

APPENDIX



astoria company - 300m

No reviews, be the first!

Producer: **shinyhunters** - 5.0 

Price: **\$250000.0** | CAD 326550.0 | EUR 211175.0 | GBP 188175.0 | RUB 18856925.0 | AUD 343325.0 | NZD 371975.0

Third Stage of dumps!

Data Includes: Name, email, IP address, DOB, address, SSN - social security numbers (approximately 40m SSN), thousands of lead fields including driver information, vehicle VINs, auto accidents, medical history, income, property value, insurance information, family information, education, and much more.

contact: shinyhunters@xmpp.gg

Refund Policy

None

Figure 1 Dark0de listing by "shinyhunters" asked USD \$250,000.00 for Astoria Company - 300m

SELLING **SOLD!** [100m USA DB] Astoria Company (with SSN, Bank Accounts, DOB, IP)
 by seller13 - February 14, 2021 at 08:59 PM Thread Closed

February 14, 2021 at 08:59 PM. This post was last modified: February 19, 2021 at 04:28 AM by seller13. Edited 2 times in total. Edit Reason: Add new sample

SOLD!

100m USA database - Astoria Company

Greets to @[ShinyHunters](#) for the hack

Total Users: 100m U.S.
Fields (all): Name, Email address, date of birth, address, mobile, IP address for all users.
Fields (half of db): Social security numbers and checking account and routing numbers, drivers license number, vehicle VIN and much more.

Total size: 1TB

Sample Data (from one table - all tables are different)

Sample

Database Tables

Sample2 - Proof of Valid Data

Total Tables: 300+


Partial Table List and Record Count

Price: 3 BTC
 Serious buyers only.

Figure 2. "Seller13" listed Astoria data for sale for 3 BTC on Raid Forums on February 14. It would later be updated as "SOLD!" on February 19.

S SELLING: 100m U.S. consumers SSN, bank account, DOB, Mobile, IP

By Seller13, February 15 in [Spam] - mailings, databases, responses, mail-dumps, software

Seller13
byte
●

Paid registration
● 0
3 posts
Joined
02/15/21 (ID: 114099)
Activity
хакинг / hacking

Posted February 15 (edited)

Selling: [100m] USA database - Astoria Company

Greets to @ShinyHunters for the hack

Total Users: 100m U.S.

Fields: Name, Email address, date of birth, address, mobile, IP address for all users.
Also for most user: Social security numbers and checking account and routing numbers, drivers license number, vehicle v

Total size: 1TB

Sample Data (from one table - all tables are different)

Database Tables

Total Tables: 300+

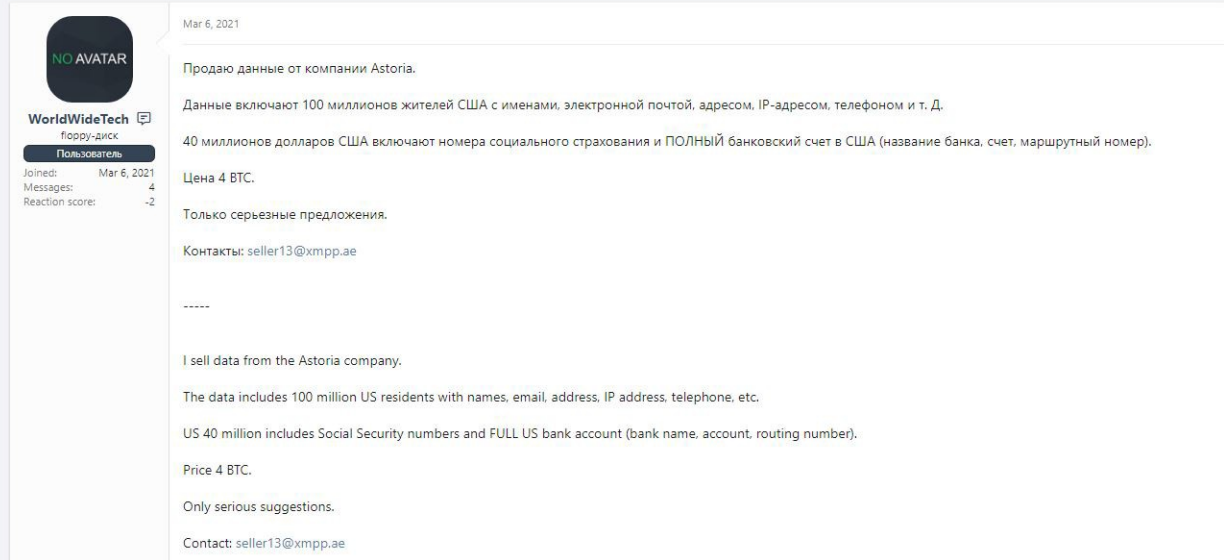
Partial list of DB tables:

- bol_client_transaction_details 58,821,656
- clientpp_detail 2,452
- clientpp_detail_backup_2018_11_01 1,226
- clientpp_detail_deleted 217
- clientpp_lead_detail 1,762,199
- clientpp_lead_ping_detail 509,401
- clientpp_lead_post_detail 21,240
- client_fixed_price 242,439
- client_insurance_company_mapping 25,569
- client_insurance_company_mapping_copy 16,286
- client_insurance_company_mapping_copy_2019 16,111
- client_vendor_setting 64,130
- client_zipcodes 64,833
- data_autoInsurance_OLD 550,092

Figure 3. "Seller13" listed Astoria data for sale for 5 BTC on Exploit.in on February 15. The contact Jabber provided was Seller13@xmpp.ae

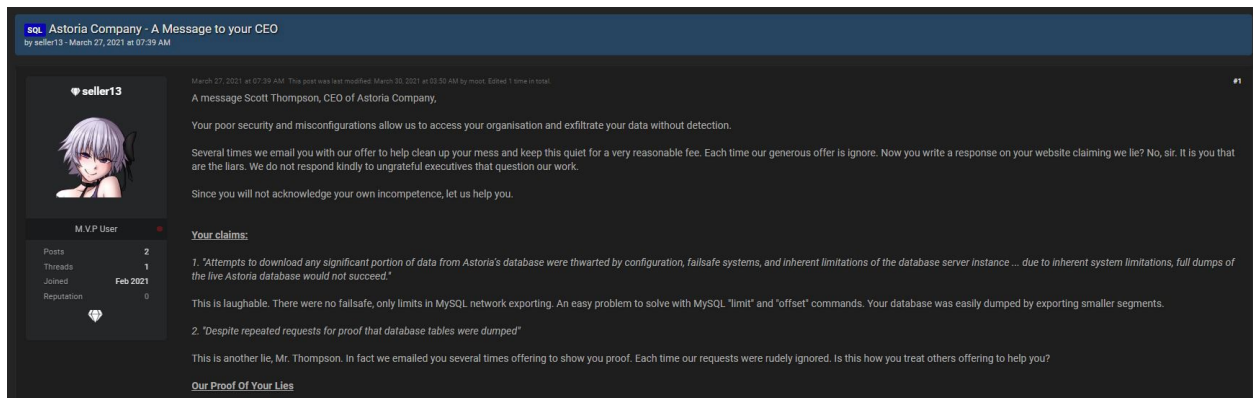
SELL: Astoria Company (U.S. Leads with SSN and Bank Account)

WorldWideTech · Mar 6, 2021



The screenshot shows a forum post by user 'WorldWideTech' (profile picture: NO AVATAR). The post is dated March 6, 2021. The user's profile information includes: 'Пользователь' (User), 'Joined: Mar 6, 2021', 'Messages: 4', and 'Reaction score: -2'. The post content is in Russian and English. The Russian text reads: 'Продаю данные от компании Astoria. Данные включают 100 миллионов жителей США с именами, электронной почтой, адресом, IP-адресом, телефоном и т. Д. 40 миллионов долларов США включают номера социального страхования и ПОЛНЫЙ банковский счет в США (название банка, счет, маршрутный номер). Цена 4 BTC. Только серьезные предложения. Контакты: seller13@xmpp.ae'. The English text reads: 'I sell data from the Astoria company. The data includes 100 million US residents with names, email, address, IP address, telephone, etc. US 40 million includes Social Security numbers and FULL US bank account (bank name, account, routing number). Price 4 BTC. Only serious suggestions. Contact: seller13@xmpp.ae'.

Figure 4. "World Wide Tech" listed Astoria data for sale on March 6 on XSS.is. The contact Jabber provided was Seller13@xmpp.ae



The screenshot shows a forum post by user 'seller13' (profile picture: anime girl) titled 'sql Astoria Company - A Message to your CEO'. The post is dated March 27, 2021, at 07:39 AM. The user's profile information includes: 'M.V.P User', 'Posts: 2', 'Threads: 1', 'Joined: Feb 2021', and 'Reputation: 0'. The post content is in English and reads: 'A message Scott Thompson, CEO of Astoria Company, Your poor security and misconfigurations allow us to access your organisation and exfiltrate your data without detection. Several times we email you with our offer to help clean up your mess and keep this quiet for a very reasonable fee. Each time our generous offer is ignore. Now you write a response on your website claiming we lie? No, sir. It is you that are the liars. We do not respond kindly to ungrateful executives that question our work. Since you will not acknowledge your own incompetence, let us help you. Your claims: 1. "Attempts to download any significant portion of data from Astoria's database were thwarted by configuration, failsafe systems, and inherent limitations of the database server instance ... due to inherent system limitations, full dumps of the live Astoria database would not succeed." This is laughable. There were no failsafe, only limits in MySQL network exporting. An easy problem to solve with MySQL "limit" and "offset" commands. Your database was easily dumped by exporting smaller segments. 2. "Despite repeated requests for proof that database tables were dumped" This is another lie, Mr. Thompson. In fact we emailed you several times offering to show you proof. Each time our requests were rudely ignored. Is this how you treat others offering to help you? Our Proof Of Your Lies'.

Figure 5. "Seller13" sends a message to Astoria's CEO, claiming that they exfiltrated the data via SQL commands. Partial image.

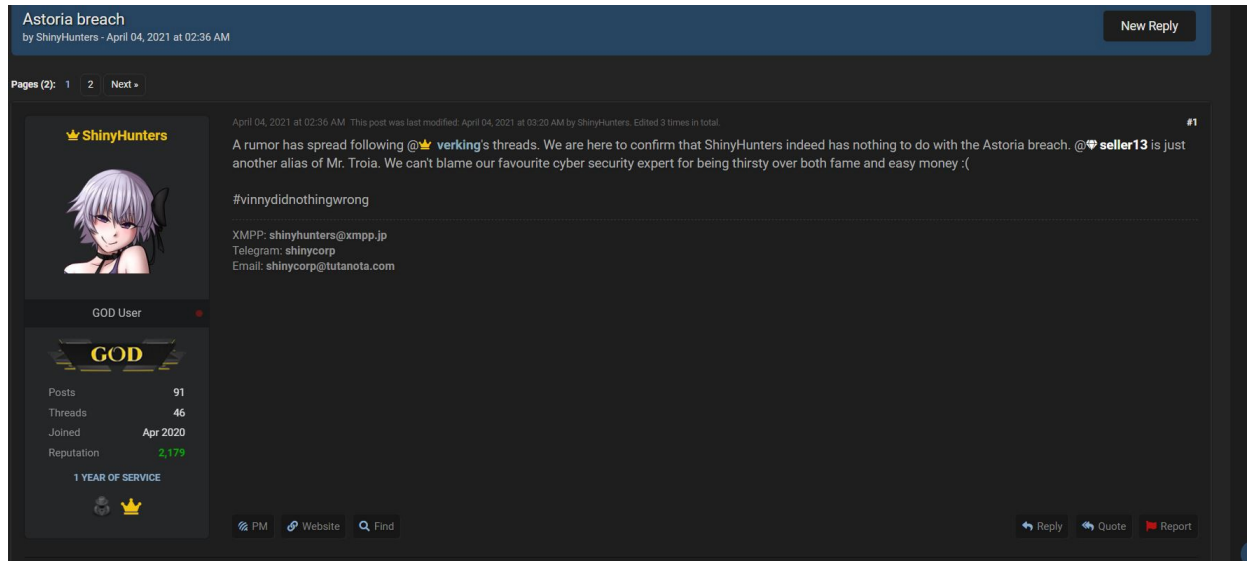


Figure 6. ShinyHunters denies involvement in Astoria incident and claims that Seller13 is really Troia.

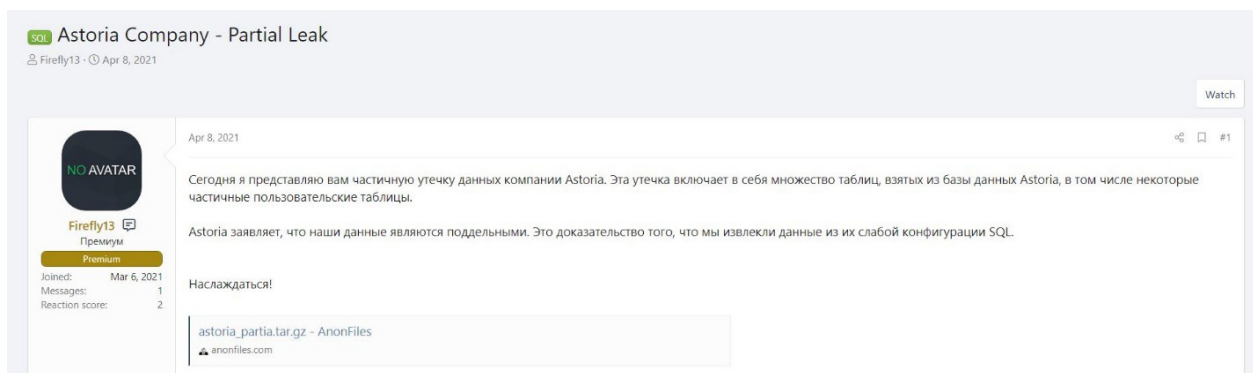


Figure 7. "Firefly13" offers some of the Astoria data for free on XSS.is. Russian version.

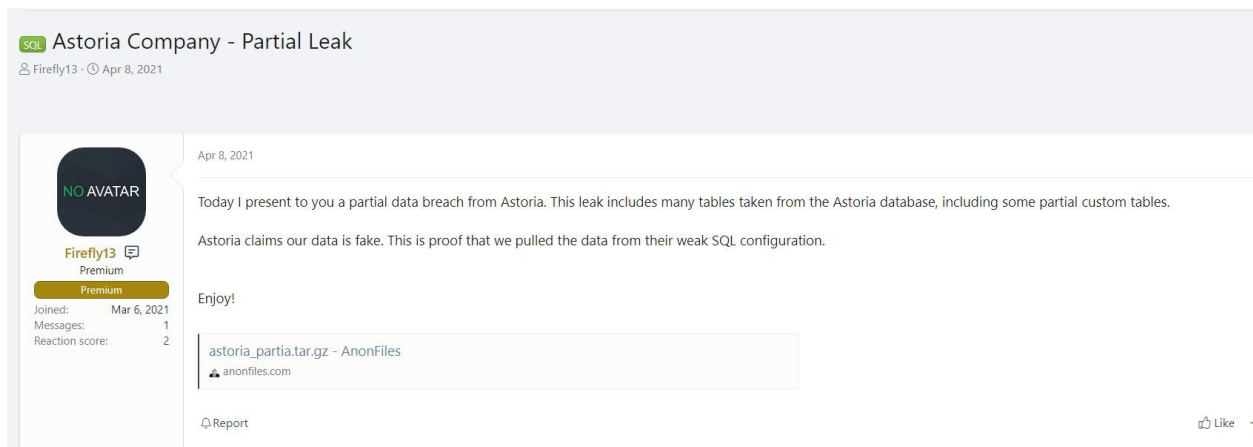


Figure 8 "Firefly13" offers some of the Astoria d