Fun with Mac Malware Attribution

Joshua Long

*with a few notes added to the slides for clarity

Objective by the Sea

intego

Joshua Long

Joshua Long (@theJoshMeister) is the Chief Security Analyst at Intego, and is a renowned security researcher and writer.

Josh has a master's degree in IT concentrating in Internet Security, and has taken doctorate-level coursework in Business Administration and Computer & Information Security.

For two decades, Josh has been battling spam, phishing scams, malicious sites, and malware to help protect others online.

Apple has publicly acknowledged Josh for discovering an Apple ID password validation vulnerability.

His research has been featured by many fine publications such as CNET, CBS News, ZDNet UK, Lifehacker, CIO, Macworld, The Register, MacTech Magazine, Naked Security, and The Mac Security Blog.

He regularly writes, podcasts, and speaks about Apple security and privacy topics.

Fun with Mac Malware Attribution

- Who makes Mac malware, and why?
- Attribution challenges
- Does this presentation help the bad guys?
- Why does attribution matter?
- 5 case studies (the fun stuff! 😈)

Who makes malware? Why?

*curiosity or self-aggrandizement

- Past: 🤔 😎
- Now:

💰

*monetary or political motivations

Attribution Challenges

- Some are just sneakier
- False flags
- Code reuse

Will this help the bad guys?

No.

*Plenty of DFIR and OSINT resources go deeper on these topics.

Why attribution matters

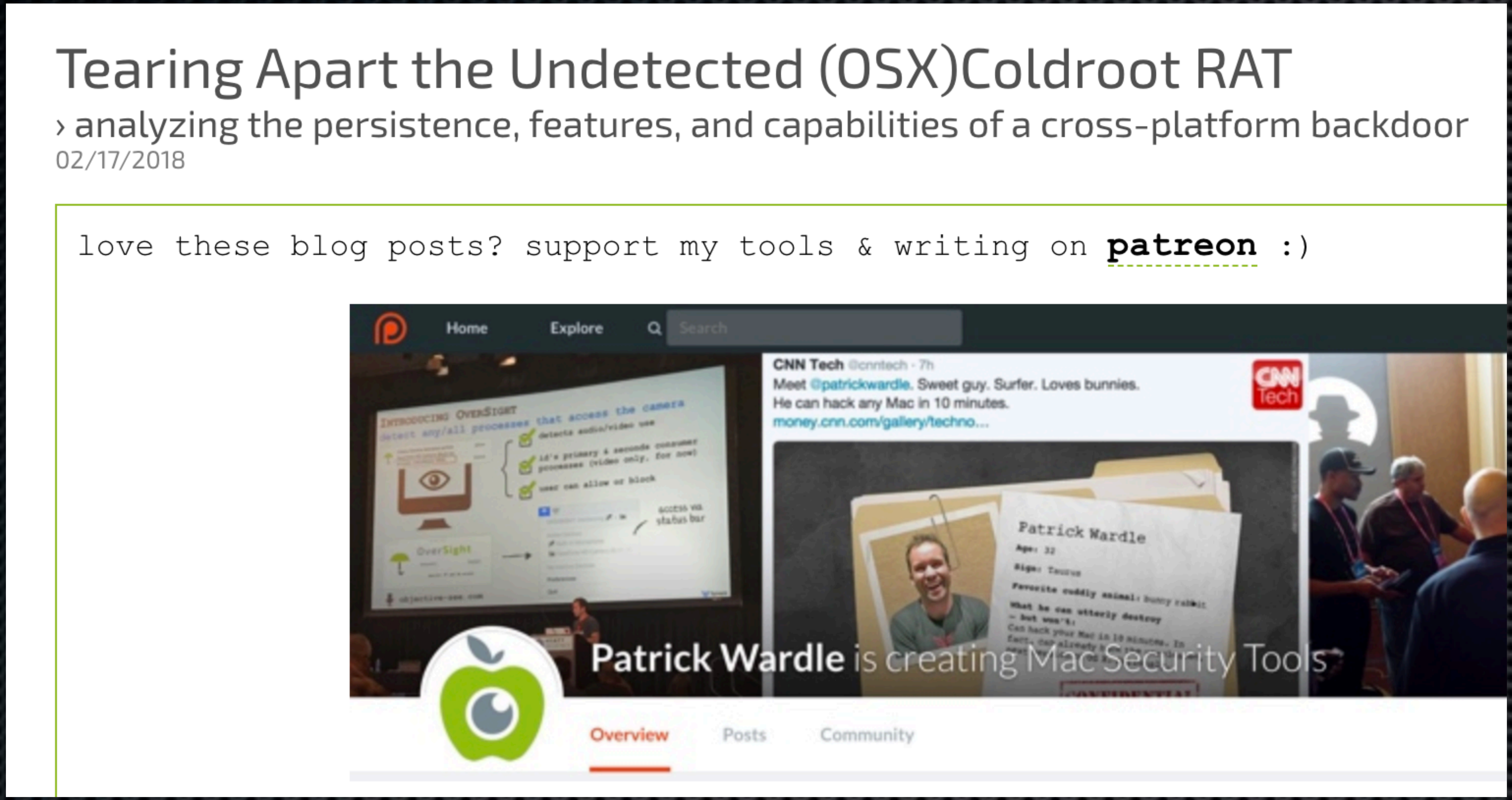
- Huge demotivator for potential malware makers
- …But don’t dox people

The Good Stuff

😈

Coldroot RAT

Coldroot RAT



Tearing Apart the Undetected (OSX)Coldroot RAT

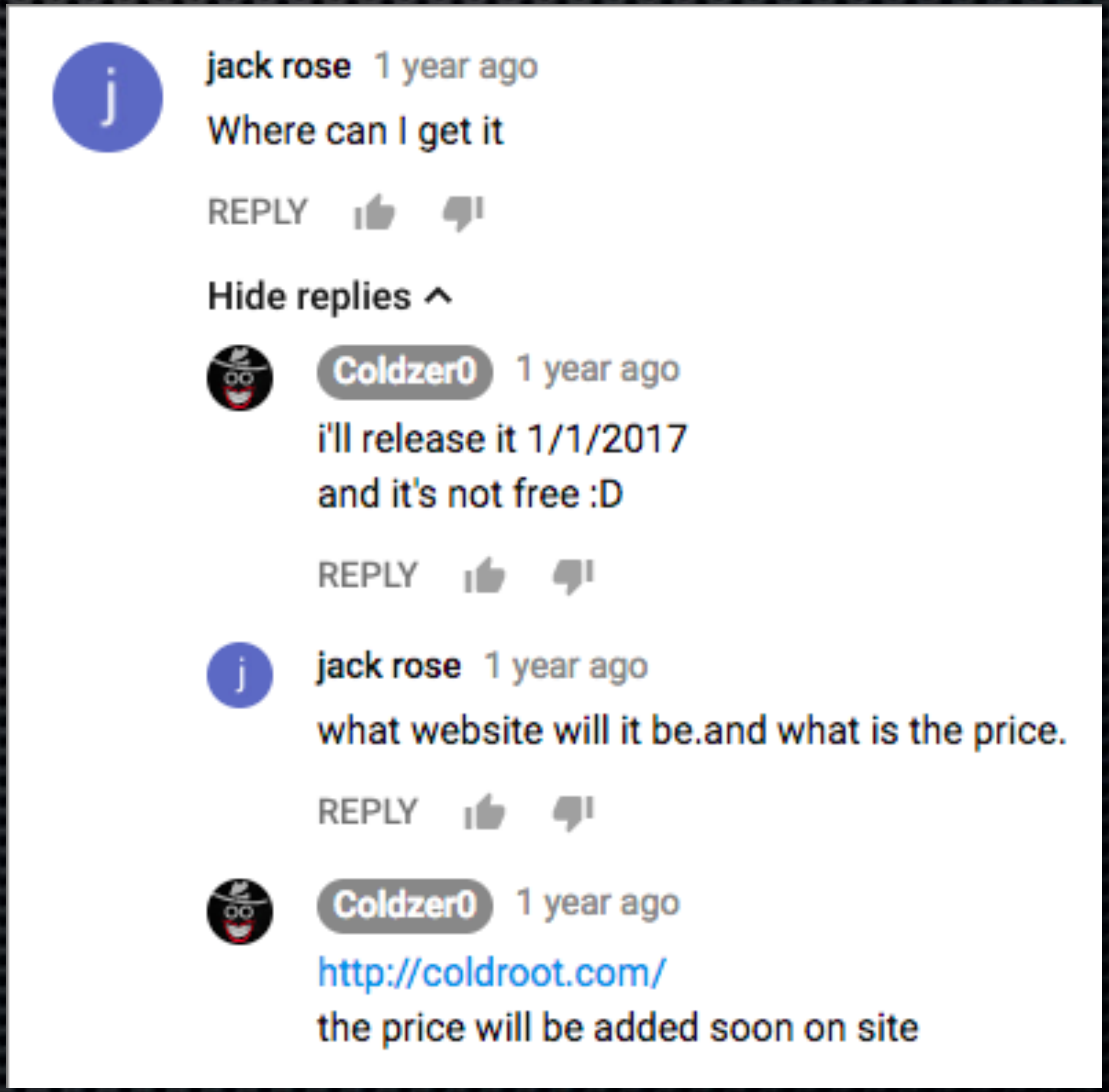
› analyzing the persistence, features, and capabilities of a cross-platform backdoor

02/17/2018

love these blog posts? support my tools & writing on **patreon** :)

CNN Tech @cnntech · 7h
Meet @patrickwardle. Sweet guy. Surfer. Loves bunnies.
He can hack any Mac in 10 minutes.
money.cnn.com/gallery/techno...

Patrick Wardle is creating Mac Security Tools



jack rose 1 year ago
Where can I get it

REPLY

Hide replies ^

Coldzer0 1 year ago
i'll release it 1/1/2017
and it's not free :D

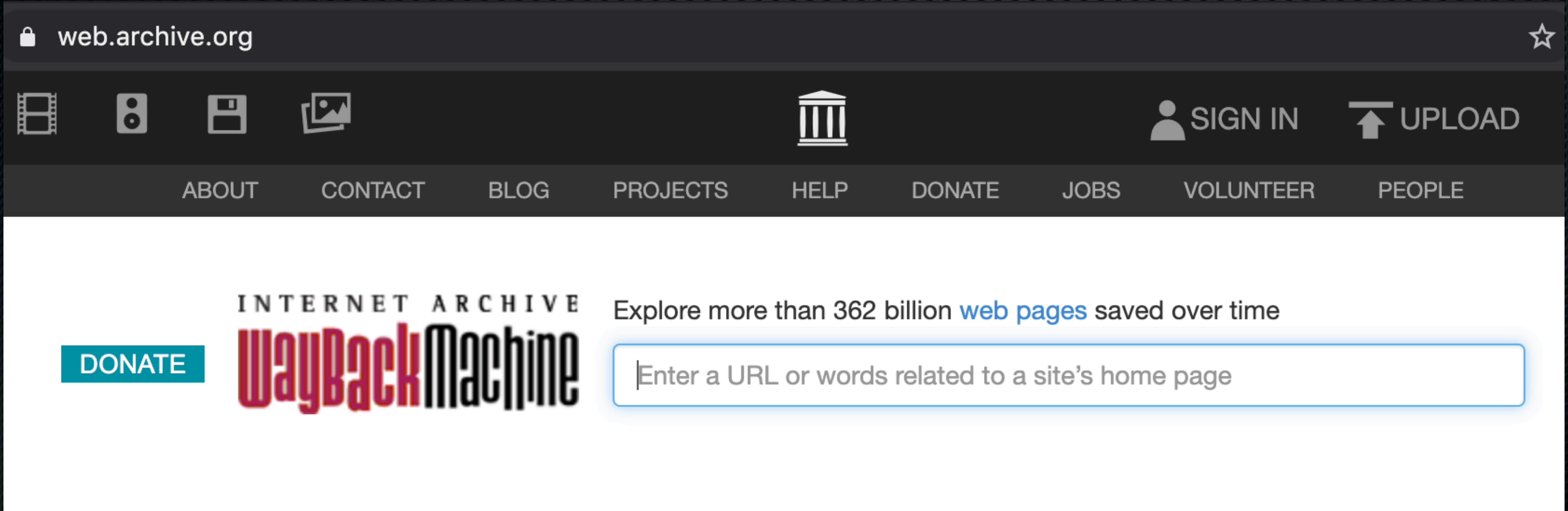
REPLY

jack rose 1 year ago
what website will it be.and what is the price.

REPLY

Coldzer0 1 year ago
http://coldroot.com/
the price will be added soon on site

Coldroot RAT



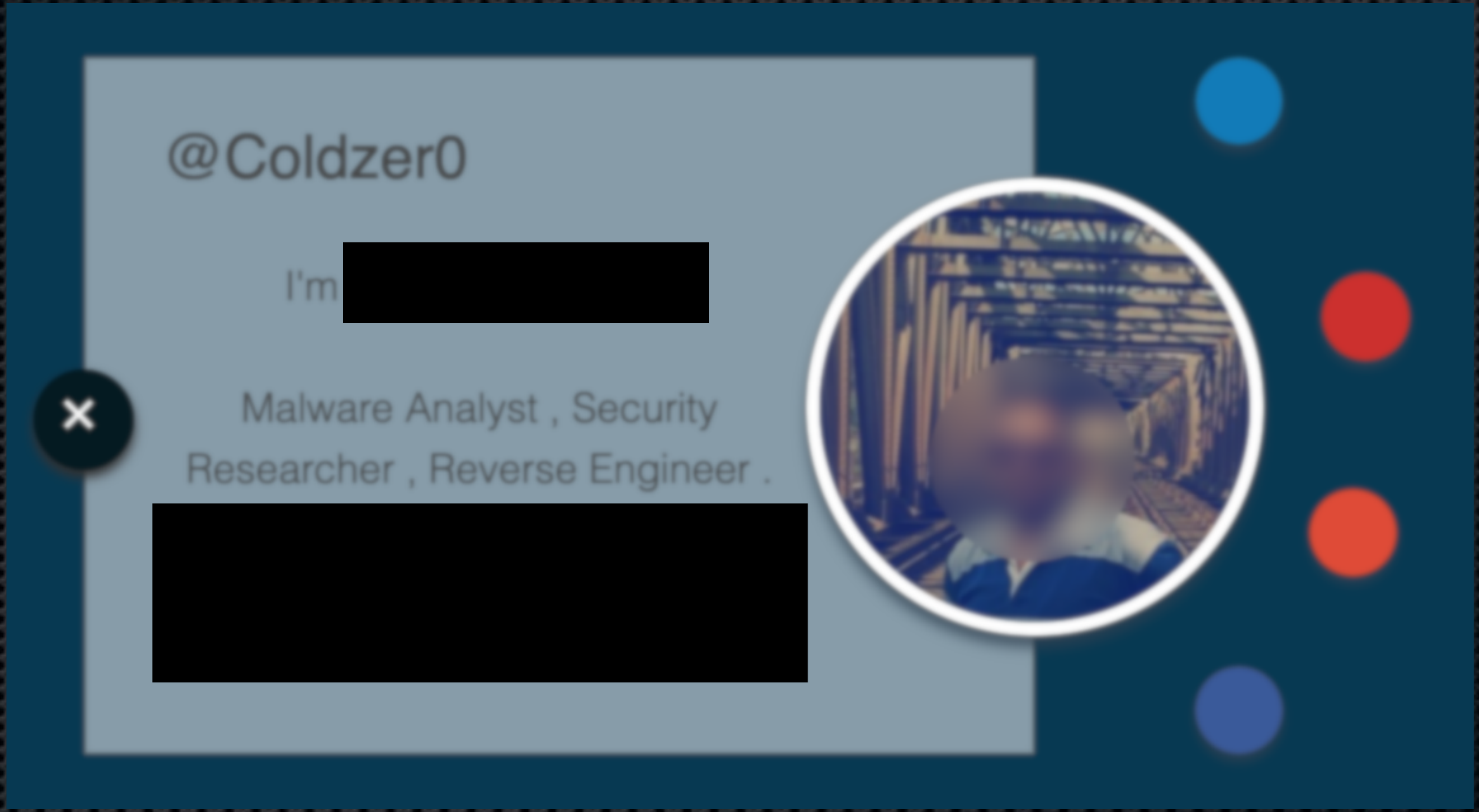
web.archive.org

Explore more than 362 billion web pages saved over time

Enter a URL or words related to a site's home page

Coldroot RAT

coldroot.com from about Nov 2015 to Aug 2016:



@Coldzer0

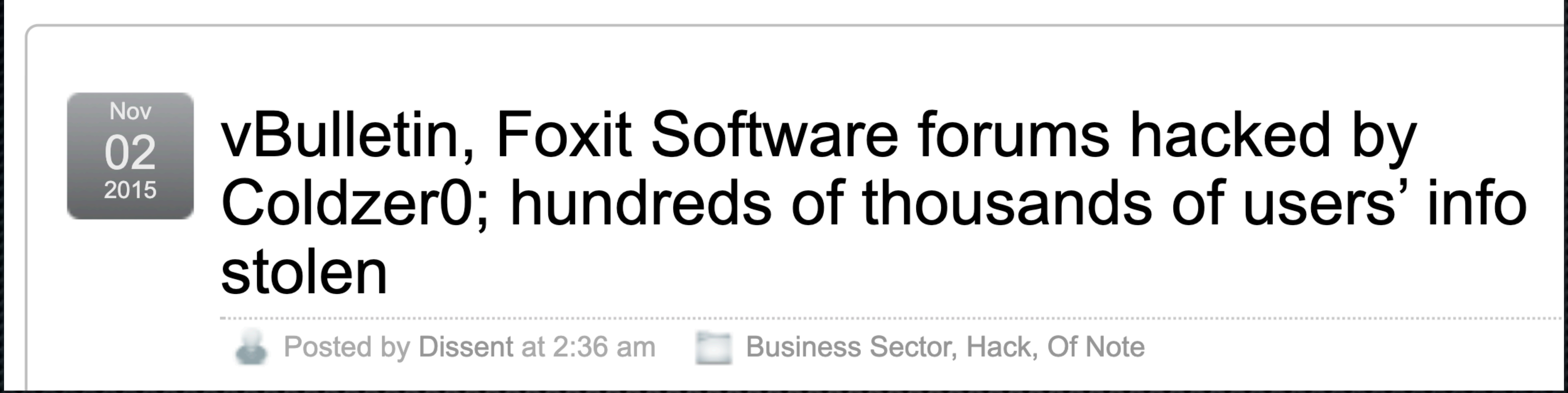
I'm [redacted]

Malware Analyst , Security Researcher , Reverse Engineer .

[redacted]

*The colored bubbles are links to his LinkedIn, YouTube, Google+, and Facebook, all of which used his hacker nickname, Coldzer0.

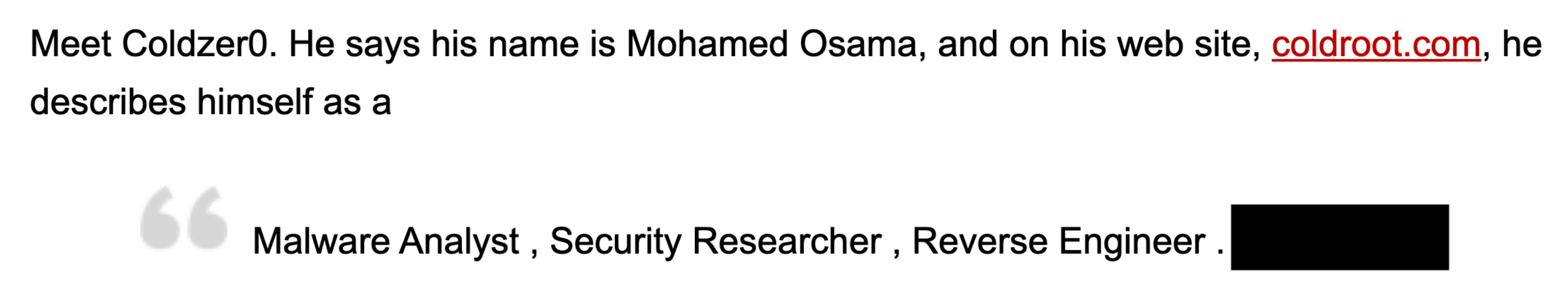
Coldroot RAT



Nov 02 2015

vBulletin, Foxit Software forums hacked by Coldzer0; hundreds of thousands of users' info stolen

Posted by Dissent at 2:36 am Business Sector, Hack, Of Note



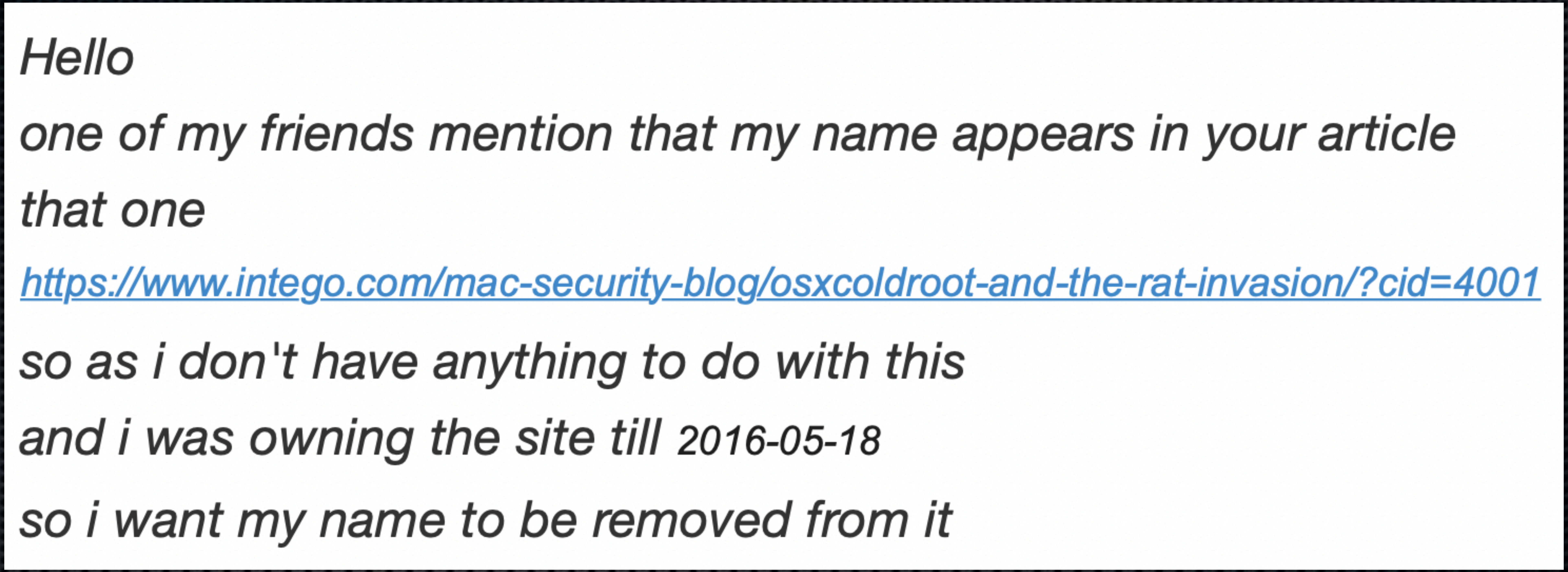
Meet Coldzer0. He says his name is Mohamed Osama, and on his web site, coldroot.com, he describes himself as a

> Malware Analyst , Security Researcher , Reverse Engineer . [redacted]

*He had previously been called out by name on another site a couple years earlier.
Intego published a report about Coldroot RAT, mentioning its developer, which led to an…

Coldroot RAT

e-mail from Mohamed Osama:



Hello

one of my friends mention that my name appears in your article

that one

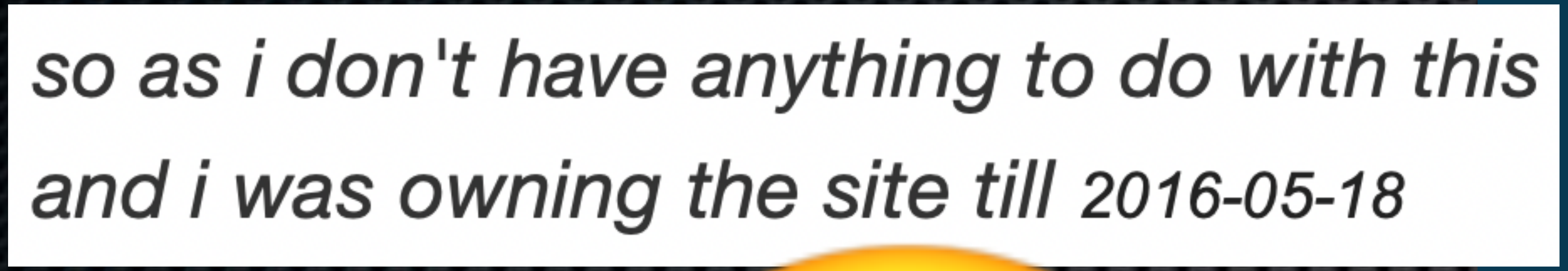
https://www.intego.com/mac-security-blog/osxcoldroot-and-the-rat-invasion/?cid=4001

so as i don't have anything to do with this

and i was owning the site till 2016-05-18

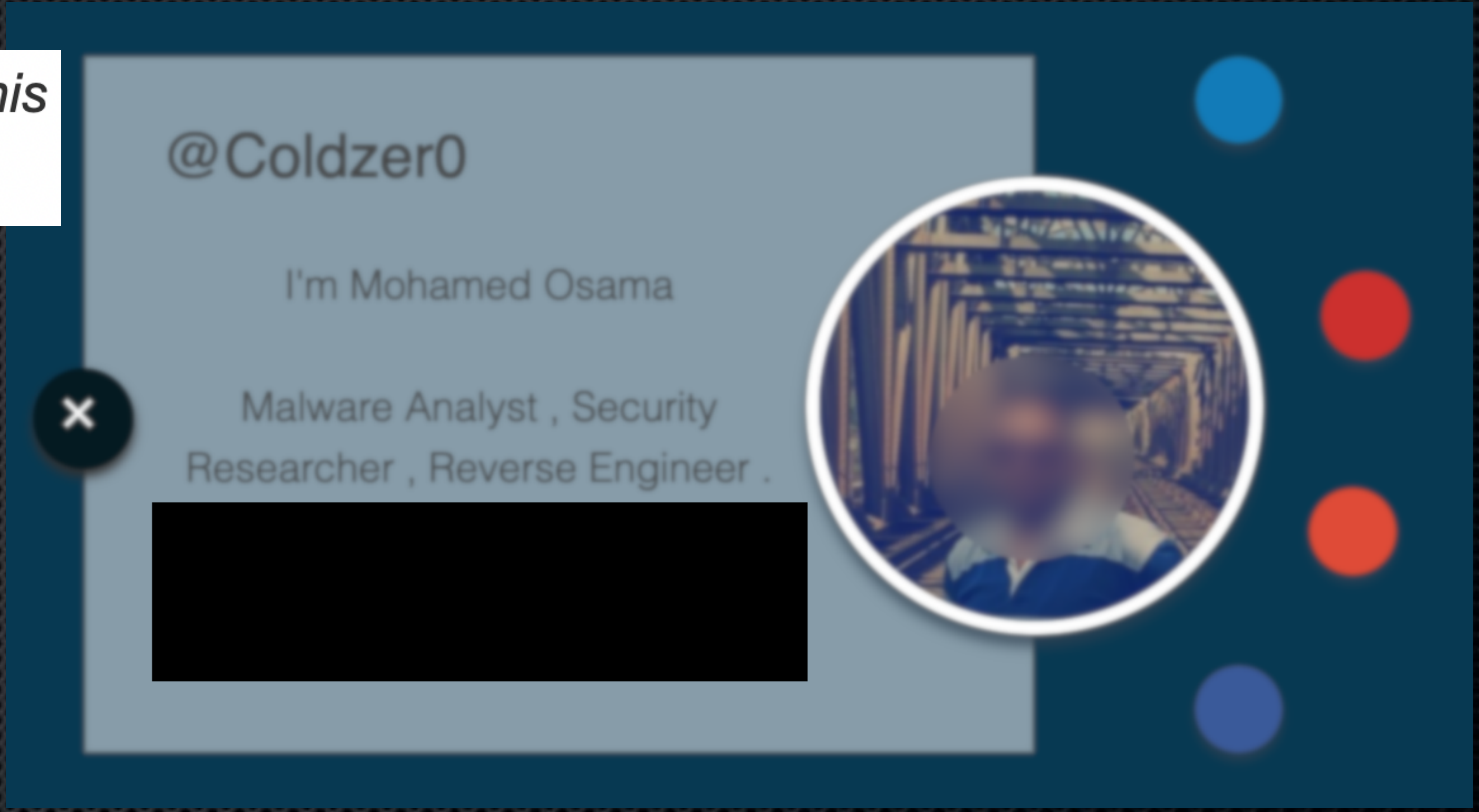
so i want my name to be removed from it

Coldroot RAT



so as i don't have anything to do with this and i was owning the site till 2016-05-18

coldroot.com from about Nov 2015 to Aug 2016:



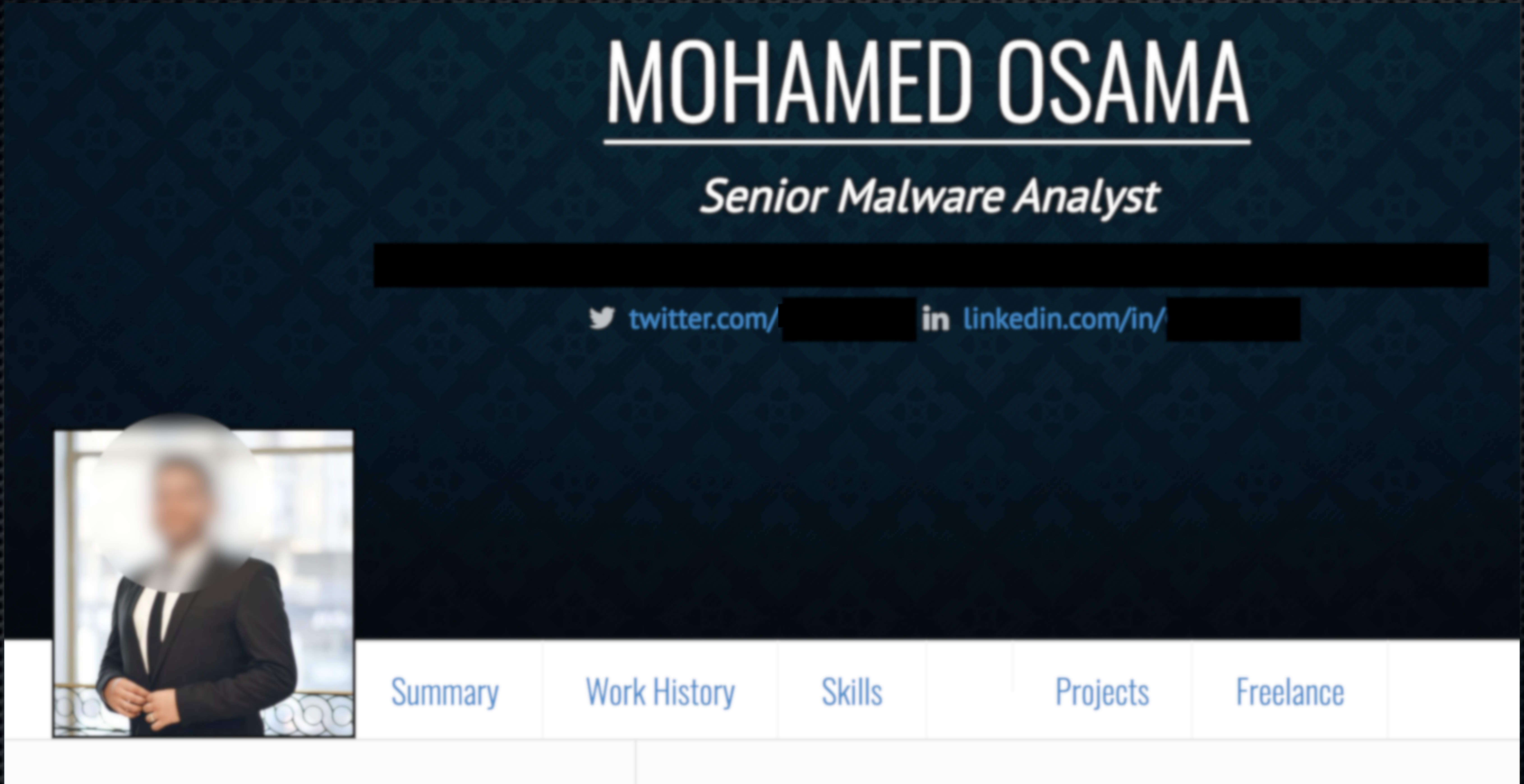
@Coldzer0

I'm Mohamed Osama

Malware Analyst , Security Researcher , Reverse Engineer .

[redacted]

Coldroot RAT



MOHAMED OSAMA

Senior Malware Analyst

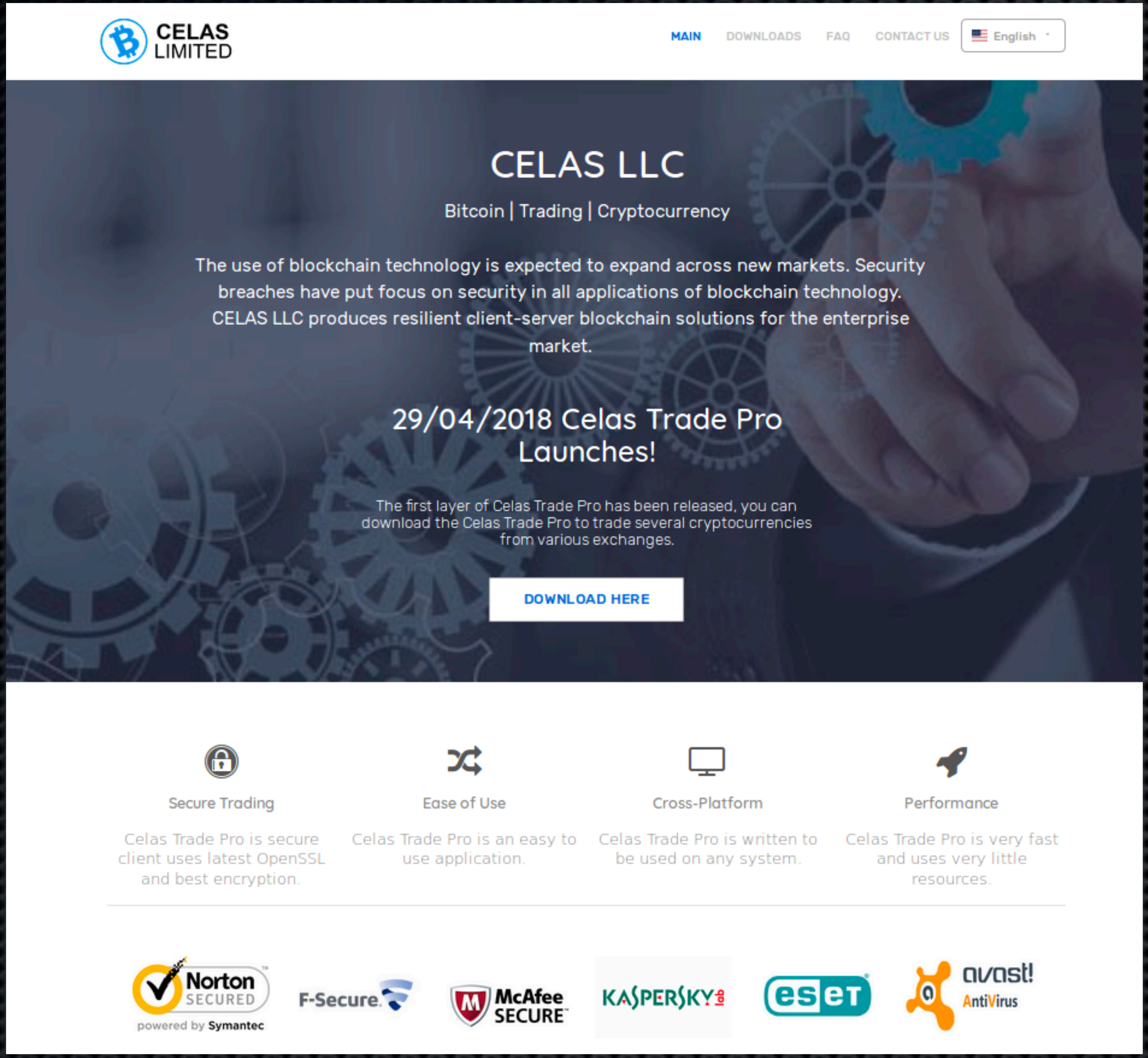
[redacted]

twitter.com/[redacted] linkedin.com/in/[redacted]

*To this day, he still uses the nickname Coldzer0 together with his real name.

Operation AppleJeus

Operation AppleJeus



CELAS LLC

Bitcoin | Trading | Cryptocurrency

The use of blockchain technology is expected to expand across new markets. Security breaches have put focus on security in all applications of blockchain technology. CELAS LLC produces resilient client-server blockchain solutions for the enterprise market.

29/04/2018 Celas Trade Pro Launches!

The first layer of Celas Trade Pro has been released, you can download the Celas Trade Pro to trade several cryptocurrencies from various exchanges.

Secure Trading

Celas Trade Pro is secure client uses latest OpenSSL and best encryption.

Ease of Use

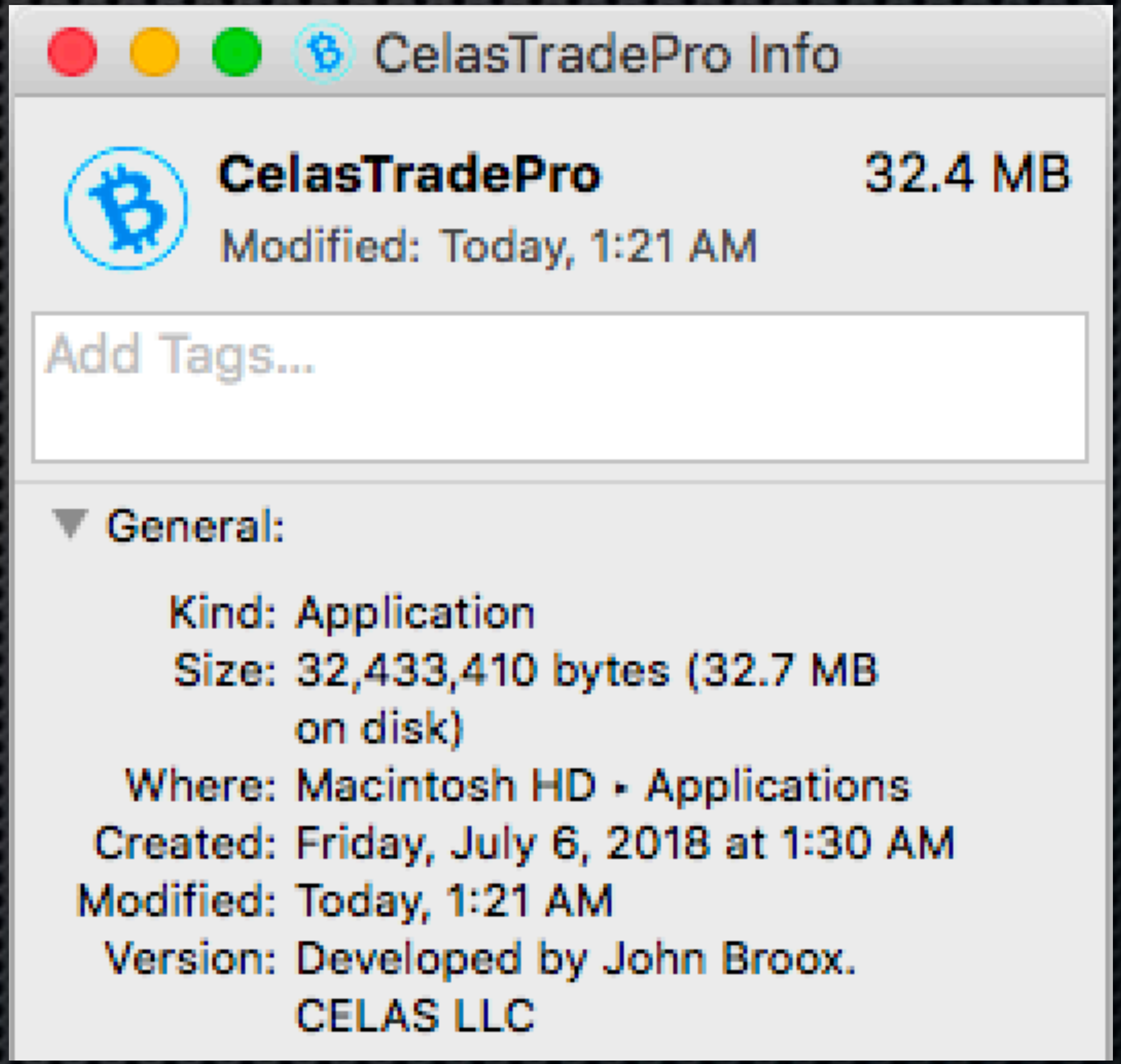
Celas Trade Pro is an easy to use application.

Cross-Platform

Celas Trade Pro is written to be used on any system.

Performance

Celas Trade Pro is very fast and uses very little resources.



CelasTradePro 32.4 MB

Modified: Today, 1:21 AM

General:

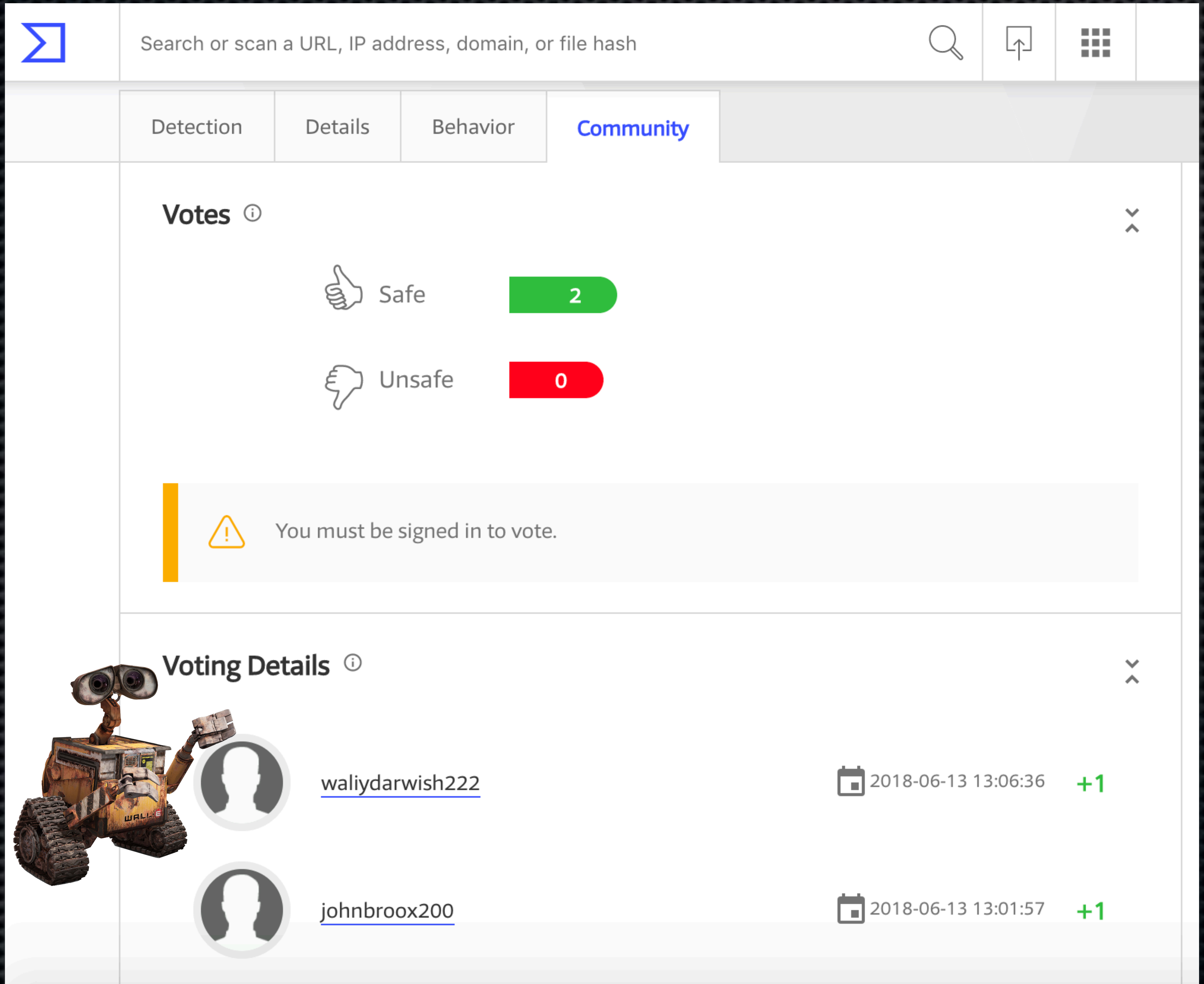
Kind: Application
Size: 32,433,410 bytes (32.7 MB on disk)
Where: Macintosh HD ▸ Applications
Created: Friday, July 6, 2018 at 1:30 AM
Modified: Today, 1:21 AM
Version: Developed by John Broox. CELAS LLC

*"Broox" with an *x* is an extremely uncommon and possibly made up surname, but another developer's name surfaced…

Operation AppleJeus

*Walliy!

Operation AppleJeus



Search or scan a URL, IP address, domain, or file hash

Detection | Details | Behavior | **Community**

Votes

Safe 2

Unsafe 0

You must be signed in to vote.

Voting Details

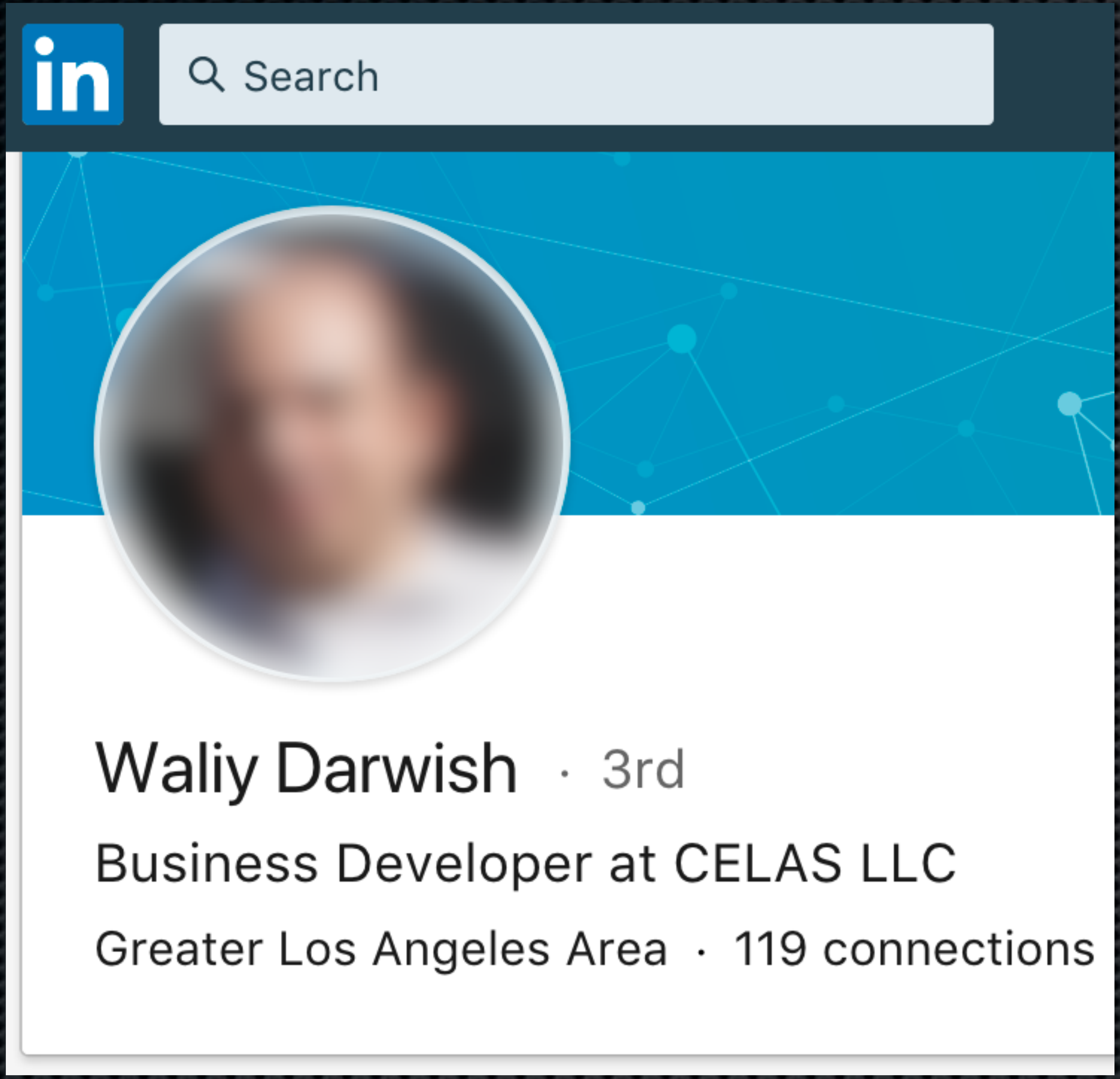
waliydarwish222	2018-06-13 13:06:36	+1
johnbroox200	2018-06-13 13:01:57	+1

*Within minutes of when the Windows version was compiled, it was uploaded to VirusTotal, where two people rated the file as Safe:

- John Broox
- Walliy Darwish

Operation AppleJeus

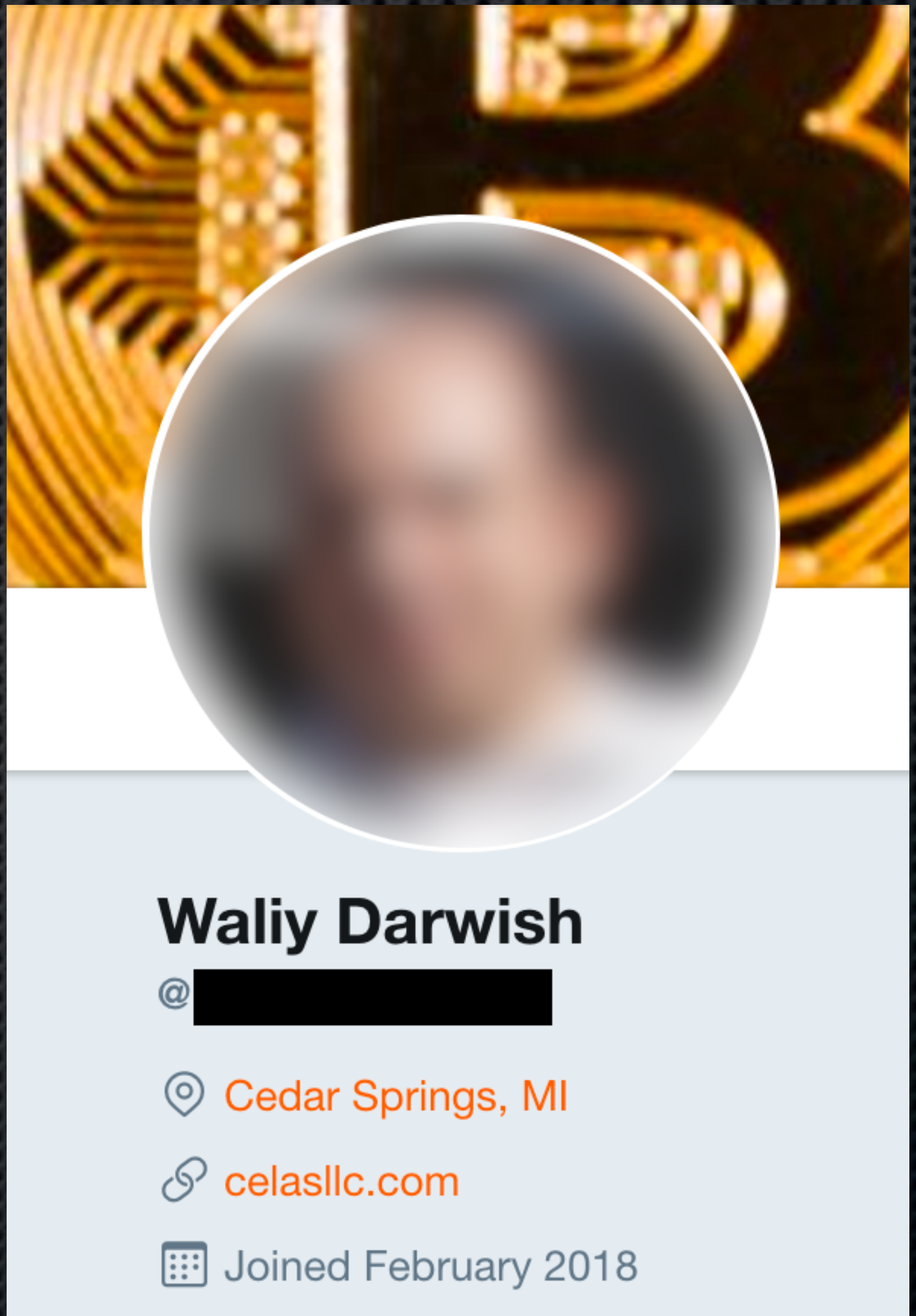
*Being a third-degree LinkedIn connection seemed to give slight credence to the possibility that he may be a real person.



Waliy Darwish · 3rd

Business Developer at CELAS LLC

Greater Los Angeles Area · 119 connections



Waliy Darwish

@[redacted]

Cedar Springs, MI

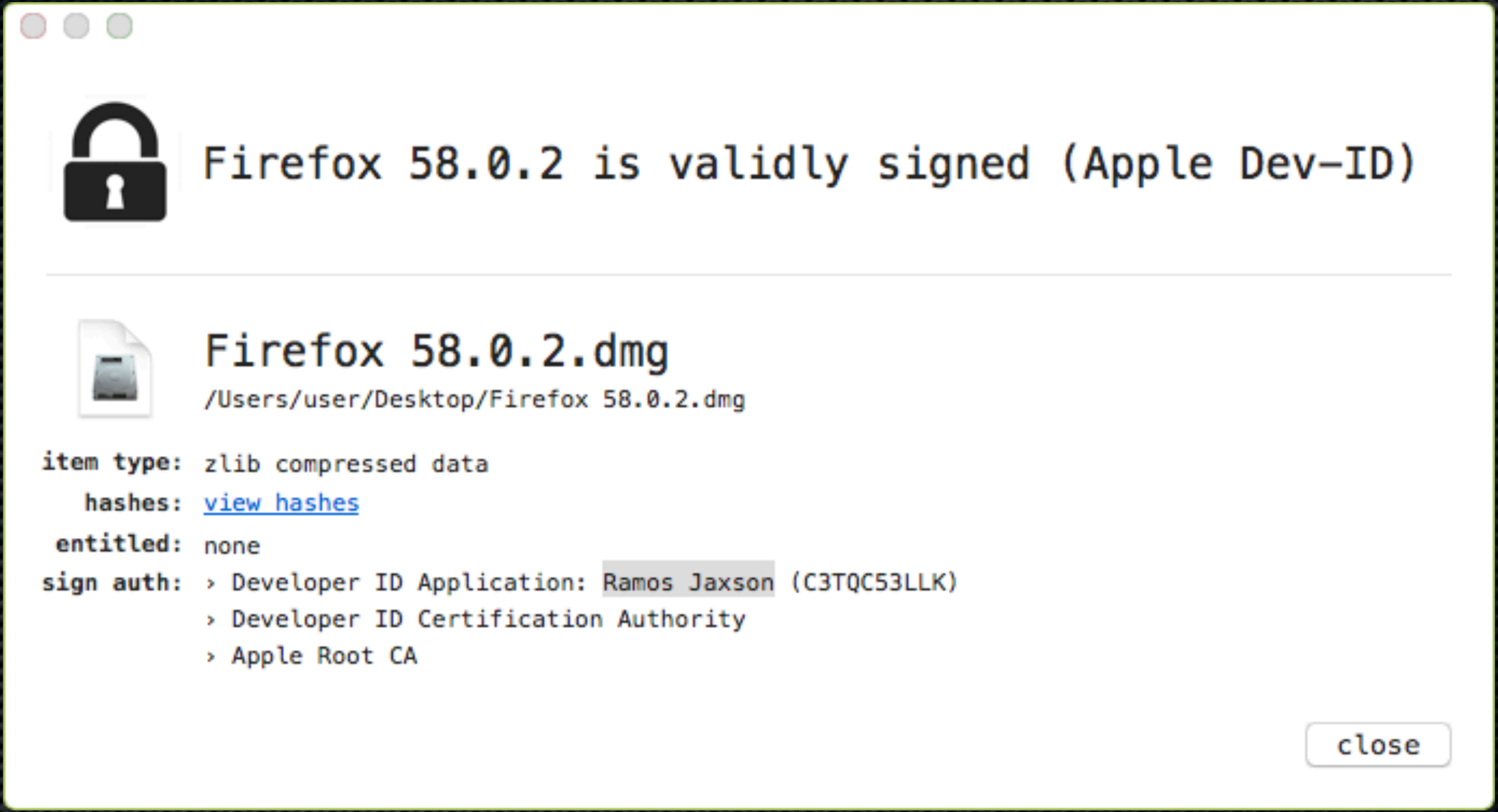
celasllc.com

Joined February 2018

*If he's real, it's unclear whether he knew about the connection with Lazarus Group before writing code for CelasTradePro, or whether he was unknowingly hired by a threat actor and deceived into making software that would be subsequently exploited and Trojanized. 🤷‍♂️

CreativeUpdater

CreativeUpdater



Firefox 58.0.2 is validly signed (Apple Dev-ID)

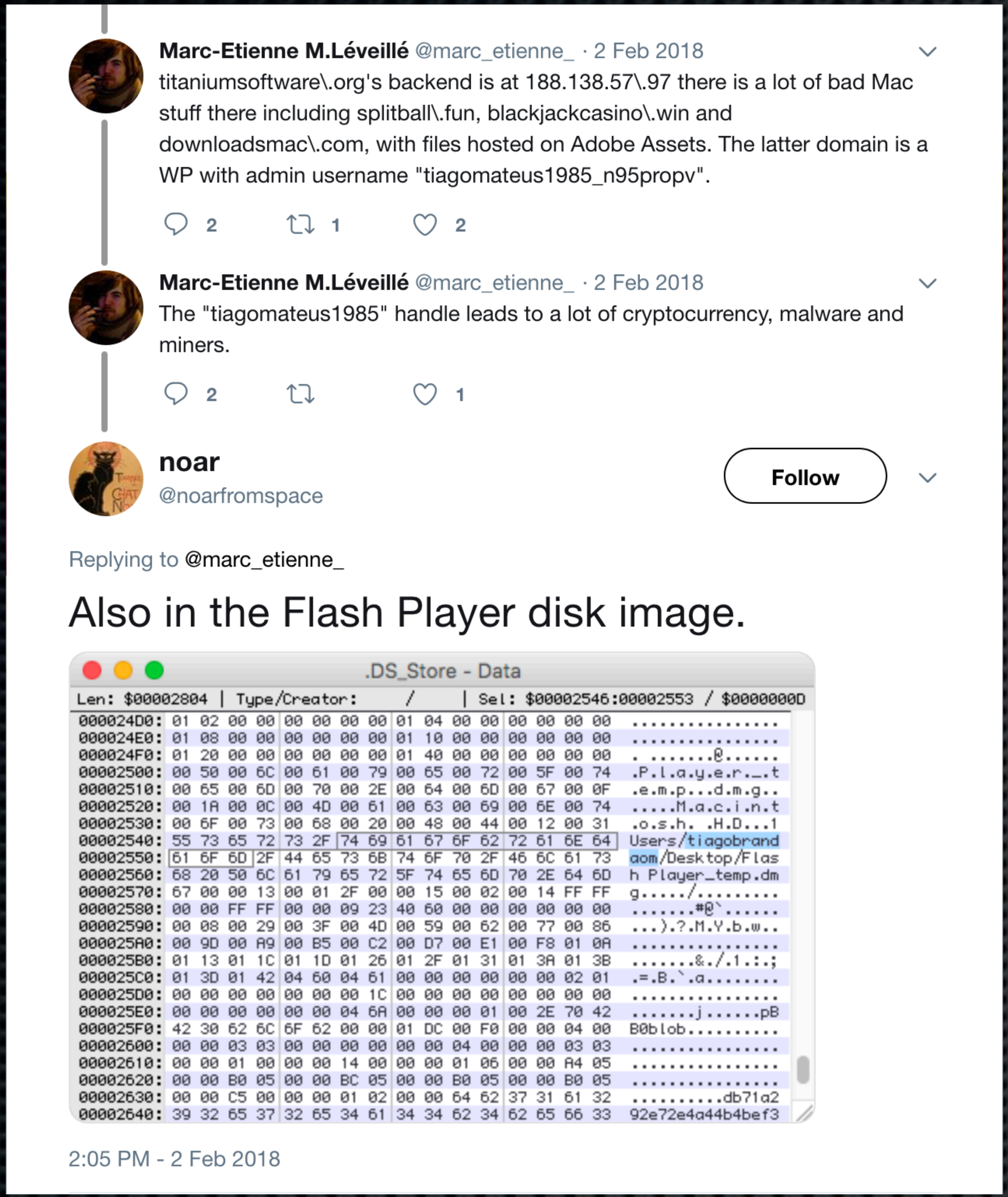
Firefox 58.0.2.dmg

/Users/user/Desktop/Firefox 58.0.2.dmg

```
item type: zlib compressed data
   hashes: view hashes
 entitled: none
sign auth: › Developer ID Application: Ramos Jaxson (C3TQC53LLK)
           › Developer ID Certification Authority
           › Apple Root CA
```

*Little info about "Ramos Jaxson" has been found to date, but another dev's name surfaced…

CreativeUpdater



Marc-Etienne M.Léveillé @marc_etienne_ · 2 Feb 2018

titaniumsoftware\.org's backend is at 188.138.57\.97 there is a lot of bad Mac stuff there including splitball\.fun, blackjackcasino\.win and downloadsmac\.com, with files hosted on Adobe Assets. The latter domain is a WP with admin username "tiagomateus1985_n95propv".

2 1 2

Marc-Etienne M.Léveillé @marc_etienne_ · 2 Feb 2018

The "tiagomateus1985" handle leads to a lot of cryptocurrency, malware and miners.

2 1

noar
@noarfromspace

Replying to @marc_etienne_

Also in the Flash Player disk image.

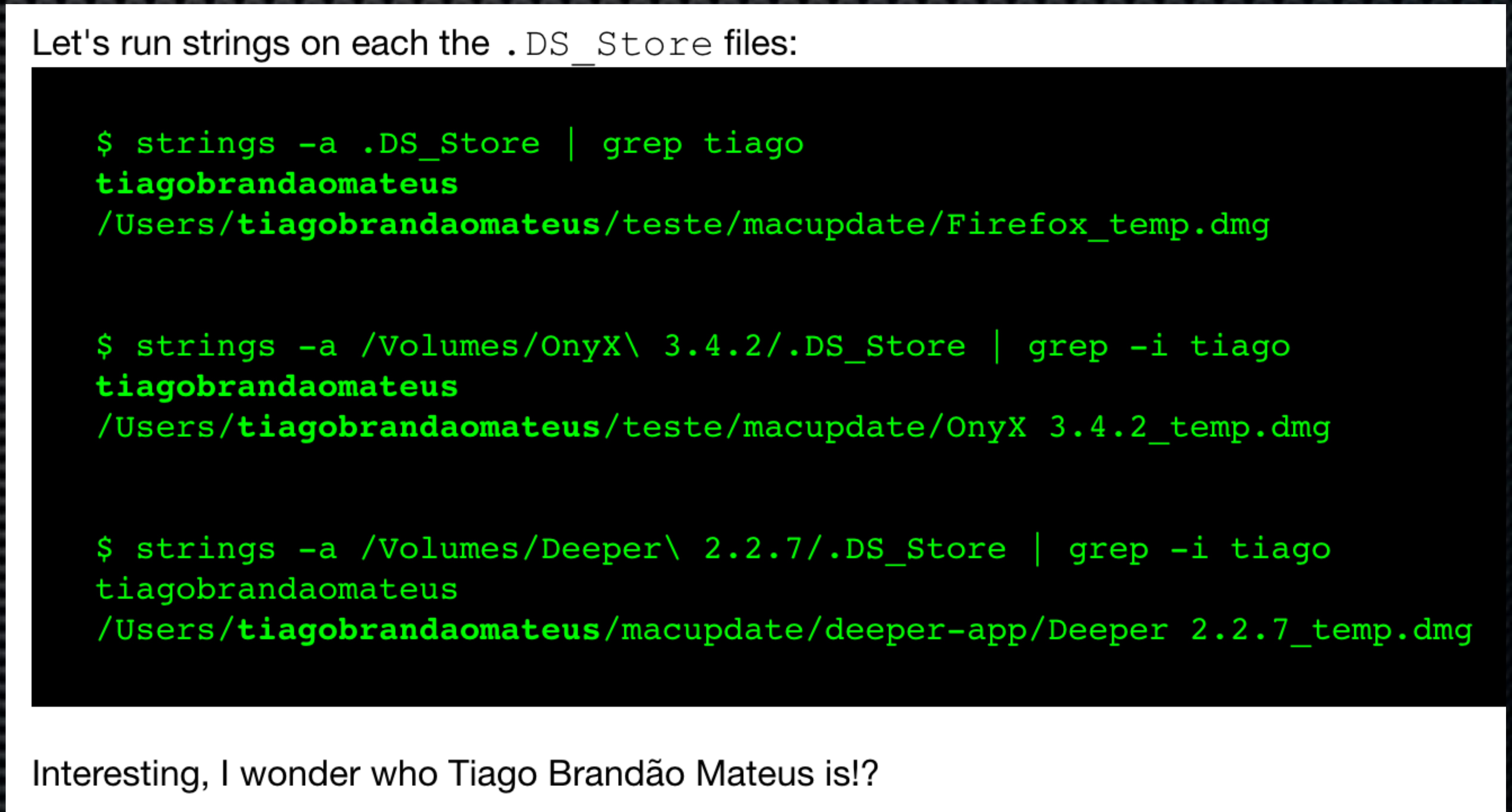
.DS_Store - Data

```
Len: $00002804 | Type/Creator:      /      | Sel: $00002546:00002553 / $0000000D
000024D0: 01 02 00 00 00 00 00 00 01 04 00 00 00 00 00 00  ................
000024E0: 01 08 00 00 00 00 00 00 01 10 00 00 00 00 00 00  ................
000024F0: 01 20 00 00 00 00 00 00 01 40 00 00 00 00 00 00  . .......@......
00002500: 00 50 00 6C 00 61 00 79 00 65 00 72 00 5F 00 74  .P.l.a.y.e.r._.t
00002510: 00 65 00 6D 00 70 00 2E 00 64 00 6D 00 67 00 0F  .e.m.p...d.m.g..
00002520: 00 1A 00 0C 00 4D 00 61 00 63 00 69 00 6E 00 74  .....M.a.c.i.n.t
00002530: 00 6F 00 73 00 68 00 20 00 48 00 44 00 12 00 31  .o.s.h. .H.D...1
00002540: 55 73 65 72 73 2F 74 69 61 67 6F 62 72 61 6E 64  Users/tiagobrand
00002550: 61 6F 6D 2F 44 65 73 6B 74 6F 70 2F 46 6C 61 73  aom/Desktop/Flas
00002560: 68 20 50 6C 61 79 65 72 5F 74 65 6D 70 2E 64 6D  h Player_temp.dm
00002570: 67 00 00 13 00 01 2F 00 00 15 00 02 00 14 FF FF  g...../.........
00002580: 00 00 FF FF 00 00 09 23 40 60 00 00 00 00 00 00  .......#@`......
00002590: 00 08 00 29 00 3F 00 4D 00 59 00 62 00 77 00 86  ...).?.M.Y.b.w..
000025A0: 00 9D 00 A9 00 B5 00 C2 00 D7 00 E1 00 F8 01 0A  ................
000025B0: 01 13 01 1C 01 1D 01 26 01 2F 01 31 01 3A 01 3B  .......&./.1.:.;
000025C0: 01 3D 01 42 04 60 04 61 00 00 00 00 00 00 02 01  .=.B.`.a........
000025D0: 00 00 00 00 00 00 00 1C 00 00 00 00 00 00 00 00  ................
000025E0: 00 00 00 00 00 00 04 6A 00 00 00 01 00 2E 70 42  .......j......pB
000025F0: 42 30 62 6C 6F 62 00 00 01 DC 00 F0 00 00 04 00  B0blob..........
00002600: 00 00 03 03 00 00 00 00 00 00 04 00 00 00 03 03  ................
00002610: 00 00 01 00 00 00 14 00 00 00 01 06 00 00 A4 05  ................
00002620: 00 00 B0 05 00 00 BC 05 00 00 B0 05 00 00 B0 05  ................
00002630: 00 00 C5 00 00 00 01 02 00 00 64 62 37 31 61 32  ..........db71a2
00002640: 39 32 65 37 32 65 34 61 34 34 62 34 62 65 66 33  92e72e4a44b4bef3
```

2:05 PM - 2 Feb 2018

tiagomateus1985 tiagobrandaom

tiagobrandaomateus



Let's run strings on each the `.DS_Store` files:

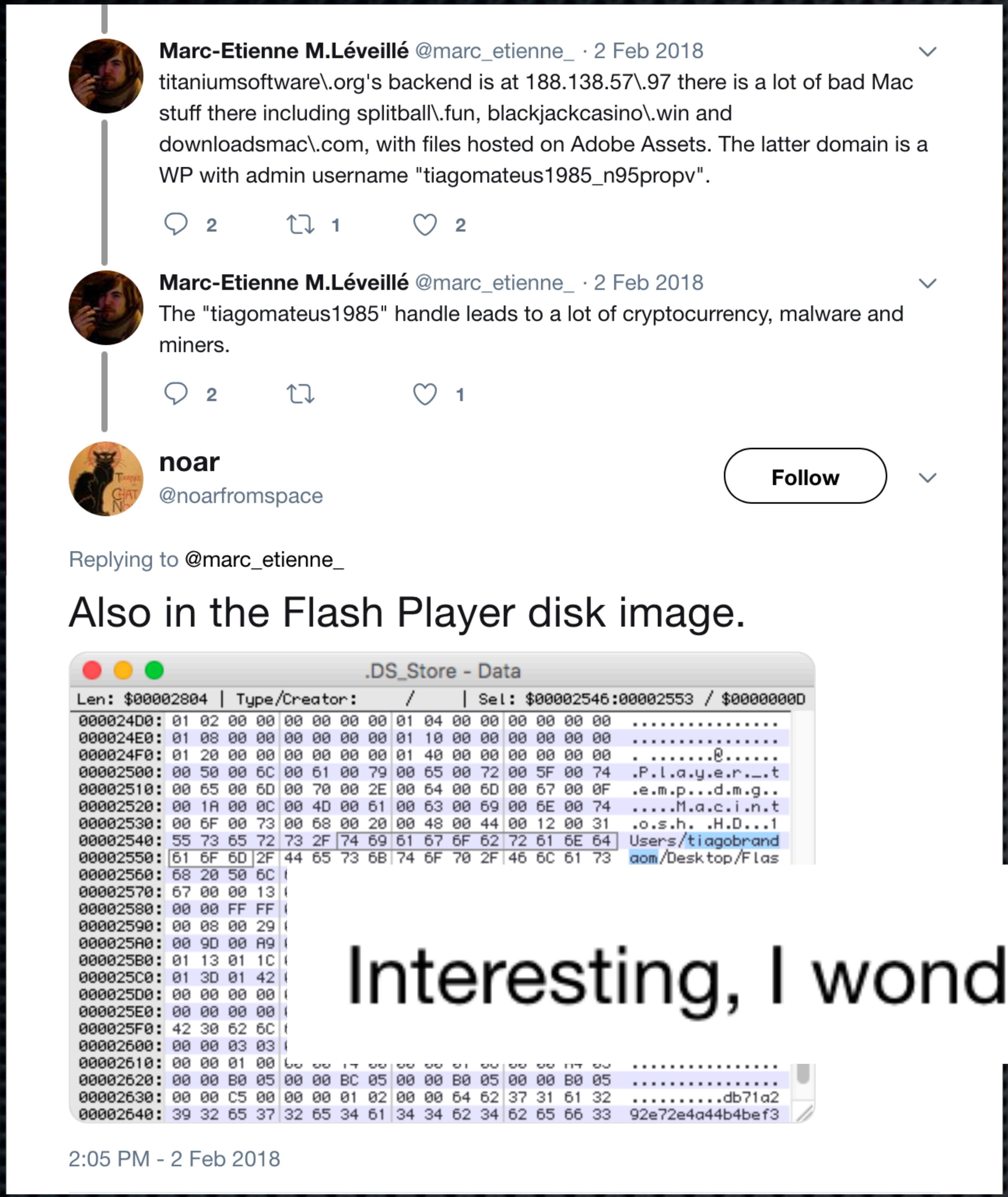
```
$ strings -a .DS_Store | grep tiago
tiagobrandaomateus
/Users/tiagobrandaomateus/teste/macupdate/Firefox_temp.dmg


$ strings -a /Volumes/OnyX\ 3.4.2/.DS_Store | grep -i tiago
tiagobrandaomateus
/Users/tiagobrandaomateus/teste/macupdate/OnyX 3.4.2_temp.dmg


$ strings -a /Volumes/Deeper\ 2.2.7/.DS_Store | grep -i tiago
tiagobrandaomateus
/Users/tiagobrandaomateus/macupdate/deeper-app/Deeper 2.2.7_temp.dmg
```

Interesting, I wonder who Tiago Brandão Mateus is!?

CreativeUpdater



Marc-Etienne M.Léveillé @marc_etienne_ · 2 Feb 2018

titaniumsoftware\.org's backend is at 188.138.57\.97 there is a lot of bad Mac stuff there including splitball\.fun, blackjackcasino\.win and downloadsmac\.com, with files hosted on Adobe Assets. The latter domain is a WP with admin username "tiagomateus1985_n95propv".

Marc-Etienne M.Léveillé @marc_etienne_ · 2 Feb 2018

The "tiagomateus1985" handle leads to a lot of cryptocurrency, malware and miners.

noar
@noarfromspace

Replying to @marc_etienne_

Also in the Flash Player disk image.

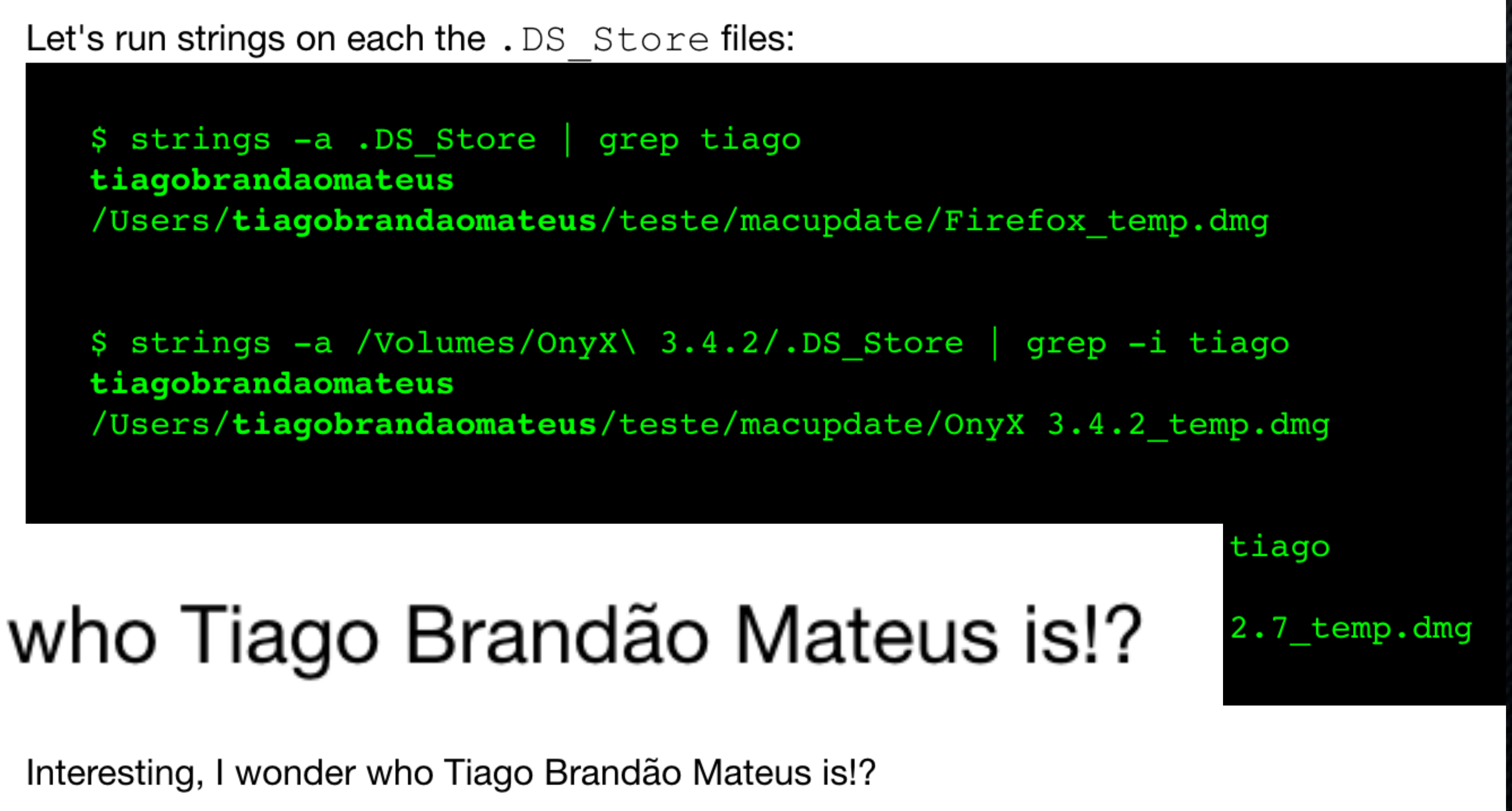
.DS_Store - Data

```
Len: $00002804 | Type/Creator:      /     | Sel: $00002546:00002553 / $0000000D
000024D0: 01 02 00 00 00 00 00 00 01 04 00 00 00 00 00 00  ................
000024E0: 01 08 00 00 00 00 00 00 01 10 00 00 00 00 00 00  ................
000024F0: 01 20 00 00 00 00 00 00 01 40 00 00 00 00 00 00  . .......@......
00002500: 00 50 00 6C 00 61 00 79 00 65 00 72 00 5F 00 74  .P.l.a.y.e.r._.t
00002510: 00 65 00 6D 00 70 00 2E 00 64 00 6D 00 67 00 0F  .e.m.p...d.m.g..
00002520: 00 1A 00 0C 00 4D 00 61 00 63 00 69 00 6E 00 74  .....M.a.c.i.n.t
00002530: 00 6F 00 73 00 68 00 20 00 48 00 44 00 12 00 31  .o.s.h. .H.D...1
00002540: 55 73 65 72 73 2F 74 69 61 67 6F 62 72 61 6E 64  Users/tiagobrand
00002550: 61 6F 6D 2F 44 65 73 6B 74 6F 70 2F 46 6C 61 73  aom/Desktop/Flas
00002560: 68 20 50 6C
00002570: 67 00 00 13
00002580: 00 00 FF FF
00002590: 00 08 00 29
000025A0: 00 9D 00 A9
000025B0: 01 13 01 1C
000025C0: 01 3D 01 42
000025D0: 00 00 00 00
000025E0: 00 00 00 00
000025F0: 42 30 62 6C
00002600: 00 00 03 03
00002610: 00 00 01 00                                      ................
00002620: 00 00 B0 05 00 00 BC 05 00 00 B0 05 00 00 B0 05  ................
00002630: 00 00 C5 00 00 00 01 02 00 00 64 62 37 31 61 32  ..........db71a2
00002640: 39 32 65 37 32 65 34 61 34 34 62 34 62 65 66 33  92e72e4a44b4bef3
```

2:05 PM - 2 Feb 2018

tiagomateus1985 **tiagobrandaom**

tiagobrandaomateus



Let's run strings on each the `.DS_Store` files:

```
$ strings -a .DS_Store | grep tiago
tiagobrandaomateus
/Users/tiagobrandaomateus/teste/macupdate/Firefox_temp.dmg


$ strings -a /Volumes/OnyX\ 3.4.2/.DS_Store | grep -i tiago
tiagobrandaomateus
/Users/tiagobrandaomateus/teste/macupdate/OnyX 3.4.2_temp.dmg

                                                           tiago

                                                           2.7_temp.dmg
```

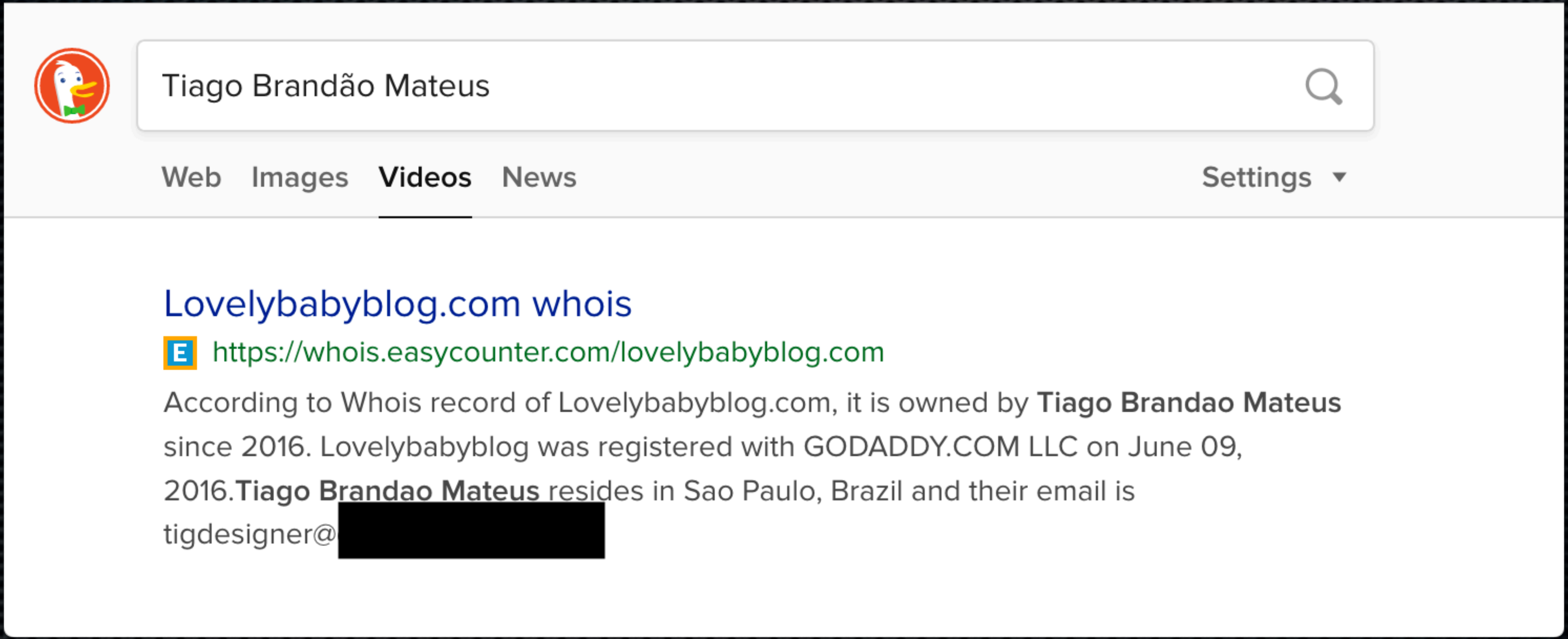
Interesting, I wonder who Tiago Brandão Mateus is!?

Interesting, I wonder who Tiago Brandão Mateus is!?

*Patrick asked…

CreativeUpdater

CreativeUpdater



Tiago Brandão Mateus

Lovelybabyblog.com whois

https://whois.easycounter.com/lovelybabyblog.com

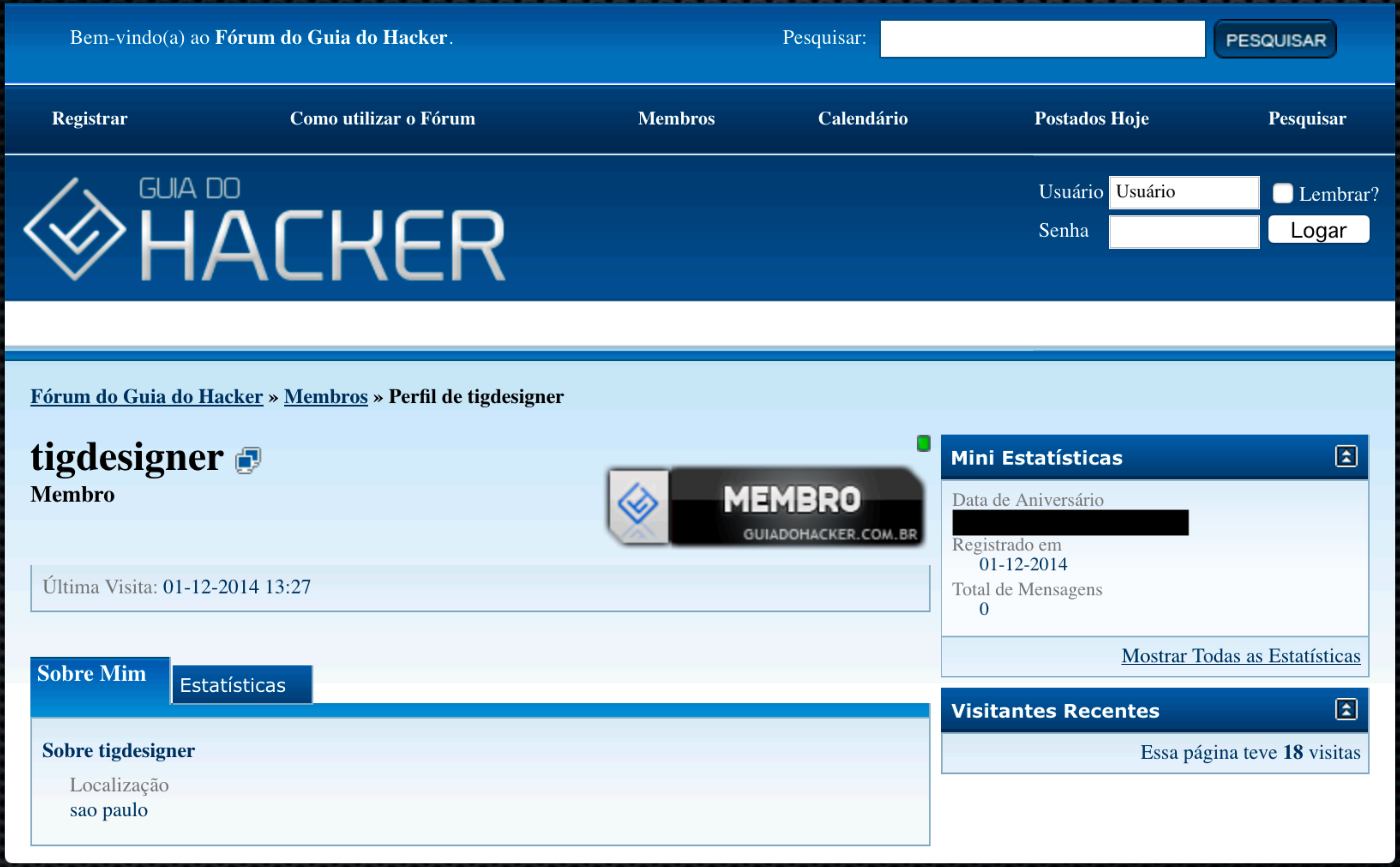
According to Whois record of Lovelybabyblog.com, it is owned by **Tiago Brandao Mateus** since 2016. Lovelybabyblog was registered with GODADDY.COM LLC on June 09, 2016.**Tiago Brandao Mateus** resides in Sao Paulo, Brazil and their email is tigdesigner@[redacted]

*We know Tiago registers domains (he did for CreativeUpdater), so "tigdesigner" seemed worth investigating.

Objective by the Sea

intego

CreativeUpdater



Bem-vindo(a) ao **Fórum do Guia do Hacker**.

Pesquisar: PESQUISAR

Registrar | Como utilizar o Fórum | Membros | Calendário | Postados Hoje | Pesquisar

GUIA DO HACKER

Usuário Usuário □ Lembrar?

Senha Logar

Fórum do Guia do Hacker » Membros » **Perfil de tigdesigner**

tigdesigner

Membro

MEMBRO GUIADOHACKER.COM.BR

Última Visita: 01-12-2014 13:27

Sobre Mim | Estatísticas

Sobre tigdesigner

Localização
sao paulo

Mini Estatísticas

Data de Aniversário
[redacted]

Registrado em
01-12-2014

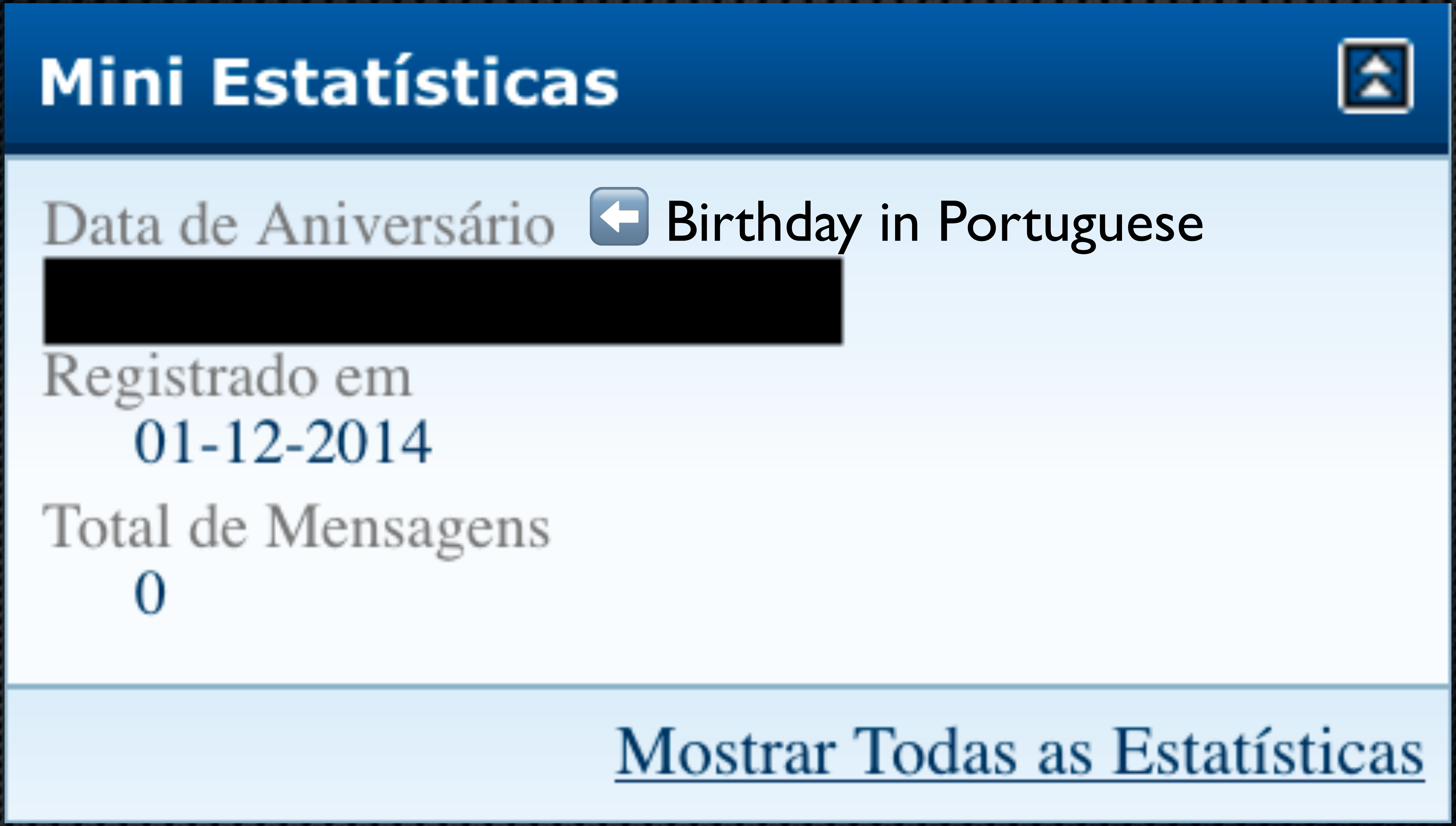
Total de Mensagens
0

Mostrar Todas as Estatísticas

Visitantes Recentes

Essa página teve **18** visitas

CreativeUpdater



Mini Estatísticas

Data de Aniversário ⬅ Birthday in Portuguese

[redacted]

Registrado em

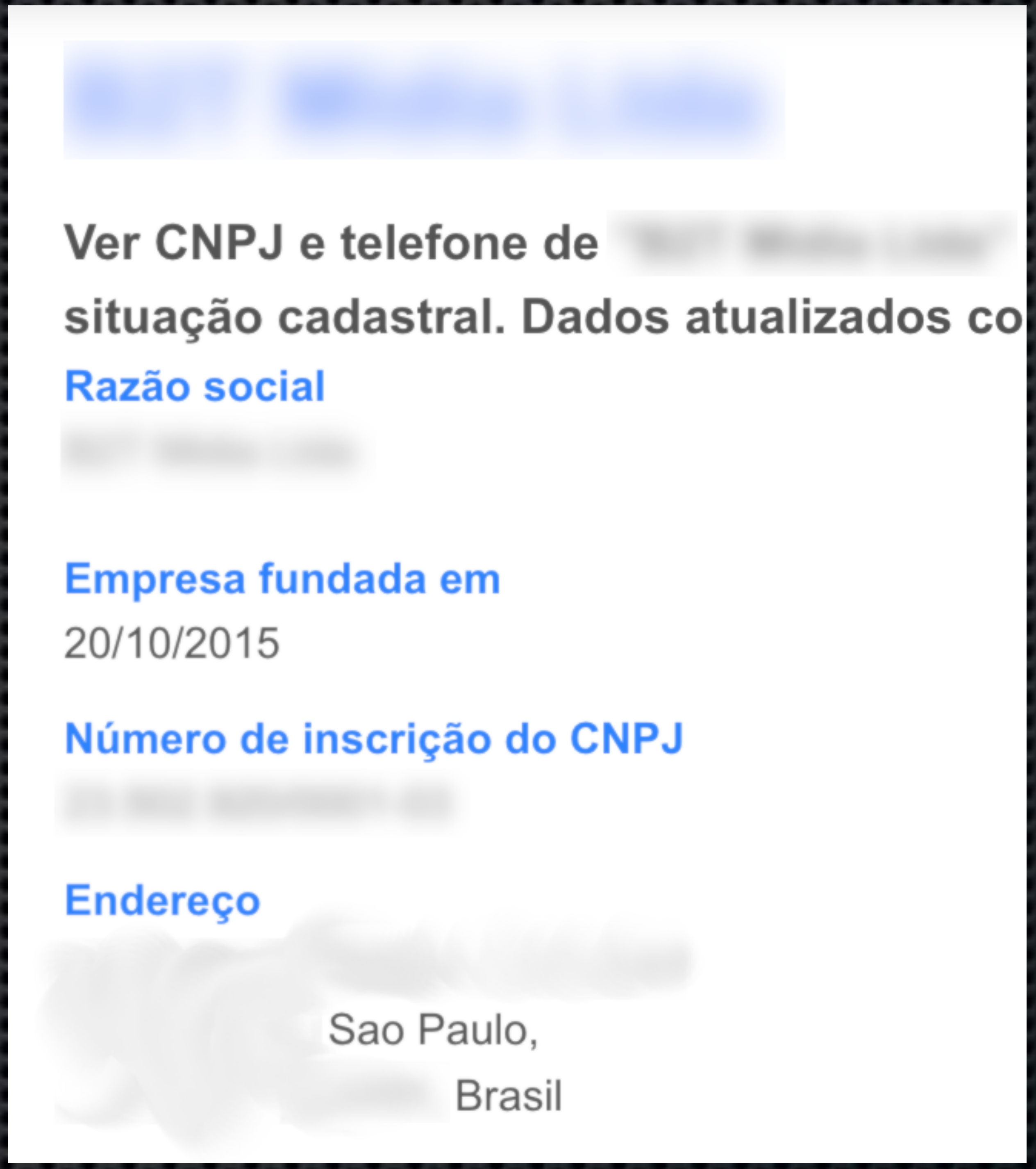
01-12-2014

Total de Mensagens

0

Mostrar Todas as Estatísticas

CreativeUpdater



[redacted]

Ver CNPJ e telefone de [redacted] situação cadastral. Dados atualizados co

Razão social

[redacted]

Empresa fundada em

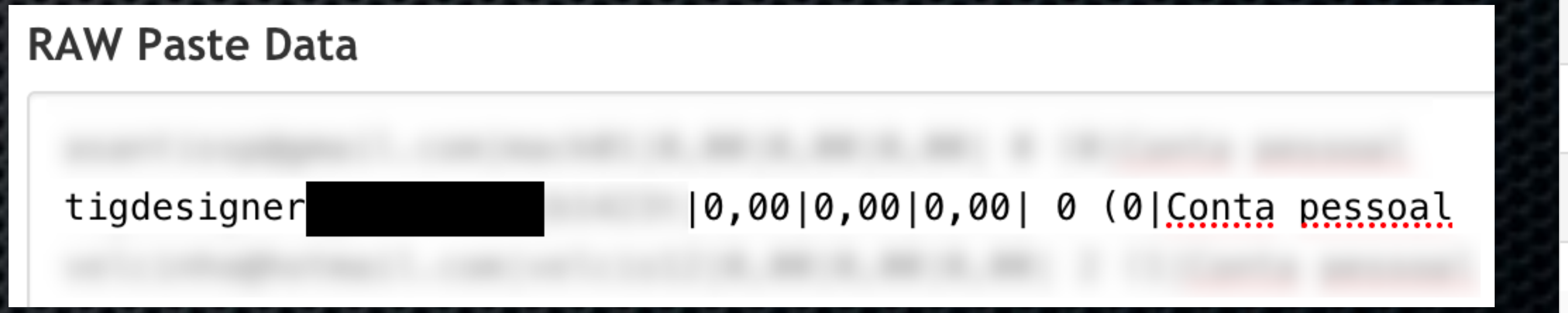
20/10/2015

Número de inscrição do CNPJ

[redacted]

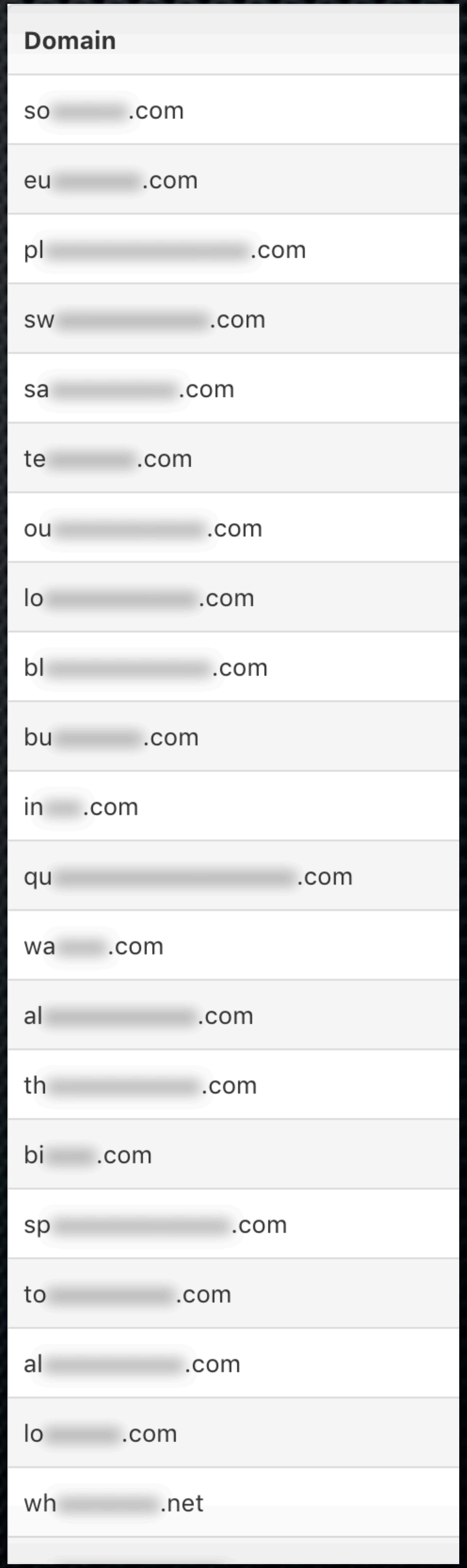
Endereço

[redacted]
Sao Paulo,
Brasil



RAW Paste Data

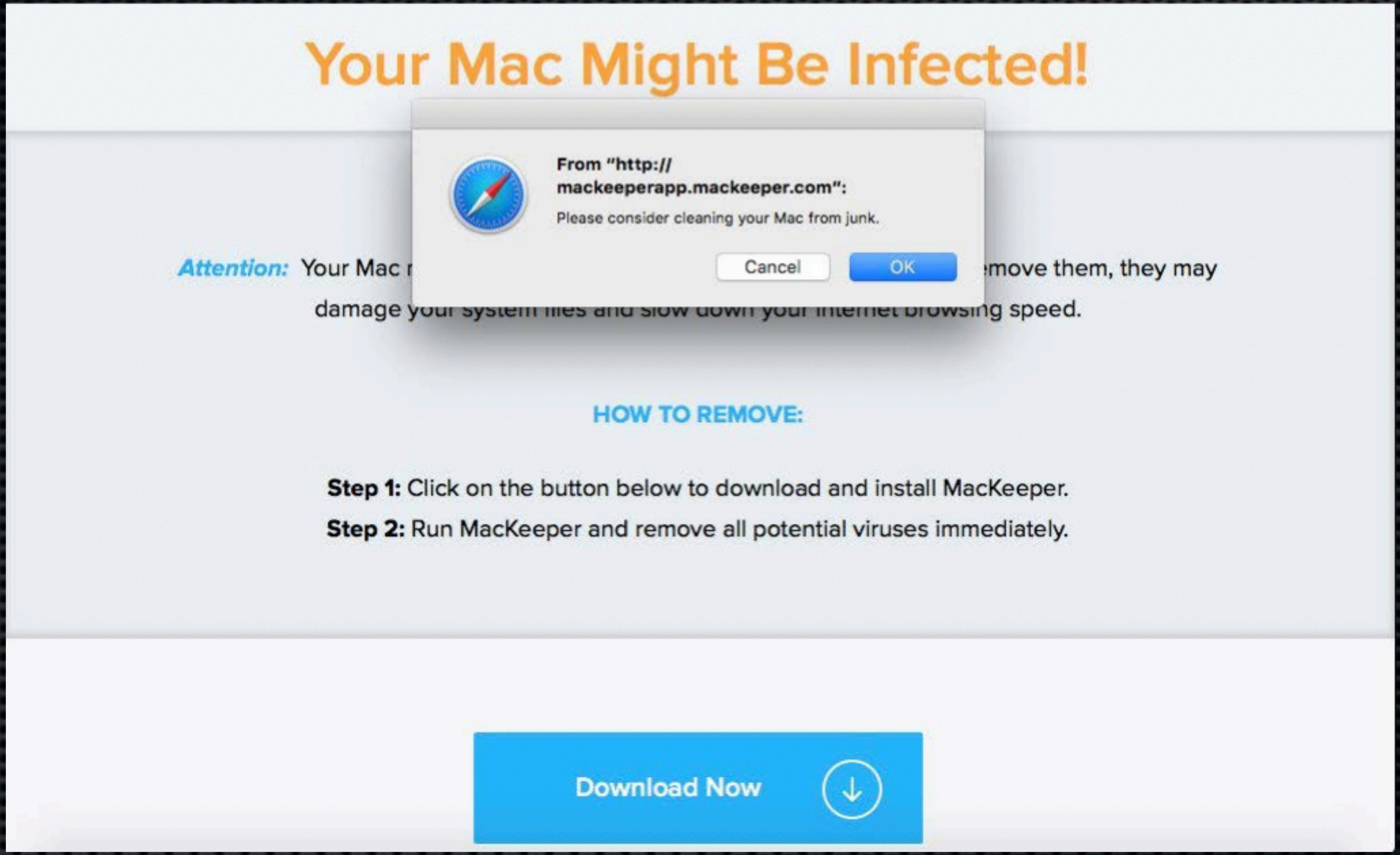
```
[redacted]
tigdesigner[redacted]|0,00|0,00|0,00| 0 (0|Conta pessoal
[redacted]
```



Domain
so[redacted].com
eu[redacted].com
pl[redacted].com
sw[redacted].com
sa[redacted].com
te[redacted].com
ou[redacted].com
lo[redacted].com
bl[redacted].com
bu[redacted].com
in[redacted].com
qu[redacted].com
wa[redacted].com
al[redacted].com
th[redacted].com
bi[redacted].com
sp[redacted].com
to[redacted].com
al[redacted].com
lo[redacted].com
wh[redacted].net

*Searching public docs, found home address, phone number, several businesses and domains he manages, and a 6-character password he's used.

Pirrit



Your Mac Might Be Infected!

From "http://mackeeperapp.mackeeper.com":

Please consider cleaning your Mac from junk.

Attention: Your Mac r… …move them, they may damage your system files and slow down your internet browsing speed.

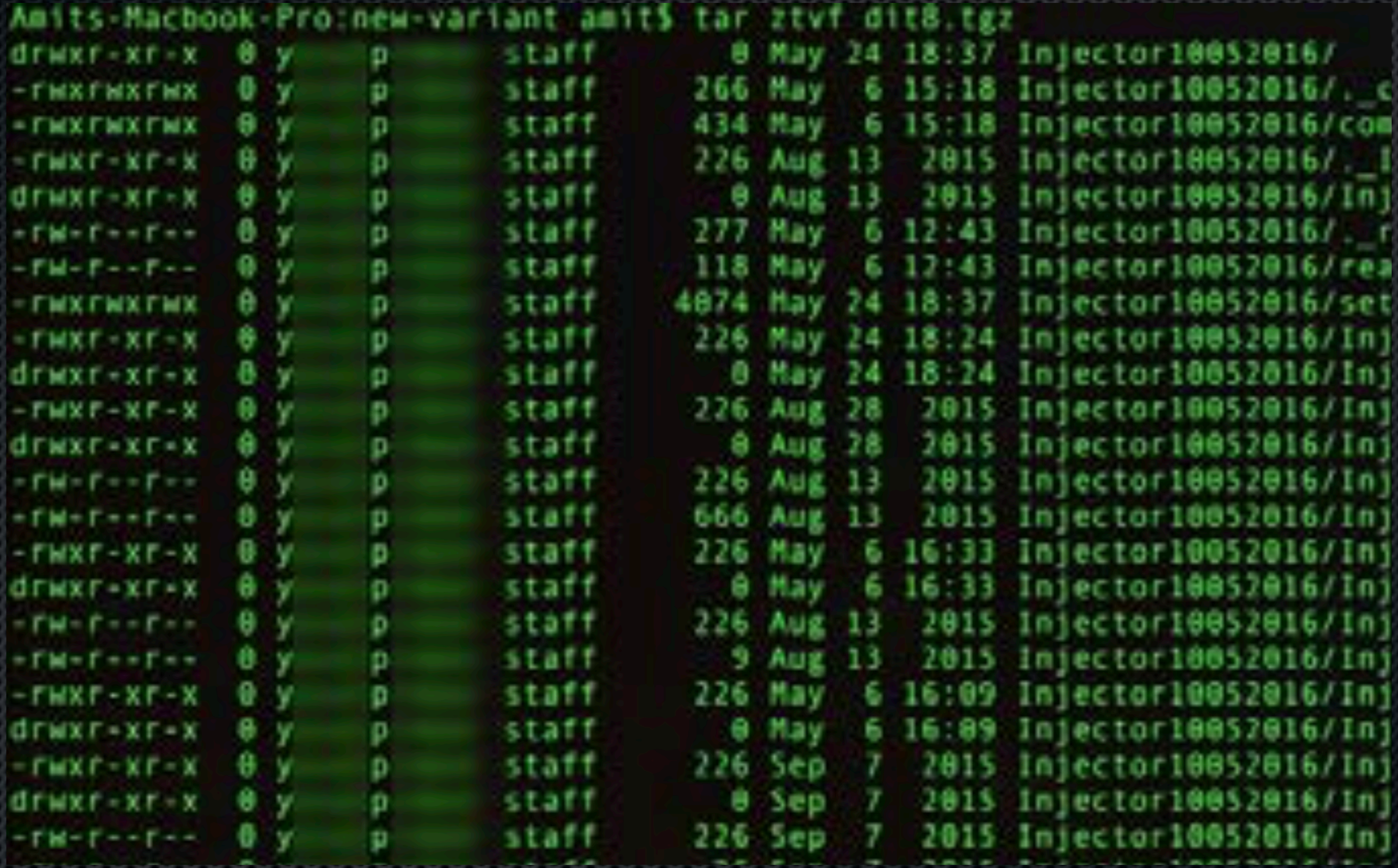
HOW TO REMOVE:

Step 1: Click on the button below to download and install MacKeeper.

Step 2: Run MacKeeper and remove all potential viruses immediately.

*Pirrit is harmful adware. (Credit to Amit Serper for this research)

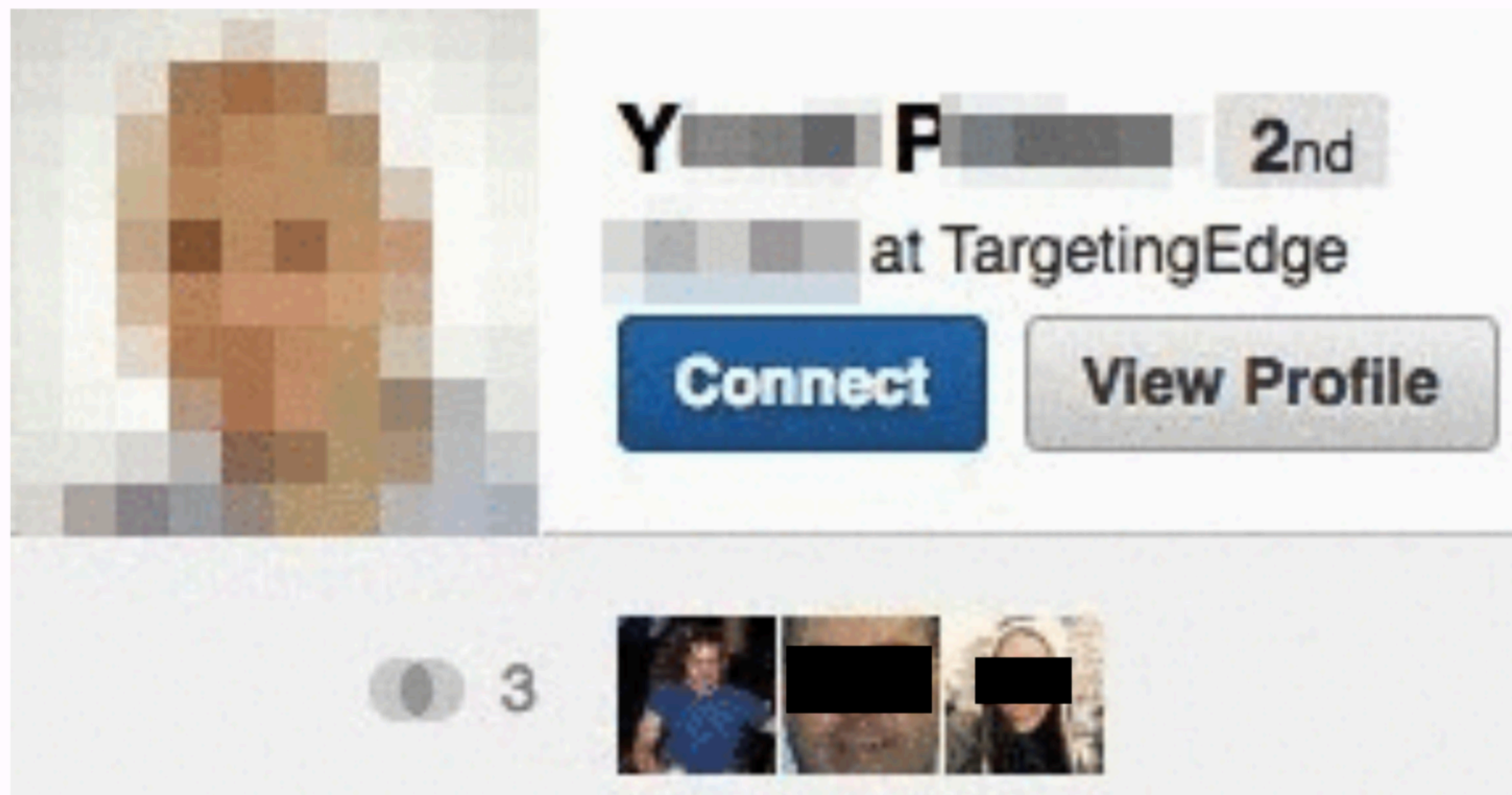
Pirrit



```
Amits-Macbook-Pro:new-variant amit$ tar ztvf dit8.tgz
drwxr-xr-x  0 y[redacted] p[redacted] staff      0 May 24 18:37 Injector10052016/
-rwxrwxrwx  0 y[redacted] p[redacted] staff    266 May  6 15:18 Injector10052016/._c
-rwxrwxrwx  0 y[redacted] p[redacted] staff    434 May  6 15:18 Injector10052016/com
-rwxr-xr-x  0 y[redacted] p[redacted] staff    226 Aug 13  2015 Injector10052016/._I
drwxr-xr-x  0 y[redacted] p[redacted] staff      0 Aug 13  2015 Injector10052016/Inj
-rw-r--r--  0 y[redacted] p[redacted] staff    277 May  6 12:43 Injector10052016/._r
-rw-r--r--  0 y[redacted] p[redacted] staff    118 May  6 12:43 Injector10052016/rea
-rwxrwxrwx  0 y[redacted] p[redacted] staff   4074 May 24 18:37 Injector10052016/set
-rwxr-xr-x  0 y[redacted] p[redacted] staff    226 May 24 18:24 Injector10052016/Inj
drwxr-xr-x  0 y[redacted] p[redacted] staff      0 May 24 18:24 Injector10052016/Inj
-rwxr-xr-x  0 y[redacted] p[redacted] staff    226 Aug 28  2015 Injector10052016/Inj
drwxr-xr-x  0 y[redacted] p[redacted] staff      0 Aug 28  2015 Injector10052016/Inj
-rw-r--r--  0 y[redacted] p[redacted] staff    226 Aug 13  2015 Injector10052016/Inj
-rw-r--r--  0 y[redacted] p[redacted] staff    666 Aug 13  2015 Injector10052016/Inj
-rwxr-xr-x  0 y[redacted] p[redacted] staff    226 May  6 16:33 Injector10052016/Inj
drwxr-xr-x  0 y[redacted] p[redacted] staff      0 May  6 16:33 Injector10052016/Inj
-rw-r--r--  0 y[redacted] p[redacted] staff    226 Aug 13  2015 Injector10052016/Inj
-rw-r--r--  0 y[redacted] p[redacted] staff      9 Aug 13  2015 Injector10052016/Inj
-rwxr-xr-x  0 y[redacted] p[redacted] staff    226 May  6 16:09 Injector10052016/Inj
drwxr-xr-x  0 y[redacted] p[redacted] staff      0 May  6 16:09 Injector10052016/Inj
-rwxr-xr-x  0 y[redacted] p[redacted] staff    226 Sep  7  2015 Injector10052016/Inj
drwxr-xr-x  0 y[redacted] p[redacted] staff      0 Sep  7  2015 Injector10052016/Inj
-rw-r--r--  0 y[redacted] p[redacted] staff    226 Sep  7  2015 Injector10052016/Inj
```

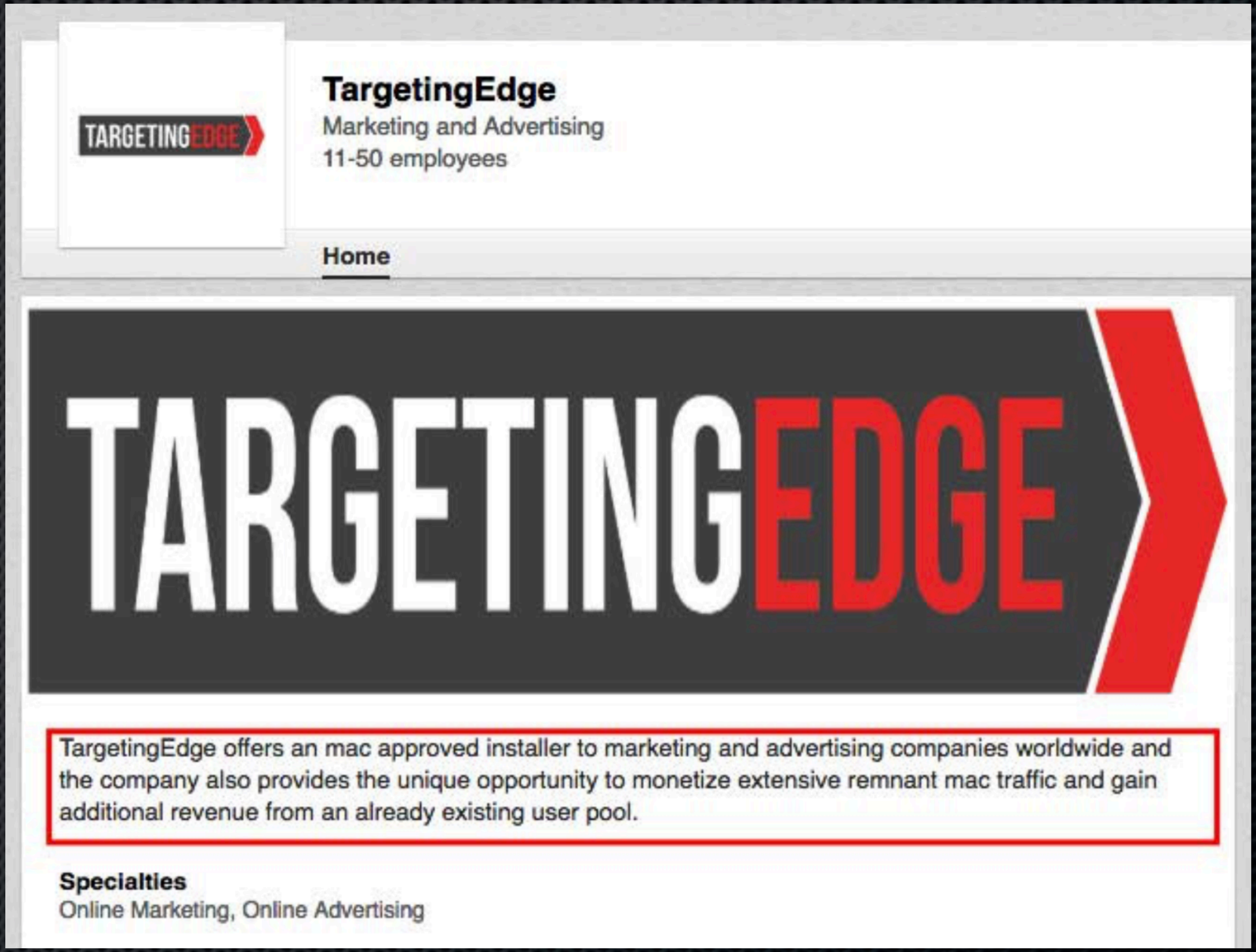
*The dev's real name was embedded in the metadata of a .tgz archive dropped by the malware.

Pirrit



Y[redacted] P[redacted] 2nd

[redacted] at TargetingEdge



TargetingEdge

Marketing and Advertising

11-50 employees

TargetingEdge offers an mac approved installer to marketing and advertising companies worldwide and the company also provides the unique opportunity to monetize extensive remnant mac traffic and gain additional revenue from an already existing user pool.

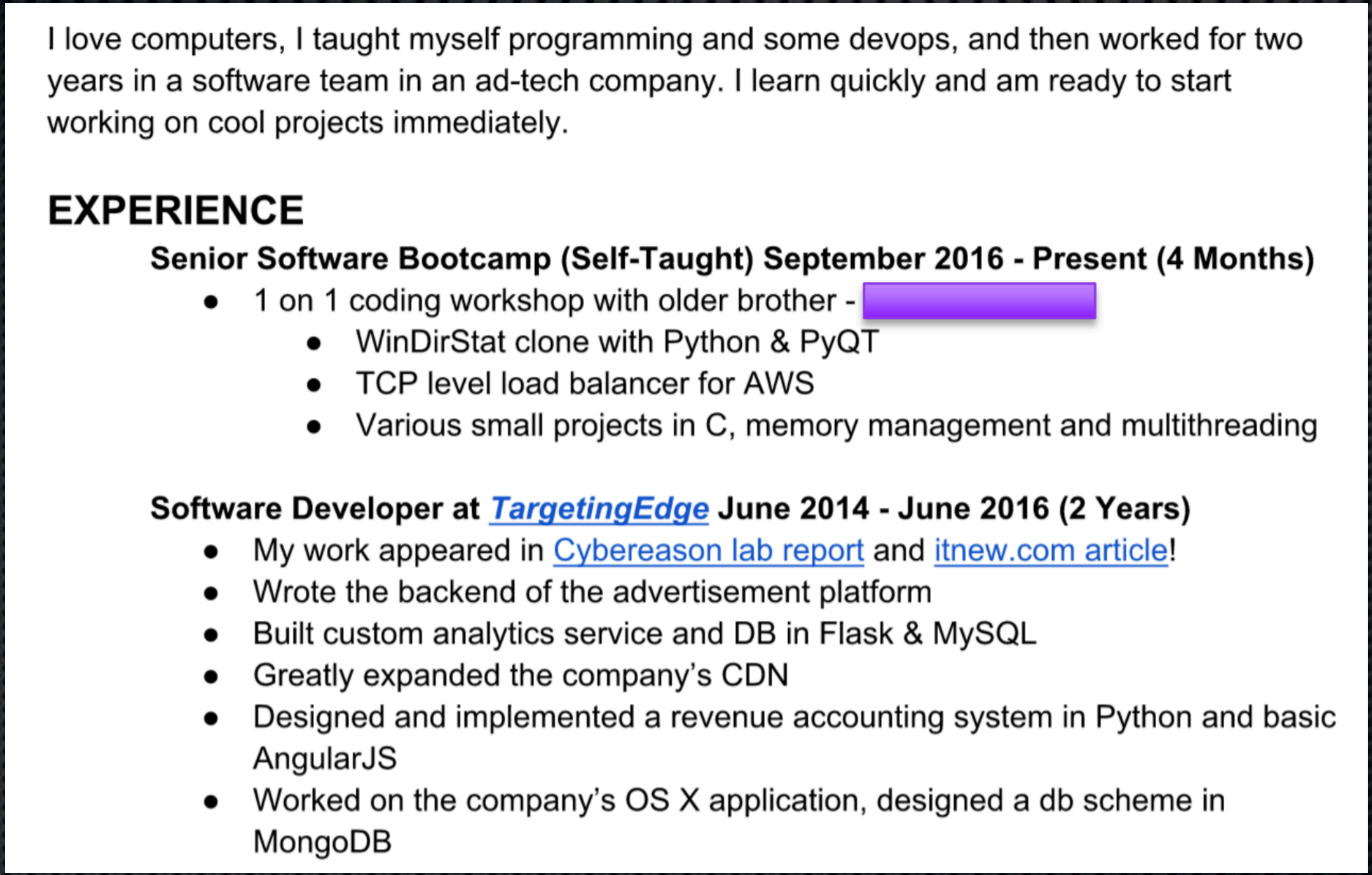
Specialties

Online Marketing, Online Advertising

*Not wanting to make the same mistake twice, the dev started using an account named…

*...Batman!

Pirrit



I love computers, I taught myself programming and some devops, and then worked for two years in a software team in an ad-tech company. I learn quickly and am ready to start working on cool projects immediately.

EXPERIENCE

Senior Software Bootcamp (Self-Taught) September 2016 - Present (4 Months)

- 1 on 1 coding workshop with older brother - [redacted]
    - WinDirStat clone with Python & PyQT
    - TCP level load balancer for AWS
    - Various small projects in C, memory management and multithreading

Software Developer at *TargetingEdge* June 2014 - June 2016 (2 Years)

- My work appeared in Cybereason lab report and itnew.com article!
- Wrote the backend of the advertisement platform
- Built custom analytics service and DB in Flask & MySQL
- Greatly expanded the company's CDN
- Designed and implemented a revenue accounting system in Python and basic AngularJS
- Worked on the company's OS X application, designed a db scheme in MongoDB

*A different Pirrit dev later applied for a job where Serper works.

Fruitfly

* The FBI tracked down Phillip R. Durachinsky, the creator of the Fruitfly (aka Quimitchin) malware, which Durachinsky had been using for 14 years to spy on victims in the U.S. Although not all of the FBI's research methodologies are known to the public, it is clear that they have a lot more resources than the average malware researcher. Durachinsky is still awaiting trial.

The Lesson

*"Kids, you tried your best, and you failed miserably. The lesson is: never try." –Homer J. Simpson

https://youtu.be/F6uUY-BNLbY

©Fox

Resources

- New white paper has all the links!
- The Mac Security Blog : intego.com/mac-security-blog

Thanks!

- Fred Blaison, Amit Serper, Patrick Wardle, Thomas Reed, Arnaud Abbati, and Nicholas Ptacek for their research and/or feedback

Questions?

Josh Long • jlong@intego.com

@theJoshMeister • thejoshmeister.com

Objective by the Sea

intego

@intego_security /Intego @IntegoSecurity

Image credits

- Apple juice/apples image by Phongnguyen1410; CC-BY-SA-4.0
- Pirrit screenshots from Amit Serper's RSAC 2017 slides (PDF)
- Fruitfly image by Katja Schulz via Wikimedia Commons; CC-BY-2.0
- All other images, logos, etc. are the property of their respective owners