb'



By [Ryan Naraine](#) for Zero Day | February 16, 2012

 [Follow @ryanaraine](#)

Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)



Andy Greenberg, Forbes Staff


Covering the worlds of data security, privacy and hacker culture.

[+ Follow](#) (553)

SECURITY | 3/21/2012 @ 9:08AM | 128,694 views







He says he takes a 15% commission on sales and is on track to earn more than \$1 million from the deals this year.

“I refuse to deal with anything below mid-five-figures these days,” he says.

- The Grugg, quoted in Forbes, March 2012



Chaouki Bekrar and the VUPEN team



“We wouldn’t share this with Google for even \$1 million.

We don’t want to give them any knowledge that can help them in fixing this exploit or other similar exploits. We want to keep this for our customers.”

- Chaouki Bekrar, Interview with Forbes, Mar 2012



“We don’t work as hard as we do to help multibillion-dollar software companies make their code secure.”

“If we wanted to volunteer, we’d help the homeless.”

- Chaouki Bekrar, Interview with Forbes, Mar 2012

**Secrecy surrounding 'zero-day exploits'
industry spurs calls for government oversight**

The Washington Post

By James Ball, Published: September 1



Only available for trusted countries and Government agencies

Because of the sensitive nature of the information provided through this service, VUPEN has built **transparency** and defined **very strict eligibility criteria** for participants.

Access to this service is possible to:

- Government organizations only (Law Enforcement and Intelligence agencies) which:
Are in countries members or partners of NATO, ANZUS and ASEAN organizations
And are fully meeting the requirements of our "Know Your Customer" program



NATO Partners include:

Azerbaijan, Turkmenistan, Egypt, Morocco, Qatar and Pakistan.

ASEAN Members include:

Indonesia, Burma and Vietnam.



Christopher Soghoian @csoghoian

11 Sep

VUPEN: We don't sell security exploits to govs of Lebanon or Belarus. We are happy to sell to Turkmenistan though.

bit.ly/mjwsWt

Details



Chaouki Bekrar VUPEN @cBekrar

11 Sep

[@csoghoian](#) We don't even know where that country is, anyway if you are not happy write to European Union and the US to add them to the list

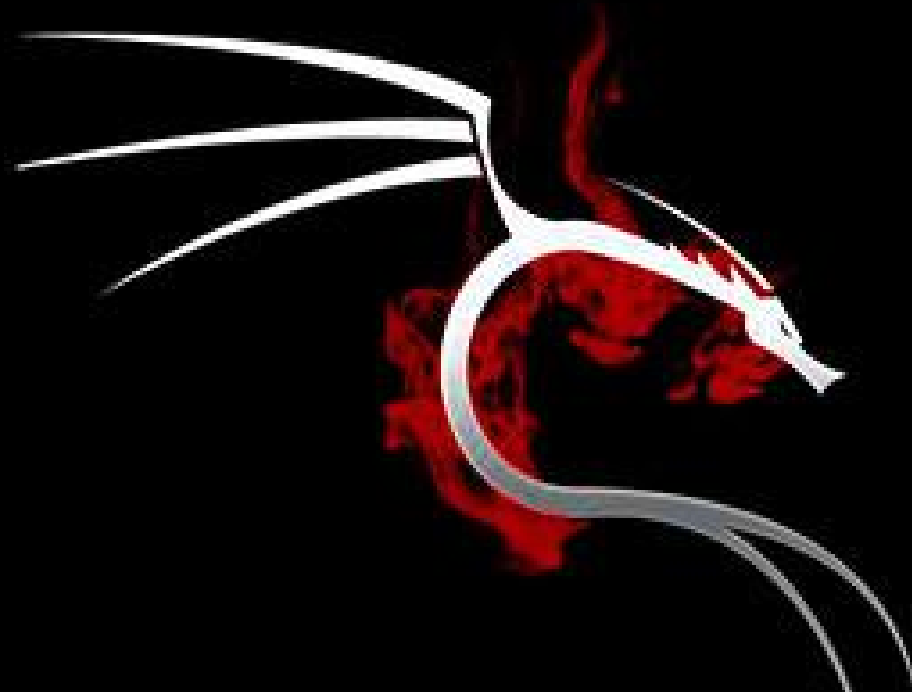
Details [← Reply](#) [↻ Retweet](#) [★ Favorite](#)



Simultaneous developments elsewhere



Martin J. Muench



<< back|track
network security suite.

Backtrack.com

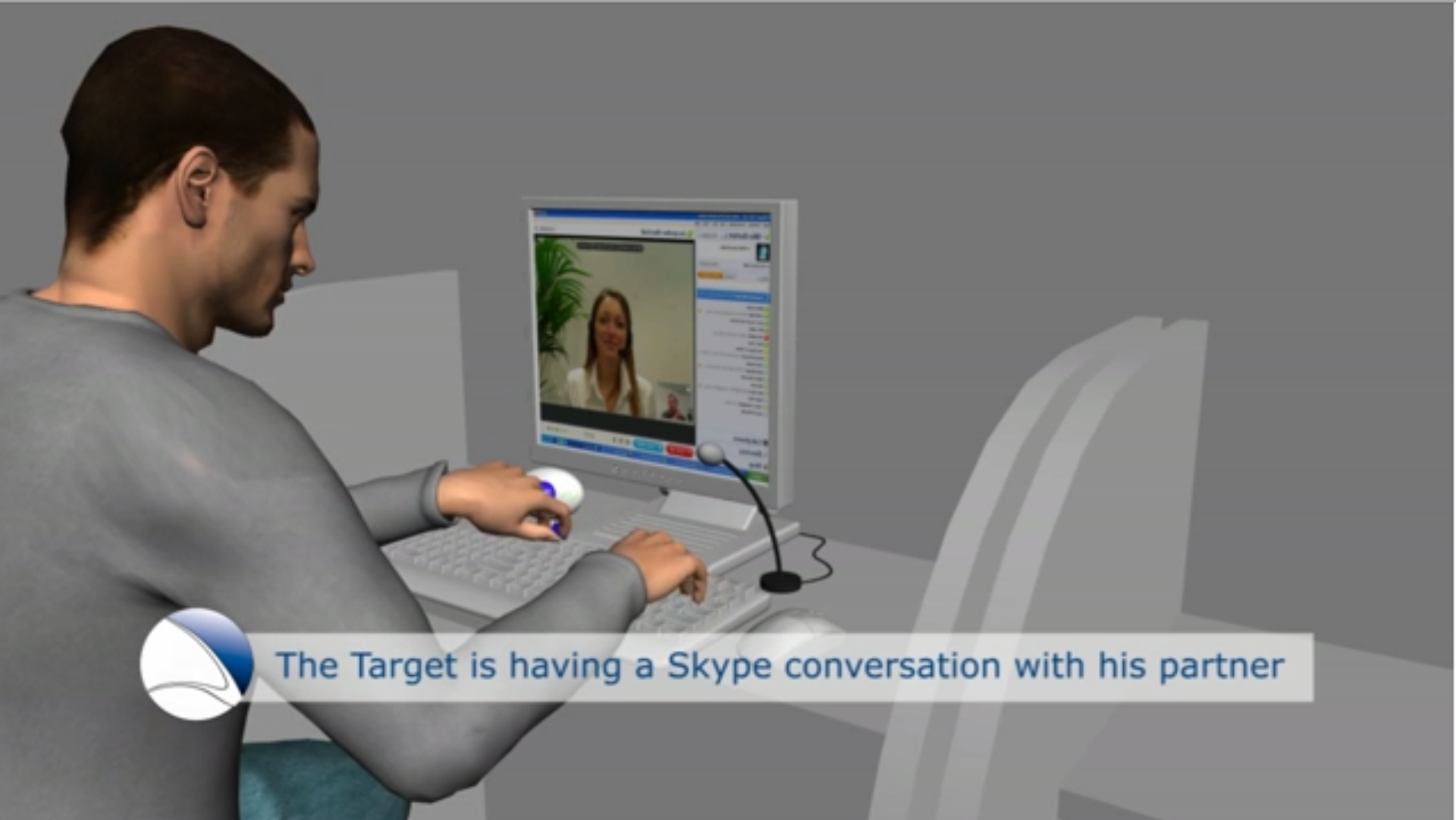


FINFISHER™

IT INTRUSION

GOVERNMENTAL IT INTRUSION

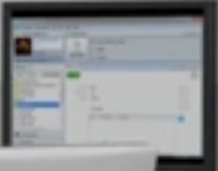
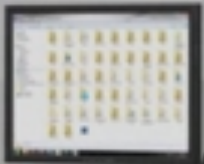
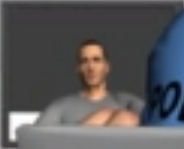
AND REMOTE MONITORING SOLUTIONS



The Target is having a Skype conversation with his partner




Hi, how are you
Any news regard_



POLICE



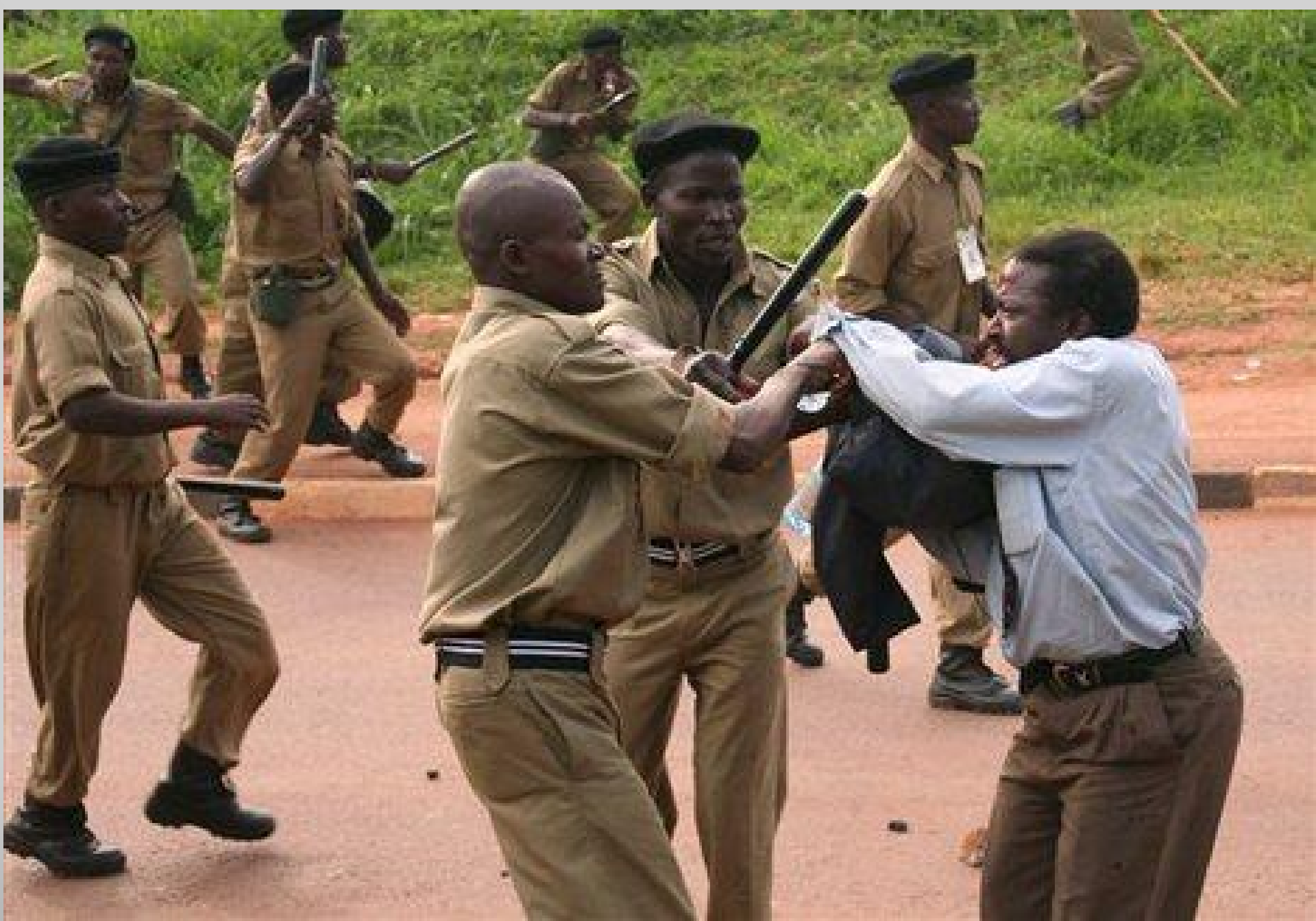
The Headquarter has full access to the Target System



Gamma Group sells FinSpy to governments only to monitor criminals and it is frequently used “against pedophiles, terrorists, organized crime, kidnapping and human trafficking.”

- Martin Muench, New York Times interview,
Aug 2012









**GAMMA INTERNATIONAL
UK LIMITED**
Europe • Asia • Middle East • Africa

TO: State Security Investigation Department
Cairo
Egypt

OFFER NO. 0610-FF-GUK-061
DATE Tuesday June 29, 2010
CUSTOMER ID EGY-SSD
PAGE 6 / 12

A	Remote Intrusion Solution
1	FinSpy
1.1	FinSpy Software
1.1.1	FinSpy Proxy License FinSpy Master License FinSpy Generation License
1.1.2	FinSpy Agent License (per client)
1.1.3	FinSpy Activation License: - Windows - OSX (Q4/2010)
	Including Finline Support: FinSpy Update & Upgrade (Year 1)


UK firm denies 'cyber-spy' deal with Egypt

By Stephen Grey

File on 4, BBC Radio 4

The files from the Egyptian secret police's Electronic Penetration Division described Gamma's product as "the only security system in the world" capable of bugging Skype phone conversations on the internet.

They detail a five-month trial by the Egyptian secret police which found the product had "proved to be an efficient electronic system for penetrating secure systems [which] accesses email boxes of Hotmail, Yahoo and Gmail networks".

AUGUST 13, 2012, 9:00 AM |  18 Comments

Elusive FinSpy Spyware Pops Up in 10 Countries

By NICOLE PERLROTH

Australia, Bahrain, Brunei, Czech Republic, Estonia, Ethiopia, Indonesia, Qatar, Latvia, Mongolia, the Netherlands, Turkmenistan, United Arab Emirates and United States.

European Union Bans Exports to Syria of Systems for Monitoring Web, Phones

By Vernon Silver - Dec 1, 2011 10:57 AM PT



IRAN

EU bans export of Internet surveillance gear to Iran

© fotolia

New measures would forbid EU companies from selling monitoring equipment to the Islamic Republic. Previously, companies like Creativity Software and Nokia Siemens Networks have been accused of selling spyware to Iran.

Crackdown on sale of UK spyware over fears of misuse by repressive regimes

Decision to stop sale of spying software to Egypt puts other deals with repressive regimes in doubt

Jamie Doward

The Observer, Saturday 8 September 2012

'No spyware for repressive regimes': Germany's Foreign Minister speaks out against surveillance tech exports

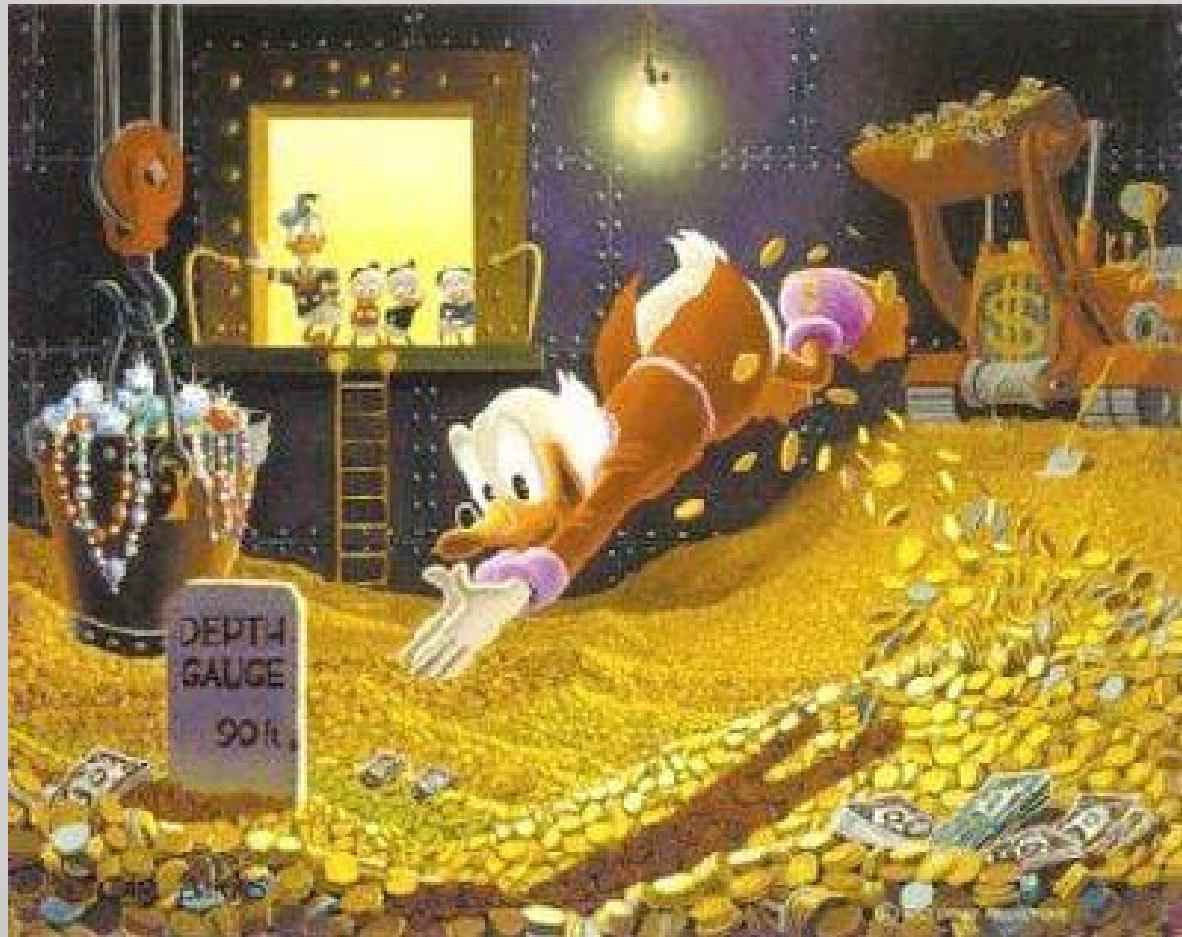
BY: [GEORGIA ARDIZZONE](#) ON: 19-SEP-2012

SHARE: [!\[\]\(5eb1325dfdc3f1cad8426726c0db51cd_img.jpg\)](#) [!\[\]\(312638b5686dbc3f6ff8424fd17b3fb2_img.jpg\)](#) [!\[\]\(88e39a015d99d67943a7ca963c140a17_img.jpg\)](#)



The exploit and surveillance industry has a bit of an image problem.






The first rule of exploit selling is:






Others keep talking though.



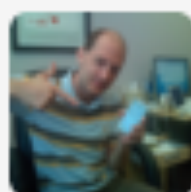
“I do it for money, because I like it, and because most of the time I don't need to wear pants. I spend approximately no seconds of any day worrying about the imaginary ethical implications of every little thing I do, and I am not particularly unique.”

- Ben Nagy, post to ‘dailydave’, 2012



“Given that a can of fizzy drink or a car battery can be abused and used as an implement of torture it is of no surprise to anyone if our products can be abused too.”

- Martin Muench, email interview with ABC Radio (Australia), September 2012.



Charlie Miller 0@xcharlie

4 Aug


@csoghoian people should be free to try to avoid being spied upon, but people should also be free to write and sell exploits

[Details](#)



**Regulate sales of exploits =
Limit freedoms**





Politicians will take an interest in exploit sales and call for regulation



“I think that the zero-day exploit market should be regulated. We're selling bullets and computers are the guns, there's no doubting that.”

- Adriel Desautels, post to 'dailydave', August 2012




**If the industry wants to avoid regulation, it
needs to regulate itself.**

THE FOLLOWING **PREVIEW** HAS BEEN APPROVED

ALL AUDIENCES

BY THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.

THE FILM ADVERTISED HAS BEEN RATED

R	RESTRICTED	
	UNDER 17 REQUIRES ACCOMPANYING PARENT OR ADULT GUARDIAN	
STRONG GRAPHIC VIOLENCE, SEXUALITY, NUDITY AND LANGUAGE		


©

www.filmratings.com

www.mpa.com



NATIONAL
DO NOT CALL
REGISTRY



If the Grugq remains the poster child for the industry, the response from Washington DC and Brussels will not be pretty.



Thank you

csoghoian@aclu.org