Analysis of the CardingMafia March 2021 data breach

xorl.wordpress.com/2021/04/23/analysis-of-the-cardingmafia-march-2021-data-breach/

April 23, 2021

leave a comment »

One relatively large carding forum, the CardingMafia, was breached and their data were shared in darkweb channels in late March 2021. I got a hold of this data set and found some interesting information. Of course, I cannot share PII or other sensitive material in a public blog post, but I can share some of the more generic analysis to hopefully provide better insights in this underground carding community, and the overall darkweb carding communities.

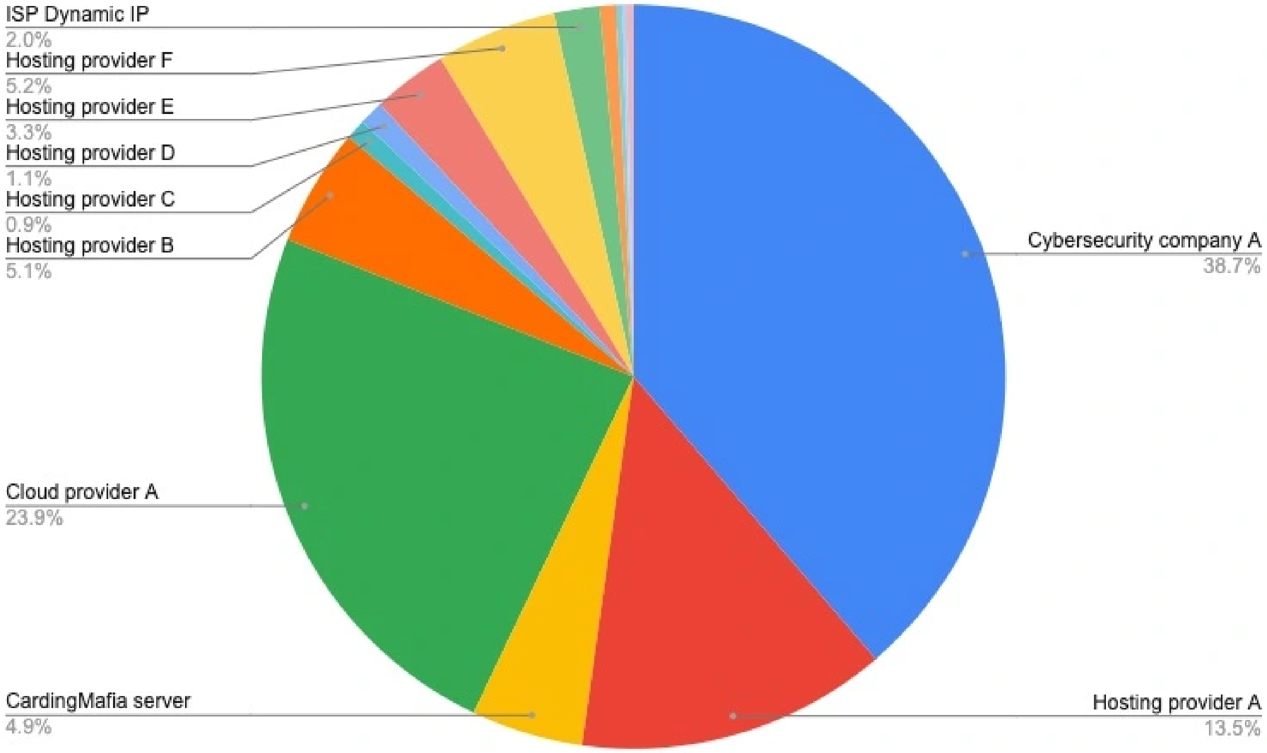
First of all, CardingMafia was both a "shopp" and an English-speaking forum. This means CardingMafia members were able to have forum discussions on topics of interest but there was also a section of the website where members could buy and/or sell stolen digital goods (compromised accounts, cardholder data, etc.)

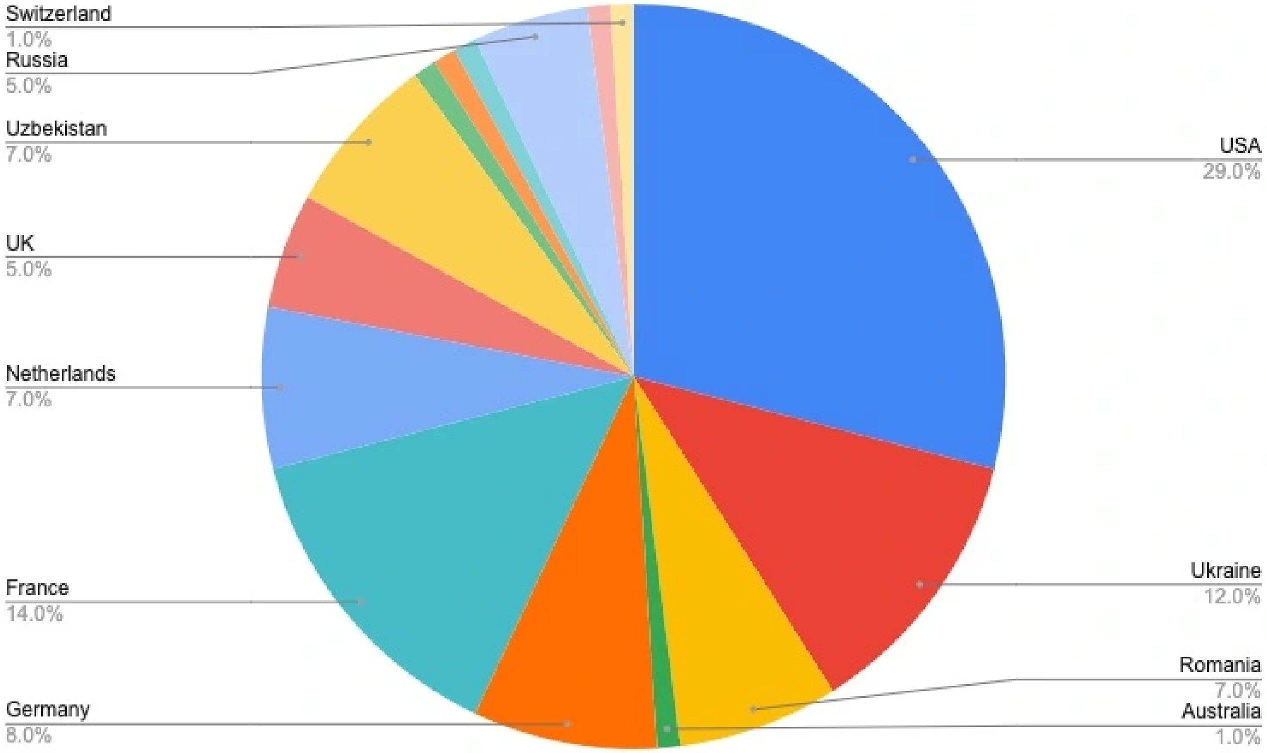
The data leak that happened in March 2021 was from the "user" table of the SQL server of the forum. In total, there were 297,076 accounts with various details such as username, IP address, creation time, hashed password, email, status, likes, etc. This is the dataset I'm using for this blog post.

As always, this is a personal research. I'm neither a lawyer nor I'm talking on behalf of my employer. This is 100% personal threat research to enrich some of my personal threat intelligence cases and projects.

The top 100 IP addresses with the highest amount of user accounts in CardingMafia are shown below. Each of those IP addresses had anything from 180 to over 13,000 unique forum accounts associated with it.

Although some were automated accounts (probably from darkweb scraping bots), it appears that many legitimate users were also using those services to hide their real IP addresses (proxies, VPNs, hosted jumphosts, etc.)

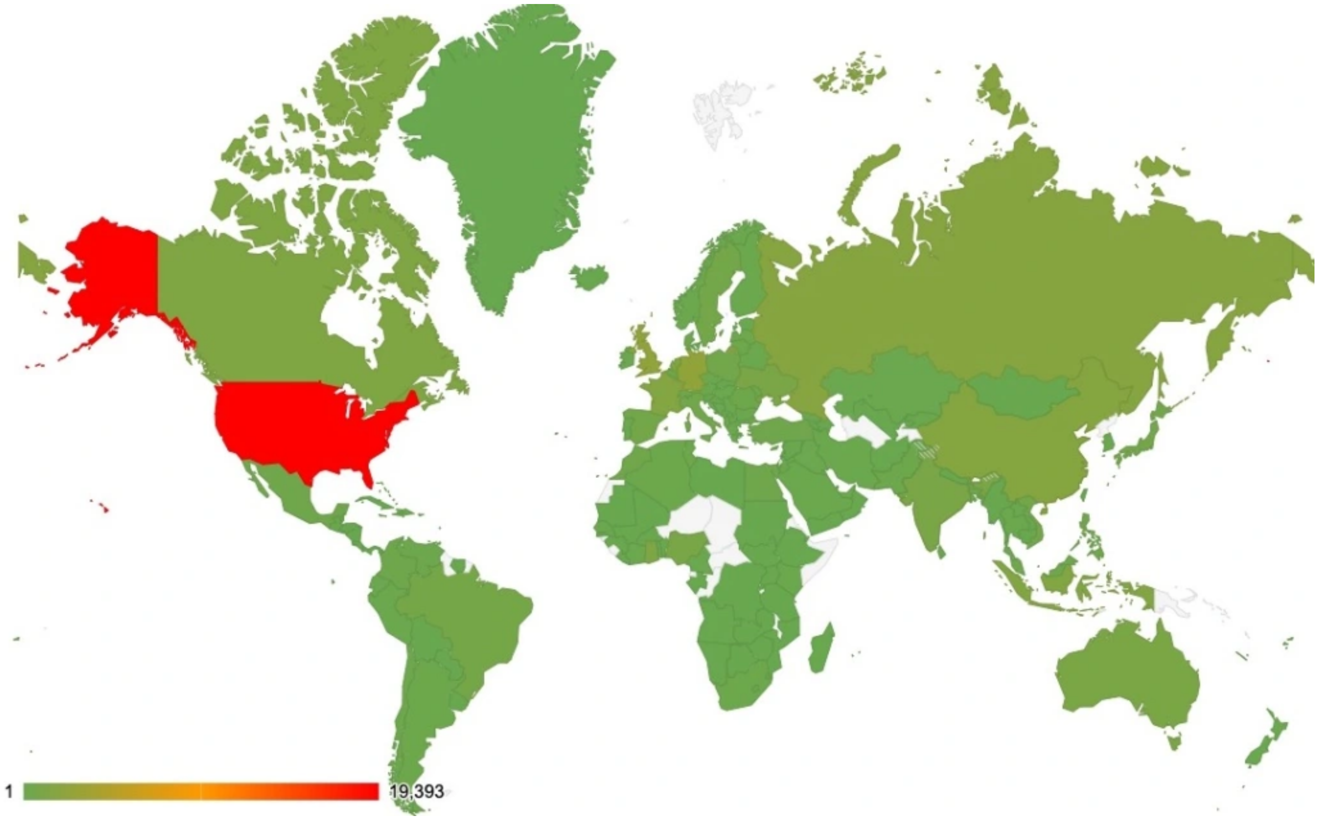




From those top 100 IP addresses you can see that the vast majority were coming from the US (29%), France (14%) and Ukraine (12%). Again, this doesn't necessarily mean that the forum users were actually from these countries, but that they were using services from those countries to access the forum.

To have a more holistic view, the following geo-heatmap is **based on all of the 297,076 IP addresses**. It’s worth noting here that in reality there were only 56,685 unique IP addresses that were used to open CardingMafia forum accounts.

With this bigger picture view, we get a better understanding of likely the real countries of the forum members since many of them were connecting directly from ISPs. The United States is probably skewed due to the amount of cloud services and proxies, but the rest should be closer to reality.

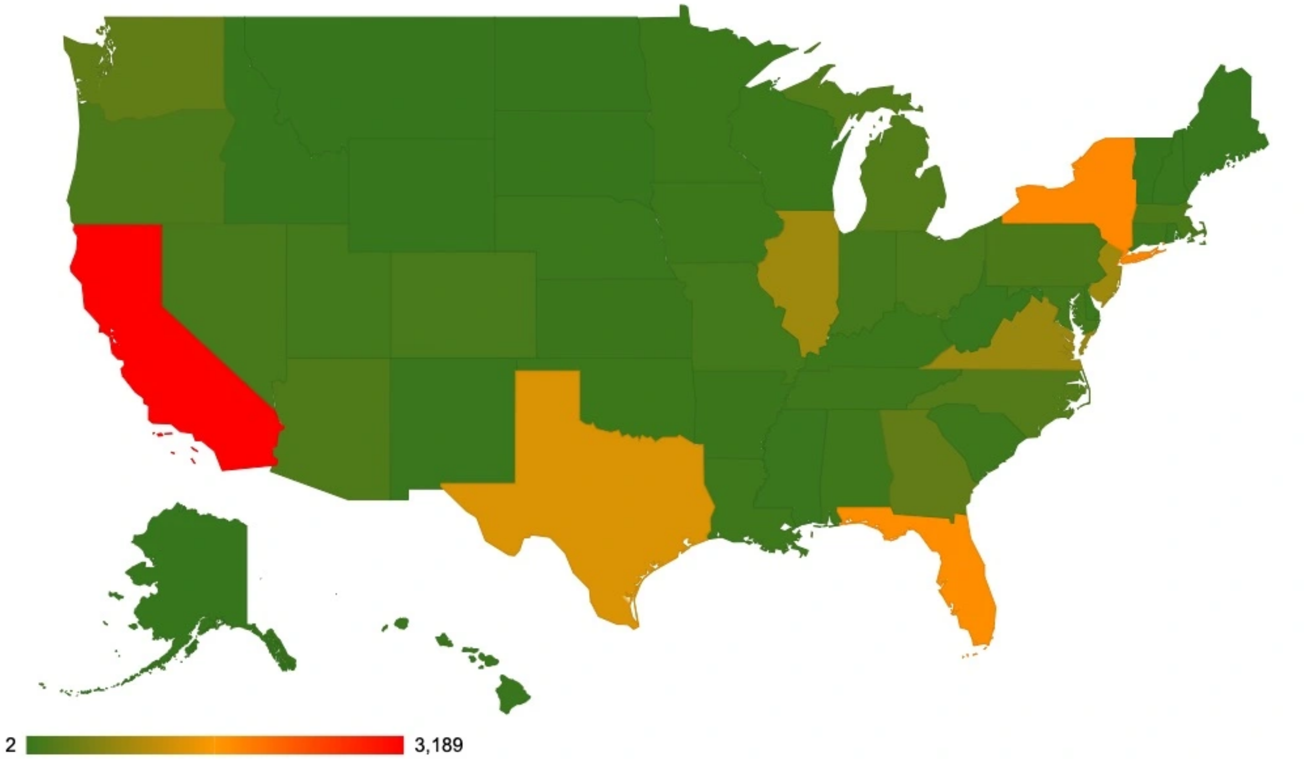


To make this clearer, below you can find the **top 20 countries** along with the amount of CardingMafia accounts based on geolocation data of the IP addresses recorded with each of the CardingMafia forum accounts.

1. USA (19393 accounts)
2. Germany (2553 accounts)
3. United Kingdom (2479 accounts)
4. Russia (1841 accounts)
5. China (1781 accounts)
6. France (1632 accounts)
7. Indonesia (1559 accounts)
8. Netherlands (1458 accounts)
9. Canada (1410 accounts)
10. Ghana (1384 accounts)
11. Australia (1138 accounts)
12. India (1042 accounts)

13. Ukraine (1016 accounts)
14. Nigeria (992 accounts)
15. Brazil (705 accounts)
16. Spain (663 accounts)
17. Japan (647 accounts)
18. Hong Kong (586 accounts)
19. Vietnam (572 accounts)
20. Singapore (560 accounts)

Since the United States is the top one in all of the above statistics (although it’s mainly due to the amount of cloud and proxy services based in the US), here is a similar geo-heatmap per US state.

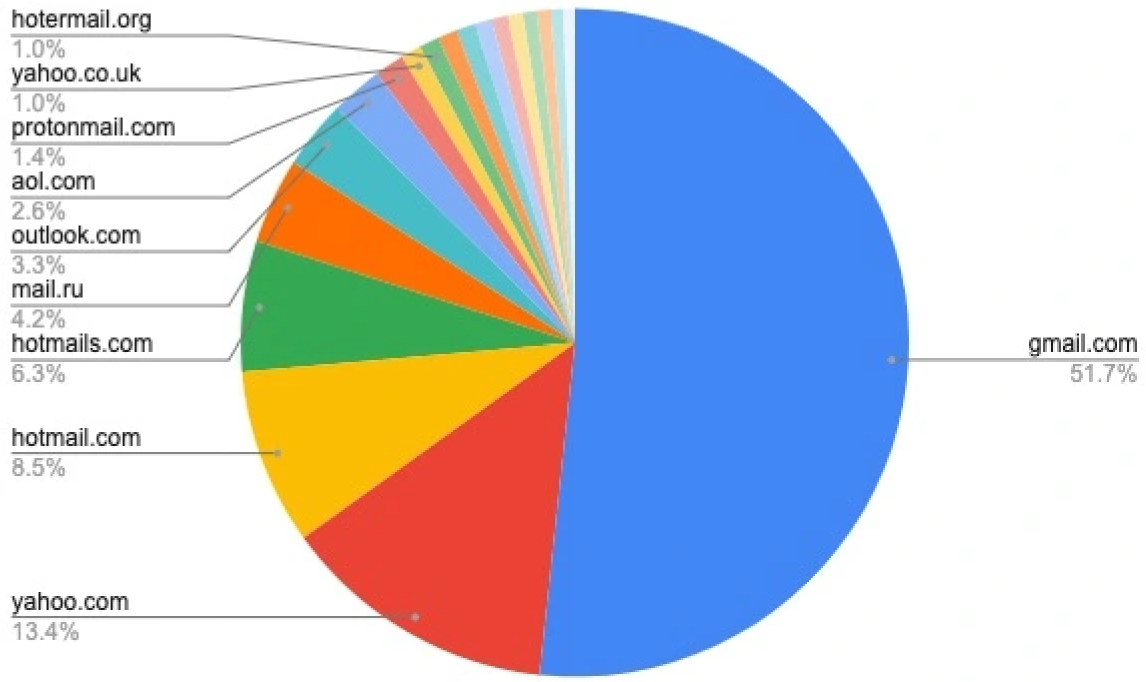


And the top 5 states with the highest amount of CardingMafia accounts created from IP addresses geolocated in there were the following:

1. California (3189 accounts)
2. New York (1771 accounts)
3. Florida (1721 accounts)
4. Texas (1302 accounts)
5. Illinois (823 accounts)

The email addresses used by the CardingMafia members also provide some interesting insights. For example, there were 294,887 unique email addresses. To avoid clutter, I picked the top 20 email service providers used for those accounts and you can see them here.

Unsurprisingly, GMail.com is the top one with 51.7%, followed by Yahoo.com (13.4%) and Hotmail.com (6.3%).



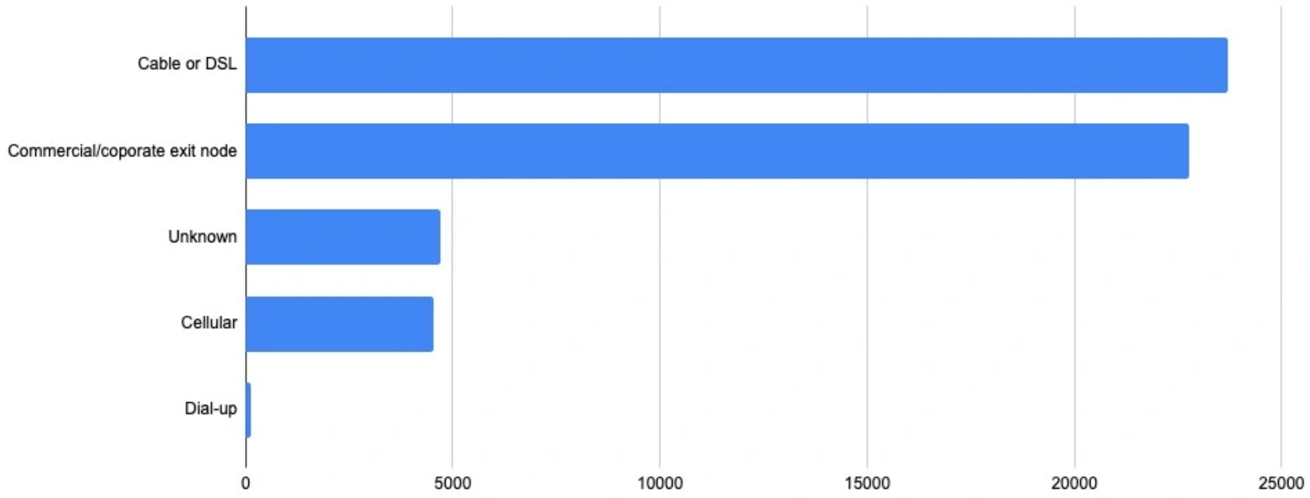
There is something else which is interesting though. There were some email addresses from corporate accounts which again, could be benign but it it could also be an insider threat. I will not list those here but it was everything from small businesses to large multi-national corporations across various industries.

Something else which is notable is that only a tiny percentage of the forum members were using privacy-focused email service providers. For example, using the top 5 list from CyberNews we have:

1. ProtonMail: 3155 accounts (1.07% of the total accounts)
2. Tutanota: 375 accounts (0.13% of the total accounts)
3. Zoho Mail: 60 accounts (0.02% of the total accounts)
4. Thexyz: 0 accounts
5. Startmail: 4 accounts (0.000014% of the total accounts)

I want to highlight this since we keep on hearing how cyber-criminals are very privacy-/anonymous-aware by many government officials, but the above is a clear indication that the vast majority (over 97%) of the members of a relatively large cyber-criminal forum were using unencrypted email providers.

The above is also supported by breaking down the type of connections used for the creation of each of those accounts. Based on the enriched IP addresses described earlier, here are the connectivity types.



Suggestions for threat intelligence production

I didn’t want this blog post to be just a selection of statistics for a carding forum, so here are some suggestions for turning this data breach into actionable intelligence. There are other use cases too in the more generic threat research space, but I tried to keep it limited to actionable threat intelligence suggestions.

> Check if any accounts where created with your domain name(s) as it could be benign (curious employees, threat researchers, etc.) but it could also be an insider threat.
>
> If you are an email service provider, use the dataset to find out which of your users have been using your services to host and/or access cyber-criminal content. Again, it could be benign (threat research, law enforcement, etc.) but it could also lead you to some real cyber-criminals.
>
> If you are a hosting provider, use the IP dataset to find out which of your customers have been using your services to host and/or access cyber-criminal content. Again, it could be benign (threat research, law enforcement, etc.) but it could also lead you to some real cyber-criminals.
>
> If you are a national CERT (or similar entity) use this dataset filtering on your ASNs and TLDs to better understand the threat landscape of your country and potentially even uncover some cyber-criminal activity.
>
> If you are working on de-anonymization or tracking of a cyber-criminal use this dataset for enrichment and pivot searching (e.g. emails, hashed passwords, IP addresses).
>
> Check if any accounts were created from your IP address ranges (there are some originating from corporate networks). That could be anything from a curious individual, to a threat researcher or even an insider threat.

> You can use the email addresses of the CardingMafia members to identify and profile high-risk individuals/customers you might have. For example, if you are a payments platform and you have CardingMafia members with accounts on your platform it might worth some proactive fraud investigation.

Written by xorl

April 23, 2021 at 18:17

Posted in threat intelligence

Leave a Reply

Fill in your details below or click an icon to log in:

You are commenting using your WordPress.com account. (Log Out / Change)

You are commenting using your Twitter account. (Log Out / Change)

You are commenting using your Facebook account. (Log Out / Change)

Cancel
Connecting to %s