

The Tale Of Phineas Fisher



Who Am I

Jake~

@CyberPunkJake

JAKE@LOWLIFE.TECH

✦ Member of the ORG (@OpenRightsGroup) supporter Council

✦ Organiser for ORG Birmingham (@OpenRightsBrum)

✦ Co-Founder of @DC44121

✦ Club 2077

First of all

What do two titans of the surveillance industry, a bitcoin broker, a police union, a national bank and a leading political party all have in common?



Gamma Industries

"Hacking is a tool.

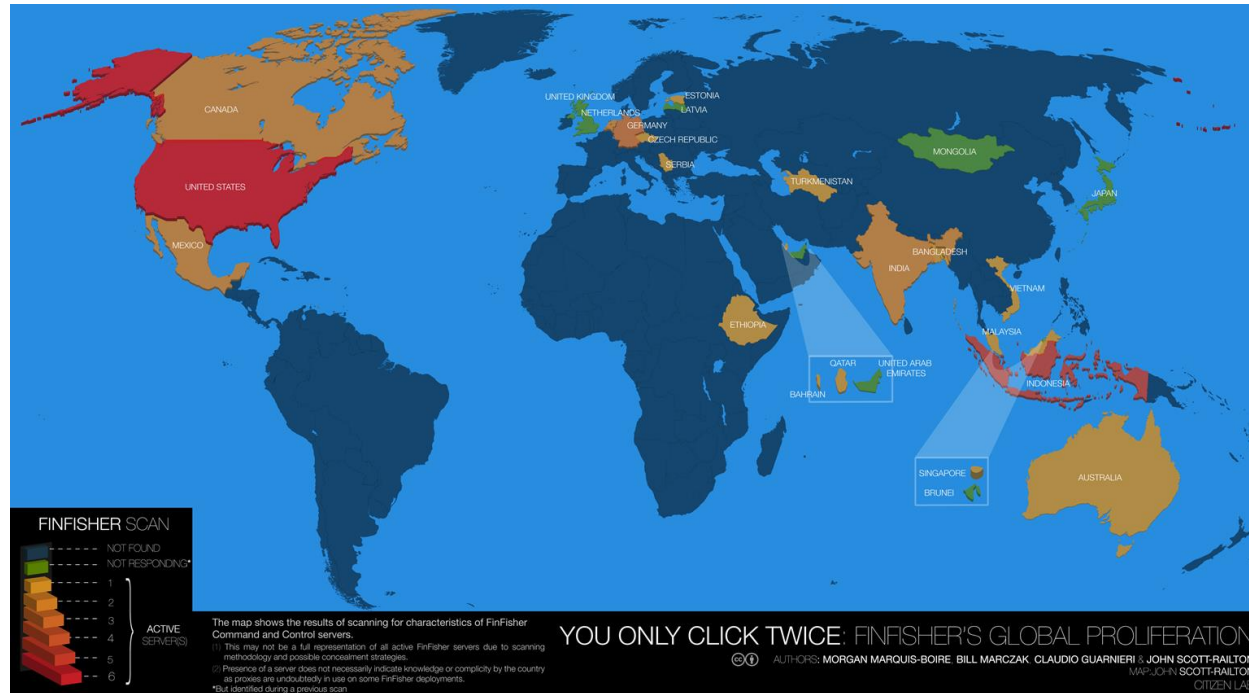
*It's not selling hacking tools that makes Gamma evil, It's who their customers are targeting
and with what purpose that makes them evil."*

-Phineas Fisher



FINFISHER™
EXCELLENCE IN
CYBER INVESTIGATION

GI - *why?*



GI - Chapter 1 The Support Site

"In the case of FinFisher what led me to the vulnerable finsupport.finfisher.com was simply a whois lookup of finfisher.com which found it registered to the name."

-Phineas Fisher



FINFISHER™
EXCELLENCE IN
CYBER INVESTIGATION

GI - Chapter 2 Escalation & Pivot

*“Finsupport was running the latest version of Debian with no local root exploits”
-Phineas Fisher*



FINFISHER™
EXCELLENCE IN
CYBER INVESTIGATION

GI - Prologue

The **gateam/** folder is a copy of what appeared to be a QA server with copies of all their Finspy Mobile malware.

www/FinFisher folder – Where customers downloaded their products after purchase. Encrypted ZIPs and GPG files. Never been decrypted.

The **www/GGI** folder is a copy of <http://finsupport.finfisher.com/> dump of the database which held all the information around customer support tickets.



FINFISHER™
EXCELLENCE IN
CYBER INVESTIGATION

GI-Prologue

Bahraini group, in support requests they ask for help setting up a website targetting activists in 14 Feb"

-Phineas Fisher

Intelligence-Security Agency of Bosnia and Herzegovina

SSNS - NBSZ Hungary secret service

Technical engineer for KLPD (dutch police)

PCS Security Pte Ltd



FINFISHER™
EXCELLENCE IN
CYBER INVESTIGATION

Hacking Team

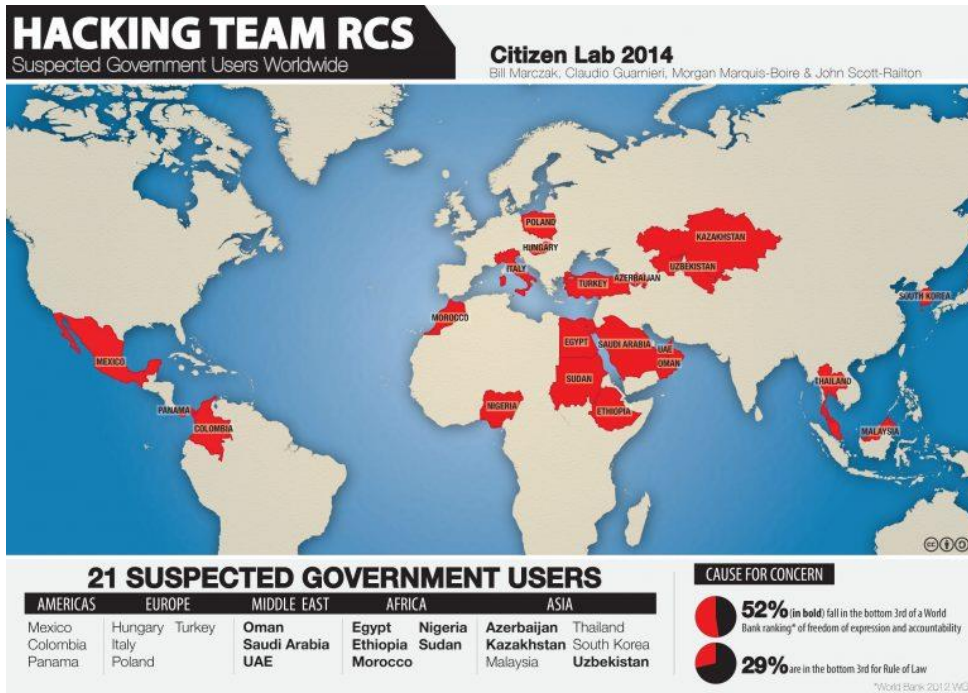
“Hacking Team had very little exposed to the internet. For example, unlike Gamma Group, their customer support site needed a client certificate to connect.

A mail server, a couple routers, two VPN appliances, and a spam filtering appliance.”

-Phineas Fisher

]HackingTeam[

HT - why?



HT - Chapter 1 Getting In

Hacking Team's Public IP range:

```
inetnum:      93.62.139.32 - 93.62.139.47  
netname:      FASTWEB-HT  
descr:        HT public subnet
```

]HackingTeam[

“I had three options”

A) 0day in Joomla?

B) 0day in postfix?

C) 0day in an embedded device?

*“Oday in an embedded device seemed like the easiest option
and after two weeks of work reverse engineering.*

I got a remote root exploit.”

- Phineas Fisher

C) Oday in a SonicWall VPN appliance

~~A) Oday in Joomla~~

~~B) Oday in postfix~~

HT - Chapter 2 Listening

"Now inside their internal network, I wanted to take a look around and think about my next steps"

-Phineas Fisher

Remote Control System

The hacking suite for governmental interception.

Da Vinci

]HackingTeam[

HT - Chapter 2 Listening

"Their insecure backups were the vulnerability that opened their doors."

-Phineas Fisher

]HackingTeam[

2.3 SAN (Storage Area Network) primaria

La tabella seguente illustra le caratteristiche della SAN primaria (Equallogic PS4000).

Equallogic PS4000	
Slot	16
NIC(s)	6
HD(s)	16 x 9.31.51 Gb SATA 7,200 rpm
Indirizzi IP	19.2.168.130.103 (iSCSI)
	19.2.168.130.104 (iSCSI)
	19.2.168.200.12 (mgmt.)

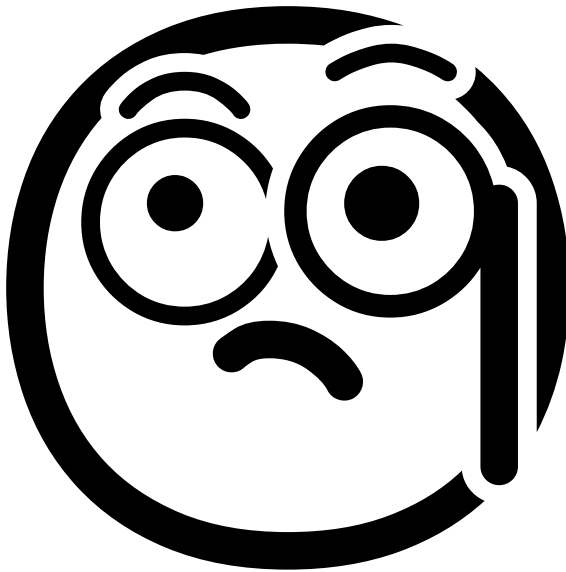
2.4 SAN (Storage Area Network) di backup

La tabella seguente illustra le caratteristiche della SAN di backup (Dell MD3000).

Dell MD3000	
Slot	14
NIC(s)	4
HD(s)	8 x 136.73 Gb + 5 x 419.87 Gb SAS 15 rpm
Indirizzi IP	19.2.168.130.101 (iSCSI)
	19.2.168.130.102 (iSCSI)
	19.2.168.200.10 (mgmt.)
	19.2.168.200.11 (mgmt.)

]HackingTeam[

HT - Chapter 3 From backups to domain admin



HT - Chapter 3 From backups to domain admin

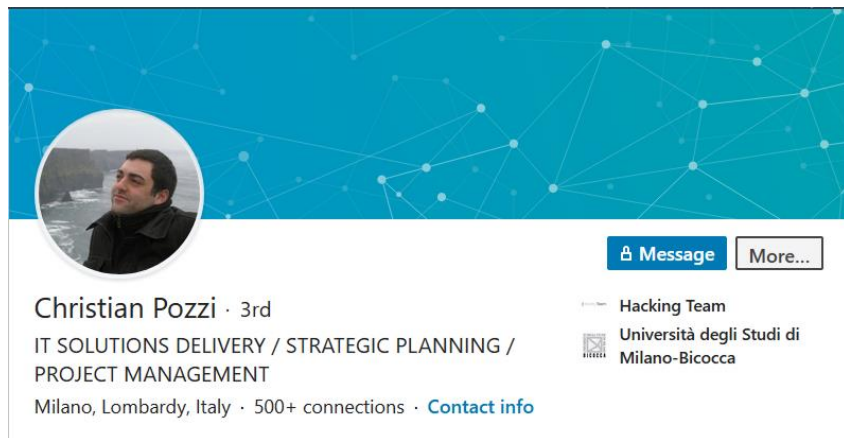
```
HACKINGTEAM BESAdmin      bes32678!!!
HACKINGTEAM Administrator uu8dd8nndd12!
HACKINGTEAM c.pozzi        P4ssword      <---- lol great sysadmin
HACKINGTEAM m.romeo        ioLK/(90
HACKINGTEAM l.guerra        4luc@=.=
HACKINGTEAM d.martinez      W4tudul3sp
HACKINGTEAM g.russo         GCBrs0705!
HACKINGTEAM a.scarafile     Cd4432996111
HACKINGTEAM r.viscardi      Ht2015!
HACKINGTEAM a.mino          A!e$$andra
HACKINGTEAM m.bettini       Ettore&Bella0314
HACKINGTEAM m.luppi         Blackou7
HACKINGTEAM s.gallucci      159i8m4o!
HACKINGTEAM d.milan         set!dob66
HACKINGTEAM w.furlan        Blu3.B3rry!
HACKINGTEAM d.romualdi      Rd13136f@#
HACKINGTEAM l.invernizzi    L0r3nz0123!
HACKINGTEAM e.ciceri        202571&2E
HACKINGTEAM e.rabe          erab@4HT!
```

HT - Chapter 3 From backups to domain admin

Name	Last modified	Size
⤴ Go to parent directory		
Amministrazione/	06-Jul-2015 04:42	-
Client Wiki/	06-Jul-2015 04:41	-
Confluence/	06-Jul-2015 03:52	-
FAE DiskStation/	06-Jul-2015 04:46	-
FileServer/	06-Jul-2015 04:33	-
KnowledgeBase/	06-Jul-2015 05:04	-
audio/	06-Jul-2015 08:40	-
c.pozzi/	06-Jul-2015 04:03	-
git/	06-Jul-2015 05:28	-
gitlab/	06-Jul-2015 04:53	-
m.romeo/	06-Jul-2015 04:12	-
mail/	06-Jul-2015 21:51	-
mail2/	06-Jul-2015 21:05	-
mail3/	06-Jul-2015 21:49	-
rds-dev\share/	06-Jul-2015 04:53	-
Exploit_Delivery_Network_android.tar.gz	06-Jul-2015 06:43	797.1M
Exploit_Delivery_Network_windows.tar.gz	06-Jul-2015 06:42	716.5M
HackingTeamDataDump_archive.torrent	06-Jul-2015 03:49	2.4K
HackingTeamDataDump_files.xml	02-Dec-2018 19:19	55.9M
HackingTeamDataDump_meta.xml	17-Aug-2018 02:17	816.0B
__ia_thumb.jpg	07-Jul-2018 07:26	17.0K
hackedteam.torrent	06-Jul-2015 03:49	23.6M
hackedteam_torrent.txt	06-Jul-2015 21:51	29.1M
support.hackingteam.com.tar.gz	06-Jul-2015 21:00	15.2G

HT - Chapter 4 Hunting Sysadmins

"I searched the computers of Mauro Romeo and Christian Pozzi to see how they administer the Sviluppo network"



Christian Pozzi · 3rd

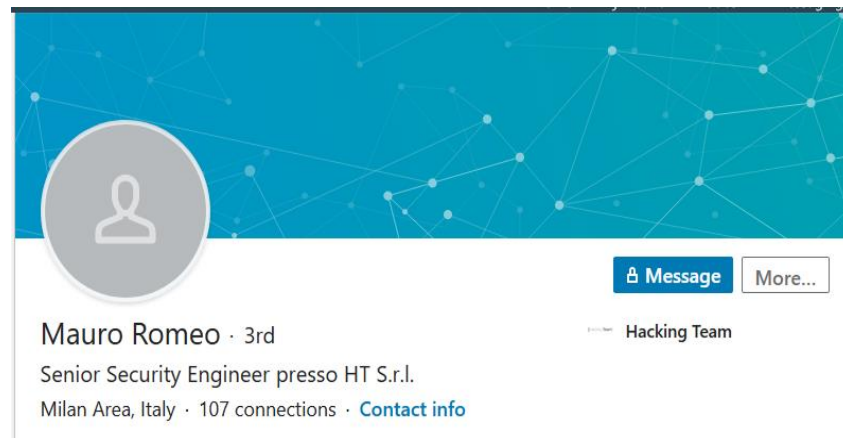
IT SOLUTIONS DELIVERY / STRATEGIC PLANNING / PROJECT MANAGEMENT

Milano, Lombardy, Italy · 500+ connections · [Contact info](#)

[Message](#) [More...](#)

Hacking Team

Università degli Studi di Milano-Bicocca



Mauro Romeo · 3rd

Senior Security Engineer presso HT S.r.l.

Milan Area, Italy · 107 connections · [Contact info](#)

[Message](#) [More...](#)

Hacking Team

HT - Chapter 5 The Bridge

*“I’d found the bridge I needed.”
-Phineas Fisher*

]HackingTeam[

Sindicat De Mossos d'Esquadra

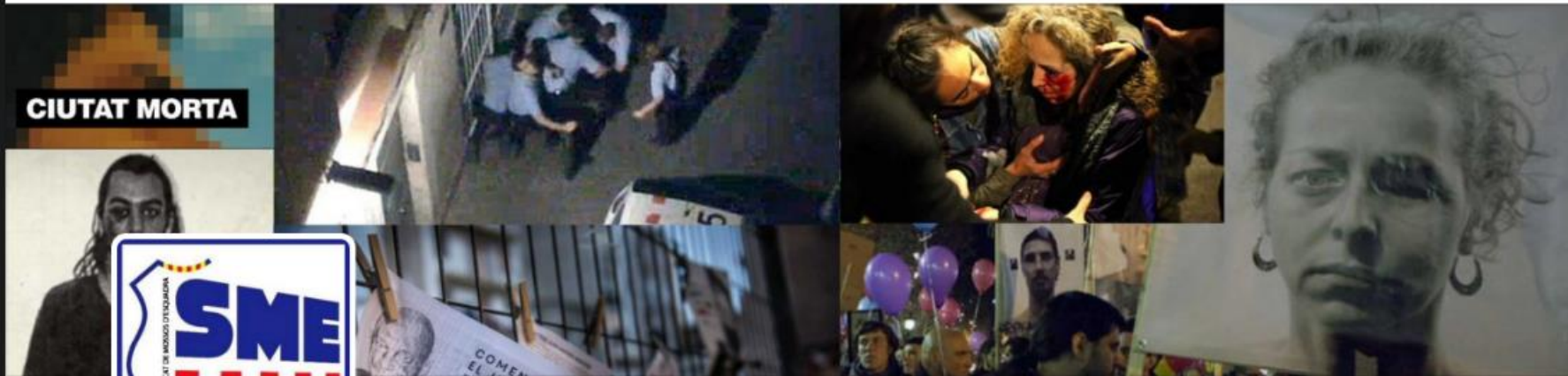




SME - Chapter 3 Taking Backups



SME - Chapter 3 Taking Backups



CIUTAT MORTA

SME
SINDICAT DE MOSSOS D'ESQUADRA
pels drets humans

SME
@smemossos

Compte de twitter del Sindicat de Mossos d'Esquadra pels Drets Humans. Aprenent dels errors, per refundar-nos

📍 CATALUNYA

🌐 sme-mossos.cat

📅 Joined March 2010

📷 317 Photos and videos

Colau ordena tancar un poema antipolicial frente a una comisaria en Barcelona

TWEETS 3,908 FOLLOWING 238 FOLLOWERS 2,088 LIKES 1,049

[Follow](#)

Tweets Tweets & replies Media

SME Retweeted

Anton Uró @AntonUro · 5h
Tenim un problema si llegeixes un text i dius: "Per fi un comunicat assenyat" i llavors t'adones de k és hack...

SME @smemossos
El nostre web està tenint problemes i esta caigut per maneniment. Podeu veure el nostre comunicat aqui: archive.is/Z17tt

15 13

New to Twitter?
Sign up now to get your own personalized timeline!

[Sign up](#)

You may also like · Refresh

SPC - Mossos i PL
@SPC_me

toni castejon
@CastejonToni

The Bank Job

TBJ - Chapter 1 Anarchy



Rojava

“Rojava is one of the most inspiring revolutionary projects in the world today. I just donated €10,000 in bitcoin”

-Phineas Fisher



TBI - Chapter 2 Rojava

9 January 2014

- The PYD officially announced its regional autonomy and formed the Constitution of Rojava.
- Dubbed the start of a social revolution in the area which promotes:
 - A Cooperative economy
 - Direct democracy
 - Ethnic minority rights
 - Restorative justice
 - Women's rights
 - Banning of child marriages and honour killings
 - Religious freedom



Turkey strikes Kurdish city of Afrin northern Syria, civilian casualties reported

February 19, 2016 Kurdish Region, Syria with 1 Comment

Share this:



Turkish army troops at the Syrian border. File photo

TBI - Chapter 3 Disclosure



TBJ - Chapter 3 Disclosure

Transaction View information about a bitcoin transaction

b264bf297f21ec53d7dfc4aa408ed64a8794c9def013c82c89aa64ae27a429ac

1P8qg7S5D8qy6EQj3b5SbTZsHDhb1mQKzn
12xTHFgdQNEAQaJ2Nf2js5JFsPYEdzjjxp



19CwNSMC7eMqTHMf6iKLqB2KweLNHD2aqq
1D7HwrSysVgWz3s1KMyqA1GD6dvX9zGbR7

3.86268491 BTC
25.54408909 BTC

29.406774 BTC

TBJ - Chapter 3 Disclosure

A DIY guide to rob banks

$$\begin{array}{c} \wedge \quad \wedge \\ \text{---} \\ (\circ\circ) \backslash \text{-----} \\ (\quad \text{---}) \backslash \qquad \qquad \qquad) \backslash / \backslash \\ \text{---}) / \quad || \text{-----} w \quad | \\ (.) / \quad || \qquad \qquad \qquad || \\ \sim \end{array}$$

AKP

“it was a total shitshow and didn’t accomplish anything, but the public narrative of what happened is not correct”

-Phineas Fisher



AKP - Chapter 1 Wikileaks

On 19 July 2016, wikileaks released part I of leaked AKP emails, AKP is the ruling political party in Turkey, the emails leaked date back to 2010

They then post part II in 5 August 2016

The leaks are from the party's TLD akparti.org.tr

Turkey blocked Wikileaks in return.



AKP - Chapter 1 Wikileaks

“.... attempted to seize control of several key places in Ankara, Istanbul, and elsewhere, but failed to do so after forces loyal to the state defeated them. The Council cited an erosion of secularism, elimination of democratic rule, disregard for human rights, and Turkey’s loss of credibility in the international arena as reasons for the coup.”

Taken from Wikipedia ~



AKP - Chapter 2 Misunderstanding



Aftermath

Aftermath - SME

“I think the Mossos just arrested some people that retweeted the link to their personal info”

-Phineas Fisher

Aftermath - *Hacking Team*





BitcoinGiftCard.org

You have: \$0.00 + 0.000000 = \$0.00

Buy BTC at \$2,721.52

[1. Verify Your ID](#)[2. Order Coins](#)[3. Shipping Address](#)[4. Make a Payment](#)[Your Gift Cards](#)

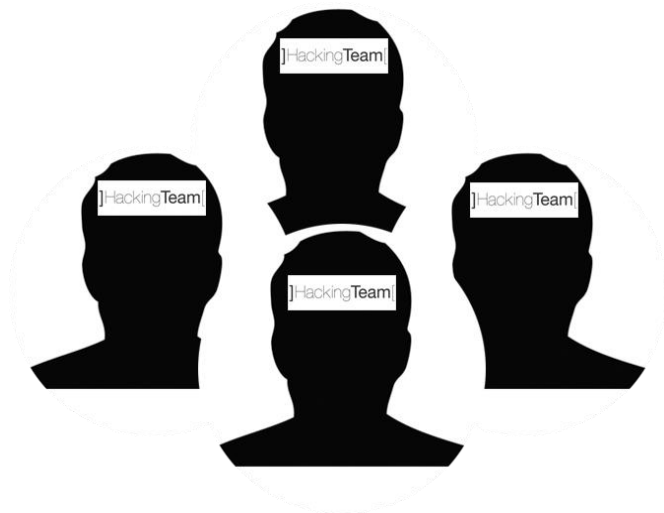
Welcome to the home of the Bitcoin gift card.

Our brand new bitcoin gift card is a simple and secure way to buy bitcoins, delivered to you through the mail. Each of our cards is the size of a business card and comes with a secure private key written on the back. To get your bitcoins, scratch off your gift card and then enter its key online at our website. If you already have a bitcoin wallet, you can enter your bitcoin address and withdraw your bitcoins immediately. Or, you can choose to use the physical gift card as your bitcoin wallet. Our cards come in \$5, \$20, \$50, \$100 and \$500 gift card amounts.

When you scratch off and redeem a gift card, it will be automatically converted into Bitcoins at the current exchange rate. The exchange rate that you get will be whatever is currently listed on [Coinbase](#), a trusted and low-priced Bitcoin exchange. Our bitcoin giftcards are designed for resale; they can easily be given away to friends or sold in physical locations such as convenience stores.

You can pay for your Bitcoins through Paypal. Our gift cards ship to the United States and Canada within a few days.





Former Hacking Team employees

“...the company was more worried about selling spyware than keeping away hackers”

“If it wasn't for that system [Phineas Fisher] would have never arrived at the internal dev network”



*Daniele Milan
(former chief operations
manager)*

“The company didn’t want too much security otherwise it would hinder the speed of software development”

“No one was assigned to the task of updating software”



David Vincenzetti CEO

- Claimed former employees were “infidels” and “traitors”
- Staff that left plotted to destroy the company and the breach was one of those plots.



David Vincenzetti CEO

Facts:

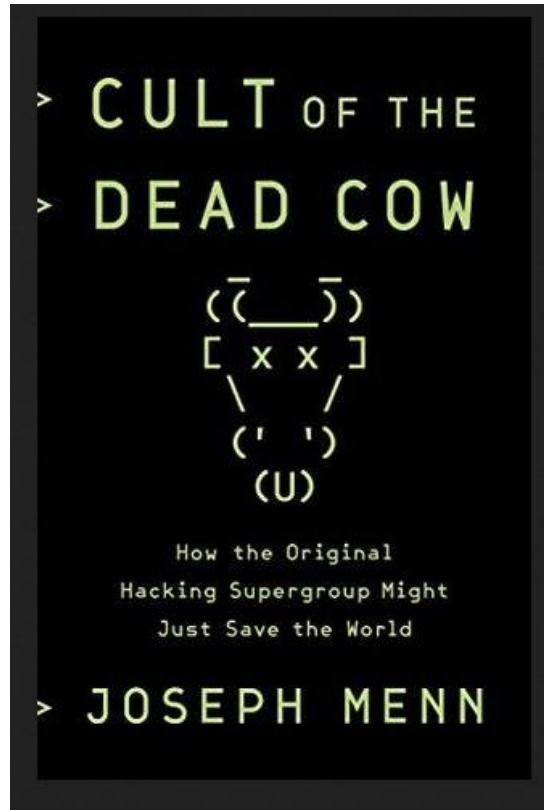
- Refused to upgrade his VPN software, forcing the IT workers at Hacking Team to keep older, legacy service running
- Started a witch hunt which ruined former employees and got caught trying to frame one of his staff members

Aftermath - *Hacking Team*

“lol what’s that even mean”

- Phineas Fisher

Aftermath - Joseph Menn



Aftermath - Phineas Bug Bounty

companies whose leaks I would love to pay for are:

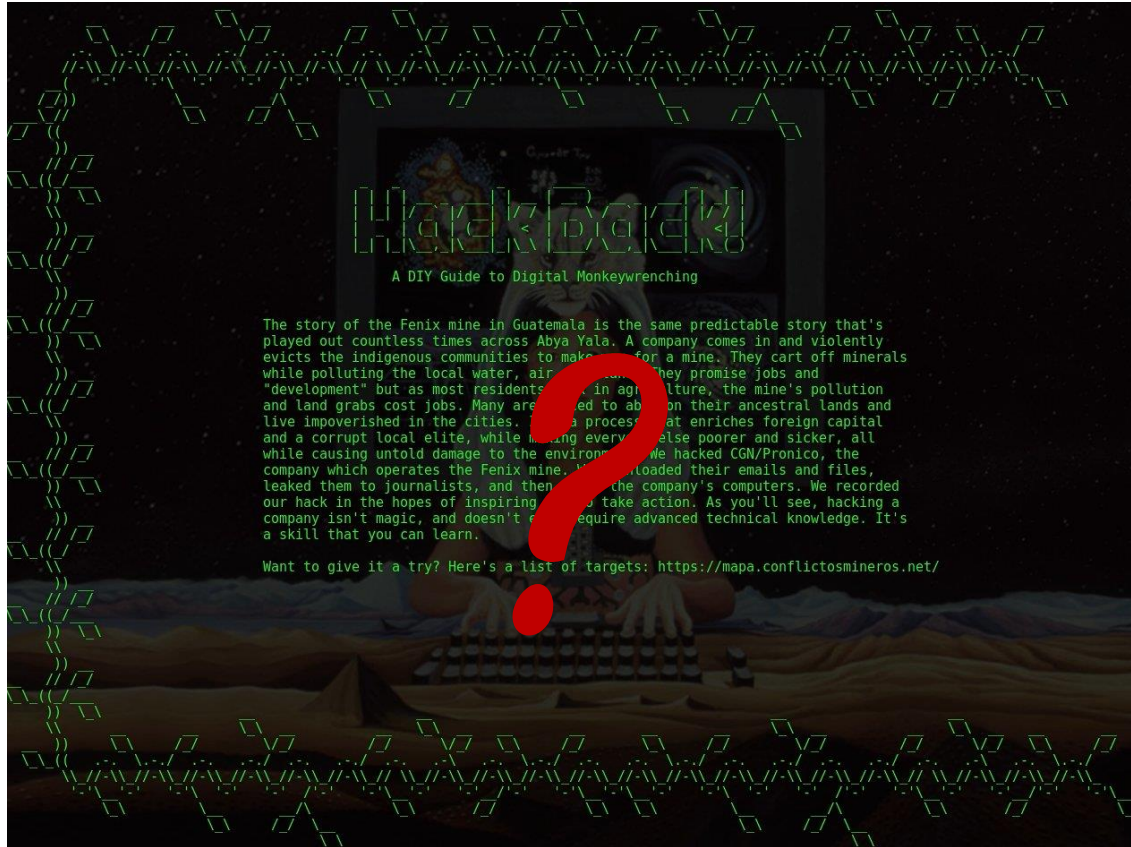
- the mining, logging and livestock companies that plunder our beautiful Latin America (and kill land and territory defenders trying to stop them)
- companies involved in attacks on Rojava such as Baykar Makina or Havelan
- surveillance companies such as the NSO group
- war criminals and birds of prey such as Blackwater and Halliburton
- private penitentiary companies such as GeoGroup and CoreCivic / CCA, and corporate lobbyists such as ALEC

Aftermath - Phineas Bug Bounty Payouts

Milico – \$10,000 – First bounty to be paid

[illegible]

Aftermath - *Extractivist* Leaks



Thank you!

@CyberPunkJake
JAKE@LOWLIFE.TECH

