ShinyHunters Selling Alleged AT&T Database with 70 million SSN and Date of birth; AT&T Denies it originated from their systems

blog.cyble.com/2021/08/19/shinyhunters-selling-alleged-att-database-with-70-million-ssn-and-date-of-birth/

August 20, 2021

It was not a long ago when we encountered a massive data breach at T-mobile, which affected millions of users' SSN, mobile numbers, driving licenses, etc. This time it seems to be different, and perhaps, more concerning.

The notorious cybercriminal group, ShinyHunters, claims to have gained access to the AT&T database, affecting over 70 Million users' SSNs and Dates of Birth.

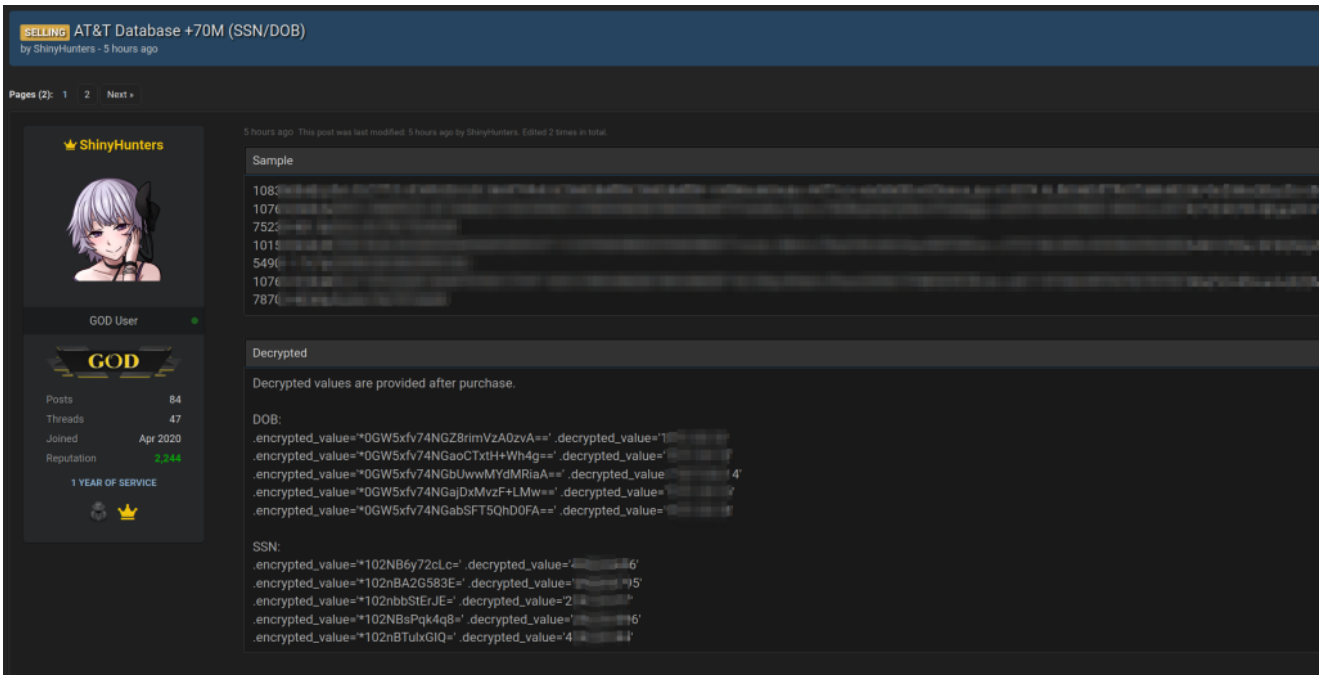
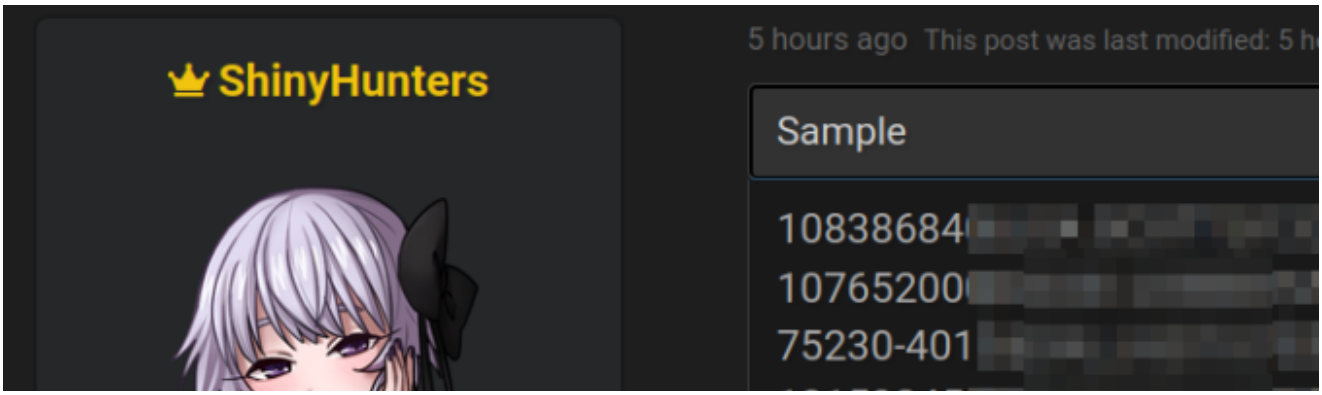


Figure 1: ShinyHunters Post for Selling AT&T database on RaidForums

The actor has put the database for an auction, as shown in the image below.



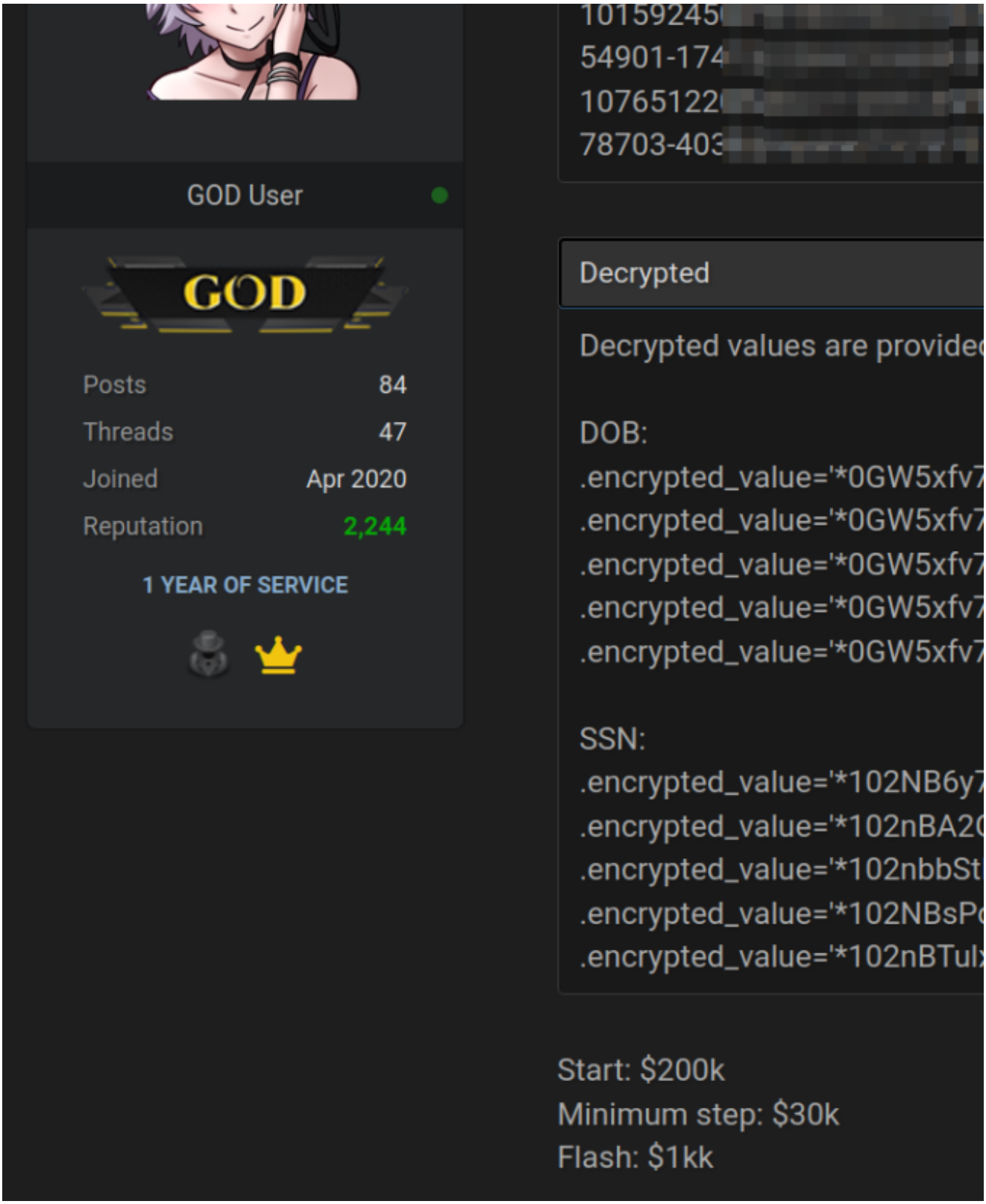
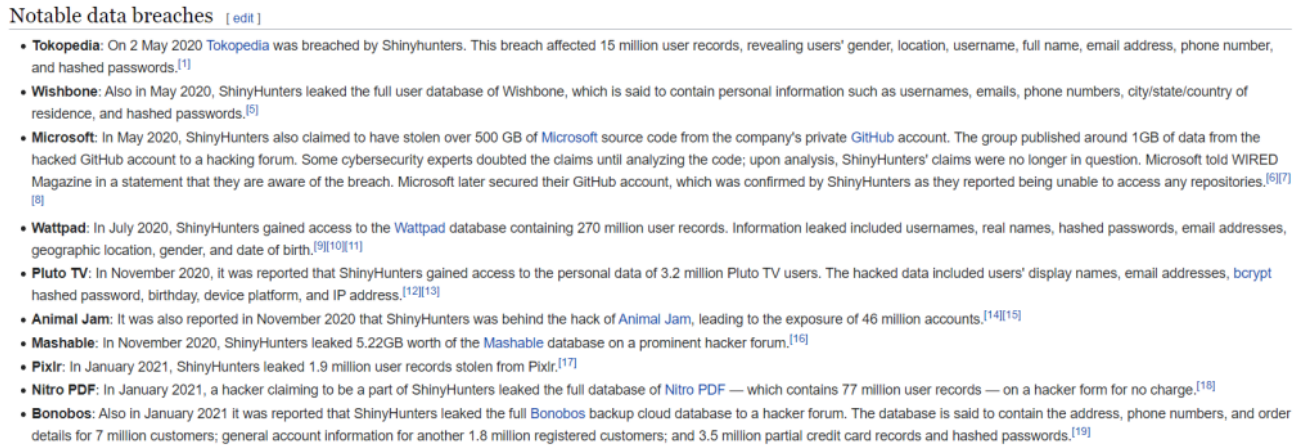


Figure 2: ShinyHunters group are willing to sell this for $1 Million as a flash sale

ShinyHunters Linked Data Breaches

Several high-profile breaches since 2020 are linked to this group directly. Some of them are below (source: Wikipedia):



Notable data breaches [edit]

- **Tokopedia**: On 2 May 2020 Tokopedia was breached by Shinyhunters. This breach affected 15 million user records, revealing users' gender, location, username, full name, email address, phone number, and hashed passwords.[1]
- **Wishbone**: Also in May 2020, ShinyHunters leaked the full user database of Wishbone, which is said to contain personal information such as usernames, emails, phone numbers, city/state/country of residence, and hashed passwords.[5]
- **Microsoft**: In May 2020, ShinyHunters also claimed to have stolen over 500 GB of Microsoft source code from the company's private GitHub account. The group published around 1GB of data from the hacked GitHub account to a hacking forum. Some cybersecurity experts doubted the claims until analyzing the code; upon analysis, ShinyHunters' claims were no longer in question. Microsoft told WIRED Magazine in a statement that they are aware of the breach. Microsoft later secured their GitHub account, which was confirmed by ShinyHunters as they reported being unable to access any repositories.[6][7][8]
- **Wattpad**: In July 2020, ShinyHunters gained access to the Wattpad database containing 270 million user records. Information leaked included usernames, real names, hashed passwords, email addresses, geographic location, gender, and date of birth.[9][10][11]
- **Pluto TV**: In November 2020, it was reported that ShinyHunters gained access to the personal data of 3.2 million Pluto TV users. The hacked data included users' display names, email addresses, bcrypt hashed password, birthday, device platform, and IP address.[12][13]
- **Animal Jam**: It was also reported in November 2020 that ShinyHunters was behind the hack of Animal Jam, leading to the exposure of 46 million accounts.[14][15]
- **Mashable**: In November 2020, ShinyHunters leaked 5.22GB worth of the Mashable database on a prominent hacker forum.[16]
- **Pixlr**: In January 2021, ShinyHunters leaked 1.9 million user records stolen from Pixlr.[17]
- **Nitro PDF**: In January 2021, a hacker claiming to be a part of ShinyHunters leaked the full database of Nitro PDF — which contains 77 million user records — on a hacker form for no charge.[18]
- **Bonobos**: Also in January 2021 it was reported that ShinyHunters leaked the full Bonobos backup cloud database to a hacker forum. The database is said to contain the address, phone numbers, and order details for 7 million customers; general account information for another 1.8 million registered customers; and 3.5 million partial credit card records and hashed passwords.[19]

Figure 3: ShinuHunters Group linked data breaches. Source – https://en.wikipedia.org/wiki/ShinyHunters

Other data breaches [edit]

The following are other hacks that have been credited to or allegedly done by ShinyHunters. The estimated impacts of user records affected are also given.[20][21][22]

- JusPay - 100 million user records[23]
- Zoosk - 30 million user records[24]
- Chatbooks -15 million user records[24]
- SocialShare - 6 million user records[24]
- Home Chef - 8 million user records[24]
- Minted - 5 million user records[24]
- Chronicle of Higher Education - 3 million user records[24]
- GuMim - 2 million user records[24]
- Mindful - 2 million user records[24]
- Bhinneka - 1.2 million user records[24]
- StarTribune - 1 million user records[24]
- Dave.com- 7.5 million users[25]
- Drizly.com - 2.4 million user records[26]
- Havenly - 1.3 million user records[26]
- Hurb.com - 20 million user records[27]
- Indabamusic - 475,000 user records[27]
- Ivoy.mx - 127,000 user records[27]
- Mathway - 25.8 million user records[27]
- Proctoru - 444,000 user records[26]
- Promo.com - 22 million user records[28]
- Rewards1- 3 million user records[27]
- Scentbird - 5.8 million user records[26]
- Swvl - 4 million user records[27]
- Glofox - Unknown[29]
- Truefire - 602,000 user records[26]
- Vakinha - 4.8 million user records[26]
- Appen.com - 5.8 million user records[26]
- Styleshare - 6 million user records[27]
- Bhinneka - 1.2 million user records[27]
- Unacademy - 22 million user records[30][31]
- In August 2020, ShinyHunters hacked Hack Forums with a defacement message, using a Pokemon image and music.[32]

Figure 4: ShinuHunters Group linked data breaches. Source – https://en.wikipedia.org/wiki/ShinyHunters

It should be noted that the group is being investigated by multiple law enforcement agencies worldwide, including the FBI.

Failed Extortion Attempt?

The research community has seen a change in its tactics in the last few months. The ShinyHuntes group extorts their victims and often shares their RaidForum profile and media press on the credibility of their claims. If a victim refuses to pay the extortion, the group puts them for sale on cybercrime forums.

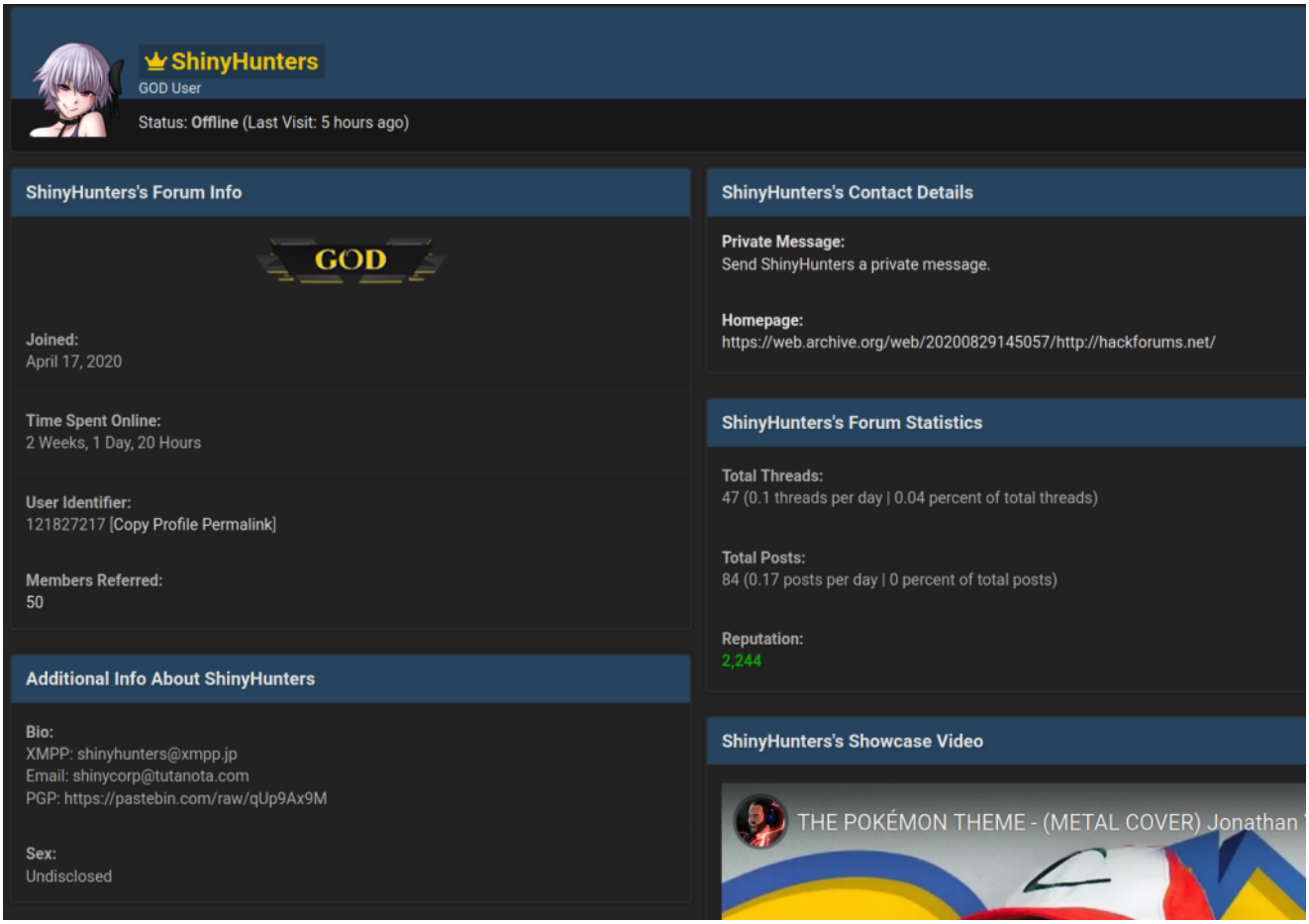


Figure 5: ShinyHunters Profile on RaidForums Website

Conclusion

The ShinyHunters group is a known and credible threat actor. The claims made by the group can not be discounted, given their history. On this issue, whether they were able to breach AT&T's infrastructure, found a misconfigured databases on the internet, or compromised the third party with AT&T information, time will tell us.

Update: "Based on our investigation today, the information that appeared in an internet chat room does not appear to have come from our systems." AT&T commented on the issue.

If the claims are genuine, this might be one of the most sensitive data breaches of 2021.

At the time of writing this blog, there are no known reports or disclosure by AT&T on this alleged data breach.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the suggestions given below:

- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and internet security software package on your connected devices.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Conduct regular backup practices and keep those backups offline or in a separate network.

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.