Proactive Password Leak Processing

Bruce K. Marshall   @PwdRsch
bkmarshall@PasswordResearch.com

Extent of Password Reuse

- What people say they do when surveyed
  - 61% reported they reused passwords across sites. CSID survey 2012 [1]
  - 46% responded ‘yes’ to question “I use the same password for several of my personal online accounts.” ESET survey 2012 [2]
  - 55% agreed “I use the same passwords for most, if not all, websites.” Ofcom interviews 2013 [3]

Extent of Password Reuse

- What people do as seen in password leaks
  - 77% of participants would either modify or reuse existing passwords. 43% would use the exact same password at different websites. The Tangled Web of Password Reuse 2014 [4]

  - Comparison of 302 common accounts between the password database breach at Yahoo! Voices and SonyPictures.com found 59% used the exact same password, with another 2% using capitalization differences. Troy Hunt 2012 [5]

Extent of Password Reuse

- What people do as seen by their web browsing behavior
  - 73% used password for online banking with at least one other non-financial site. 47% of users share both their online banking user ID and password with at least one nonfinancial website.
    Trusteer 2010 [6]
  - "One hundred fourteen of our subjects (85%) had fewer unique passwords than they did websites that they entered passwords into. Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites 2016 [7]

Account Takeover (ATO) Threat

- Password reuse becomes a problem when an attacker either captures a user’s password or compromises a site and gains access to lots of users’ passwords.

- They can then attempt the stolen credentials for one or more users on other sites. This has been called “credential stuffing”.

Account Checkers

- Account checkers are designed to try username/password pairs against a web site

- Sophisticated programs available
  - SentryMBA – https://sentry.mba
  - Shard – https://github.com/philwantsfish/shard
  - Credmap – https://github.com/lightos/credmap

Popularity of Account Checking

- 2013 Google: “We’ve seen a single attacker using stolen passwords to attempt to break into a million different Google accounts every single day, for weeks at a time. A different gang attempted sign-ins at a rate of more than 100 accounts per second.” [8]

- 2016 Microsoft: “we detect more than 10 million credential attacks every day across our identity systems.” [9]

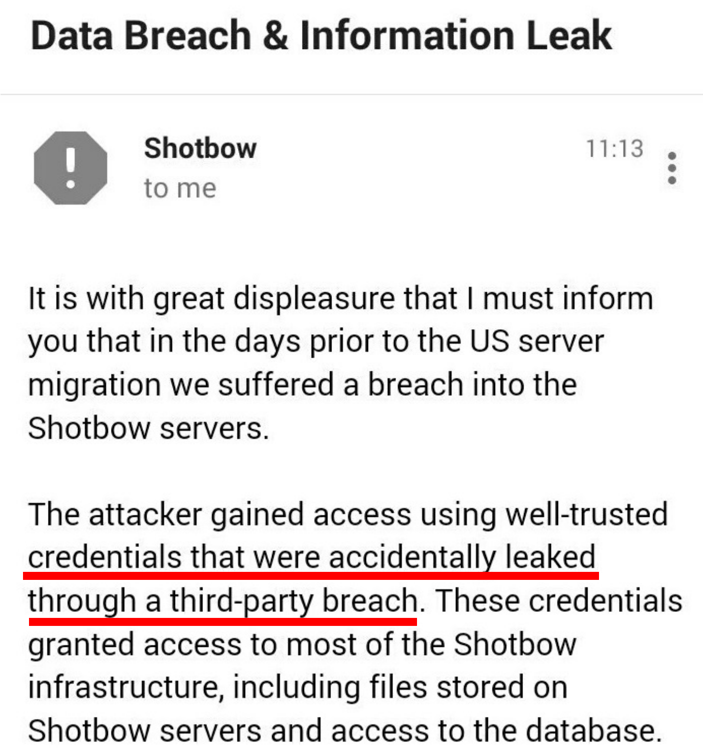
Popularity of Account Checking

- 2016 Akamai [10]
  - “999,980 IPs were involved in the attacks against the customer's login page.” 427 million accounts were checked in a one week period.
  - 817,390 IPs making 388 million login attempts using 65 million email addresses.
  - Comparing source IPs of both attacks, they found 70% match, implying the same org responsible for both, or that they used the same botnet.

Password Leaks Spur ATO

- “ATO attacks seem to spike in activity after a major data breach, due to the common practice of password reuse.” Akamai [10]

- Taobao attacked over a few days in Oct 2015 [11]
  - Used 99M credentials collected from other sites.
  - 20.5 million matched Taobao accounts, which was about 1 in 20 of their total annual active buyers.
  - Wasn’t detected until November, however Alibaba says at the time their security systems discovered and blocked the vast majority of log-in attempts.
  - Still resulted in around $1 million of fraud transactions on the site.

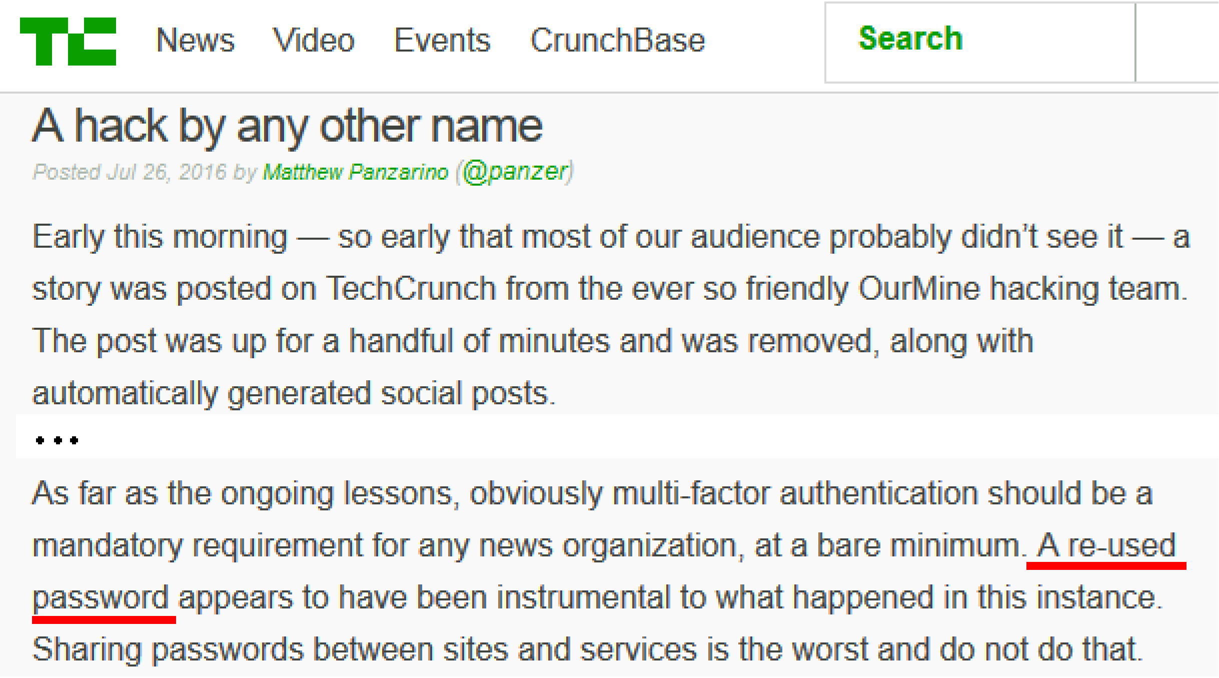


Data Breach & Information Leak

Shotbow 11:13
to me

It is with great displeasure that I must inform you that in the days prior to the US server migration we suffered a breach into the Shotbow servers.

The attacker gained access using well-trusted credentials that were accidentally leaked through a third-party breach. These credentials granted access to most of the Shotbow infrastructure, including files stored on Shotbow servers and access to the database.



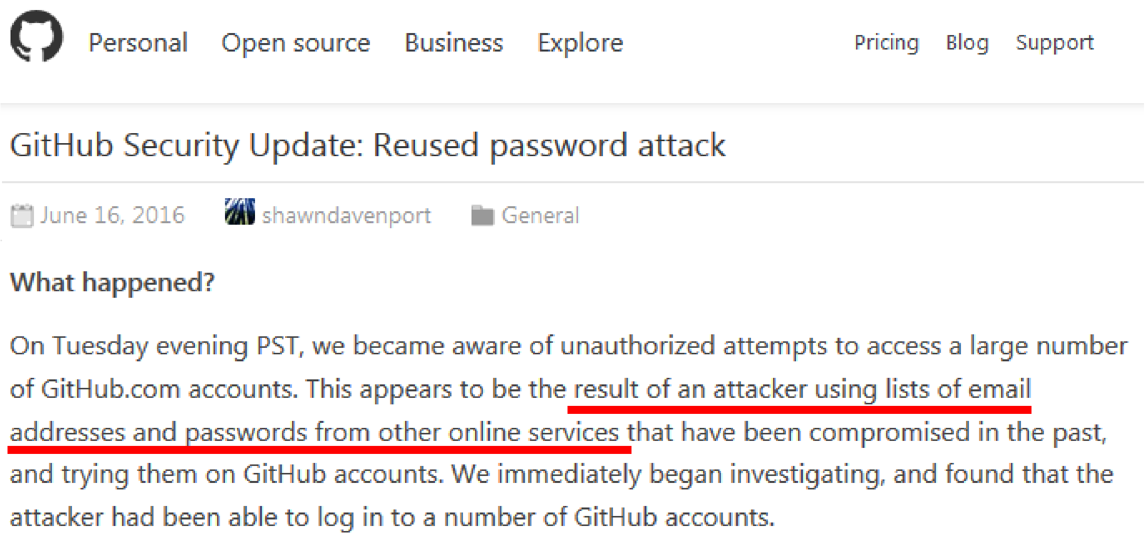
A hack by any other name

Posted Jul 26, 2016 by Matthew Panzarino (@panzer)

Early this morning — so early that most of our audience probably didn't see it — a story was posted on TechCrunch from the ever so friendly OurMine hacking team. The post was up for a handful of minutes and was removed, along with automatically generated social posts.

• • •

As far as the ongoing lessons, obviously multi-factor authentication should be a mandatory requirement for any news organization, at a bare minimum. A re-used password appears to have been instrumental to what happened in this instance. Sharing passwords between sites and services is the worst and do not do that.



GitHub Security Update: Reused password attack

June 16, 2016 shawndavenport General

What happened?

On Tuesday evening PST, we became aware of unauthorized attempts to access a large number of GitHub.com accounts. This appears to be the result of an attacker using lists of email addresses and passwords from other online services that have been compromised in the past, and trying them on GitHub accounts. We immediately began investigating, and found that the attacker had been able to log in to a number of GitHub accounts.

Users Experiencing ATO

- Roughly 27% of 4,000 US & UK respondents surveyed had one or more online accounts compromised in the past year. Gigya 2016 [12]

Value of ATO to Attackers

- Access to money or possessions
- Access to credits that can be converted into services or products
- Access to in-game items
- Scamming or trying to infect contacts
- Sending spam
- Social boosting
- Selling accounts to someone who wants to do one of the above

Is It Our Responsibility to Care?

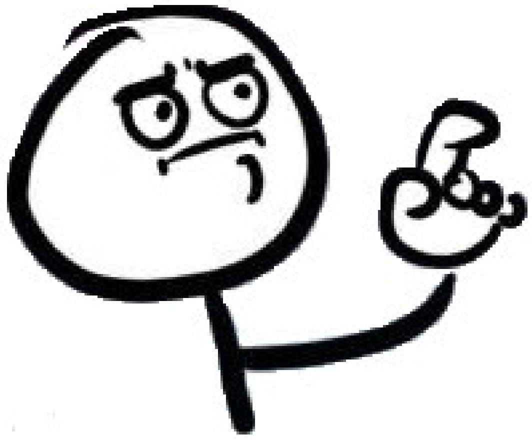
- User made a decision to reuse their password
- Should you just wait to see if reuse causes a problem on your site and then react?

User Perspectives on Reuse

- 2015 paper I Added ! at the End to Make It Secure [13] asked about password reuse:
  - ‘I know password reuse is a terrible idea, but it does not keep me awake at night… I have never seen any negative consequences.’
  - ‘I usually use the same password for many things, but am not concerned since I’ve been doing this for a long time.’
  - ‘I should worry about consequences of password reuse, but I don’t.’

User Perspectives on Reuse

- Part of the problem is the average user's perception about what risks they face.

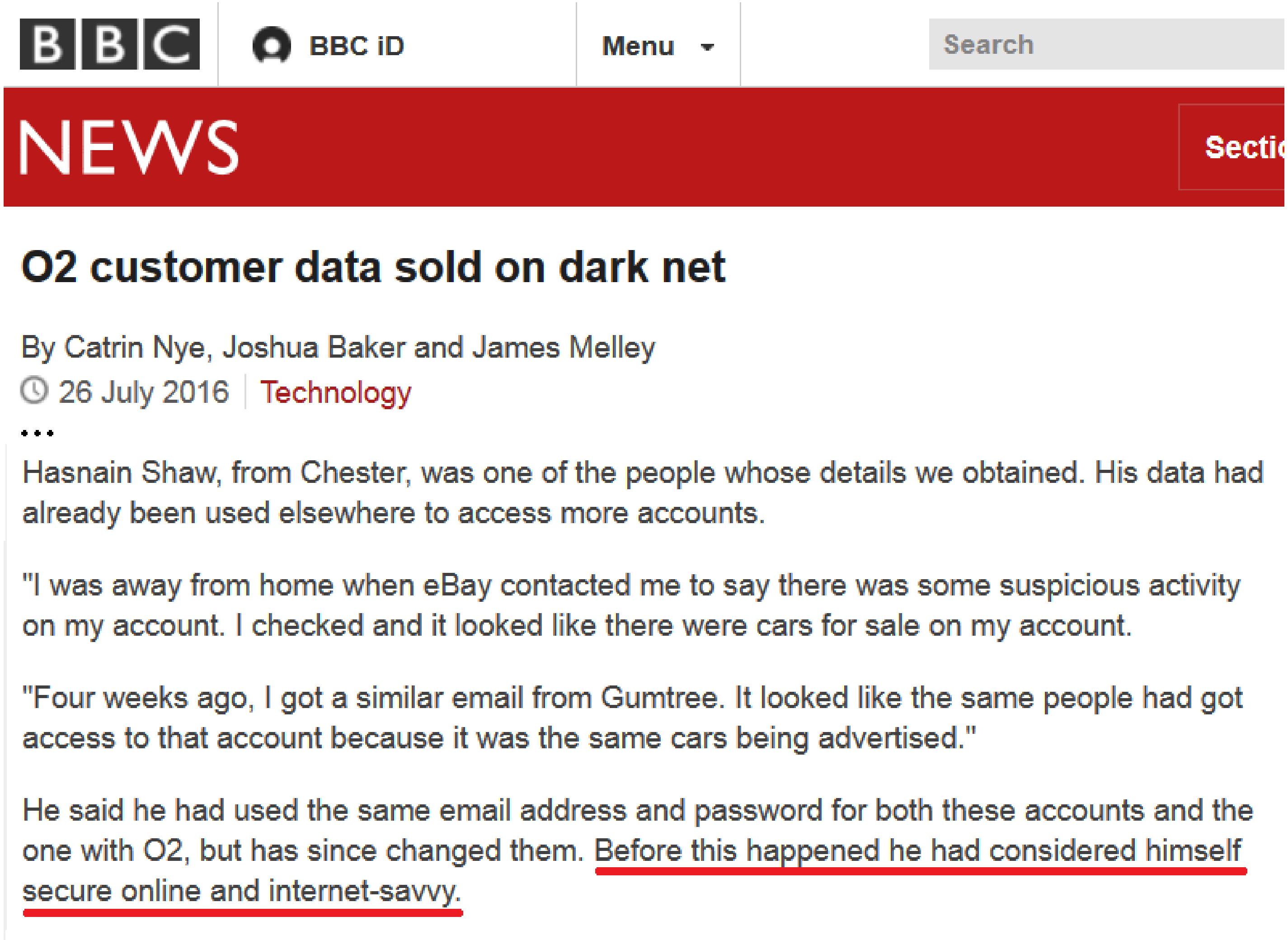


'I reuse passwords all the time if the password is a good one.'

'My reused password is not easily guessed.'

'No one can guess my reused password.'

User Perspectives on Reuse



O2 customer data sold on dark net

By Catrin Nye, Joshua Baker and James Melley

26 July 2016 | Technology

…

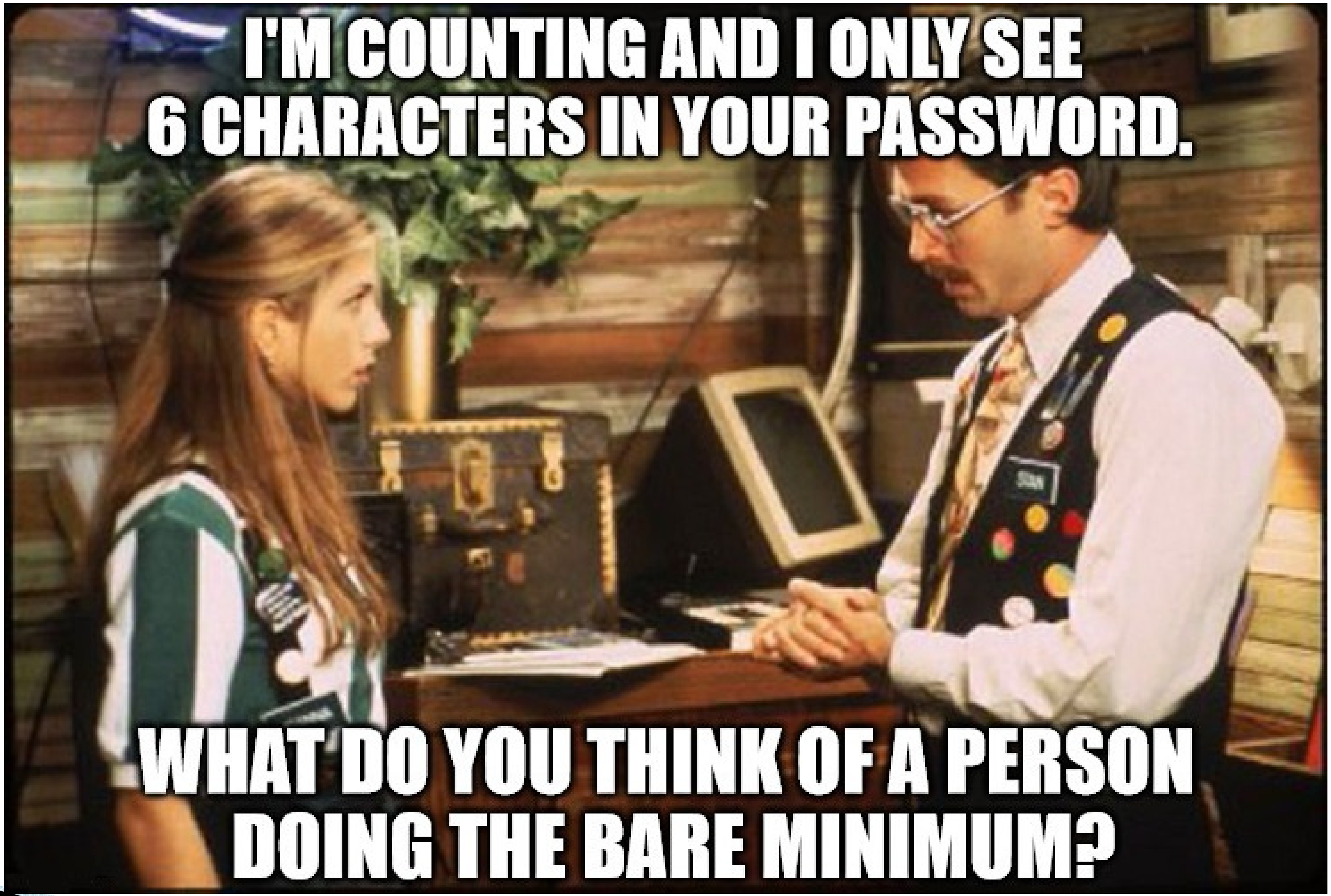
Hasnain Shaw, from Chester, was one of the people whose details we obtained. His data had already been used elsewhere to access more accounts.

"I was away from home when eBay contacted me to say there was some suspicious activity on my account. I checked and it looked like there were cars for sale on my account.

"Four weeks ago, I got a similar email from Gumtree. It looked like the same people had got access to that account because it was the same cars being advertised."

He said he had used the same email address and password for both these accounts and the one with O2, but has since changed them. Before this happened he had considered himself secure online and internet-savvy.

Users Also Rely On Our Guidance


I'M COUNTING AND I ONLY SEE 6 CHARACTERS IN YOUR PASSWORD.
WHAT DO YOU THINK OF A PERSON DOING THE BARE MINIMUM?

Users Also Rely On Our Guidance

- 56% said the sites they visited had ultimate responsibility for online account protection. TeleSign 2014 [14]

- 39% of users believe websites are to blame for online account compromises by not offering sufficient security features. Imperium 2013 [15]

One Man’s Opinion

“The biggest challenge facing Yahoo? I think by far the biggest challenge is user security. It’s not people breaking into us, it’s making our product safe for normal users.

The ‘death of the password’ paradigm and replacing it is by far the worst thing. There’s, in theory, nothing we can do. In practice it means we need to rebuild how we interact with Sally so that she isn’t using the same password everywhere. And if she loses her password it’s not a complete disaster.

So yeah, by far the password problem is my biggest problem.”

--Alex Stamos (then Yahoo CISO) [16]

Measures to Combat Reuse

- Enforce regular or incident-driven password expiration
- Design unusual password policy requirements
- Assign random passwords to users
- Eliminate password use altogether
- Implement 2FA/2SV
- Create a blacklist from leaked passwords
- Utilize contextual/risk-based authentication
- Proactive seek out password leaks and compare to your own users

Goals of Password Leak Processing

- Reduce ATO based on known risks
- Save time/money preventing ATO instead of dealing with impacts after it occurs
- Demonstrate security commitment to your users / investors

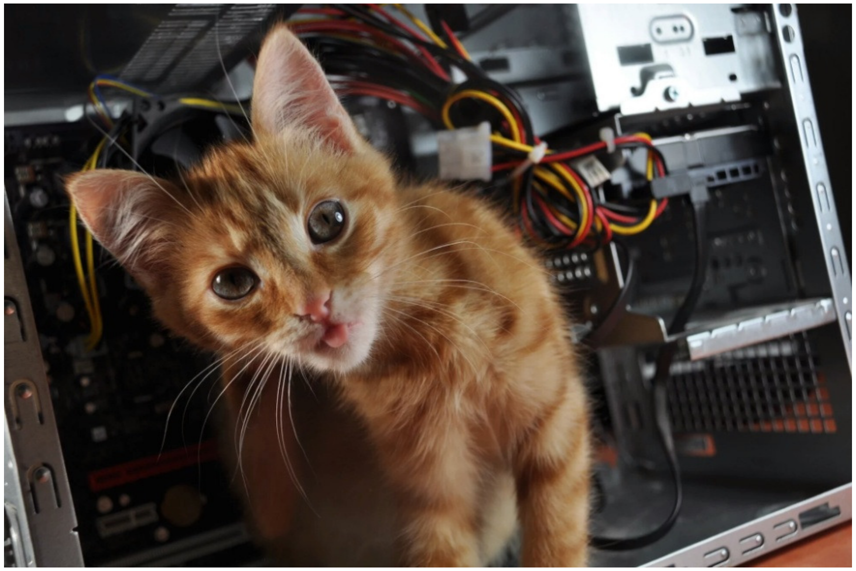


Photo credit:
Zach Whitaker

Where Do Leaks Come From?

- Common Sources
  - Server compromises & SQL injection
  - Trojans & malware
  - Phishing
  - MITM
  - Compilations of above sources

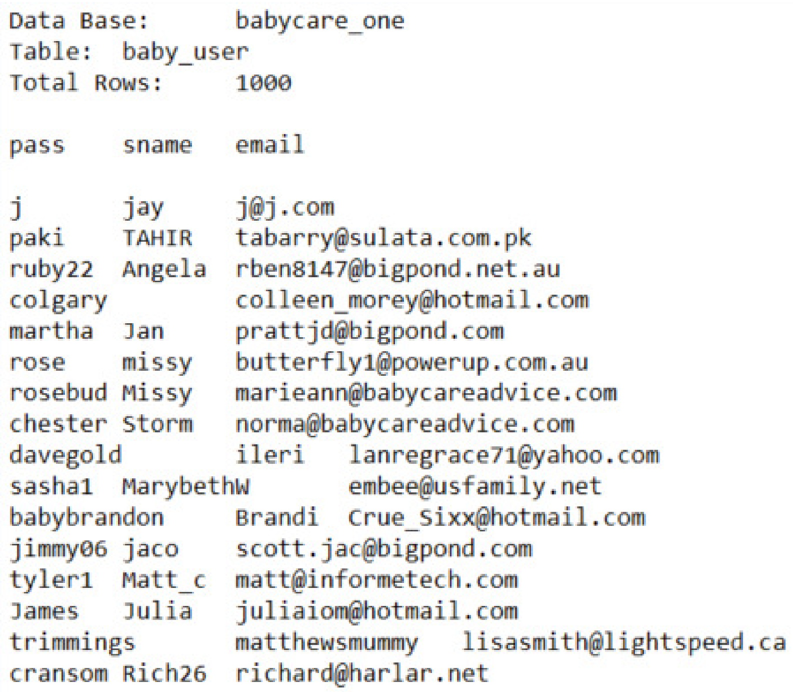
- Some will be duplicates, possibly with someone else claiming credit or changing alleged origin
- Some leaks will not be limited just to account database and will have superfluous data

What Password Leaks to Process?

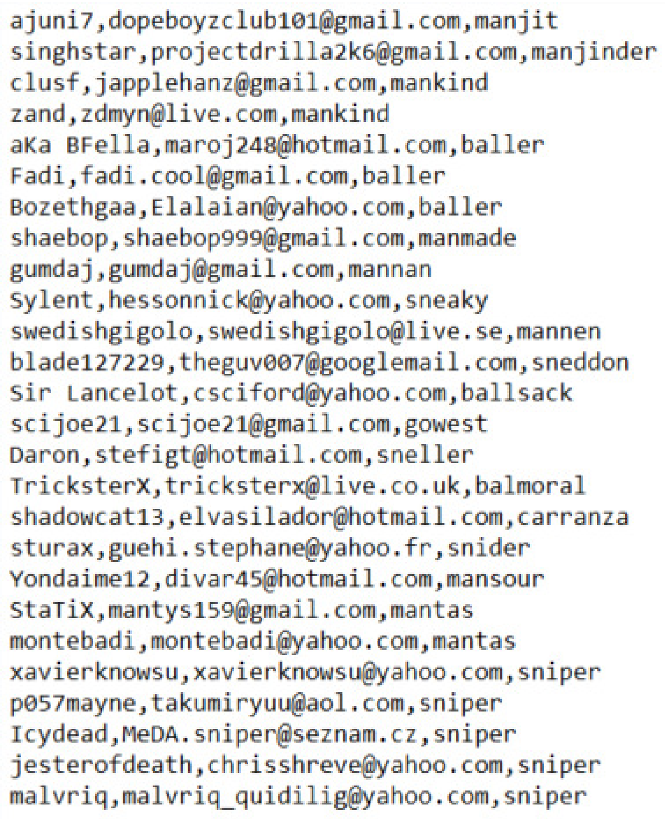
- Leaks alleged to be from your site or users
- Easy leaks to process
- Large leaks (e.g. LinkedIn, MySpace)
- All leaks you can find

THOMAS SAUR, Isomedien

What Do Password Leaks Look Like

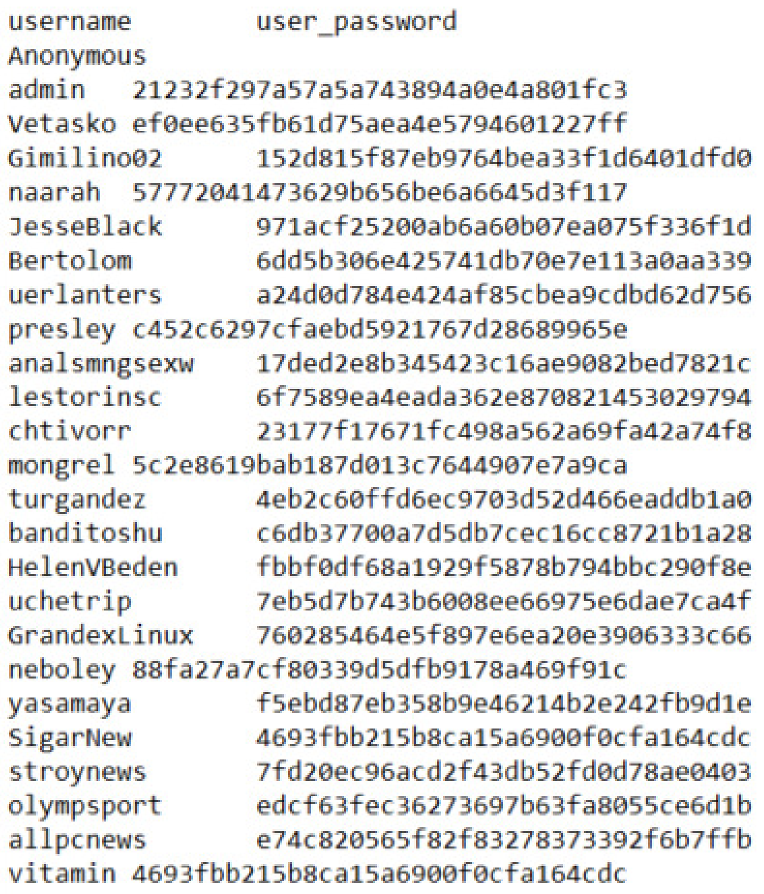


```
Data Base:      babycare_one
Table:  baby_user
Total Rows:     1000

pass    sname   email

j       jay     j@j.com
paki    TAHIR   tabarry@sulata.com.pk
ruby22  Angela  rben8147@bigpond.net.au
colgary         colleen_morey@hotmail.com
martha  Jan     prattjd@bigpond.com
rose    missy   butterfly1@powerup.com.au
rosebud Missy   marieann@babycareadvice.com
chester Storm   norma@babycareadvice.com
davegold        ileri   lanregrace71@yahoo.com
sasha1  MarybethW       embee@usfamily.net
babybrandon     Brandi  Crue_Sixx@hotmail.com
jimmy06 jaco    scott.jac@bigpond.com
tyler1  Matt_c  matt@informetech.com
James   Julia   juliaiom@hotmail.com
trimmings       matthewsmummy   lisasmith@lightspeed.ca
cransom Rich26  richard@harlar.net
```

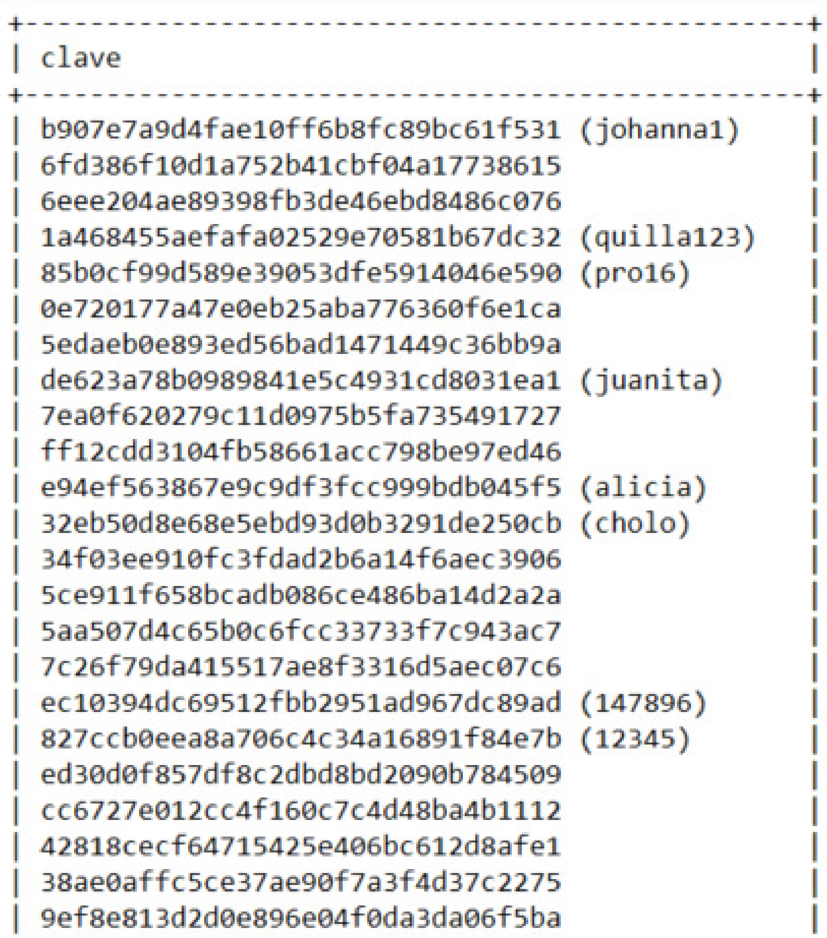


```
ajuni7,dopeboyzclub101@gmail.com,manjit
singhstar,projectdrilla2k6@gmail.com,manjinder
clusf,japplehanz@gmail.com,mankind
zand,zdmyn@live.com,mankind
aKa BFella,maroj248@hotmail.com,baller
Fadi,fadi.cool@gmail.com,baller
Bozethgaa,Elalaian@yahoo.com,baller
shaebop,shaebop999@gmail.com,manmade
gumdaj,gumdaj@gmail.com,mannan
Sylent,hessonnick@yahoo.com,sneaky
swedishgigolo,swedishgigolo@live.se,mannen
blade127229,theguv007@googlemail.com,sneddon
Sir Lancelot,csciford@yahoo.com,ballsack
scijoe21,scijoe21@gmail.com,gowest
Daron,stefigt@hotmail.com,sneller
TricksterX,tricksterx@live.co.uk,balmoral
shadowcat13,elvasilador@hotmail.com,carranza
sturax,guehi.stephane@yahoo.fr,snider
Yondaime12,divar45@hotmail.com,mansour
StaTiX,mantys159@gmail.com,mantas
montebadi,montebadi@yahoo.com,mantas
xavierknowsu,xavierknowsu@yahoo.com,sniper
p057mayne,takumiryuu@aol.com,sniper
Icydead,MeDA.sniper@seznam.cz,sniper
jesterofdeath,chrisshreve@yahoo.com,sniper
malvriq,malvriq_quidilig@yahoo.com,sniper
```

What Do Password Leaks Look Like

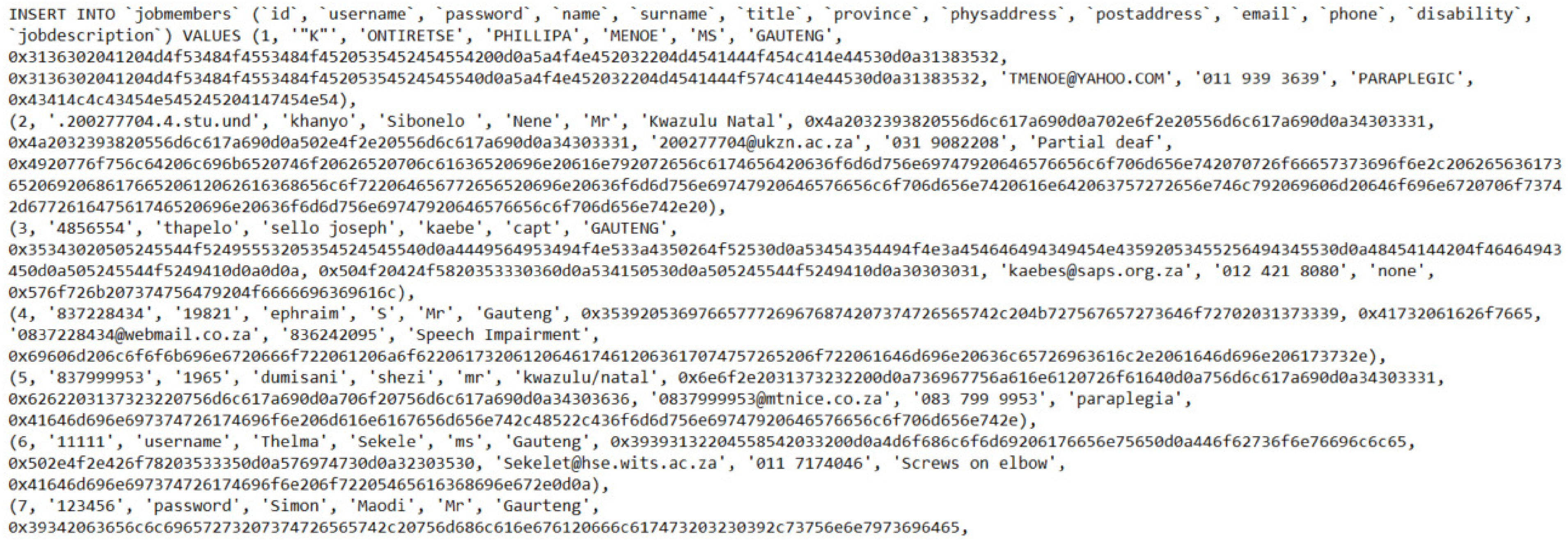


```
username        user_password
Anonymous
admin   21232f297a57a5a743894a0e4a801fc3
Vetasko ef0ee635fb61d75aea4e5794601227ff
Gimilino02      152d815f87eb9764bea33f1d6401dfd0
naarah  57772041473629b656be6a6645d3f117
JesseBlack      971acf25200ab6a60b07ea075f336f1d
Bertolom        6dd5b306e425741db70e7e113a0aa339
uerlanters      a24d0d784e424af85cbea9cdbd62d756
presley c452c6297cfaebd5921767d28689965e
analsmngsexw    17ded2e8b345423c16ae9082bed7821c
lestorinsc      6f7589ea4eada362e870821453029794
chtivorr        23177f17671fc498a562a69fa42a74f8
mongrel 5c2e8619bab187d013c7644907e7a9ca
turgandez       4eb2c60ffd6ec9703d52d466eaddb1a0
banditoshu      c6db37700a7d5db7cec16cc8721b1a28
HelenVBeden     fbbf0df68a1929f5878b794bbc290f8e
uchetrip        7eb5d7b743b6008ee66975e6dae7ca4f
GrandexLinux    760285464e5f897e6ea20e3906333c66
neboley 88fa27a7cf80339d5dfb9178a469f91c
yasamaya        f5ebd87eb358b9e46214b2e242fb9d1e
SigarNew        4693fbb215b8ca15a6900f0cfa164cdc
stroynews       7fd20ec96acd2f43db52fd0d78ae0403
olympsport      edcf63fec36273697b63fa8055ce6d1b
allpcnews       e74c820565f82f83278373392f6b7ffb
vitamin 4693fbb215b8ca15a6900f0cfa164cdc
```



```
+-----------------------------------------------+
| clave                                         |
+-----------------------------------------------+
| b907e7a9d4fae10ff6b8fc89bc61f531 (johanna1)   |
| 6fd386f10d1a752b41cbf04a17738615              |
| 6eee204ae89398fb3de46ebd8486c076              |
| 1a468455aefafa02529e70581b67dc32 (quilla123)  |
| 85b0cf99d589e39053dfe5914046e590 (pro16)      |
| 0e720177a47e0eb25aba776360f6e1ca              |
| 5edaeb0e893ed56bad1471449c36bb9a              |
| de623a78b0989841e5c4931cd8031ea1 (juanita)    |
| 7ea0f620279c11d0975b5fa735491727              |
| ff12cdd3104fb58661acc798be97ed46              |
| e94ef563867e9c9df3fcc999bdb045f5 (alicia)     |
| 32eb50d8e68e5ebd93d0b3291de250cb (cholo)      |
| 34f03ee910fc3fdad2b6a14f6aec3906              |
| 5ce911f658bcadb086ce486ba14d2a2a              |
| 5aa507d4c65b0c6fcc33733f7c943ac7              |
| 7c26f79da415517ae8f3316d5aec07c6              |
| ec10394dc69512fbb2951ad967dc89ad (147896)     |
| 827ccb0eea8a706c4c34a16891f84e7b (12345)      |
| ed30d0f857df8c2dbd8bd2090b784509              |
| cc6727e012cc4f160c7c4d48ba4b1112              |
| 42818cecf64715425e406bc612d8afe1              |
| 38ae0affc5ce37ae90f7a3f4d37c2275              |
| 9ef8e813d2d0e896e04f0da3da06f5ba              |
```

What Do Password Leaks Look Like



```
INSERT INTO `jobmembers` (`id`, `username`, `password`, `name`, `surname`, `title`, `province`, `physaddress`, `postaddress`, `email`, `phone`, `disability`,
`jobdescription`) VALUES (1, '"K"', 'ONTIRETSE', 'PHILLIPA', 'MENOE', 'MS', 'GAUTENG',
0x3136302041204d4f53484f4553484f4520535452454554200d0a5a4f4e452032204d4541444f454c414e44530d0a31383532,
0x3136302041204d4f53484f4553484f45205354524545540d0a5a4f4e452032204d4541444f574c414e44530d0a31383532, 'TMENOE@YAHOO.COM', '011 939 3639', 'PARAPLEGIC',
0x43414c4c43454e545245204147454e54),
(2, '.200277704.4.stu.und', 'khanyo', 'Sibonelo ', 'Nene', 'Mr', 'Kwazulu Natal', 0x4a2032393820556d6c617a690d0a702e6f2e20556d6c617a690d0a34303331,
0x4a2032393820556d6c617a690d0a502e4f2e20556d6c617a690d0a34303331, '200277704@ukzn.ac.za', '031 9082208', 'Partial deaf',
0x4920776f756c64206c696b6520746f206265206c6163656520696e20616e792072656c6174656420636f6d6d756e69747920646576656c6f706d656e742070726f66657373696f6e2c206265636173
6520692068617665206120626163686656c6f72206465677265652069e20636f6d6d756e697479206465766656c6f706d656e7420616e6420637572726656e746c792069606d20646f696e6720706f7374
2d677261647561746520696e20636f6d6d756e69747920646576656c6f706d656e742e20),
(3, '4856554', 'thapelo', 'sello joseph', 'kaebe', 'capt', 'GAUTENG',
0x3534302050524544f52495553205354524545540d0a4449564953494f4e533a4350264f52530d0a53454354494f4e3a454646494349454e435920534552564943455530d0a48454144204f46464943
450d0a505245544f5249410d0a0d0a, 0x504f20424f5820353330360d0a534150530d0a505245544f5249410d0a30303031, 'kaebes@saps.org.za', '012 421 8080', 'none',
0x576f726b2073747564479204f6666696369616c),
(4, '837228434', '19821', 'ephraim', 'S', 'Mr', 'Gauteng', 0x35392053697665777269676874207374726565742c204b7275676657273646f72702031373339, 0x41732061626f7665,
'0837228434@webmail.co.za', '836242095', 'Speech Impairment',
0x69606d206c6f6f6b696e6720666f722061206a6f62206173206120646174612063617074757265206f722061646d696e20636c65726963616c2e2061646d696e206173732e),
(5, '837999953', '1965', 'dumisani', 'shezi', 'mr', 'kwazulu/natal', 0x6e6f2e2031373232200d0a736967756a616e6120726f61640d0a756d6c617a690d0a34303331,
0x626220313732322075d6c617a690d0a706f20756d6c617a690d0a34303636, '0837999953@mtnice.co.za', '083 799 9953', 'paraplegia',
0x41646d696e6973747261746696f6e206d616e6167656d656e742c48522c436f6d6d756e69747920646576656c6f706d656e742e),
(6, '11111', 'username', 'Thelma', 'Sekele', 'ms', 'Gauteng', 0x39393132204558542033200d0a4d6f686c6f6d69206176656e75650d0a446f62736f6e76696c6c65,
0x502e4f2e426f78203533350d0a576974730d0a32303530, 'Sekelet@hse.wits.ac.za', '011 7174046', 'Screws on elbow',
0x41646d696e697374726174696f6e206f72205465616368696e672e0d0a),
(7, '123456', 'password', 'Simon', 'Maodi', 'Mr', 'Gaurteng',
0x39342063656c6c69657273207374726565742c20756d686c616e676120666c617473203230392c73756e6e7973696465,
```

Where to Find Password Leaks

- Pastebin.com and similar paste sites

	Dec 2012	Jan 2013
Dumps	154 (125 named)	110 (90 named)
Plaintext passwords	66 (221k)	40 (61k)
Hashed passwords	82 (222k)	64 (101k)
Less than 1K	103	73
More than 10k	7	2
Emails included	N/A	87%

[17]

Where to Find Password Leaks

- Where available (torrents, file sharing)

Site	Accounts	Format
Mate1.com	27M	Plaintext
LinkedIn	117M	SHA-1
MySpace	360M	SHA-1
Tumblr	65M	Salted/hashed
“Twitter”	32M (400M)	Plaintext
VK.com	100M	Plaintext
Badoo.com	127M	MD5

Tools/Sites To Help Find Leaks

- Tools
  - Netflix's Scumblr https://github.com/netflix/scumblr/wiki
  - Dumpmon https://github.com/jordan-wright/dumpmon

- Sites
  - https://hashes.org/public.php
  - https://forum.insidepro.com/

Dark Web & Feds

- Your local underground goods dealer
- Law enforcement

Password Leak Providers

- Hold Security
- LeakedSource
- Threat Intelligence service providers?

Steps to Processing Leaks

- Is it a dump that you've already processed?
- Clean up & convert data into usable format
  - Remove headers, footers, separators, leading/trailing spaces, malformed data
  - Determine relevant fields and their order
  - Filter out records that don't correspond with accounts (email addresses) on your system
- Decide which users you are worried about
  - Any user with email appearing in leak
  - Any user with username appearing in leak
  - Only users whose email/password matches leak

Steps to Processing Leaks

- If plaintext, hash with same scheme you normally use and compare results to matching user account

- If hashed, identify hash and put in a baseline level of effort to crack the easier passwords
  - Any already cracked hashes available?
  - Try brute force, wordlist, hybrid
  - Spend a ‘reasonable’ amount of time

Common Leak Hash Formats

- Top hash types in leaks collected over 6 month period

630	MD5
134	MD5(MD5(p).s)
120	MD5(s.p)
108	MD5(MD5(s).MD5(p))
94	SHA1
53	MySQL5
38	MD5(p.s)
36	Crypt-DES
34	MySQL323
28	SHA512(p.s)
20	MD5(MD5(p))

KoreLogic 2014 [18]

Alternatives to Cracking

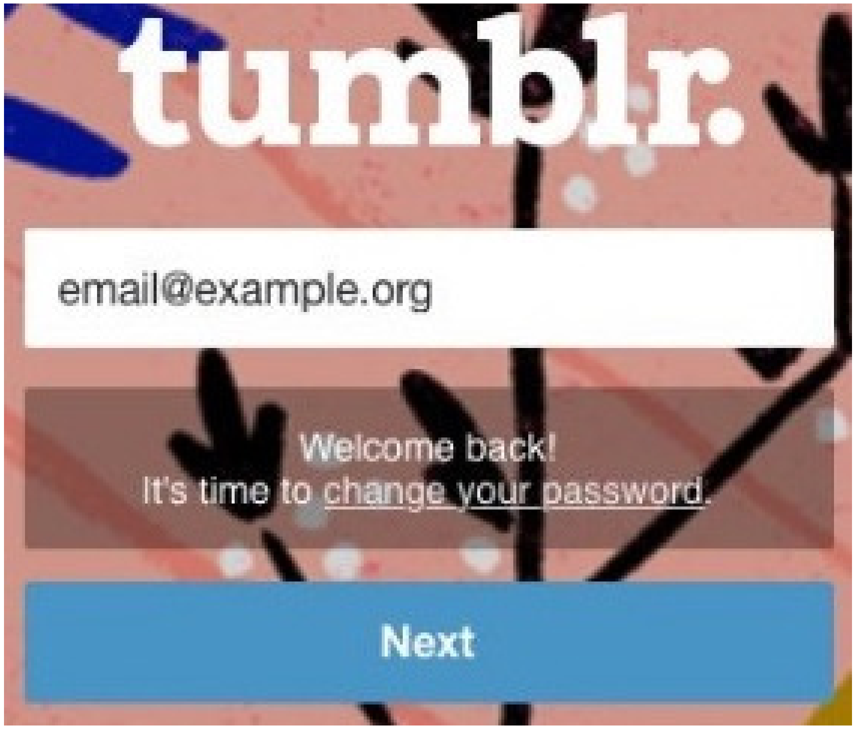
- Hash user plaintexts first using simple, popular hash and then your stronger hash
- When processing leaks with same simple hash you can feed them through your normal hashing process (minus initial step)
- Might have to create additional password hash records if you want to support more than one simple base hash

Alternatives to Cracking

- Determine if you can identify and duplicate the hashing process
- Add step during user login to hash plaintext password using leak processing if user has matching email
- Not as timely as cracking immediately and may require you to maintain database of leaked credentials indefinitely

What To Do & Tell Your Users

- Just notify users of risk and let them decide what to do
- Lock accounts
  - Custom unlock workflow
  - Normal forgotten password workflow
- Flag accounts for secondary auth
- Invalidate session tokens



email@example.org

Welcome back!
It's time to change your password.

What To Do & Tell Your Users

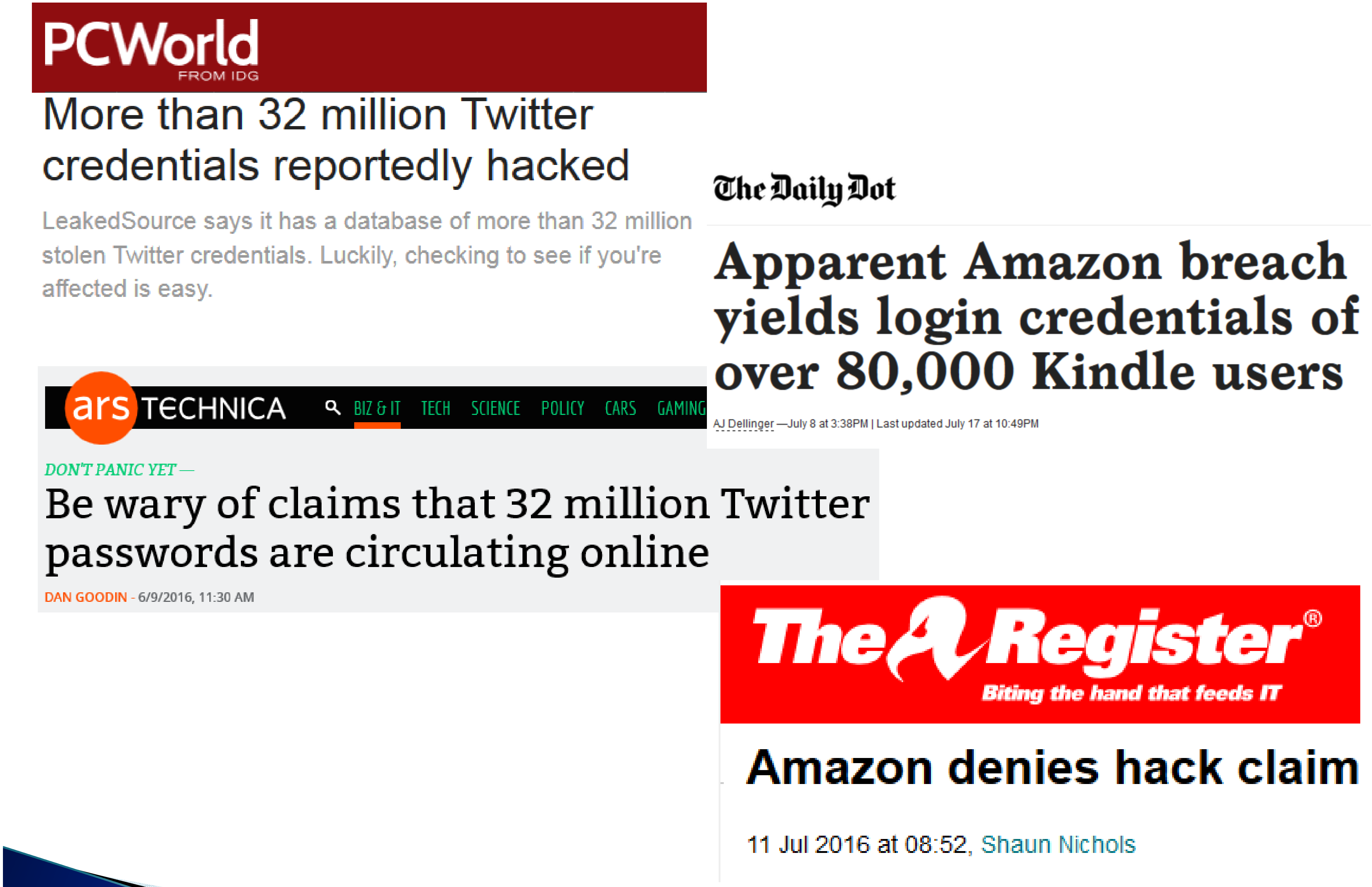
- Inform users of reason for change
  - That their email/password for your site was exposed due reusing it at compromised third-party
  - The name of the third-party?
  - That your site wasn’t compromised
  - Whether or not unauthorized access was detected
  - How to reset their password and regain access
  - Encouragement to turn on/update MFA
  - Educate them on better password practices (e.g. like using password manager)
  - Media release / blog post if needed

Risks of Processing 3rd Party Leaks

- May attract/have to deal with 'nuisance' leaks
  - Fake or old compilation leaks generated by hackers to gain notoriety or money
  - Probably more of a result of you being an interesting target rather than them knowing that you process leaks

Risks of Processing 3rd Party Leaks

- Leak allegedly from large email providers
  - Google found only 2% (476,000) of the 23.8 million combinations were a match for valid accounts. [19]
  - Microsoft found of 33 million combinations 9.6% of the usernames matched an account, and only 0.1% matched password. [9]
  - Mail.ru found of 57 million combos 99.982% invalid [20]



PCWorld FROM IDG

More than 32 million Twitter credentials reportedly hacked

LeakedSource says it has a database of more than 32 million stolen Twitter credentials. Luckily, checking to see if you're affected is easy.

The Daily Dot

Apparent Amazon breach yields login credentials of over 80,000 Kindle users

AJ Dellinger —July 8 at 3:38PM | Last updated July 17 at 10:49PM

ars TECHNICA

DON'T PANIC YET —

Be wary of claims that 32 million Twitter passwords are circulating online

DAN GOODIN - 6/9/2016, 11:30 AM

The Register®

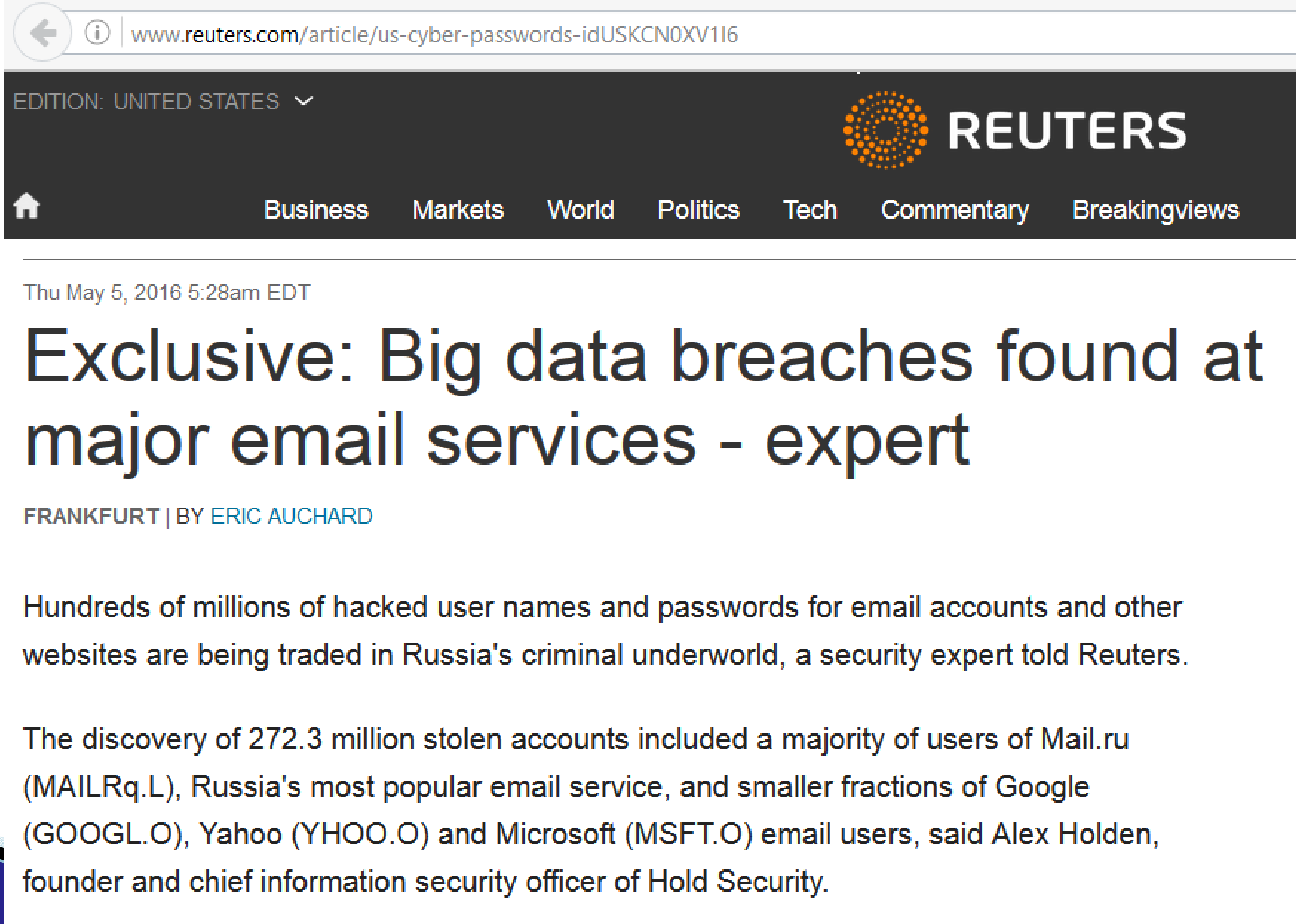
Biting the hand that feeds IT

Amazon denies hack claim

11 Jul 2016 at 08:52, Shaun Nichols

Risks of Processing 3rd Party Leaks

- User confusion about if you’ve been hacked



Thu May 5, 2016 5:28am EDT

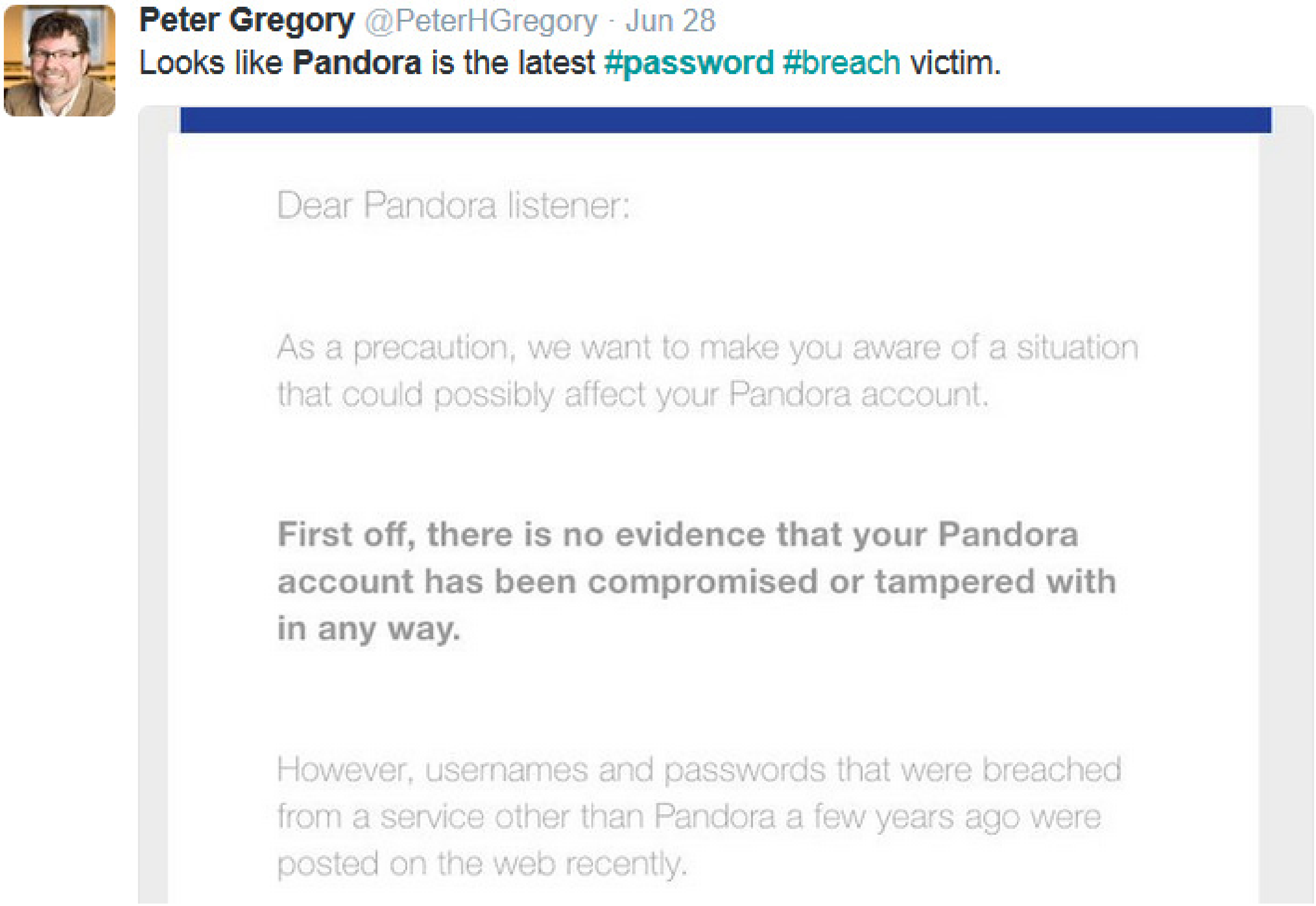
Exclusive: Big data breaches found at major email services - expert

FRANKFURT | BY ERIC AUCHARD

Hundreds of millions of hacked user names and passwords for email accounts and other websites are being traded in Russia's criminal underworld, a security expert told Reuters.

The discovery of 272.3 million stolen accounts included a majority of users of Mail.ru (MAILRq.L), Russia's most popular email service, and smaller fractions of Google (GOOGL.O), Yahoo (YHOO.O) and Microsoft (MSFT.O) email users, said Alex Holden, founder and chief information security officer of Hold Security.

Risks of Processing 3rd Party Leaks



Peter Gregory @PeterHGregory · Jun 28

Looks like **Pandora** is the latest #password #breach victim.

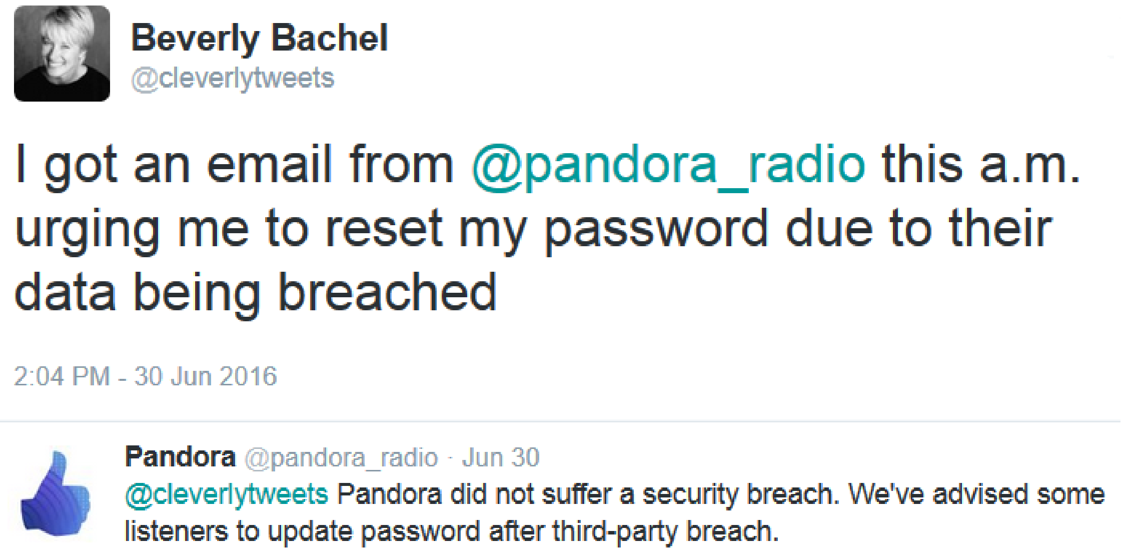
Dear Pandora listener:

As a precaution, we want to make you aware of a situation that could possibly affect your Pandora account.

First off, there is no evidence that your Pandora account has been compromised or tampered with in any way.

However, usernames and passwords that were breached from a service other than Pandora a few years ago were posted on the web recently.

Risks of Processing 3rd Party Leaks

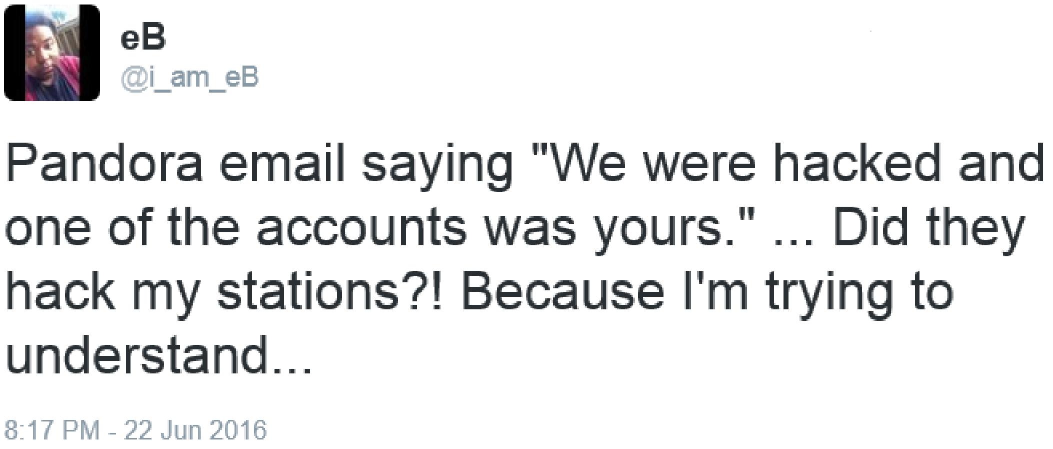


Beverly Bachel
@cleverlytweets

I got an email from @pandora_radio this a.m. urging me to reset my password due to their data being breached

2:04 PM - 30 Jun 2016

Pandora @pandora_radio · Jun 30
@cleverlytweets Pandora did not suffer a security breach. We've advised some listeners to update password after third-party breach.



eB
@i_am_eB

Pandora email saying "We were hacked and one of the accounts was yours." ... Did they hack my stations?! Because I'm trying to understand...

8:17 PM - 22 Jun 2016

Risks of Processing 3rd Party Leaks

- Users confused about how you could know that their passwords matched
- Users locked out of accounts because recovery options don't work for them
- Users concerned that your knowledge of their accounts elsewhere violates their privacy
- Users very concerned if named third-party hosted sensitive content
- Users suffering from notification fatigue

Risks of Processing 3rd Party Leaks

- Legal Risks – THIS IS NOT LEGAL ADVICE
  - Password leaks are stolen data
  - 18 U.S.C. § 1030 (a)(6) AKA CFAA – "knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization…"
  - 18 U.S. Code § 1029 – Fraud and related activity in connection with access devices
  - Intellectual property / trade secret law
  - Avoid testing credentials on third-party

Successes from Leak Processing

- Wordpress – found 100,000 users with same email/password as ‘Gmail’ leak [21]
- Yahoo – finds 10% – 20% of entries in a “bad password dump” match their users [16]
- Twitter – “Our goal is to protect [user] accounts. Through our defensive actions to protect users and available info on how to further secure accounts I feel we’ve had a good response.”

HOORAY, I PLUGGED THE PASSWORD LEAK!
imgflip.com

Conclusions

- Leak processing won’t eliminate ATO
  - Not all leaks are publicly shared
  - Will miss users signing up after leak processing
  - Attackers still compromise via other weaknesses
- May address the most at-risk population of your users
- Demonstrates your commitment to the integrity of your users’ accounts

References

1. Consumer Survey: Password Habits. CSID. September 2012. http://www.passwordresearch.com/stats/statistic258.html
2. ESET & Harris Interactive Password Poll. ESET. October 2012. http://www.passwordresearch.com/stats/statistic268.html
3. Adults Media Use and Attitudes Report 2013. Ofcom. April 2013. http://www.passwordresearch.com/stats/statistic317.html

References

4. The Tangled Web of Password Reuse. Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, XiaoFeng Wang. February 2014. Network and Distributed System Security (NDSS) Symp. http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled_web.pdf
5. What do Sony and Yahoo! Have in common? Passwords!. Troy Hunt. July 2012. http://www.passwordresearch.com/stats/statistic312.html
6. Reused Login Credentials. Trusteer. Feb 2010. http://www.passwordresearch.com/stats/statistic276.html

References

7. Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. Rick Wash, Emilee Rader, Ruthie Berman, Zac Wellmer. Twelfth Symposium on Usable Privacy and Security, SOUPS ‘16. June 2016. http://rickwash.com/papers/security-passwords-field-study.pdf
8. An Update on Our War Against Account Hijackers. Mike Hearn (Google). February 2013. https://googleblog.blogspot.com/2013/02/an-update-on-our-war-against-account.html

References

9. How We Protect #AzureAD and Microsoft Account from Lists of Leaked Usernames and Passwords. Alex Weinert. Microsoft. May 10, 2016. https://blogs.technet.microsoft.com/ad/2016/05/10/how-we-protect-azuread-and-microsoft-account-from-leaked-usernames-and-passwords/
10. Akamai's State of the Internet / Security Q1 2016. Akamai. June 2016. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q1-2016-state-of-the-internet-security-report.pdf

References

11. Taobao hack: Cyber-attack on 'Chinese eBay' leaves 20 million-plus user accounts exposed. Jason Murdock. International Business Times. February 4, 2016. http://www.ibtimes.co.uk/taobao-hack-cyber-attack-chinese-ebay-leaves-20-million-plus-user-accounts-exposed-1542013
12. Survey Guide: Businesses Should Begin Preparing for the Death of the Password. Gigya. May 2016, http://info.gigya.com/rs/672-YBF-078/images/original-201603_gigya_wp_businesses_preparing_death_password-web4.pdf

References

13. "I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. Proceedings of the 11th Symposium on Usable Privacy and Security, SOUPS '15. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ur.pdf
14. Bad Password Practices Put UK Identities, Accounts at Risk. TeleSign. Nov 27, 2014. https://www.telesign.com/resources/newsroom/bad-password-practices-put-uk-identities-accounts-at-risk/

References

15. Imperium Study Unearths Consumer Attitudes Toward Internet Security. June 27, 2013. http://www.passwordresearch.com/stats/statistic382.html
16. AppSec is Eating Security. Alex Stamos. AppSec California 2015. April 27, 2015. https://www.youtube.com/watch?v=2OTRU--HtLM
17. Passwords Found in the Wild for January 2013. Bruce Marshall. February 7, 2013. http://blog.passwordresearch.com/2013/02/passwords-found-in-wild-for-january-2013.html

References

18. Your Password Complexity Requirements are Worthless. Rick Redman. OWASP AppSecUSA 2014. September 25, 2014. https://www.youtube.com/watch?v=zUM7i8fsf0g&feature=youtu.be&t=33m41s
19. Cleaning up after password dumps. Google. September 10, 2014. http://googleonlinesecurity.blogspot.se/2014/09/cleaning-up-after-password-dumps.html
20. 99% of Alex Holden's Database Entries Are Invalid, Mail.Ru Group's Security Analysis Shows. Mail.ru. June 5, 2016 https://corp.mail.ru/en/press/releases/9613/

References

21. Gmail Password Leak Update. Daryl Houston, WordPress.com. September 2014. http://en.blog.wordpress.com/2014/09/12/gmail-password-leak-update/

Contact Info & Slides

- Bruce K. Marshall   @PwdRsch
- bkmarshall@PasswordResearch.com
- Slides available at www.PasswordResearch.com/passwordleaks.html