Credential Stuffing: Attacks and Economies
The 773 Million Record "Collection #1" Data Breach

17 January 2019

Many people will land on this page after learning that their email address has appeared in a data breach I’ve called "Collection #1." Most of them won’t have a tech background or be familiar with the concept of credential stuffing so I’m going to write this post for the masses and link out to more detailed material for those who want to go deeper.

Let’s start with the raw numbers because that’s the headline, then I’ll drill down into where it’s from and what it’s composed of. Collection #1 is a set of email addresses and passwords totalling 2,692,818,238 rows. It’s made up of many different individual data breaches from literally thousands of different sources. (And yes, fellow techies, that’s a sizeable amount more than a 32-bit integer can hold.)

In total, there are 1,160,253,228 unique combinations of email addresses and passwords. This is when...
Account Takeover

BUY CREDENTIALS

VERIFY CREDENTIALS

LOGIN

FINANCIAL GAIN

FRAUDSTER

BOTNET

CUSTOMER SITE

END USER ASSETS

CREDENTIAL ABUSE

ACCOUNT TAKEOVER

SHOPPING

ACCOUNTS

DATA

LOGIN

Unrecognized Password
Credential Attacks Per Day (All Industries)

Date: October 24, 2018
Login Attempts: 285,983,922

Date: June 2, 2018
Login Attempts: 252,176,323

Date: October 27, 2018
Login Attempts: 287,168,120
Attacks Per Day (Media companies only)

Vertical: Video Media
Date: June 3, 2018
Login Attempts: 133,861,006

Vertical: Video Media
Date: October 25, 2018
Login Attempts: 175,981,359

Vertical: Video Media
Date: October 27, 2018
Login Attempts: 196,087,155
Credential Stuffing: Media vs Financial Services

- Media: 91%
- FiServe: 9%

Source
SOTI Security, v5 Special Edition
April 8, 2019
(Data collected 050118-120118)
Why is Media such a popular target?

NSW man charged over Netflix, Spotify scam

With the help of the FBI, Australian police have charged a Sydney man they say was selling stolen account details for various online subscription services.

An IT worker who allegedly made hundreds of thousands of dollars from selling stolen subscription details for streaming services including Netflix and Spotify has been granted bail after facing a Sydney court.

Evan Leslie McMahon, 21, was arrested after the Australian Federal Police were alerted by the FBI to his alleged activities via a website called WickedGen.com in May 2018.
BEGINNERS GUIDE : BASICS OF SNIPR/HOW TO USE.
Fixn M · 3.9K views · 6 months ago
This guide will go over the basics of snipr, How to use it and browse the interface and how to check/crack accounts :) SNIPR ...

* UPDATED * BEGINNERS GUIDE/TUTORIAL ON HOW TO USE SNIPR
Fixn M · 2K views · 5 months ago
SNIPR website: https://snipr.gg/ SDZ Discord: https://discord.gg/thk4Sv8 My SNIPR Profile: https://snipr.gg/profile/2387-fixn/ ...

SNIPR Multi Account Checker New 2018
New Tech Everyday · 19K views · 11 months ago
About This Software (Snipr v3.4.1.4) : Snipr is a paid multi checker tool (you can buy it from their website https://snipr.gg ...
Do the Math!

Example

At a conservative rate of 1% success

Earning for 100,000 login attempts = $1000
Earning for attempts against 5 different targets = $5000
Cost of attack = $450

The attacker stands to make **10 times the cost**!
# Top Attack Sources

<table>
<thead>
<tr>
<th>SOURCE COUNTRY</th>
<th>ATO.HEUR.LOGINS</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>4,016,181,582</td>
</tr>
<tr>
<td>Russia</td>
<td>2,509,810,095</td>
</tr>
<tr>
<td>Canada</td>
<td>1,498,554,065</td>
</tr>
<tr>
<td>Vietnam</td>
<td>626,028,826</td>
</tr>
<tr>
<td>India</td>
<td>625,476,485</td>
</tr>
<tr>
<td>Brazil</td>
<td>585,805,408</td>
</tr>
<tr>
<td>Malaysia</td>
<td>369,345,043</td>
</tr>
<tr>
<td>Indonesia</td>
<td>367,090,420</td>
</tr>
<tr>
<td>Germany</td>
<td>354,489,922</td>
</tr>
</tbody>
</table>
Top Attack Destinations

<table>
<thead>
<tr>
<th>DESTINATION COUNTRY</th>
<th>ATO.HEUR.LOGINS</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>12,522,943,520</td>
</tr>
<tr>
<td>India</td>
<td>1,208,749,669</td>
</tr>
<tr>
<td>Canada</td>
<td>1,025,445,535</td>
</tr>
<tr>
<td>Germany</td>
<td>760,722,969</td>
</tr>
<tr>
<td>Australia</td>
<td>104,655,154</td>
</tr>
<tr>
<td>Korea</td>
<td>37,112,529</td>
</tr>
<tr>
<td>China</td>
<td>26,173,541</td>
</tr>
<tr>
<td>Gibraltar</td>
<td>6,559,360</td>
</tr>
<tr>
<td>Netherlands</td>
<td>4,991,790</td>
</tr>
<tr>
<td>Japan</td>
<td>3,424,334</td>
</tr>
<tr>
<td>Italy</td>
<td>2,601,632</td>
</tr>
<tr>
<td>France</td>
<td>1,864,733</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>1,305,262</td>
</tr>
</tbody>
</table>
Protect Your Business From Credential Stuffing
Q&A