DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Daten-Klau Thema Cit0Day im November 2020

Inhaltsverzeichnis

Hier geht es zu den Artikeln im Internet

1. Wurden Daten aus all diesen 23'000 Websites entwendet?
2. Sonderfall «Cit0day»: Wurden 23'000 Websites gehackt?
3. Was heisst jetzt das für die User?
4. «Hey, warum steht meine Domain in der Liste?!»
5. Die 92 .ch-Domains im Cit0day-Breach
6. Die 848 .de-Domains im Cit0day-Breach
7. Die 121 .at-Domains im Cit0day-Breach

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Wurden Daten aus all diesen 23'000 Websites entwendet?

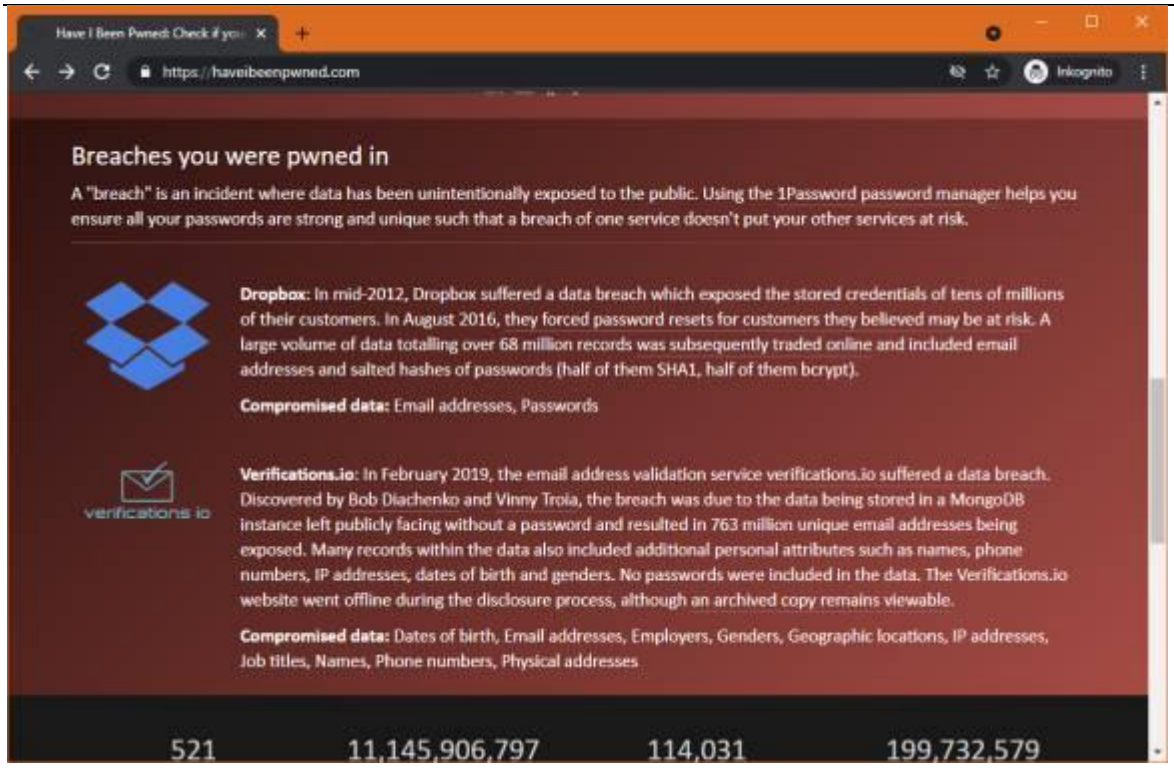
Laut einer in Hackerforen im November 2020 gefundenen Datenbank mit rund 226 Millionen Mailadressen sollen 23'000 kleinere Websites aus aller Welt gehackt worden sein. Ein Leser fand seine Adresse in diesem «Cit0day»-Breach. Was heisst das?

Unangenehmer Fund eines Lesers: Seine Mailadresse wurde im «Cit0day»-Breach entdeckt. Was nun? Und was heisst das?
(Quelle: Leser-Screenshot)

Aber der Reihe nach. Der PCtipp berichtete über einen anfangs April 2021 publizierten Leak zu rund 530 Millionen Facebook-Konten. Ob man Opfer eines solchen Datendiebstahls geworden ist, sollte man als User direkt vom betroffenen Anbieter selbst erfahren. Manchmal erfährt man erst durch die Medien davon. Und manchmal durch eine simple Abfrage in der Datenbank «Have I been pwned?» (kurz «HIBP») des renommierten Sicherheitsexperten Troy Hunt.

Ein typischer Fall wäre dieser: Eine Abfrage ergibt zum Beispiel, dass die Mailadresse im «Dropbox-Datenleak von 2012» enthalten war. Sofern nicht schon geschehen, loggt man sich in einem solchen Fall beim betroffenen Dienst (hier wäre es Dropbox.com) ein und ändert das Passwort. Wenn Sie für jeden Dienst ein anderes (und zwar ein gutes) Passwort verwenden, wie wir es immer wieder dringend empfehlen, dann ist das meistens alles, was Sie tun müssen und können. Ist ein Social-Media-, E-Mail- oder ein Forums-Account betroffen, prüfen Sie, ob Ihre Kontaktdaten noch stimmen (besonders die Mailadresse oder Handynummer für die Passwortwiederherstellung!) und ob vielleicht ein Angreifer bereits Nachrichten aus diesem Konto verschickt hat.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55



Ein recht klarer Fall: Die Mailadresse in diesem Beispiel befand sich im 2012er Dropbox-Datenleak
Quelle: PCtipp.ch

Falls man dasselbe Passwort auch für andere Dienste benutzt hat, sollte man es bei diesen unbedingt ebenfalls ändern. Und zwar bei jedem Dienst auf ein anderes. Jedes Passwort sollte nur für genau einen Dienst benutzt werden. Der Grund ist einfach: Wenn Angreifer von einem User die Mailadresse (das ist meist gleichzeitig der Benutzername) und ein Passwort haben, dann werden sie dieselbe Mailadressen-/Passwort-Kombination bei etlichen anderen Diensten ausprobieren. Wenn der User leichtsinnig genug war, für alle Dienste dasselbe Kennwort zu verwenden, dann ist der Hacker vielleicht im Facebook-, Google-, Twitter-Konto usw. ebenfalls drin. Und das wollen Sie nicht.

Sonderfall «Cit0day»: Wurden 23'000 Websites gehackt?

Ein Leser meldete sich bei uns, weil seine Mailadresse laut seiner Abfrage bei «Have I been pwned?» in einem so genannten «Data Breach» mit dem Arbeitstitel «Cit0day» gefunden wurde. Was ist das? Und warum ist dieser Fall so speziell?

Troy Hunt (der HIBP-Betreiber) hat darüber gebloggt (engl.). Die Seite «Cit0day.in» war ein Dienst von Onlinekriminellen für andere Onlinekriminelle. Jener beschaffte und verkaufte Daten aus zahlreichen eher kleineren Datendiebstählen und hat im September 2020 seinen Dienst eingestellt. Dies angeblich, weil er von den US-Ermittlungsbehörden hopsgenommen worden sei. Das US-Portal ZDNet berichtete jedoch (engl.), dass die behördlich aussehende Meldung auf der damaligen Seite gefälscht und keine Verhaftung erfolgt sei.

Um Anfang November 2020 herum tauchte jedenfalls eine ominöse, mit «Cit0day» bezeichnete Datenbank mit rund 226 Millionen Mailadressen in einem Hackerforum auf. Die Struktur bestand aus rund 23'000 Paketen, die alle unterschiedliche Namen von Domains trugen, z.B. chordie.com, siehe nachfolgenden Screenshot. Darin enthalten waren die Files mit offenbar zugehörigen Mailadressen. Das lässt den Schluss zu, dass die in jedem Paket enthaltenen Mailadressen und sonstigen Daten bei Online-Einbrüchen bei den jeweiligen Domains geklaut wurden.

Name	Date modified	Type	Size
chordie.com {1515111} [HASH] [NOHASH].txt	11/09/2018 21:03	TXT File	92,049 KB
NotFound.txt	24/09/2018 06:03	TXT File	19,643 KB
Rejected.txt	24/09/2018 06:03	TXT File	139 KB
Result(HEX).txt	24/09/2018 06:03	TXT File	16 KB
Result.txt	24/09/2018 06:03	TXT File	37,982 KB

Zu jeder der 23'000 mutmasslich kompromittierten Domains gab es solche Files
Quelle: Screenshot Troy Hunt

Troy Hunt hat die Daten analysiert und in HIBP eingepflegt. Waren es nur Daten, die schon in anderen Breaches vorhanden waren? Waren es gefälschte Daten? Zu beidem: eher nein, wie es aussieht. Nach dem Datenabgleich fand er heraus, dass nur 65% der Mailadressen bereits in anderen Breaches vorhanden waren. Ein paar einzelne Breaches der erwähnten Sites waren zudem auch schon bekannt. Er nennt das Beispiel von hookers.nl, das bereits in seiner Datenbank steckte. Uns ist unter den aufgelisteten Breaches jener von forum.zonealarm.com noch geläufig, siehe Bericht von Securityweek (engl.) vom November 2019. Ausserdem hat Troy Hunt einige ausgesuchte Accounts verschiedener Domains geprüft. Aufgrund seiner Stichproben kam er zum Schluss, dass die Accounts wahrscheinlich echt waren und tatsächlich zu den in Dateinamen angegebenen Domains gehörten.

Aber was bedeutet das jetzt für User, deren Mailadressen laut «Have I been pwned?» in diesem «Cit0day»-Paste gefunden werden?

Was heisst jetzt das für die User?

Wenn «Have I been pwned?» einem User mitteilt, seine Mailadresse stecke in diesem «Cit0day»-Breach, stellen sich ihm eigentlich nur zwei Fragen:

- Aus welcher Domain wurde meine Adresse mutmasslich geklaut?
- Weil: Bei welchem Dienst muss ich in diesem Fall mein Kennwort ändern?

Das sagt der HIBP-Dienst dem User nicht. Es sind einfach zu viele Domains! Aber Troy Hunt hat in seinem Blogpost zwei Textdateien mit den Namen der rund 23'000 betroffenen Domains verlinkt:

- hier die erste
- und hier die zweite

Also «viel Spass beim Durchsuchen»? Wir machen es Ihnen etwas einfacher. Die Autorin hat die in diesem Breach vorkommenden Domainlisten heruntergeladen und – Excel sei Dank! – nach Top-Level-Domains, also nach Domain-Endungen gefiltert. Die meisten User im deutschsprachigen Raum dürften sich wohl primär bei Domains mit Endungen .ch, .de, .at, .com, .net und .org registrieren.
Daher hat die Autorin die Domains pro Top-Level-Domain auseinandergedröselt. **Auf den Folgeseiten sind die betroffenen Sites mit Top-Level-Domains .ch, .de und .at aufgelistet.**
Jene der .com, .org und .net-Domains sind etwas lang, darum diese hier als gezippte Textdateien:
Downloads
Liste mit den .com-Domains aus dem Cit0day-Breach
Downloads
Liste mit den .net-Domains aus dem Cit0day-Breach
Downloads
Liste mit den .org-Domains aus dem Cit0day-Breach
Wenn Ihre Mailadresse laut «Have I been pwned?» im erwähnten Cit0day-Breach gefunden wurde, schauen Sie sich die Domains in Ruhe an. Falls Sie eine entdecken, bei der Sie irgendwann mal ein Konto eingerichtet haben, dann loggen Sie sich dort ein, prüfen Sie Ihre Daten und ändern Sie Ihr Kennwort.

«Hey, warum steht meine Domain in der Liste?!»

Sind Sie allenfalls sogar selbst Betreiber einer dieser Domains? Dieser Artikel ist nicht als Pranger gedacht, sondern als Hilfe für die User, die sich im Cit0day-Breach wieder finden und gerne wüssten, bei welcher Domain wohl die Adresse abgegriffen wurde.

Solche Datenpannen können passieren. Sogar aus dem Forum des Sicherheitsanbieters ZoneAlarm wurden durch einen Angreifer Benutzerdaten entwendet. Wir stellen hier nicht die Behauptung auf, dass die von Troy Hunt analysierten Daten alle zu 100% echt sind. Wir neigen aber aufgrund seiner Analyse dazu, die Daten für plausibel zu halten. Und falls es einen «Cyber-Einbruch» in die Datenbank Ihrer registrierten Nutzer gegeben hat, wissen wir nicht, wann dieser stattgefunden hat. Es kann auch mehrere Jahre her sein. Prüfen Sie, ob Sie auf Ihrem Server aktuelle Software laufen haben, denn auch WordPress, Drupal, Typo3 und wie die ganzen Content-Management-Systeme für Websites alle heissen, haben haufenweise Sicherheitslücken, die gestopft werden müssen. Sorgen Sie dafür, dass keine Zahlungsinformationen zugänglich sind. Sorgen Sie dafür, dass die Passwörter nur verschlüsselt gespeichert werden. Stellen Sie sicher, dass nur jene Benutzerkonten Zugang zu solchen Daten haben, die dies auch wirklich brauchen. Setzen Sie die Kennwörter der betroffenen User zurück, sofern nicht schon erledigt.

Anbieter, die in ihren eigenen Sites einen Breach (Datenklau durch einen Angreifer) feststellen, sollten zudem nicht nur die eigene Nutzerschaft, sondern auch den Datenschutzbeauftragten darüber informieren. Derzeit ist letzteres zwar noch nicht Pflicht, aber das wird sich laut Jurist Martin Steiger in der nächsten Revision des Schweizer Datenschutzgesetzes ändern.

Einige der Sites haben wir im Sinne einer Stichprobe in einem geschützten Browser geöffnet. Viele davon sind heute gar nicht mehr erreichbar oder begrüssen einen mit Fehlermeldungen. Einige der noch erreichbaren Sites schienen allerdings sogar die minimalen Sicherheitsmassnahmen zu vernachlässigen, denn diese waren nur via http erreichbar – nicht via https. Der Fall zeigt: Viele Webseitenbetreibende haben punkto Sicherheit noch viel Arbeit vor sich.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Die 92 .ch-Domains im Cit0day-Breach

Hier finden Sie die 92 .ch-Domains aus dem Cit0day-Breach. Falls Sie bei einer dieser Domains ein Konto haben, könnte dieses vom Cit0day-Breach betroffen sein. Ändern Sie bei dem Konto sicherheitshalber das Kennwort.

```
2012.openairgampel.ch
2017.luff.ch
aircenter.ch
allevamenti.ch
amadeusmusic.ch
anzeiger24.ch
apprentis.ch
aska.jpn.ch
babycake.ch
baechler.ch
balik.ch
bateau-sport.transmova.ch
bernweb.ch
bern-web.ch
bg-aarwangen.ch
bhi-coiffure-lausanne.ch
binichschoen.ch
blunier-edv.ch
budokai.ch
bwfk.ch
c64.ch
cocagne.ch
curling-schaffhausen.ch
daniel-felix.ch
dicentra.ch
diddl-boutique.ch
duvoisinnautique.ch
elite-escorts.ch
emmental-web.ch
ensemble-enscene.ch
entretiens.ch
espace-fribourg.ch
etujobs.ch
ferrari-kaffee.ch
forum.solidarite-bosnie.ch
galerie.transitmag.ch
gay-mega-store.ch
gomaths.ch
grandevasion.ch
groovemusic.ch
hirschen-langnau.ch
i-kultur.ch
jojobagold.ch
jugendeinewelt.ch
languages-for-life.ch
lottomania.ch
lucvolleyball.ch
m.co-2.ch
mail.co-2.ch
mao-massages.ch
marinepro.ch
meatpoint.ch
meteocentrale.ch
mobil.flirtsaal.ch
```

mondialprodukte.ch
mypizza.ch
notrepanierbio.ch
nukoko.ch
osas.rc-timing.ch
panier-bio.ch
passeportbeaute.ch
photographes.ch
pommes.ch
praktikumsstellen.wiss.ch
presse.pearl.ch
rockaltitude.ch
rro.ch
ruettihubelbad.ch
sackgeldjobs.ch
seelandweb.ch
showticket.ch
skool.ch
softairclub.ch
solidarite-bosnie.ch
sssl.ch
steingravur.ch
swisstime.e-unit.ch
test.cilike.ch
thz-trucks.ch
transitmag.ch
transmova.ch
troedelmarkt.ch
tuningpresse.ch
unserbiokorb.ch
vacc.ch
vbckantibaden.ch
ww.anzeiger24.ch
ww.co-2.ch
ww.swissdjcharts.ch
www.anzeiger24.ch
wwww.swissdjcharts.ch
zytglogge.ch

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Die 848 .de-Domains im Cit0day-Breach

Hier finden Sie die 848 .de-Domains aus dem Cit0day-Breach. Falls Sie bei einer dieser Domains ein Konto haben, könnte dieses vom Cit0day-Breach betroffen sein. Ändern Sie bei dem Konto sicherheitshalber das Kennwort.
Allfällige Umlaut-Domains stehen doppelt drin, einmal mit Punycode (xn-irgendwas) und einmal in der lesefreundlichen Schreibweise.

030casting.de
123-finder.de
123php.de
2lpc.de
3d-ring.de
4metal.de
aachen-marktplatz.de
abo.bbv-net.de
absolutmedien.de
adriamedia.de
aerzteverbund-opf.de
afg-haustechnik.de
agenda21-karlsruhe.de
agents.ncl.de
agf-deutschland.de
agm-online.de
agrarmodellbau.de
agsmodeling.de
airports.de
akadsek.de
ak-lsa.de
aktienbrief-online.de
aktionswoche-alkohol.de
alathair.de
alice-community.de
alles-aus-plexiglas.de
allex-pankow.de
alt.tsvroedgen.de
alt.tvp-textil.de
alte-maelzerei.de
ameros.de
amsommertalweg.de
amtsvordrucke.de
andretrapp.de
anstoss-online.de
anugafoodtec.de
anzeige-net.de
anzeigenkompass.de
a-pickel.de
apothekerkammer-nds-intern.de
apresski24.de
arameo.de
arbeitgeber-bewertungen.de
arbeitsrecht.de
archiv.mwonline.de
archivdigital.de
arrangement-verlag.de
artisan-n-artist.de
asiatische-waffen.de
asn-concepts.de
assistance-sachsen.de
asthmazentrum-pfalz.de

atae.de
auction.flinky.de
augenzentrum-rn.de
auktionshaus.de
ausstellerdaten.de
australien-recht.de
autogather.de
autoglas-discounter.de
autohaus-brueggemann.de
automatenvideothek.de
automiller.de
avia-braun.de
avila-immobilien.de
avilia.de
aw-online.de
babyzimmer.de
badmobelsalgar.de
baerchenrecords.de
bahnhofsmission.de
bamcases.de
bananario.de
bandboard.customer.tuplus-idl.de
bandboard.de
bantleon-energie.de
batterielager.de
batterie-lager.de
baubiologie-regional.de
baumbachhaus-kranichfeld.de
bauset.de
bdsm-club.de
bem-management.de
bergedorf.de
bergwerkbeinacht.de
betreuer-weiterbildung.de
bfi-photokina.de
biblino.de
bikereisen.de
bildungsinstitut-rlp.drk.de
billung.rowing.de
biohandel-online.de
biom131.imbi.uni-freiburg.de
bistum-muenster.de
bkav.de
blattgold-wasner.de
blesch-kachelofen.de
blog-webkatalog.de
bmw-forum.de
bodensee-konstanz-citytour.de
bogencenter.de
bonuspay.de
bootsclub-ochsenfurt.de
bowlingverband-niedersachsen.de
branchenbuch-meissen.de
braunschweigflirt.de
briefmarken.de
brn-ag.de
brueckmann-reisen.de
bst-clan.de
bsv.gleidingen.de
buhlbikers.fc-hellertal-sassenroth.de
bulgaria-shop.de

bullchart.de
bundestieraerztekammer.de
burg-gymnasiumwettin.de
busreisen-kaiser.de
bw.kulturkurier.de
bwguide.f-thies.de
camping-in-deutschland.de
campingineuropa.de
camping-in-europa.de
carasana.de
cardium-kongress.de
carlotta.de
case-factory.de
cashecho.de
ccfreunde.de
cdu-malsch.de
cg.informatik.uni-siegen.de
chat.tycoon-world.de
chatwahn.de
check-your-love.de
cheerspizza.de
chinaboutique.de
chinthe.de
cina.de
citadel-miniaturen.de
citdoks.de
city-onlinemarketing.de
classic.partycard-berlin.de
cm07.cmcitymedia.de
coaches-im-netz.de
congress-compact.de
consolorama.de
contributorcharts.multimedia.de
copyshop-versand.de
corlog.de
cpmonitor.de
cres-losinj.de
crimpen.de
critic.de
crokkys.de
cutman-friseur.de
dana-vinaiki.de
danialu.de
danzberger-reisen.de
dartberlin.de
dasautokaufhaus.de
dasfirmenportal.de
dating365.de
db.car-xchange.de
deckenbach-touristik.de
dehoga-akademie.de
demonlords.de
dersonny.de
derteichhof.de
deutsche-dj-playlist.de
deutscher-hopfen.de
d-gem.de
dienstzeitende.de
dieregistratur.de
digibo.de
digitalvd.de

diiicard.de
dimplex.de
dinoparts.de
dlhvirtual.de
dlrk2018.dglr.de
d-o-o.de
download.optotronix.de
downloadshop.phpscriptshop.de
dream-boating.de
dresdenflirt.de
dresden-flirt.de
dresdensingles.de
druuck.de
dso-planer.de
dtmb.p4systems.de
dxr-cap-company.de
ebb.hsp-bonn.de
ebs-finanzakademie.de
eddh.de
educcare.de
efg-neu-anspach.de
eic-wurst.de
einkaufen-in-grossenhain.de
elektriker-finden.de
elektrobetriebe.de
elektroseiten.de
elektro-zone.de
embryologie.uni-goettingen.de
e-mentor.de
emfanshop.de
en.joydivision-international-ag.de
engel-orakel.de
entsorgung-regional.de
epicsurf.de
ereturn.de
e-riesengebirge.de
erlabrunn-erzgebirge.de
ermasport.de
erotik.de
ersatzteildiscount24.de
es.joydivision-international-ag.de
esistore.de
estrella-software.de
etahits.de
eurocrane.de
evangelische-jugend.de
events-aus-leidenschaft.de
evoteli.de
excel-werkstatt.de
exercitus-wow.de
expedientenportal.de
expogamma.de
fachwerkhaussanierung.de
fahrplan-online.de
fahrradstar.de
fanport.de
faq.natterer-modellbau.de
farbsucht.de
fc.munichirishrovers.de
federn-service.de
federscheiben.de

fellner.com.de
fenstermodus.de
ferienhaus-linkliste.de
ferienhaus-mia.de
ferienhaus-privat.de
feuerflamme.de
fifa-town.de
filmmuseum-hamburg.de
finanznavigator.de
finianz.de
fire-emblem.de
firmenlauf-reutlingen.de
fiwotextil.de
fjr-1300.de
flexotube.de
flightcheckers.de
flingern-mobil.de
flirtforyou.de
flohr-automobile.de
fogaco.de
fooserama.de
forum.agsmodeling.de
forum.readmore.de
FPortal.de
fpv-community.de
fr.joydivision-international-ag.de
franksbaumwolle.de
franks-golfshop.de
frank-wille.de
freepoc.de
freizeitpark-planspiel.de
freshlegumes.de
fritz-motorsport.de
fruitpunks.de
ftor.de
f-tor.de
funfail.de
fussballtraining-online.de
fuw-rsk.de
gabelstaplertechnik.de
gaed.de
gaertnermuseum.de
gaestefuehrer-weinerlebnis.de
games-news.de
gamessphere.de
gars-ilf.de
gasfeder-shop.de
gastro-edelstahl.de
gastro-seller.de
gay-kennt-wen.de
gcf.de
g-d-o.de
gemeinde-wartenberg.de
gepps.de
gesundheitstheke.de
ggm-re.de
glass-hobby-design.de
global-tec.de
globus-wapienica.de
gmw.com.de
goagemeinde.de

```
go-crazy.de
gokkel.de
gpk.de
gplrank.schuerkamp.de
gunnarwinkler.de
hairsecrets.de
hallertauerhopfen.de
hamboerse.de
hamburgturm.de
hanauer-parkhaus.de
handelsstation.de
handschuh-dach.de
handwerkerportal.de
handwerkerverbund-deutschland.de
hansa-auktion.de
hantelshop.de
happyandsmiley.de
hausligabowling.de
hausziege.de
hcr-business-center.de
heartland.de
heidi-steinhaus.de
heilfastenkur.de
heimarbeit-verzeichnis.de
heimkinoraum.de
helm.motorrad-daten.de
hempelt-modellbahn.de
hentschke-keramik.de
herkules-motor.de
hessenparty.de
heumannzweirad.de
hg8.giatamedia.de
hgkdirekt.de
hh-cologne.de
hiphopbeat.de
hochzeit.qunix.de
hogwartsnet.de
holab.de
holst-garn.de
horselife.de
hotel-fleischerei-schneider.de
hourofpower.de
hoyer-aus32blue.de
hs-owl.de
h-tuning.de
humboldt05.de
icolumbo.de
iglam.de
igpm-zollernalb.de
ilrm.de
imap.ftor.de
immobilien.baubeteiligte.de
immobilien-streuer.de
immo-mit-bild.de
immo-pforzheim.de
immo-stuttgart.de
immo-ulm.de
importantrecords.de
important-records.de
infosoftware.de
inlove24.de
```

inodom.de
insel-losinj.de
insel-travel.de
intellego.de
intervox.de
ipp-netzwerk.hamburg.de
jae-tagung.de
jalousie-welt.de
jede.de
jhg-münchen.de
jobvermittlung.ihk-bildungshaus-schwaben.de
jswelt.de
jukeboxparty.de
junge-tafel.de
k-1sport.de
kaiserau-apotheke.de
ka-nightlife.de
kartenarchiv.de
katherinafuerst.de
kauf-ein-tier.de
kd.wrocklage.de
keihome.de
khat-systems.de
kiel.de
kieler-woche.de
kielive.de
kjfoods.de
klemts-spielzeughandel.de
klinikum-kassel.de
kloecker.de
kloeppelbuch-labrenz.de
klosterbezirk.de
knittel.de
kochaudio.de
koka36.de
komweyel.de
kontaktinkrisen.de
kreis.aw-online.de
kreisklassengoetter.de
kreutzerarchitekten.de
krimmel-gmbh.de
ks-networx.de
ktk-motorsport.de
kuebel-klub.de
kulturinfranken.de
kulturkurier.de
kvaw.de
labelocean.de
lachundschiess.de
laienkuenstler.de
lake-news.de
la-rive.de
layer7-haus.de
lebenshilfe-nordhorn.de
ledergeldbeutel.de
lehrmittel-reinhold.de
lfs-sh.de
lfvmv.de
lhvhs-lauda.de
limbo-ug.de
live1.turnierauskunft.de

```
lizensio.de
lmm.hs-bremerhaven.de
loady.de
local-network.de
lokal.games-workshop.de
lokmuseum.de
loopersparadise.de
ludwigspark.de
m.dating365.de
m.oldenburgische-volkszeitung.de
mac-newsticker.de
maedla.de
magdeburg-dating.de
magdeburgflirt.de
magdeburg-flirt.de
magdeburgsingles.de
magdeburg-singles.de
magdeflirt.de
mai-hof.de
mail.ftor.de
mail.f-tor.de
malabrigo-garn.de
mallorca-outdoor-event.de
malzkornfoto.de
mangaguide.de
mannheim.fruehstueckstreff.de
marmelade-fuer-alle.de
massi.de
matzelder.de
maxiad.de
maz-sound.de
mcl2k.de
mcschueler.de
mcvideomultimedia.de
media-products-demoserver1.de
medien.abhyanga.de
medizinjobs-direkt.de
medkom.tu-chemnitz.de
medmaxx.de
meinautoscout.de
meingartenshop.de
melbar.de
memoliga.de
mennraths.de
mensa-regio.de
mentalmadness.de
merz-sapori.de
mesas.de
messergrosshandel.de
messwell-party.de
metal-inquisition.de
metallwoche.de
metalspheres.de
mig.widuticket.de
migranten-ausbildung.de
mikrolaender.de
milando.de
militarycarsales.de
milwaukee-vtwin.de
misterjet.de
mixkatalog.de
```

```
mlbk.de
mobil.flirtsaal.de
mobil.philo-sophos.de
modellbahn-seyfried.de
modell-ovp.de
model-schools-india.de
moderatorenpool-deutschland.de
mode-von-fischer.de
module.kabeljournal.de
montessori-aktuell.de
moonsault.de
motorlexikon.de
mpz-bayern.de
mtb-reisen.de
muellertours.de
muenchner.de
mugs.m-blass.de
multex-investor-europe.de
multimedia.de
munich-insider.de
munichmela.de
muntplaats.de
museum-aktuell.de
musikoutlet.de
musik-schiller.de
musketier.de
mw-funktechnik.de
Mwonline.de
mybooker.de
n0z.de
nachbarschaftsstreit.de
nachtfilter.de
narwa.de
natureboost.de
naturkost.de
naturwindeln.de
ndt2.de
network.theminetv.de
netzwerk-familientherapie.de
netzwerk-psychoanalyse.de
netzwerk-tiefenpsychologie.de
neukirchener-verlage.de
newjob.de
newstix.de
nextnetz.de
nixedo.de
nomamed.de
nq-online.de
nrjmobile.de
nurberlin.de
nutritheke.de
odenthal.de
odys.de
oeffentliche-auftraege.de
officeofarts.de
offroadscramble.de
old.partycam.de
old.warwick.de
oldenburgische-volkszeitung.de
öldialyse.de
oldtimerradio.de
```

onpra.de
onskunk.de
openinnovation.bauma.de
optiker.de
orgatec.de
osterrath.de
partnerschulnetz.de
partycardberlin.de
partystrolche.de
pc1664.pharmazie.uni-marburg.de
PCMasters.de
pension.spreewelten.de
pension-buchen.de
pfaelzer-kletterer.de
pharma-kodex.de
philharmonische-gesellschaft-owl.de
photoshop-album.de
pippcity.de
pitchpool.de
pi-vier.de
pixsys-automation.de
poetrys.de
pokerchef.de
polizeiautos.de
portal-suedzucker-bkk.de
pos.extranet.mdh-holz.de
posamenten-shop.de
pragclubs.de
praktibank.de
praktisch-bunt.de
preisfair.de
preview-event.de
prima-finden.de
primus-versand.de
prionforschung.de
proclubs.de
projekt24h.de
prosweets.de
ps.fifa4fighters.de
ps.proleague.de
psychologen-im-netz.de
puppen-und-spielzeug.de
pvdagmar.de
pyroweb.de
quadro-forum.de
radderzeit.de
radio66.de
radsport-pbem.de
rae-sbk.de
ratgeber-tcm.de
rausvonzuhaus.de
rd2012.starwars-union.de
regijob.de
reifen24online.de
reiseruecktrittsversicherung-online.de
remoteschach.de
rennradreifen.de
rent-a-radio.de
reporter-forum.de
rfad.de
richter-hess.de

```
ritterburgwelt.de
rockenberg-fussball.de
rommel-energie.de
rosenstein-stuttgart.de
rosprites.simn.de
rts.eit.uni-kl.de
rustv.de
saarsex.de
samenwunder.de
sammler-fuer-sammler.de
sansibarkult.de
sascha-kocht.de
sattipp.de
sbuehner.de
scalamilano.de
scellius.de
scenemarkt.de
schimmelpilz-schnelltest.de
schloss-ahlden.de
schoenaich-handball.de
schoenen-dunk.de
schrottmail-lan.de
schukey-meyer.de
schulfreundfinder.de
schwalm-buchenau.de
schwarzwald-cup.de
schweres-warmblut.de
schwerinerkc.de
schwuppii.de
scifi-forum.de
sdv-online.de
seat-portal.de
securityresearchmap.de
seizewell.de
seminarboerse.de
servas.de
servietten-shop-diana.de
sgu-leitfaden.de
share-dev.mpisoc.mpg.de
shd.de
shd-kps.de
shirts-n-druck.de
shootyou.de
shop.kunst-spiel-und-spass.de
shop.moviestar-net.de
shop.santool.de
shop.weingut-edwinhuttner.de
shop.weingut-rainer-sauer.de
shopneu.veggie-shop.de
simon-weingut.de
single-hafen.de
skischule-neumaier.de
sky-vision.de
slv-sulek.de
sni-portal.de
soapspoiler.de
soellner-reisen.de
sokrates-digital.de
sonatech-es.de
sondermasstüren.de
soquiet.de
```

soundsum.de
sourcingmachine.de
so-war-mein-flug.de
spanking-kontakte.de
spass-am-zocken.de
special-bike-parts.de
spielwaren-kroemer.de
spirit-magazine.de
spirituellesportal.de
spirituelle-zitate.de
spitznas.de
sportkartei.de
spreewaelder-hofladen.de
spreewald-therme.de
spreewald-thermenhotel.de
spurweite-n.de
squealer-rocks.de
stadt-geislingen.de
stadtmarketingpreis-bw.de
stadtstreicher.de
stageeffects.de
ständenhof.de
starcards.de
static.137.190.4.46.clients.your-server.de
steppenhahn.de
stock-maritime.de
stornopool.de
strickideen.de
stuckradbarre.de
studserv.de
st-ursula.de
suchbuch.de
suchtgames.de
suedliches-maindreieck.de
sup2u.de
supercars.de
suzuki-hoffmann.de
t3ebus2.stadtmobil.de
tabakpfeife24.de
tafel-jugend.de
tagungsraumportal.de
tamonline.de
tanzeninkarlsruhe.de
tapetenmarkt.de
team.jade-hs.de
teamlearning.de
teams.tuslihockey.de
technische-sicherheit.de
technormen.de
tellerfedern.de
tequilla-sunrise.de
tessol.de
teuber-motorsport.de
teufelsturm.de
texmato.de
tfportal.de
theater-wahlstedt.de
theo-rost.de
theoterspeeler.de
therapeutenkatalog.de
thomasmacho.de

tieranzeigen.de
tiermeldezentrale.de
tinypic.pro.de
tip.abhyanga.de
tischdeckenshop.de
tocotronix.de
torpedomilitarysales.de
toys-kids.de
traffic-wave.de
translate-24h.de
traudich.de
trendpix.de
triggerzone.de
truckncountry.de
ttf-neckartenzlingen.de
tuerkatlas.de
tunnel.de
tunneltrade.de
Tuplus-idl.de
tvbb.tvpro-online.de
tvsh.tvpro-online.de
twintop.de
u-boote-online.de
ue-ticket.de
ugg.de
ultimo-kiel.de
unimedizin-mainz.de
unsere-werbung.de
unserfbgewinnspiel.fanpage-apps.de
uptrax.de
urltausch.de
utgeurope.de
va-schrauben.de
vcfoto.de
vecona.de
veganfach.de
velkd.de
ventilator.de
verdi-gefaehrdungsbeurteilung.de
verwaltung.local-network.de
vetion.de
vetripharm.de
vfa-online.de
vgie.de
vgoed.de
vid.sid.de
video-sexboom.de
videotaxi-tuebingen.de
vielfarbwolle.de
vietnamairlines.com.de
villa-reuther.de
vinaglobo.de
vintagemovieposters.de
viralwebtraffic.de
vitasol.de
vocalsounds.de
vogeldoktor.de
vogelfreund.de
vogelnetzwerk.de
vogelsuchdienst.de
vogelzuechter.de

```
vollmer-online.de
vpnk.de
vray-materials.de
vsro.de
vw-bus-t4.de
w.doenerfreund.de
w.finanznavigator.de
w.starjays.de
w.web-site-news.de
wack.drowshow.de
waffen-welt.de
walle.yaffi.de
waltmann.de
wankmueller-gmbh.de
wasserburg.de
wbs-bedburg.de
wdpx.de
webmail.diiicard.de
web-profi.de
webshop_teha.ks-networx.de
weingut-hessler.de
weingut-oesterlein.de
weinhandel-kappus.de
weisswurschtis.de
weiterbildungsportal24.de
werbewerk24.de
westfalenhallen.de
wgh.reisewitzer.strasse23.dresden.objektseite.de
willertransport.de
windsurfers.de
wingtsun-plus.de
wohnung-mieten.de
woodevent.de
wortfindungsamt.de
wrestling-xtreme.de
wsze.de
wuest-technology.de
ww.erotikwebcam.de
ww.flinky.de
ww.w.cgn-office.de
ww.w.f-tor.de
ww.w.web-site-fotoalbum.de
ww2.sexshop-dildo-king.de
www.atl-autotechnik.de
www.finanznavigator.de
www.global-tec.de
www.k-1sport.de
www.organicstyle.de
www2.kreis-ahrweiler.de
wwww.ftor.de
wwwwiki.ritterburgwelt.de
xn--jhg-mnchen-eeb.de
xn--ldialyse-m4a.de
xn--sondermasstren-qsb.de
xn--stndenhof-w2a.de
x-unitconf.de
zakopane.reisepolen.de
zbrush.de
zeus.lkn.ei.tum.de
zigarren-bennung.de
zinorm.de
```

```
zum.de
zum-flohmarkt.de
zweirad-profi.de
```

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Die 121 .at-Domains im Cit0day-Breach

Hier finden Sie die 121 .at-Domains aus dem Cit0day-Breach. Falls Sie bei einer dieser Domains ein Konto haben, könnte dieses vom Cit0day-Breach betroffen sein. Ändern Sie bei dem Konto sicherheitshalber das Kennwort.

allesdvd.at
arbitration-austria.at
artelier-contemporary.at
austrodaimlermodell.at
bambusaustria.at
barpokerseries.at
basics-media.at
begraebnis.at
bergundsteigen.at
bernhardziz.at
binichschoen.at
bodydays.at
boebakademie.at
br-aktuell.at
brassband.at
calligaris.at
championsrace.at
chocolate.at
climbonmarswiese.at
community.netdoktor.at
conzept-wth.at
cura.at
der-kanal.or.at
der-versicherungsmakler.at
deussner.at
dic.co.at
dikraus.at
dtm.at
easyjobs.at
ekiz-schwaz.at
elite-escorts.at
e-pendl.at
erwin-wenzl.at
europagym.at
euro-treuhand.at
expodisplayservice.at
fc-lustenau-nw.at
ferienchecker.at
ferienhof-gerlos.at
fischers.co.at
flatsvienna.at
formelclub.at
gandler-steuerberatung.at
gartentagebuch.at
gebaeudereinigung.at
genbank.at
genuss-guide-steiermark.at
gipfeltreffen.at
global-lotto.at
haendler.nyx.at
haller-beratung.at
heimbau.at
highteclehre.at
hotel-wiese.at

hotspring.at
hundesalon-lili.at
ikk-vorarlberg.at
jollyclub.at
jugendreisen-tyrol.at
juni2.public-image.at
kaarkg.at
kassenzubehoer.at
kontaktinser.at
kreativladen.topshop4you.at
labau.co.at
lettertothestars.at
locations.co.at
loot.at
maria-lourdes.at
mein-innsbruck-foto.at
memes.at
motorsportaktiv.at
muratti.co.at
mvg.at
nagelkosmetik.at
naturhotel-laerchenhof.at
nawibuch.at
oegs.webmix.at
oesterreichischer-frauenlauf.at
packages.at
palliativkurse.at
paugger-wt.at
paulus.dip3.at
reparaturfuehrer.at
rossini.co.at
rugia-retz.at
runvienna.at
schmerzambulanz-salzburg.at
schmerzkurse.at
schneider-partner.at
schoeckelcup.at
schwabenkinder.at
schweighofer.powernight.at
seefunk.at
segafredo.at
seikreativ.at
shop.unitedoptics.at
southafrica2010.sklsport.at
sport-mental.at
stb-insieme.at
stbredl.at
steiermarkjoker.at
steuernundrat.at
stubaital-info.at
suppacher.at
tecjobs.at
topprodukt.at
tourenfex.at
tsgsteuer.at
usvkrakauebene.sportunion.at
veranstaltungsraum.kd.stebio.at
verspielt.at
volkslied.at
vsport.at
we-are-family.at

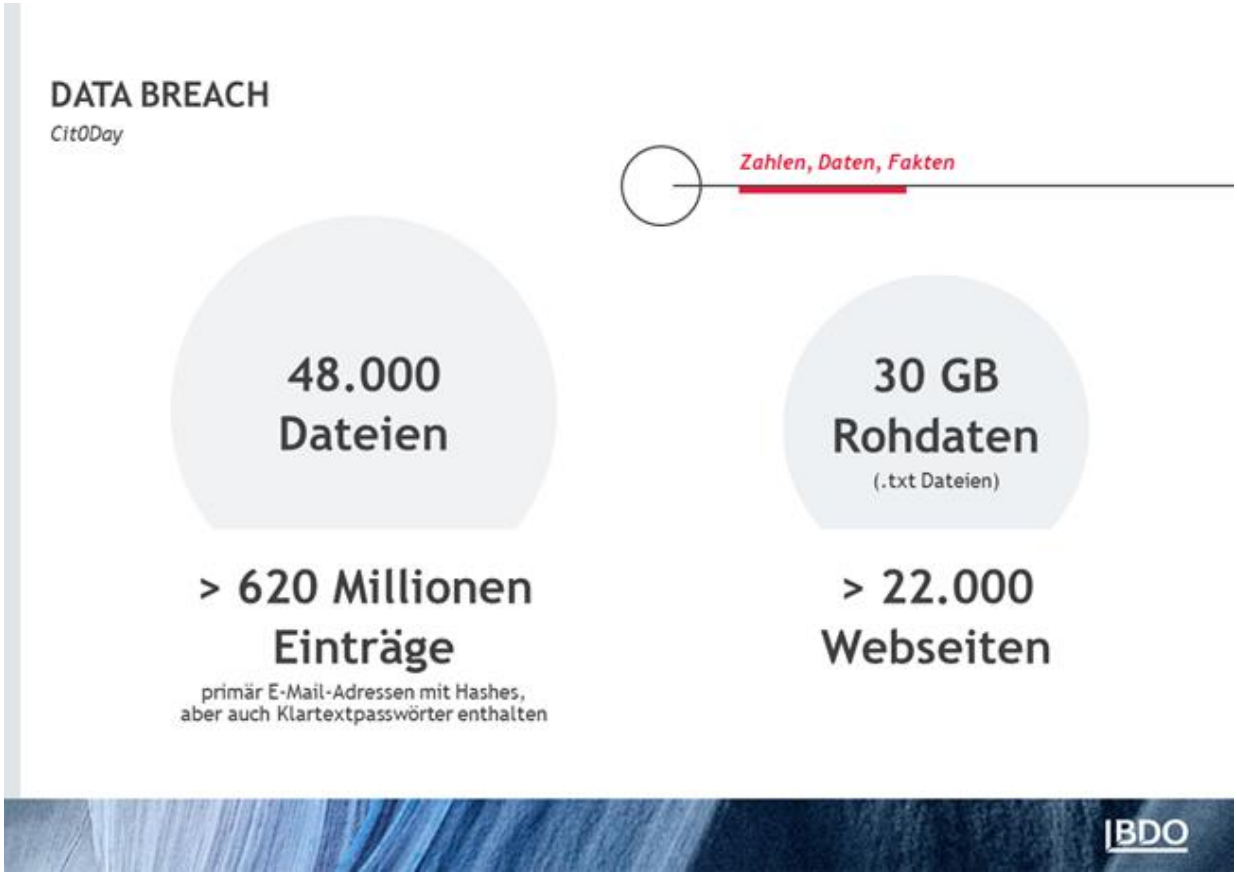
```
web.koram.at
weinshop24.at
whirlpools.at
wt-reiter.at
www.kfzmarktplatz.at
xtrose.at
```

Quelle: https://www.pctipp.ch/praxis/sicherheit/daten-all-23-000-websites-entwendet-2653984.html

Zahlen, Daten, Fakten

- In Summe sind über 620 Millionen Einträge mit Zugangsdaten in Form von E-Mail-Adressen, Passwort-Hashes und Klartextpasswörtern im Datenleck enthalten.
- Von dem Datenleck sind weltweit ca. 22.000 einzigartige Websites und mehr als 120 österreichische Webseiten (.at-Domain) betroffen.
- In dem ca. 28 GB großen Datenleck sind rund 48.000 Dateien enthalten.

Zum Vergrößern anklicken



Hintergrundinformationen

Durch die freie Verfügbarkeit von Datenlecks mit darin enthaltenen Benutzerdaten („Credentials“), hat sich im Internet eine Sammlerszene etabliert, die aus unterschiedlichen Gründen solche Datenlecks sammelt, zusammenführt und teilweise die verschlüsselten Passwörter bereits entschlüsselt („de-hashed“) zur Verfügung stellen. Die von Cyberkriminellen erbeuteten Daten werden zunächst in Untergrundforen im Web zum Verkauf angeboten. In weiterer Folge ermöglichen Sicherheitsforscher aufgrund dieser Daten die Überprüfung einer Betroffenheit.

Im Internet kursiert aktuell eine weitere Sammlung von über 23.000 Datenbanken des ehemaligen Cit0Day-Forums. Enthalten sind unterschiedlichste Benutzerdaten, inklusive Sammlungen der

ehemaligen Foren LeakedSource und WeLeakInfo. Cit0Day hat den Benutzern dieser ehemaligen Foren eine neue Plattform geboten.

Im Vergleich zu anderen bis dato bekannten Sammlungen von Datenlecks (z.B. Collection #1-#5) sind die betroffenen Webseiten und teilweise auch Passwörter im Klartext hinterlegt. Es handelt sich somit um eine verwertbare Fundstelle für Sicherheitsforscher und Cyberkriminelle.

Das Untergrundforum „Cit0Day.in“ zeigte am 14. September 2020 zunächst eine Meldung einer Beschlagnahmung durch das FBI, wobei daran gezweifelt wird, ob es sich dabei um eine echte Meldung handelt. Das FBI hat bis dato keine Festnahmen oder ähnliches bestätigt. Es ist aktuell nicht klar, ob Cit0Day von Hackern kompromittiert wurde und somit die Daten öffentlich gestellt wurden, oder ob der

Quelle: https://www.bdo.at/de-at/publikationen/2020/cit0day-datenleck

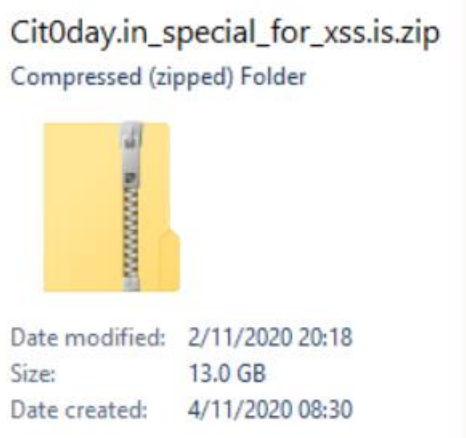
Zum Original
https://www.troyhunt.com/inside-the-cit0day-breach-collection/

Hier in Deutsch Übersetzt mit Deepl.com:

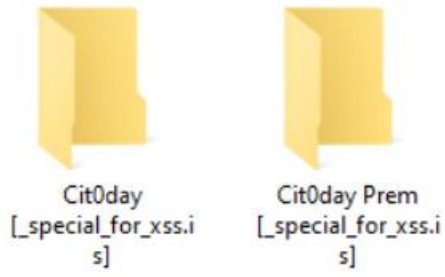
Einblick in die Cit0Day Breach Collection

19. November 2020

Es wird immer schwieriger zu wissen, was man mit Daten wie denen von Cit0Day machen soll. Wenn Ihnen der Name nicht geläufig ist, beginnen Sie mit Catalin Cimpanus Geschichte über den Untergang des Dienstes und das anschließende Leaken der Daten. Das Schwierige für mich ist, herauszufinden, ob es pwn-würdig genug ist, um die Aufnahme in Have I Been Pwned (HIBP) zu rechtfertigen, oder ob es nur weiteres Rauschen ist, das den Leuten letztendlich nicht wirklich hilft, informierte Entscheidungen über ihre Sicherheitslage zu treffen. Mehr dazu in Kürze, fangen wir damit an, was da drin ist. Wir sehen uns eine Zip-Datei namens "Cit0day.in_special_for_xss.is.zip" an, die komprimiert 13 GB groß ist:



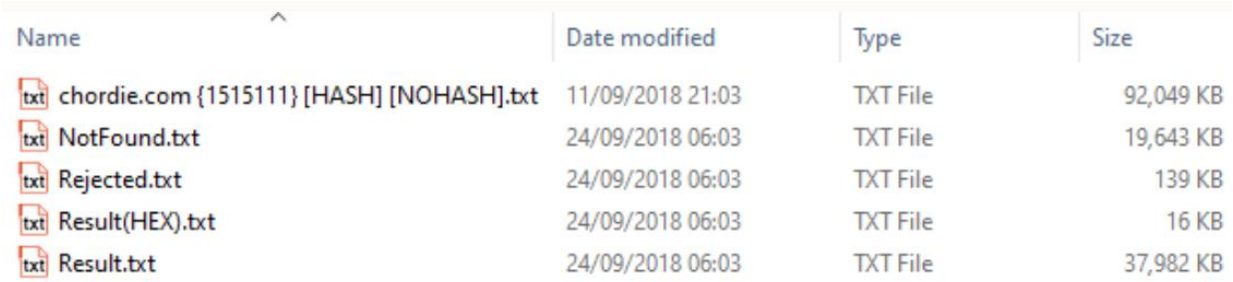
Ein paar Ordner weiter unten sind zwei weitere Ordner namens "Cit0day [_special_for_xss.is]" und "Cit0day Prem [_special_for_xss.is]"



Und hier wird es dann interessant: Im ersten Ordner befinden sich 14.669 .rar-Dateien, im zweiten weitere 8.949 .rar-Dateien, insgesamt also 23.618 Dateien. Daher kommt die Schlagzeile "mehr als 23.000 gehackte Datenbanken", denn so viele Dateien befinden sich in dem Archiv. Da es für die Geschichte relevant ist und vor allem für Leute, die ihre Daten in diesem Bruch über eine HIBP-Suche finden, werde ich die beiden Dateisätze in ihrer Gesamtheit über die folgenden Gists auflisten:

1. Citoday [_special_for_xss.is]
2. Citoday Prem [_special_for_xss.is]

Ich wähle "chordie.com {1.515.111} [HASH+NOHASH] (Arts)_special_for_XSS.IS.rar", einfach weil es eine der größeren Dateien ist. Hier ist der Inhalt:



Name	Date modified	Type	Size
chordie.com {1515111} [HASH] [NOHASH].txt	11/09/2018 21:03	TXT File	92,049 KB
NotFound.txt	24/09/2018 06:03	TXT File	19,643 KB
Rejected.txt	24/09/2018 06:03	TXT File	139 KB
Result(HEX).txt	24/09/2018 06:03	TXT File	16 KB
Result.txt	24/09/2018 06:03	TXT File	37,982 KB

Die erste und größte Datei des Archivs enthält über 1,5 Millionen Zeilen, die aus E-Mail-Adressen und MD5-Hash-Paaren bestehen. Ich werde eine bestimmte Zeile hervorheben, die eine Mailinator-Adresse verwendet, einfach weil Mailinator-Konten öffentliche E-Mail-Adressen sind, bei denen man keinerlei Privatsphäre erwarten kann. Hier ist sie:

```
traw@mailinator.com:bb796fbe5b644a2a88e3c75207ca4b54
```

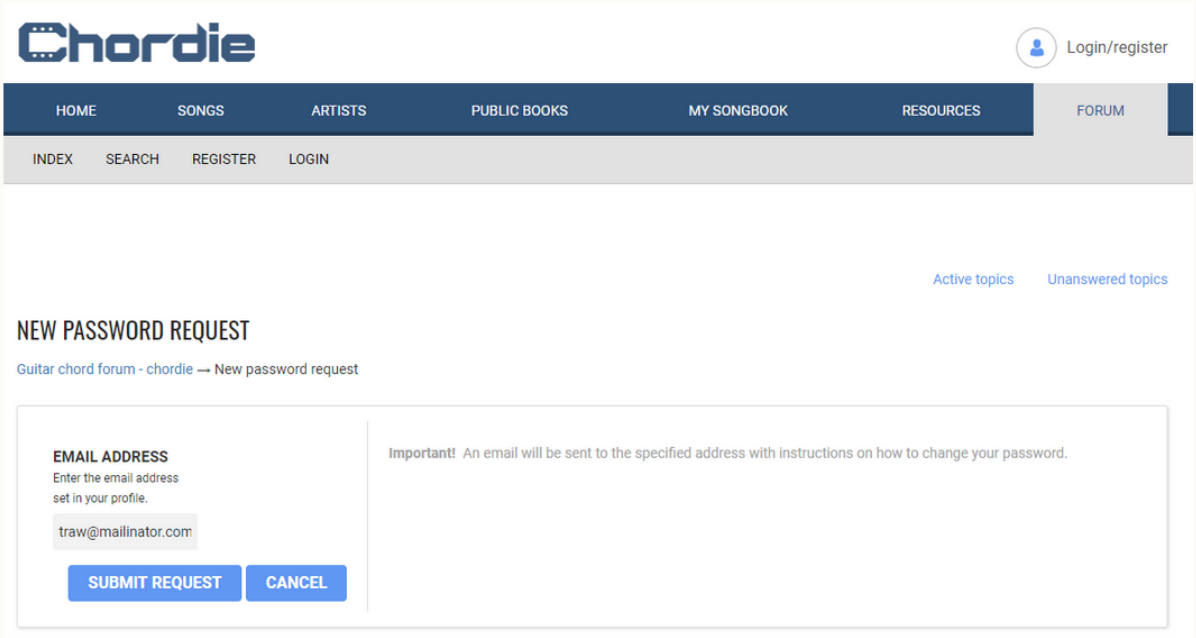
Wenn Sie sich die Datei "Results.txt" ansehen, erscheint diese E-Mail-Adresse mit einem geknackten Kennwort:

```
traw@mailinator.com:janid
```

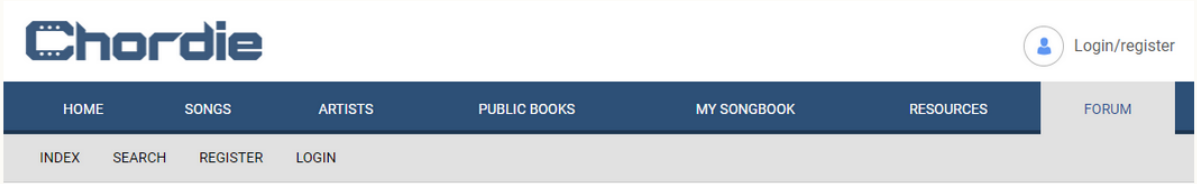
Die Datei "NotFound.txt" besteht aus E-Mail-Adressen und MD5-Hash-Paaren, und für jeden Hash, den ich zufällig gegoogelt habe, wurde kein Klartext-Ergebnis gefunden, so dass es sich hier offenbar um Hashes handelt, die nicht geknackt wurden. Die Datei "Rejected.txt" enthielt fehlerhafte E-Mail-Adressen und die Datei "Result(HEX).txt" enthielt eine kleine Anzahl von Hex-Paaren aus E-Mail-Adressen und Kennwörtern. Dasselbe Muster tauchte immer wieder in den anderen Archiven auf und gibt uns eine ziemlich gute Vorstellung davon, wofür die Daten gedacht waren: Credential Stuffing.

Ich habe alle Dateien extrahiert, mein übliches Tool zum Extrahieren von E-Mail-Adressen darüber laufen lassen (im Grunde nur ein Regex, das schnell eine große Anzahl von Dateien aufzählen kann) und insgesamt 226.883.414 eindeutige Adressen gefunden. Eine beachtliche Zahl, obwohl sie nicht einmal in den Top 10 der größten Sicherheitsverletzungen im HIBP enthalten ist.

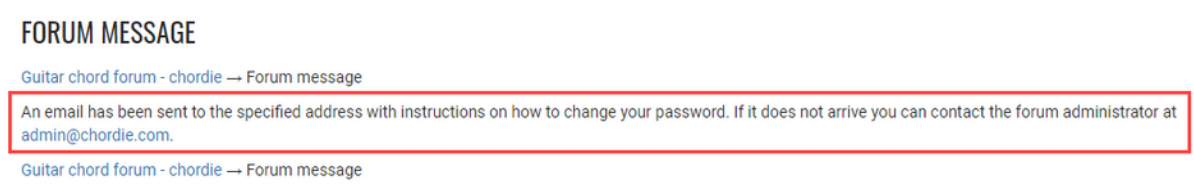
Aber ist das legitim? Ich meine, können wir darauf vertrauen, dass sowohl die E-Mail-Adressen als auch die Passwörter aus diesen angeblichen Sicherheitsverletzungen tatsächliche Konten bei diesen Diensten darstellen? Nehmen wir das obige Beispiel, das angeblich von chordie.com, einem Gitarrenforum, stammt. Gehen Sie hinüber zum Passwort-Reset und geben Sie die Mailinator-Adresse von vorher ein:



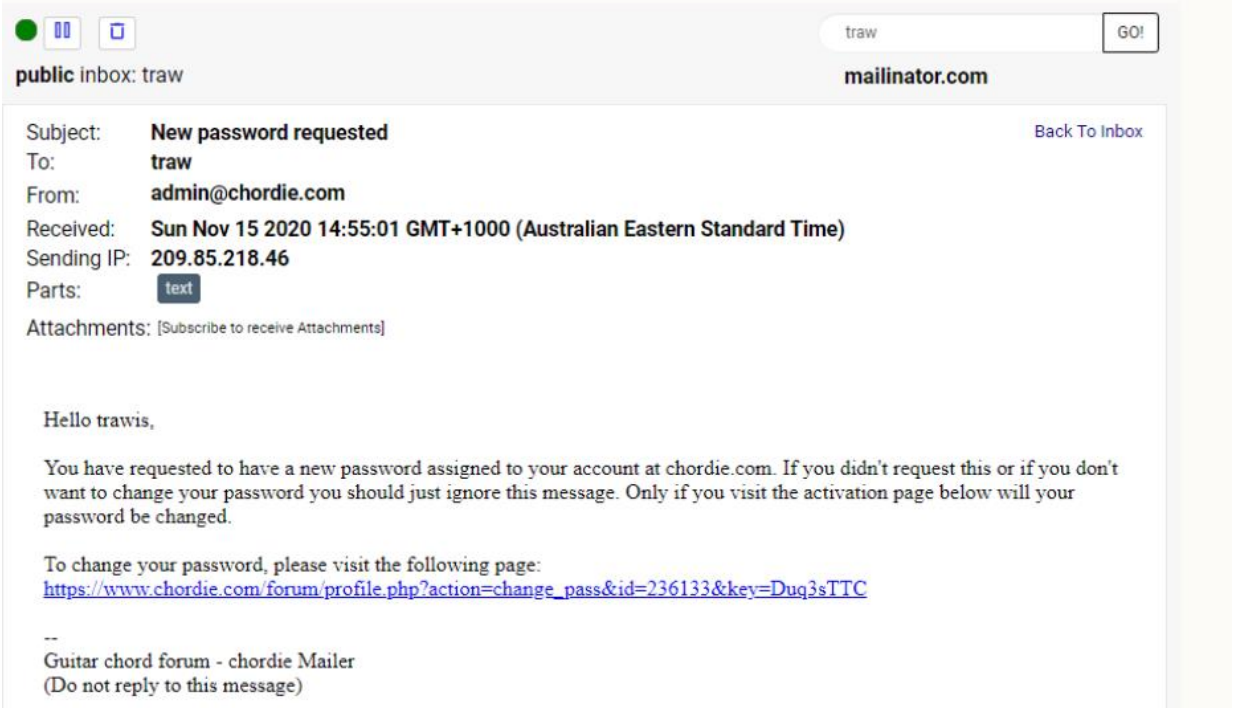
Apparently, an email has been sent to that address which indicates it does indeed exist on the site:



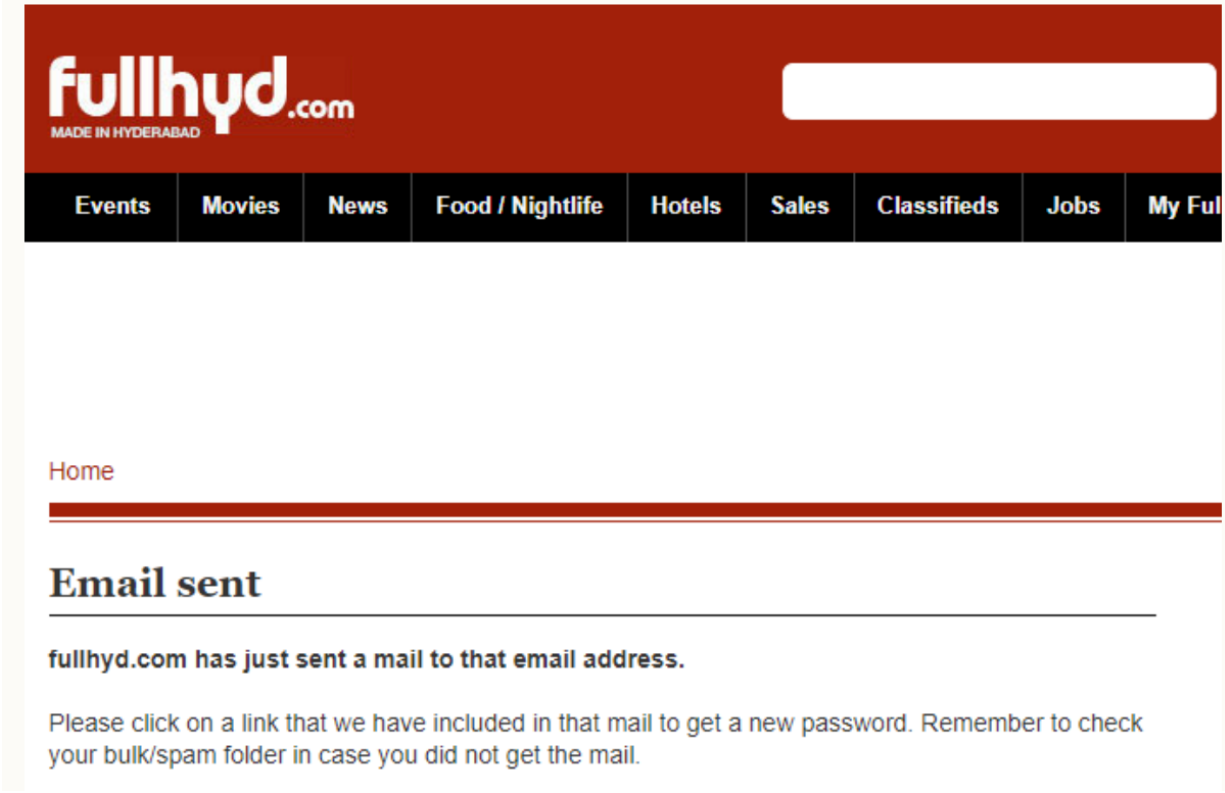
Offenbar wurde eine E-Mail an diese Adresse geschickt, was darauf hindeutet, dass sie tatsächlich auf der Website existiert:

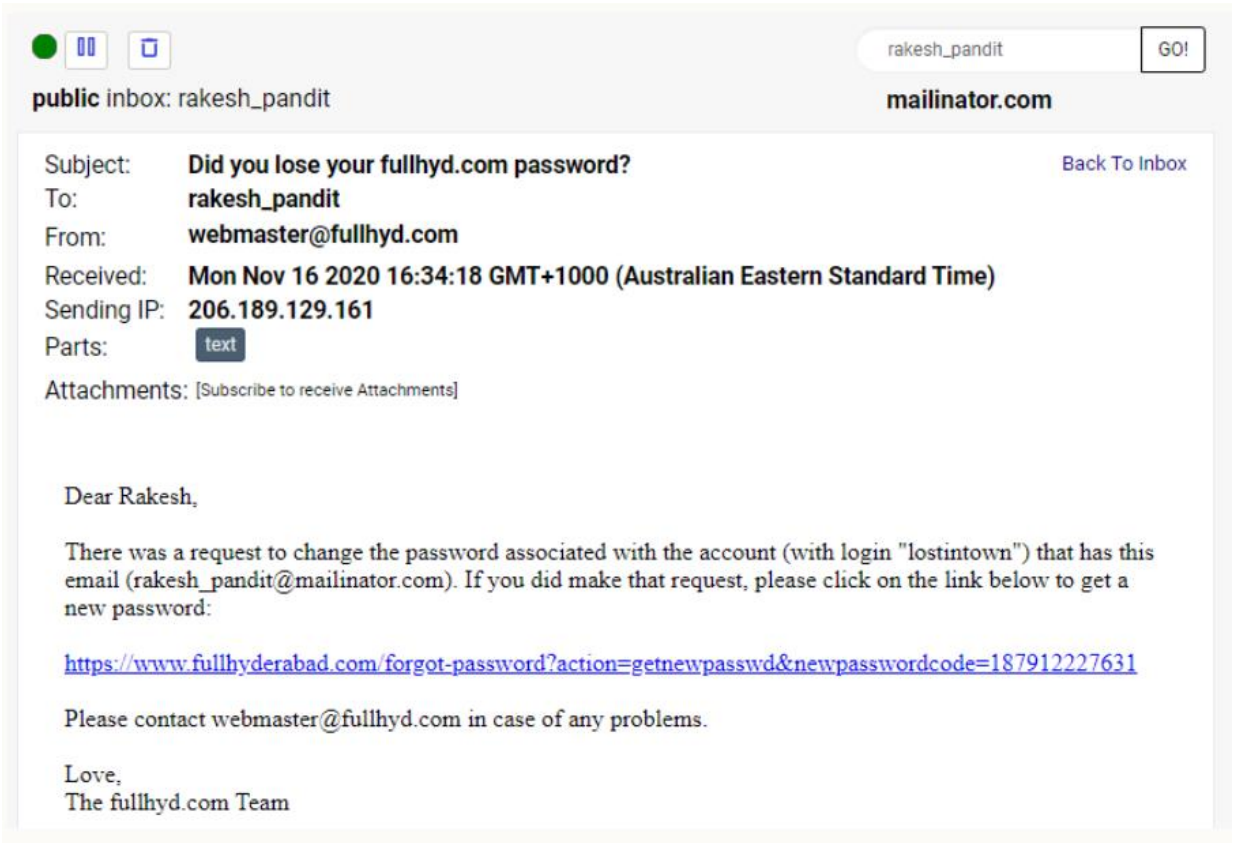


Und tatsächlich, in diesem öffentlichen Mailinator-Posteingang ist die E-Mail zum Zurücksetzen des Passworts für einen Benutzer namens "trawis":

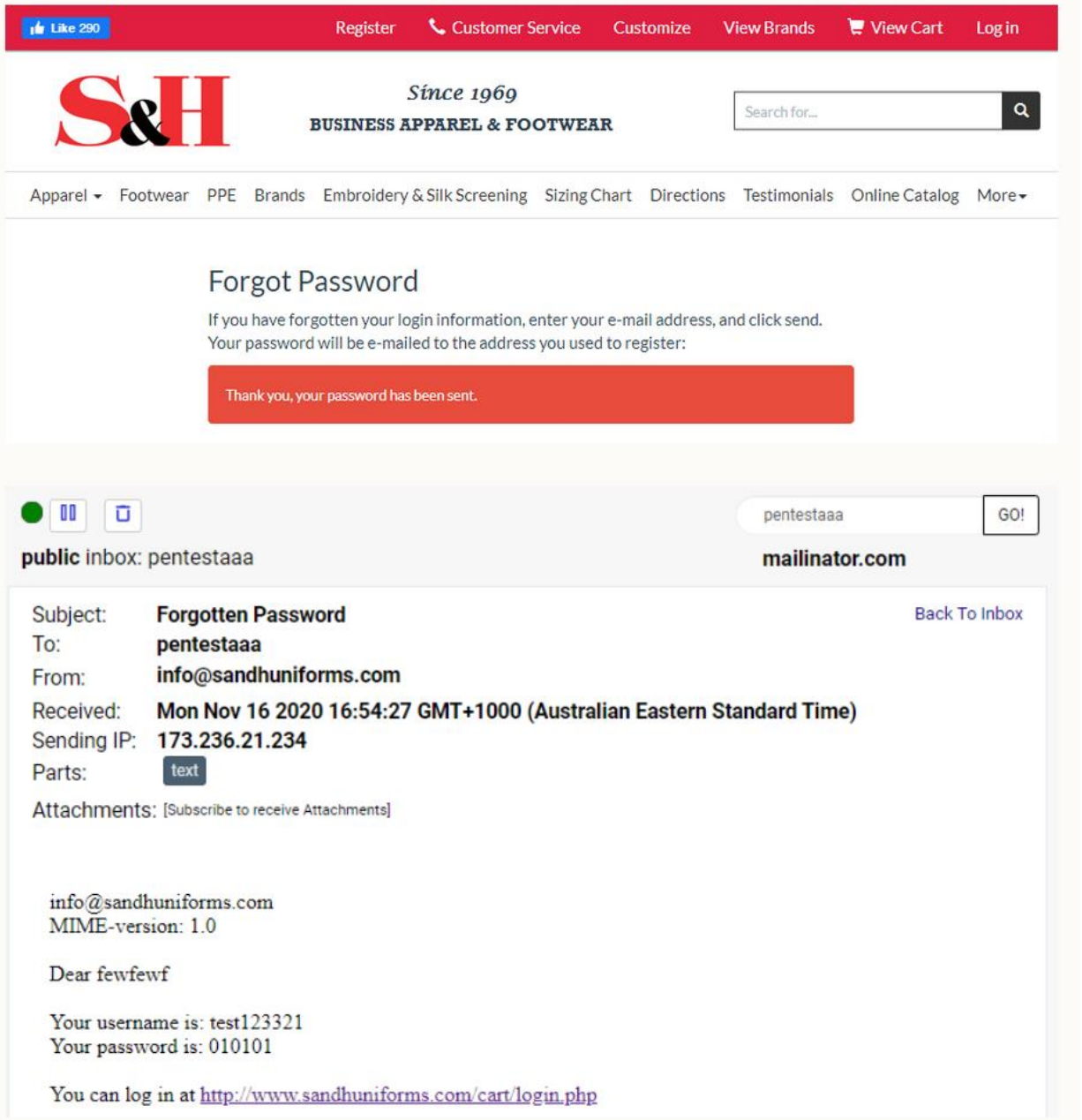


Folglich besteht eine sehr hohe Wahrscheinlichkeit, dass diese Daten echt sind. Ich habe Chordie nicht benachrichtigt, da sie eine von mehr als 23k gelisteten Seiten sind, so dass eine Offenlegung im traditionellen Sinne offensichtlich nicht funktionieren wird, zumindest nicht, wenn ich das Unternehmen privat kontaktiere. Aber jedes Mal, wenn ich nachsah, wiederholte sich das Muster: rakesh_pandit@mailinator.com hat ein Konto auf fullhyderabad.com:

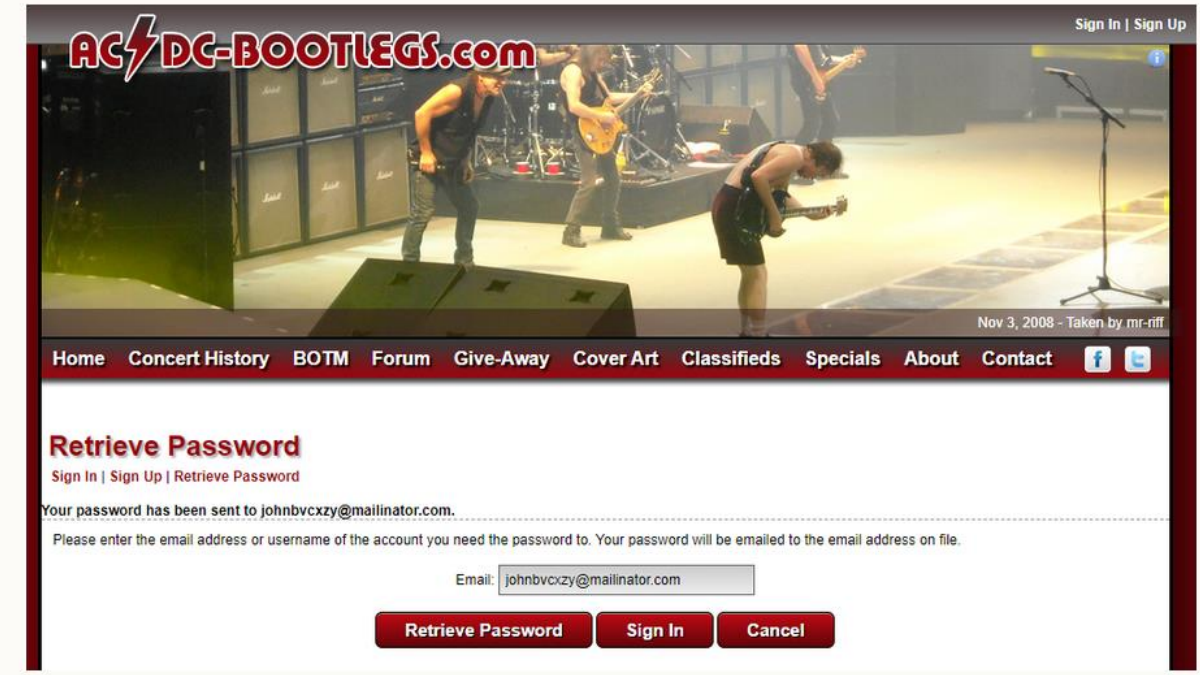


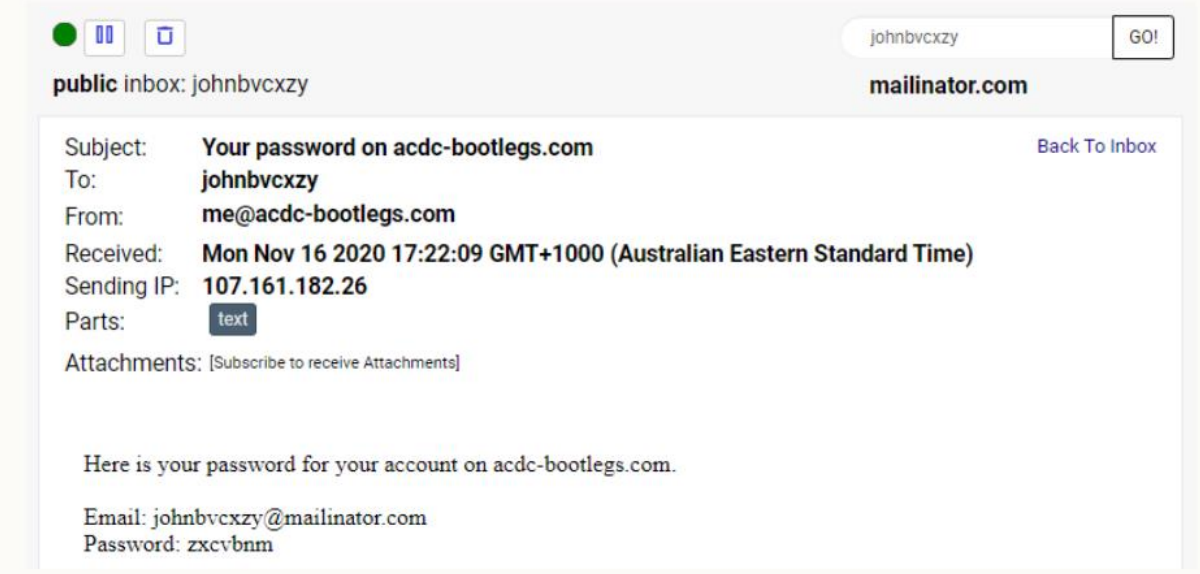


Oder drüben auf sandhuniforms.com hatte pentestaaa@mailinator.com auch einen Account:



In diesem Beispiel befanden sich die Daten in einer Datei namens "www.sandhuniforms.com {54.629} [NOHASH].txt" gefunden, und aus der E-Mail mit dem vergessenen Passwort geht hervor, dass sie gar nicht erst gehasht wurden. Dasselbe gilt auch für johnbvcxzy@mailinator.com auf acdc-bootlegs.com:



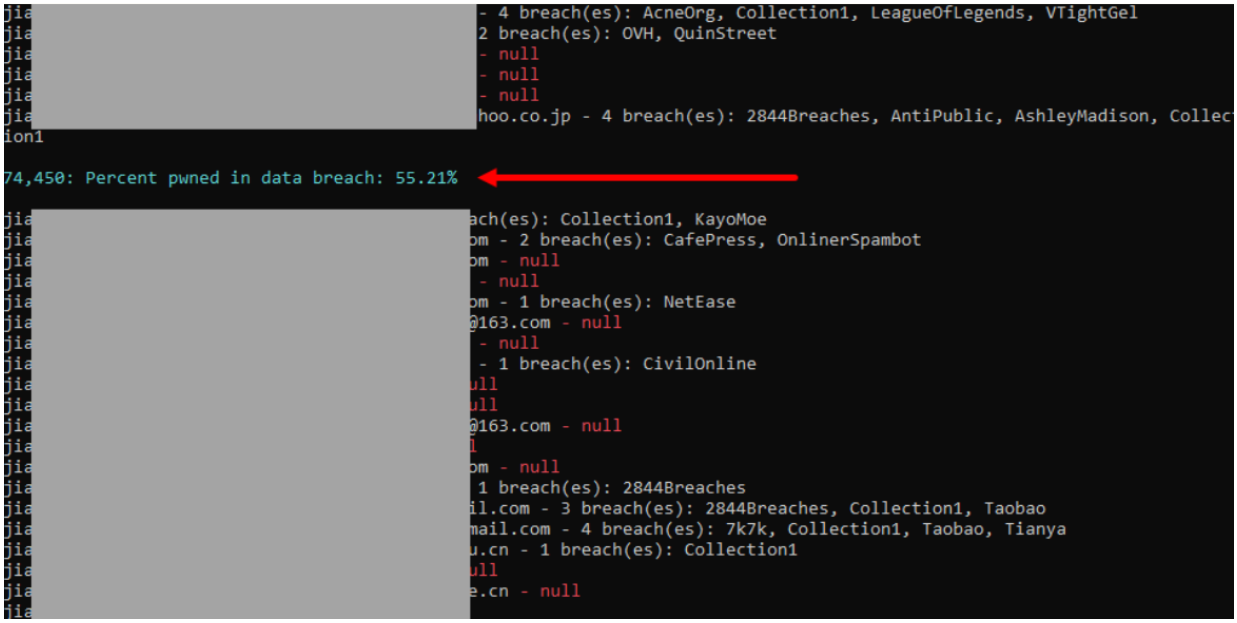


Ich bin mir bewusst, dass ich in den obigen Bildern tatsächliche E-Mail-Adressen und entweder Passwörter oder Zurücksetzungs-Tokens zeige, aber auch hier handelt es sich ganz klar um Testkonten, bei denen man keine Privatsphäre erwarten kann. Ich zeige sie nur, um einen Eindruck zu vermitteln; es handelt sich um eine ernstzunehmende Sammlung von Daten, die tatsächliche Sicherheitsverletzungen enthalten, die den Betreibern der Website mit ziemlicher Sicherheit unbekannt sind.

Viele der in dieser Datensammlung aufgeführten Websites sind inzwischen nicht mehr aktiv. Zum Beispiel gibt flyinghearts.info zum Zeitpunkt der Erstellung dieses Artikels einfach "Forbidden" zurück. Noch im Mai war es laut archive.org ein Service für Kerle, die tschechische Frauen kennenlernen wollten. Oder nehmen Sie cyberlearningmauritius.org, das heute HTTP500 zurückgibt, aber im Januar letzten Jahres ein (selbsternannter) Weltmarktführer für digitale Bildung war.

Mindestens eine weitere Site in der Sammlung war zuvor (öffentlich) als Einbruch bekannt und war in diesem speziellen Fall bereits in HIBP. Zum Beispiel ist "hookers.nl {287.560} [HASH+NOHASH] (Adult)_special_for_XSS.IS.rar" bereits in HIBP als sensible Sicherheitsverletzung enthalten. Ich bin mir sicher, dass es auch noch andere gibt, so dass es sich zwangsläufig nicht um 100% neue Daten handelt, mal sehen, ob wir das beziffern können:

Ich war neugierig, wie viele dieser Daten bereits in anderen Sicherheitsverletzungen aufgetaucht sind und ob es einen offensichtlichen Trend gibt. Handelt es sich zum Beispiel größtenteils um Daten aus der Collection #1 credential stuffing list, die ich Anfang letzten Jahres geladen habe? Ich nahm einen Teil der Adressen aus den 226 Millionen, die ich extrahiert hatte, und begann, sie mit HIBP abzugleichen. Hier ist, was ich nach der Überprüfung von über 74k Adressen gefunden habe:



Nur 55 % der Adressen im Stichprobensatz waren zuvor gesehen worden (nach dem Laden des kompletten Datensatzes in HIBP stieg diese Zahl auf 65 %). Es gab eine Reihe von Adressen im Vorfall in Sammlung 1 und auch in der Sammlung mit 2.844 Verstößen, die ich im Februar 2018 hinzugefügt habe, aber basierend auf den roten "Null"-Ergebnissen gab es eindeutig auch viele neue Adressen. Mit anderen Worten, es gab eine beträchtliche Anzahl von Personen, die vor dem Laden dieser Daten keine Treffer bei der Suche in HIBP erhielten, aber zuvor in einer Sicherheitsverletzung waren.

Dann waren da noch die Passwörter. Wenn man sich die Passwörter anschaut, sind es allesamt schreckliche Passwörter, die man bei den meisten Leuten erwarten würde. Passwörter wie "Ashtro1969", "Odette1978" und, was angesichts der Datei, die ich mir ansah, vielleicht nicht überraschend ist, "ilovechordie". Während viele der von mir getesteten Passwörter so schrecklich waren, dass sie bereits in anderen Datenschutzverletzungen aufgetaucht und zu Pwned Passwords durchgedrungen waren, gab es diese drei dort überhaupt nicht. Tatsächlich existierten über 40 Millionen von ihnen überhaupt nicht.

Die Passwörter stellen jedoch auch ein kleines Rätsel dar, wenn man sie aus Tausenden von separaten Dateien analysiert. Während viele als Kennwortpaare in den "Results.txt"-Dateien

der jeweiligen Archive vorhanden waren, existierten andere in Dateien wie "libertidating.com {1.928} decrypted.txt" (dabei handelt es sich mit ziemlicher Sicherheit eher um geknackte Hashes als um "entschlüsselte" Chiffren) und "promotionalproductsglobalnetwork.ca {2.166} [NOHASH].txt", wobei letzteres möglicherweise darauf hinweist, dass die Kennwörter nie gehasht wurden. Tausende von Dateien, unterschiedliche Namensformate, und obwohl die Struktur größtenteils konsistent ist, gibt es zwangsläufig einige Parsing-Probleme. Zum Beispiel dieses "Passwort":

```
3px;"><a href="docs/!INDEX.html"><b>Ãëàâíàÿ</b></a></div><div style="padding-left: 10px;
padding-top: 3px; padding-bottom: 3px;"><a href="docs/ondfi5.html" style="">Î êîìïàíèè</a>
<br/></div><div style="padding-left: 10px; padding-top: 3px; padding-bottom: 3px;"><a
href="docs/8qjisp.html" style="">Óñëóãè</a><br/></div><div style="padding-left: 10px; padding-
top: 3px; padding-bottom: 3px;"><a href="
```

Das wäre ein episches Passwort, wenn es tatsächlich jemand benutzt hätte, aber es ist mit ziemlicher Sicherheit ein Upstream-Parsing-Fehler. Oder nehmen Sie dieses Passwort:

```
welcometomykitchen12345678
```

Ja, ich kann mir vorstellen, dass jemand diesen Begriff auf einer Website verwendet (vielleicht auf einer, die mit Kochen zu tun hat), aber nein, ich glaube nicht, dass er 6.349 Mal verwendet wurde, was der Anzahl der Vorkommen entspricht, die im breach-Korpus gefunden wurden. Interessanterweise stammten sie alle aus "www.vcanbuy.com {134.303} [HASH] (Business and Industry).txt", und soweit ich es erkennen kann, ist vcanbuy.com eine thailändische Modeseite. Aber keines dieser Datenqualitätsprobleme spielt eine Rolle - hier ist der Grund:

Wenn diese Passwörter in Pwned Passwords einfließen, existieren sie letztlich als Hashes, die heruntergeladen oder mit k-anonymity abgefragt werden können. Niemand wird das erste Passwort mit allen Hashes verwenden, also hat es keine Auswirkungen in der realen Welt. Jemand könnte versuchen, das zweite Passwort zu verwenden, und ein Dienst, der HIBP's Pwned Passwords verwendet, könnte es dann aufgrund seiner Prävalenz ablehnen. Damit habe ich kein Problem, denn es ist kein gutes Passwort! Aber was ist mit Hash-Kollisionen? Was ist, wenn jemand anderes versucht, ein Kennwort zu verwenden, bei dem der SHA-1-Hash gleich dem SHA-1-Hash der Junk-Daten ist? Es würde einen Treffer in HIBP zurückgeben, was effektiv ein falsches Positiv wäre, aber egal, ob es eine kleine Menge an Junk-Daten gibt oder nicht (und es ist eine sehr kleine Menge - weit unter 1%), das gleiche Problem herrscht vor. Und wenn man bedenkt, dass SHA-1-Hashes insgesamt einen Zeichenraum von 16^40 belegen, kann man leicht ausrechnen, wie extrem unwahrscheinlich das ist (und die Auswirkungen sind immer noch sehr gering, wenn es doch passiert).

In Anbetracht der Anzahl der einzelnen Sicherheitsverletzungen, der Legitimität der Daten und der riesigen Anzahl von bisher ungesehenen E-Mail-Adressen und Passwörtern habe ich alles in HIBP geladen. Die Menge - sowohl E-Mails als auch Passwörter (Anmerkung: diese gehen als separate Archive hinein und niemals als Paare, lesen Sie mehr über Pwned Passwords hier). Wie bei anderen Sicherheitsverletzungen, bei denen es keinen eindeutigen Ursprung gibt, bedeutet dies, dass die Betroffenen möglicherweise nicht mehr wissen, welcher Dienst ihre Daten weitergegeben hat. Es bedeutet auch, dass sie ihr Passwort verraten finden können und nicht wissen, welcher Dienst es weitergegeben hat. Aber das spielt auch keine Rolle - hier ist der Grund:

Das Ziel von HIBP war es schon immer, Verhaltensweisen zu ändern, nämlich die Leute dazu zu bewegen, nicht mehr überall diese ein oder zwei oder drei schwachen Passwörter zu verwenden, sondern sich einen richtigen Passwort-Manager wie 1Password zuzulegen und überall starke, eindeutige Passwörter zu erstellen (volle Offenlegung: Ich bin in deren Beirat). Wenn Sie das bereits getan haben und sich dann in den Cit0day-Daten wiederfinden, dann ist das aus zwei Gründen ein Nicht-Ereignis:

1. Die Tatsache, dass Sie in einer der 23k Sicherheitslücken sind, isoliert Ihr Risiko auf diese Sicherheitslücke allein; da Sie das Passwort nirgendwo anders wiederverwendet haben, stellt die Enthüllung an diesem einen Ort kein Risiko für Sie an einem anderen Ort dar.
2. Von einem Passwort-Manager zufällig generierte Passwörter werden mit ziemlicher Sicherheit nicht geknackt; selbst wenn sie schwach gespeichert sind (z.B. als ungesalzener MD5-Hash), wird Ihre ~40-Zeichen-Zufallsfolge nicht geknackt. Wenn die Website sie jedoch im Klartext gespeichert hat, siehe Punkt 1.

Und wenn Sie noch keinen Passwort-Manager haben? Dann sollten Sie sich einen zulegen und das Passwort für alle wichtigen Konten sowieso umgehend ändern!

Aber es gibt eine Lücke, die über die Risiken hinausgeht, die allein mit offengelegten Passwörtern verbunden sind, und das sind die persönlichen Auswirkungen von anderen offengelegten Daten. Wenn Sie z.B. einen Haufen anderer persönlicher Informationen in Chordie eingegeben haben, dann wäre es vernünftig anzunehmen, dass diese nun im Besitz anderer Parteien sind und Sie würden das zu Recht wissen wollen. An dieser Stelle müssen wir die in den beiden obigen Gists genannten Seiten wirklich in die Pflicht nehmen, und ich schlage Folgendes vor: Wenn sie auf der Liste stehen, testen Sie einen Mustersatz ihrer eigenen Abonnenten-E-Mail-Adressen auf HIBP. Wenn Sie sich Sorgen machen, die persönlichen Daten von jemand anderem an meinen Dienst zu übermitteln, nehmen Sie ein paar Mailinator-Adressen und überprüfen Sie diese. Wenn sie mit Treffern gegen die Cit0day-Verletzung zurückkommen, ist das ein sehr starker Hinweis auf eine Verletzung.

Abschließend lässt sich sagen, dass es jetzt 226 Mio. weitere verletzte Konten in HIBP gibt und weitere 41 Mio. Passwörter (etwas mehr als 40 Mio. neue aus diesem Vorfall und etwas weniger als 1 Mio. aus anderen Vorfällen seit der letzten Veröffentlichung). Nur um zu unterstreichen, warum es wichtig war, diesen Datensatz in HIBP zu bekommen, wurde die Pwned Passwords k-anonymity API im letzten Monat 815M Mal angegriffen:

Das Einspeisen dieser Passwörter in den Korpus der bekannten verletzten Passwörter hat eine unmittelbare und greifbare Auswirkung auf die Übernahme von Konten, was gut für Online-Dienste, gut für Einzelpersonen und gut für das Web als Ganzes ist.

Ein letztes Wort zu diesem Thema: Bitte kontaktieren Sie mich nicht und fragen Sie mich nach Details über die Verletzung Ihrer Adresse oder das verwendete Passwort, ich betreibe dies als kostenlosen Service in meiner verfügbaren Zeit und habe nicht die Kapazität, auch nur einem winzigen Bruchteil der 226 Millionen Personen in diesem Vorfall zu antworten. Besorgen Sie sich einen Passwort-Manager, verwenden Sie starke und eindeutige Passwörter, das ist alles.

Übersetzt mit www.DeepL.com/Translator (kostenlose Version)