Tokopedia and Microsoft Breach Broker selling fresh trove of 26 million accounts

ZEROFOX

Blog

May 7, 2020 |by ZeroFox Research

Executive Summary

ZeroFox Alpha Team has identified a dark web breach broker selling three large, high-profile breaches. The dealer, who goes by the alias Shinyhunters, is offering these breach dumps for sale on a dark web forum, for prices between $1500 and $2500 USD. The ShinyHunters group has breached numerous organizations in recent weeks, including Tokopedia, a major Indonesia e-commerce company, and Unacademy, an Indian online learning platform. Allegedly, the group is also behind the recent breach of Microsoft's private GitHub repositories, containing the source code of future open-sourced projects. Although it has not yet been released, the Shinyhunters group has threatened to release the code publicly for free. The new breaches include Chicago-based home meal kit delivery service HomeChef, online printing and photo store ChatBooks, and Chronicle.com, a news website dedicated to covering colleges and universities. In total, these breaches contain the user data and passwords of 26,000,000 accounts.

HomeChef Breach

The HomeChef breach contains 8 million records, and a sample set of records was posted to a paste website. The rows contain emails, bcrypt passwords, IP addresses and a number of columns of PII such as last 4 of social security numbers, zip codes and phone numbers. The breach has a sale price of $2500 USD.

```
Schema:

"id","email","encrypted_password","reset_password_token","reset_password_sent_at","remember_created_at","sign_in_count","current_sign_in_at","last_sign_in_at","current_sign_in_ip","last_sign_in_ip","created_at","updated_at","name","customer_id","last_4_digits","provider","uid","status","servings","confirmation_token","confirmed_at","confirmation_sent_at","unconfirmed_email","phone","delivery_day","culinary_level","agreed_to_terms","discovery","weekly_meals","age","gender","region","relationship","campaign_id","promotion_type","min_age","max_age","behavior","interest","optional_1","optional_2","optional_3","optional_4","optional_5","active","signup_redemption_id","zip_code_id","completed_signup_at","current_sign_in_platform","last_sign_in_platform","web_sign_in_at","mobile_sign_in_at","experiment_data","preference_data","meal_plan_id","vendor","paypal_email","terms_accepted_at","shipping_cost_cents","accepted_agreements","uuid","brand_id","monthly_credit"

Samples:

5560369,[redacted],$2a$10$yLwsCDvxARpSY5XKvJPmPOmTYKbjXWi4JriQw.q/D6SvPJAJWYgse,,,,3,2019-01-14 00:46:17,2018-12-27 13:34:12,[redacted],2018-11-29 07:27:52,2019-01-14 00:46:17,[redacted],cus_E3rkQNOueoNydM,"7225",,,COMPLETE,2,,,,"12146798850",Friday,,,,2,,,,,,,,,,,,,,,1260411,302222,2018-11-29 07:32:23,web,web,2019-01-14 00:46:17,,,,1,0,,,1000,"{""terms_of_use_accepted_at"": ""2018-11-29T01:32:23.530-06:00"",""privacy_policy_accepted_at"": ""2018-11-29T01:32:23.530-06:00""}",c225b838-3867-4248-98fc-84ffe91fb13d,1,
5893719,[redacted],$2a$10$KzDqy.rWTdW/kUi3o2fO9e6STgGMC2QhSYH9aknnmlAMwAWvVXNN.,,,,3,2019-02-08 15:11:07,2019-01-25 17:58:56,[redacted],2019-01-14 22:41:57,2019-02-08 15:14:48,[redacted],cus_ELLPOti86nfz4B,"5510",,,COMPLETE,2,,,,"12134440528",Wednesday,,,3,,,,,,,,,,,,,,,1323988,302843,2019-01-14 23:19:28,web,web,2019-02-08 15:11:07,,,,1,0,,,1000,"{""terms_of_use_accepted_at"": ""2019-01-14T17:19:28.994-06:00"",""privacy_policy_accepted_at"": ""2019-01-14T17:19:28.995-06:00""}","95676684-647b-42a1-baa5-f473411d9a25",1,
7617790,[redacted],$2a$10$fkQ638qz0j654tpKHEooy.K/ObHk.42uVKUoUiVILXCRfGvZR9fSu,,,,1,2019-09-20 15:22:53,2019-09-20 15:22:53,[redacted],2019-09-20 15:22:53,2019-09-20 15:30:02,[redacted],,,,,on_payment_step,4,,,,,"13038030361",Wednesday,,,,3,,,,,,,,,,,,,,,,,,,,,301754,,web,web,2019-09-20 15:22:53,,,,1,0,,,,"{}","0364f053-9e3b-462b-b770-422e8defcf68",1,
7375109,kburridge-[redacted],$2a$10$tm.sInTFLAflcFRWNgvTCOk3l5h7g9rtVDHPeqXzW6yzuOGWTIQK.,,,,1,2019-08-21 22:20:55,2019-08-21 22:20:55,[redacted],2019-08-21 22:20:55,2019-08-21 22:21:39,,,,,,on_delivery_step,2,,,,,,,,,4,,,,,,,,,,,,,,,,,,web,web,2019-08-21 22:20:55,,,,1,0,,,,"{}",f71cc696-b06e-40ca-a592-76f0c09c5107,1,
6287655,[redacted],$2a$10$yYs34A2C7VlrEyav0PBKAudoYTnOBk59LnYojO7DYlqzUhhERRUxS,,,,1,2019-02-28 21:51:38,2019-02-28 21:51:38,[redacted],2019-02-28 21:51:38,2019-02-28 21:53:06,,,,,,on_delivery_step,2,,,,,,,,,2,,,,,,,,,,,,,,,,,,web,web,2019-02-28 21:51:38,,,,1,0,,,,"{}",c4fdc66b-d01a-47a1-aede-e78841213528,1,

Hash Algorithm: BCRYPT
```

Figure 1: HomeChef Breach Sample Posted by Shiny Hunters

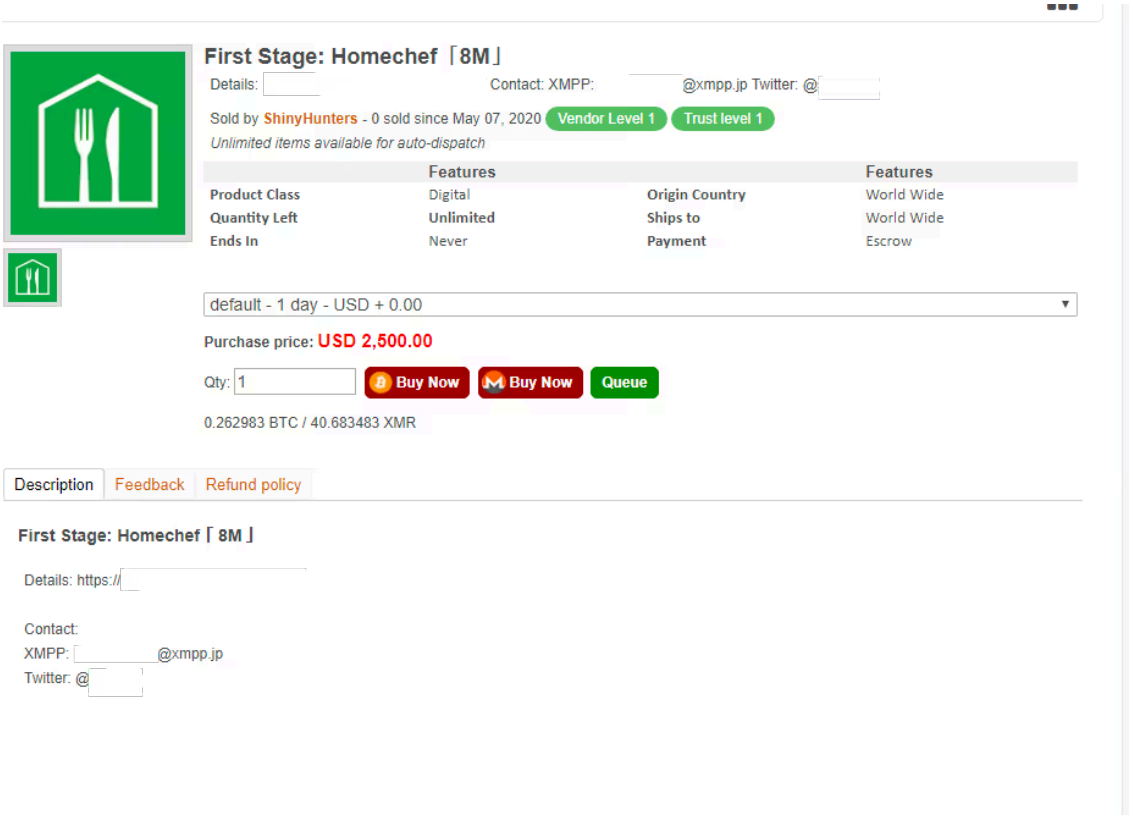

Figure 2: HomeChef Breach Sellers Page

Chatbooks Breach

The Chatbooks breach contains 15 million rows of data. Shiny Hunters also posted a sample set to a paste website. The rows contain emails, SHA-512 password hashes, social media access tokens and a number of personally identifiable information. The breach has a sale price of $2000 USD.

```
Schema:

personID,accountExp,lastLoginDate,isOnline,requiresPassword,lastLockoutDate,lastPasswordChangeDate,isLockedOut,creationDate,lastActivityDate,email,name,accountType,password,isApproved,userType,photoKey,adminPassword,administeredBy,adminUsername,instagramAccessToken,instagramID,testUser,approvedDate,inviteDate,facebookUserId,facebookToken,facebookInviteKey,coverPhotoS3Key,pendingPhotoKey,photoUploaderPersonID,inPromo,capacityLimitBytes,planType,receipt,isStripeCustomer,weeWebRef,stripeCustomerToken,phone,instagramGroupID,countryCode,instagramSubscriptionId,prodStripeCustomerToken,accessToken,ID,date

Samples:

'person_zztgws5G5YRGp7fEOH3hJFKIGEC8I4mf40fPYbQK','0001-01-01','2019-09-05','\0','\0','2019-03-06','2017-07-25','\0','2017-07-08','2017-07-25',' [redacted] ',' [redacted] ','free',' [redacted] 1PhG8jU7eRFiXr','','',NULL,NULL,NULL,NULL,NULL,NULL,'\0','2017-07-25 05:22:53',NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,0,1073741824,1,NULL,'\0',NULL,NULL,NULL,NULL,'US',NULL,NULL,'5c215d6b-16d6-4fa0-8f8c-ddf1828162fc',3853412,'2017-07-08 20:27:59'
'person_zzTcaWp6uDYwQeLGdk6T2shskBWMu5Zdv70RGOK3','0001-01-01','2019-07-27','\0','\0','2019-07-27','2019-07-27','\0','2019-07-27','2019-07-27',' [redacted] ',' [redacted] ','free','E011C76D9001327C21250B010E656D049815AECE2D9C4C20E70865C5464521F9F186E139B88D427B96D4B3264F36133F7CD1405360CF35074A17B0D39A1BC3B2:HAKKhbCO3Zo7HfBjio6UJXB8w7aeQLs9srHZe2FiLfLXETg64LYJf8kT8Mnjay8r','','',NULL,NULL,NULL,NULL,NULL,NULL,'\0','2019-07-27 10:51:42',NULL,NULL,NULL,NULL,NULL,NULL,NULL,0,1073741824,1,NULL,'\0',NULL,NULL,NULL,NULL,'US',NULL,NULL,' [redacted] ',12810210,'2019-07-27 10:50:42'

Hash Algorithm: SHA-512
```

Figure 3: ChatBooks Breach Sample Posted by Shiny Hunters

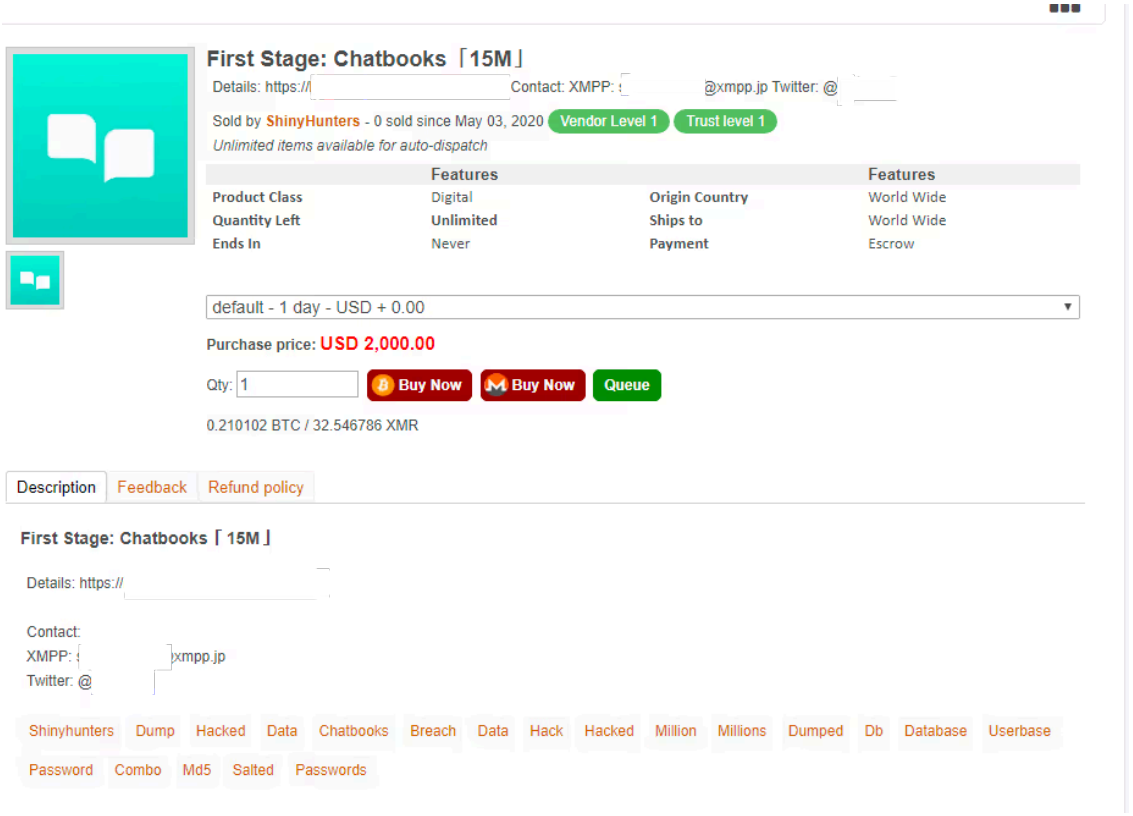

Figure 4: ChatBooks Breach Sellers Page

Chronicle.com Breach

The Chronicle.com breach contains 3 million records, but ShinyHunters did not post a sample set of data or indicate in their post what the data contains. The breach has a sale price of $1500 USD.

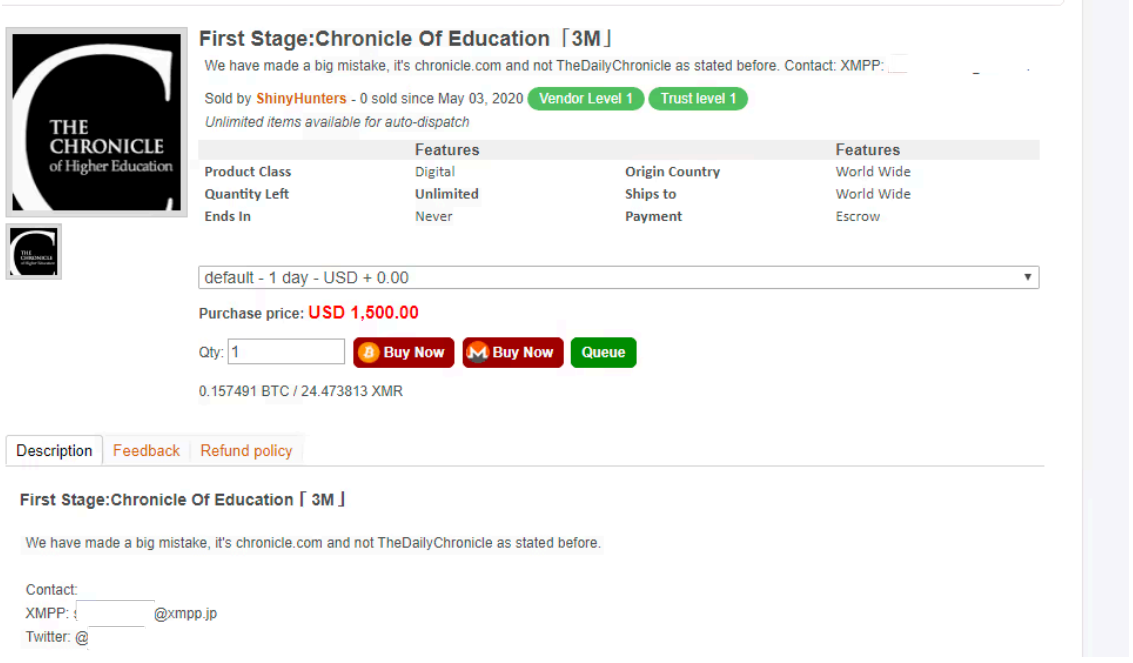

Figure 5: Chronicle.com Breach Sellers Page

Other aliases for ShinyHunters Breach Broker

ShinyHunters isn't the only moniker this actor has used. The group made a post on May 6, 2020 on a popular cybercrime forum indicating that they've pilfered 500 GB of internal source code from Microsoft.

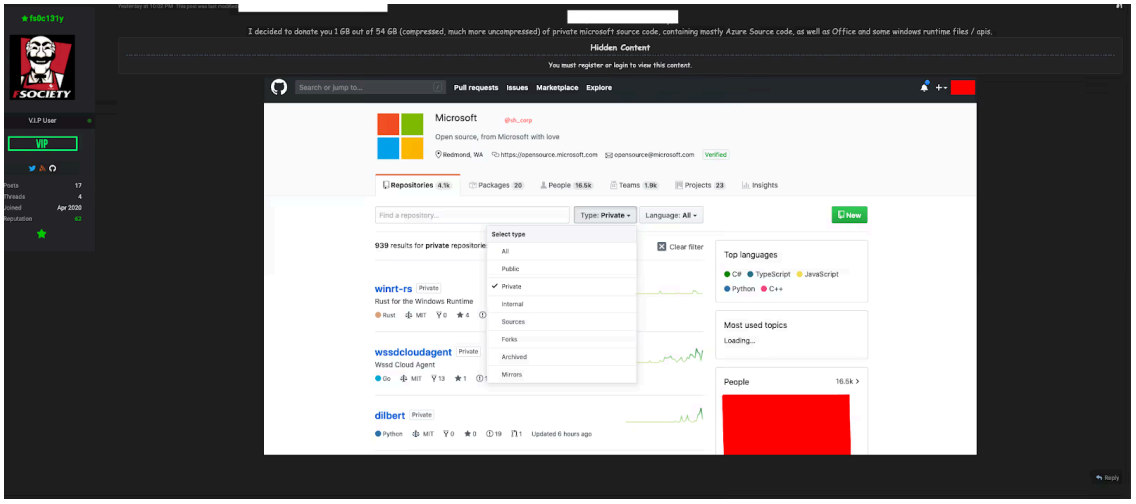

Figure 6: Microsoft Breach Post by fs0c131y/Shiny Hunters

According to BleepingComputer, ShinyHunters reached out to them directly to confirm the story. The sales ad for the Microsoft leak was authored by "fs0c131y", a popular moniker in the show Mr. Robot, as well as a popular hacker on Twitter. Using names from popular influencers on these forums is nothing new, for example Brian Krebs and Troy Hunt have impersonators. What links fs0c131y and Shiny Hunters, is that fs0c131y posted the same contact information as their shop on the dark web.

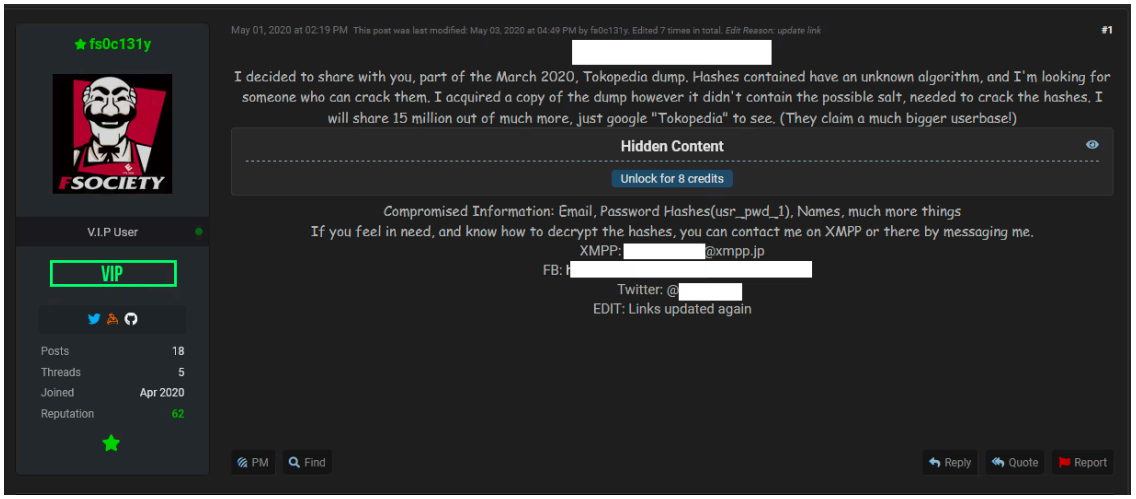

Figure 7: Tokopedia Breach Post by fs0c131y/Shiny Hunters

Conclusion

ShinyHunters is taking a page out of the book of **gnosticplayers**, the breach data broker who in 2018-2019 pilfered billions of records from dozens of companies and sold them online. Due to the verification of the Tokopedia breach by multiple researchers and the company itself, ZeroFox Alpha Team has HIGH confidence that these new breaches are legitimate, and will most likely be available on other breach marketplaces at lower prices

in the near future. It is likely that this actor will continue to breach companies and post their content for sale. These tactics proved both successful and profitable for gnosticplayers, and it is likely they will continue to appeal to other breach brokers for these reasons.

Tags: Breaches
