WHAT HAPPENED?

That is a Great Question…

ABSTRACT

Months after NightLion Security reported what they claim was a massive breach involving Astoria Company data, the two firms are still disputing the scope of the breach. As lawyers exchange letters, DataBreaches.net looks at some of the claims and controversy.

DataBreaches.net

WHAT HAPPENED??

NIGHTLION SECURITY REPORTS A MASSIVE BREACH THAT ASTORIA COMPANY DISPUTES

INTRODUCTION

Astoria Company LLC is an American lead generation and performance marketing firm. On January 29, they were contacted by Vinny Troia of **NightLion Security**, who informed them that their data appeared to be up for sale on a dark web market.

But was the data really their data? Astoria claimed that only a little data was theirs. NightLion claimed that there were massive amounts of data from their server and that consumers should be notified.

In this report, DataBreaches.net reviews the chronology of events and claims by both NightLion and Astoria. Those hoping for an absolute declaration at the end of the report stating who was right will be disappointed because this is still an open dispute under investigation.

IN THE BEGINNING…

On January 29, Vinny Troia reached out to Astoria to alert them that there was a listing on a dark web market for what was advertised as their data. That listing on Dark0de, by a user claiming to be "ShinyHunters," sought $250,000 for what was listed as Astoria -- 300m.[1] But the seller was not the real "ShinyHunters," and the real "ShinyHunters" soon contacted the administrator of Dark0de, had the listing removed, and had the impostor banned.

Two weeks later, two more listings for the alleged Astoria dump appeared. The first was on Raid Forums on February 14. The second was on Exploit.in on February 15. The listings, both by "Seller13," were almost identical except that the Raid Forums listing was priced at 3 BTC while the Exploit.in listing was priced at 5 BTC. Both listings offered "greets to ShinyHunters for the hack[2]." Was "Seller13" showing respect to ShinyHunters because they believed ShinyHunters had committed the hack or were they just trolling or trying to frame ShinyHunters? Given that they later claimed to be the hackers, and given

[1] A copy of the Dark0de listing can be found in the Appendix to this report as Fig. 1.
[2] See Figs. 2 and 3 in the Appendix.

some evidence presented on DarkOwl blog indicating that Seller13 might be just a scammer, DataBreaches.net was surprised to read that based on what Seller13 told him, Troia suspected that Seller13 and ShinyHunters were working together. More recently, in an email to DataBreaches.net, Troia noted that he was confident that Seller13 and ShinyHunters were working together. His claim is not only surprising for its reliance on what appears to be an unreliable source, but it is inconsistent with a chat he had with ShinyHunters in which he told Shiny that he did not believe Shiny was involved in Astoria. At the time, Shiny claimed that since Shiny was not responsible for Astoria, "Seller13" had to be either Troia himself or "DonJuji," someone who has worked for Troia and who has a history of hacking. Shiny subsequently revised their opinion to accuse Troia of being Seller13.

In any event, "Seller13" allegedly gave Troia details of how they were able to attack and exfiltrate massive amounts of data from Astoria. Troia's report, published on March 22, noted:

> *Night Lion's counterintelligence team contacted Seller13, who freely volunteered information on how they were able to access Astoria's database.*

Why would a criminal who wants to sell a data set for $250,000 give the data away? And why would a criminal just helpfully confess to Troia -- someone who has a history of claiming how he gives information to the FBI -- how they gained access and exfiltrated data?

On February 19, "Seller13" updated the Raid Forums listing of Astoria data to mark it "SOLD!" There is no confirmation of any sale and there does not appear to have been any middleman involvedwho might have confirmed any transaction.

On March 6, two new users registered on the Russian-language XSS.is forum: "Firefly13" and "World Wide Tech." The latter listed Astoria data for sale for 4 BTC, with contact information for the seller being Seller13's jabber account.[3] Firefly13 also registered that day but remained silent until weeks later.

On March 22, NightLion published their report: Astoria Company Data Breach Research and Analysis.

For its part, Astoria posted a statement on their web site providing their version of the incident and their preliminary findings. Of special note, their analysis suggested that two parties may have been involved, who they identified as "User A" and "User B:"

> *Two potential rogue actors were involved in the intrusion: User A, who Visited the site from Eastern-US IP Address and was subsequently traced to VPN servers located in*

[3] See Fig. 4 in the Appendix

Europe, and who we believe to be a cyber-criminal or hacker; and User B, who visited thesite and browsed the database from a collection of three Central-US IP Addresses.

If Seller13 told Troia how they were able to access the data, then are they "User A" in Astoria's report?

Importantly, Astoria denied Troia's claims about the extent of any breach, claiming that their security measures had defeated repeated attempts to exfiltrate data. A nonpublic report by external consultants in February provided more details about their findings but was provided to DataBreaches.net with the understanding that it would not be quoted or republished online. Astoria had agreed with Troia about an adminer vulnerability that had existed. That vulnerability presumably enabled an attacker to eventually get database credentials. But Astoria and Troia disagreed about whether the login credentials to adminer.php had been stored server-side or not.

So, Troia was claiming that there was a massive breach of Astoria's data, and Astoria was claiming that there was no massive breach.

Jumping into the fray on March 27, "Seller13" posted again on Raid Forums, this time posting "Astoria Company -- A Message to Your CEO." The message claimed that Seller13 had emailed Astoria several times, offering to help them clean up their mess for a fee, but their emails had been ignored. They also claimed that it was easy to circumvent Astoria's security measures by exfiltrating data in chunks of rows[4]. Astoria has never publicly commented as to whether they received any such emails from Seller13 or not.

In an updated statement of March 29, Astoria continued to insist that while some small amount of data appeared to have been exfiltrated, there was no evidence provided to them supporting any claim of a massive breach. When asked by DataBreaches.net what they found when they investigated samples of data sent to them, Astoria claimed that some samples could not be imported, some samples showed that certain data was not stored (because fields were NULLED out), and that some of the records in the samples provided to them absolutely did not match anyone in their records at all. At one point, Astoria informed DataBreaches.net that 8 out of 8 records failed to produce any hits or matches with their database, and the table sizes in the alleged dump were significantly larger than Astoria's actual tables.

On March 29, after Astoria updated their response to Troia's claims, DataBreaches.net received an email purportedly from Seller13:

> Subject: Proof of Astoria Company hack
> From: "Seller13" <leakseller1-3@pm.me>
> Date: Mon, March 29, 2021 16:53
> To: "leakseller1-3@pm.me" <leakseller1-3@pm.me>

[4] See Fig. 5 in the Appendix

> To All reporters -
>
> We are providing evidence of our hack on Astoria Company.
>
> Astoria MUST take responsibility for the data breach!
>
> Astoria claims no data was stolen. We will show the truth. Here is a sample of 50,000 records from each of the primary data tables.
>
> https://mega.nz/file/v8piUJYY#k-NgBua2oQfSUYOnxzEbFcXLK7fNXzy-EO3fQUzS3Nw

[The url in the above link no longer works]

Seller13 would send DataBreaches.net additional data a few days later.

By the end of March, both Troia and Astoria had involved lawyers. But as the lawyers did their thing, other developments continued to play out in public.

On April 4, the real (well-known) ShinyHunters posted a message on Raid Forums[5]:

> *A rumor has spread following @verking's threads. We are here to confirm thatShinyHunters indeed has nothing to do with the Astoria breach. @seller13 is just another alias of Mr. Troia. We can't blame our favourite cyber securityexpert for being thirsty over both fame and easy money :(*

ShinyHunter's accusation that Seller13 was really Troia was followed by a post by user "Pred" who offered no hard proof that Troia was Seller13, but outlined what they claimed was Troia's pattern and practice so that he could obtain stolen data while appearing to have obtained it legally. While such claims resonate with Troia's detractors, there is no hard proof to support the claims. Chat logs just do not prove anything as they can easily be altered.

Unsurprisingly, Troia has denied these accusations, but he has a long history of both using "alts" and also denying using specific "alts" that may appear to be linked to him. DataBreaches.net has mentioned this in a previous report critiquing his book and attributions concerning threat actors.

[5] See Fig. 6 in Appendix

On April 8, Firefly13 sprang into action on XSS.is. In posts in both Russian and English, Firefly13 offered partial data from Astoria for free. In those posts, Firefly13 makes it clear that they are affiliated with, or are, Seller13[6].

Less than one hour after Firefly13 posted their offer, "World Wide Tech," who had registered on the same day as FireFly13 (March 6) and had previously posted Astoria data for sale, responded to Firefly13: "You sell full data set?" There was no answer.

Also on April 8, Seller13 emailed DataBreaches.net with more data to support their claims about the breach.

Neither Seller13, Firefly13, nor World Wide Tech have been spotted online in these forums since or about April 9.

SO, *ARE* THE DATA REAL?

As noted previously, Astoria claims that while some data is real, much of the data that allegedly had come from their servers did not come from their servers.

Because DataBreaches.net had asked Troia for more information on the medical/health-related data in the dump, Troia had provided this site with a list of the data fields in a health insurance table, and then with what he described as a randomly compiled sample of more than 100 individuals' data. The fields perfectly matched the fields DataBreaches.net would later obtain from sample data posted by Seller13.

Using the data Troia provided to this site, DataBreaches.net provided Astoria with information on three of the individuals in the sample and asked them to verify whether those individuals were anywhere in their records. Astoria reported that not one of the individuals was in any of their databases.

Was Astoria lying in denying that the data are real, were they just mistaken, or was Troia lying, or was Troia just misled and believed he had Astoria's data when he did not have real data? What was really going on here?

Troia included a lot of data and analyses in his March 22 report. Partly in response to Astoria's repeated denials that the data theirs, Troia pointed DataBreaches.net to the e-mails in the data dump that he claims contain valid emails and still-working credentials for Astoria clients. In an email to DataBreaches.net, he wrote:

> *……it should be obvious that the data could ONLY have come from Astoria . For example, there are multiple sections where Astoria 's partner logins and API logins are listed out*

[6] See Fig. 7 and 8 in the Appendix

In plain text (logins/passwords). -- and yes, the few I tested are all valid.

Also, the emails generated to astoria partners (directing them to admin.astoriacompany.com) also contain plaintext credentials. Those have already been reset, but trying to log in as them, you can see that the username exists... so the data is real.

Troia also points to SSN and banking information in the data. Astoria had observed that the SSN and bank account fields in the sample sent to them were NULLed on all rows. The fact that most of those data entries were NULLed is consistent with what one would expect of Astoria's database, as Astoria claims that they do not retain SSN or other sensitive personally identifiable information past the time it would be required for the transaction. In this case, the absence of data almost appears to be evidence that the records did come from Astoria. But other data also suggests that.

In data that had not been sent to Astoria by that point, there were reportedly non-NULLed SSN and bank account details of individuals. Troia informed DataBreaches.net that he had contacted several banks to provide them with data that he claims is from their customers. Troia claims that when he submitted some of the banking data to banks, several banks confirmed to him that the data are valid. None of the banks seem to have put that confirmation in writing, though, and one bank reportedly refused his offer to provide them with what appeared to be their customers' bank account data. Troia provided this site with a copy of the email he received:

> From: "Kearn, Michael L"
> Date: Tuesday, April 13, 2021 at 12:45 PM
> To: Vinny Troia
> Subject: RE: US Bank customer exposure - IMPORTANT
>
> Good afternoon Vinny,
>
> At this time, we respectfully decline your offer.
>
> -Mike
>
> Mike Kearn CISSP, NSA-IAM
> Director, Threat Informed Defense
> U.S. Bank Information Security Services

Neither U.S. Bank nor Kearn responded to an inquiry from DataBreaches.net as to why they refused to look at data that might indicate that numerous customers had their bank account information leaked or compromised.

To this site's knowledge and to date, no organization or agency has publicly confirmed Troia's claims that the data are real and from Astoria. Troy Hunt, who had uploaded the dataset Troia provided to him to HaveIBeenPwned, subsequently backed off and re-coded the incident as "Unconfirmed" after Astoria reported that people who contacted them based on notifications from HIBP were not even in their database.

To date, the only party to back Troia's claims appears to be Seller13.

So, there is still a dispute as to whether the data are real/valid or not, although there does seem to be a lot of data that look like they come from Astoria, including logs of clients requesting refunds for certain leads, etc.

One crucial part of Astoria's denial is that their http server access logs support their statement that there were multiple failed attempts to exfiltrate data. But those logs are not conclusive proof that no exfiltration occurred. Both Troia and others point out that http access logs would not necessarily reveal attackers exporting data. "DonJuji," for one, tells DataBreaches.net that http access logs may not reveal data dumping. It depends on what kind of shell access a threat actor uses, he explained. But anyone who knows how MySQL works, he said, could circumvent any limitation on the amount of data or number of rows that can be downloaded at one time. Speaking theoretically, DonJuji explained:

> *They could make a batch script that would automate the dumping in chunked queries. Almost all Linux servers come deployed with a native command line MySQL tool that would permit the threat actor to use the native dump binary.*

His statement seems consistent with Seller13's open letter to Astoria's CEO, where Seller13 talks about circumventing download limits using MySQL commands. DonJuji has not examined Astoria's logs and wanted to be clear that his answers were in theory, but based on his statements, it appears that there may have been a way to bypass Astoria's protections, and that examination of .bash_history logs might be informative. DataBreaches.net asked Astoria if they had checked .bash_history logs but did not receive a direct reply to that question[7].

For his part, Troia informs DataBreaches.net that he has contacted the Federal Trade Commission as well as the state attorneys general of Missouri, California, and Virginia to alert them to the breach and to ask them to investigate.

[7] Astoria declined to answer several questions at this time, in part, they claim, because Troia was not honoring confidentiality and NDA and was sharing their lawyer's correspondence. DataBreaches.net hopes to get more answers from them in the future.

WHERE DID TROIA GET THE FULL DATA SET?

While some might argue that the most important part of the story is whether the data are real and whether consumers need to be notified, there is another important aspect to this story -- all the drama and accusations that surround Troia and questions about his conduct.

That Troia would aggressively insist that the data are real and refuse to retract or remove his post raises the question: how can he be so sure the data are real? Where did he get them from? Did he get them from the fake "ShinyHunters" on Dark0de? Did he get them from Seller13 on Raid Forums or another forum? How trustworthy/reliable is his source? Surely Troia must believe that the data are real if he filed complaints with regulators to try to force Astoria to notify people. But how and where did Troia get the data?

It is a simple question, but Troia has provided different answers at different times. On March 26, after DataBreaches.net began looking into the controversy, Troia informed DataBreaches.net that "It was given to me by someone. I will not reveal sources." At that point, and based solely on Astoria's first report, DataBreaches.net hypothesized that he was referring to "User A," who Astoria believed to be the hacker.

It turned out that my hypothesis was not correct.

Weeks later, Troia revised his answer, telling DataBreaches.net that he had not actually been *given* the data, but rather, he had obtained the data set when a user on a private Telegram channel posted a link to it. He did not pay for the data, he said, naming the channel and the user, with the understanding that DataBreaches.net would not name the channel in this report.

When DataBreaches.net asked for proof of his claim that the data set had been linked from that channel, Troia provided DataBreaches.net with what he described as a chat log of a lengthy conversation that shows that the data were shared by someone on the Telegram channel. Troia indicated that he was not even involved in the chat log screencap he was sending me -- he was just in the channel and clicked on the link to data provided by someone calling themself "seller." When he was asked when the chat took place, Troia had replied that he could not remember, but it would have been in January. His attempts to scroll back through the channel to locate the date exactly had failed, he claimed, saying that it appeared the logs prior to April 13 had been wiped.

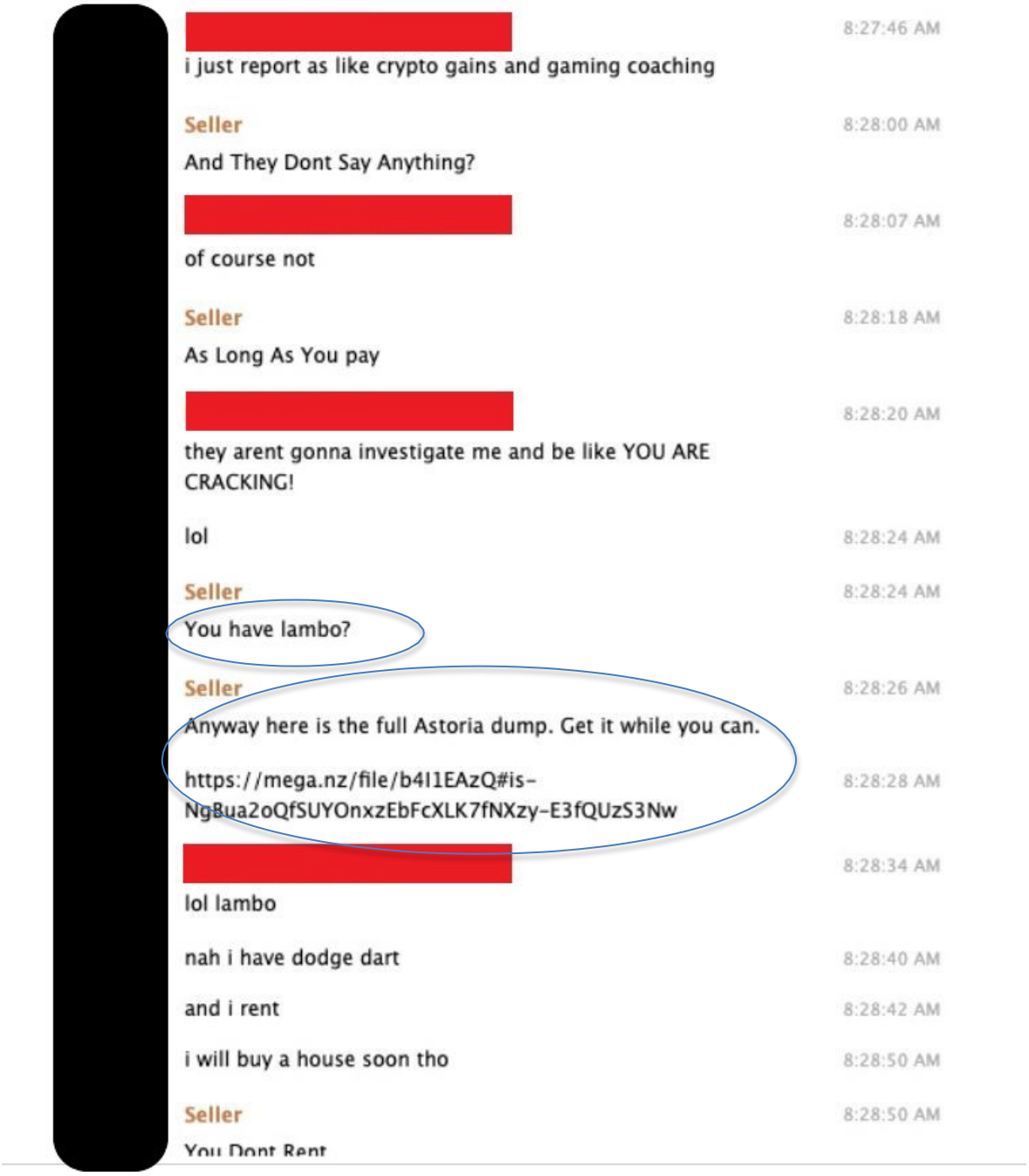


Figure 9. Screencap provided by Troia to DataBreaches.net that was alleged to show January chat in which "Seller" offered the full dump of Astoria data to channel members for free. Redacted by DataBreaches.net.

ATTEMPTING TO VERIFY TROIA'S CLAIMS

1. At DataBreaches.net's request, the administrator for the Telegram channel gave DataBreaches.net admin privileges on the channel and exported the entire chat history immediately. The details of Troia's screencap had neither been shown to, nor described to, the admin prior to exporting data and running searches. The first search run, for "lambo" returned:

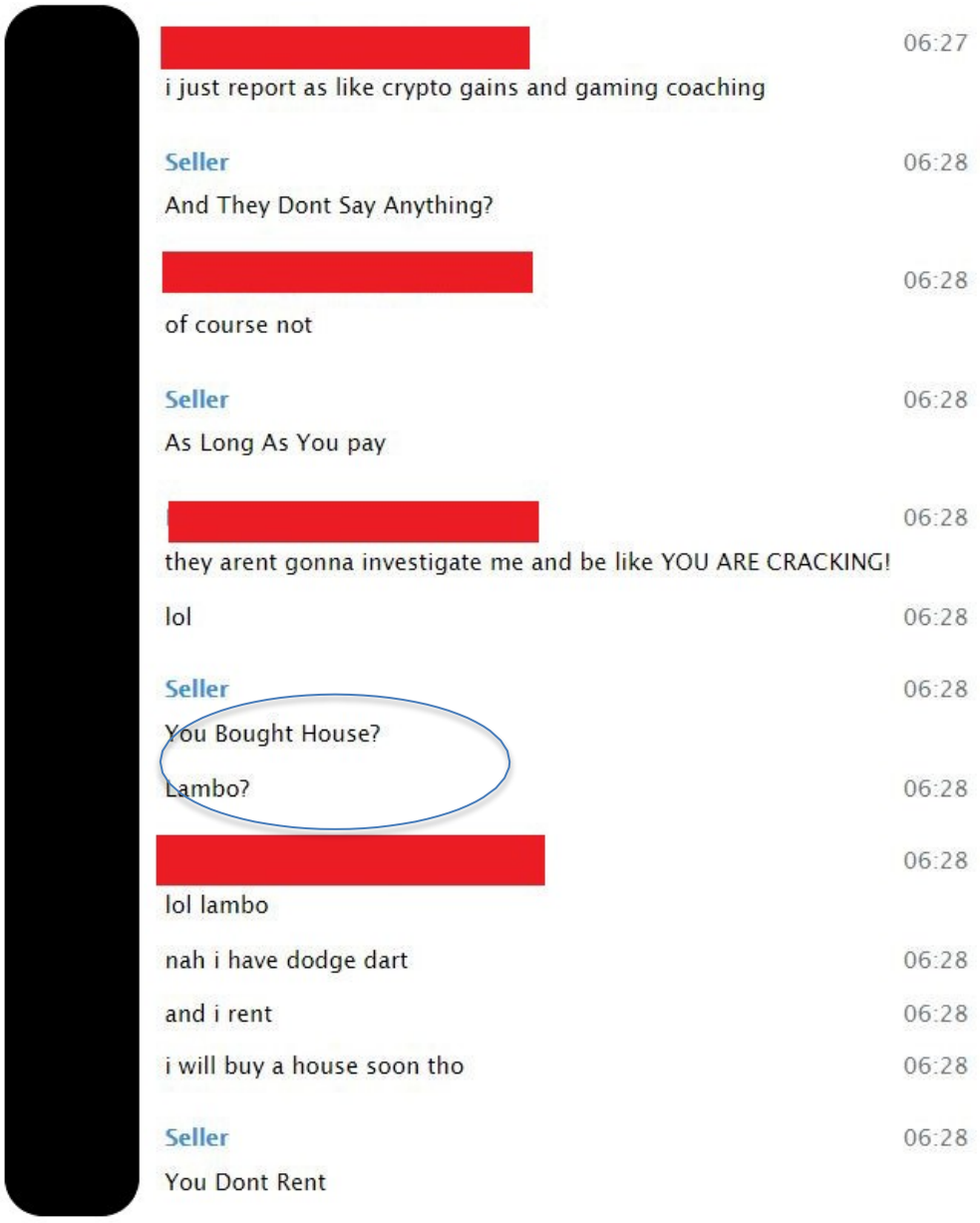
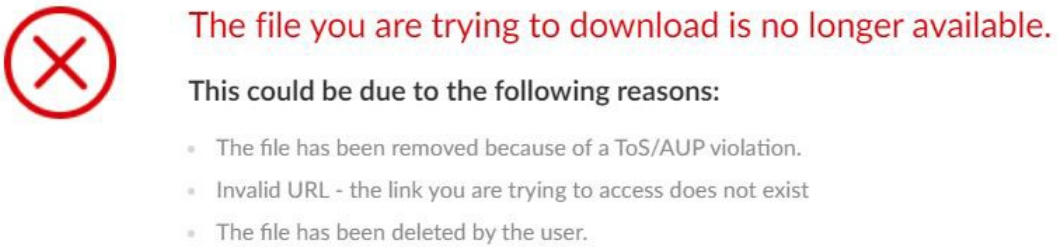


Figure 10. A search of administrator logs for "lambo" returned these results. No mention of Astoria or a link was in the log and there were two other lines that differed from what Troia provided. Redacted by DataBreaches.net.

2. Comparison of the screencaps suggests that material was added to the screencap provided by Troia (or, as Troia would later claim, material was deleted by the administrator from the administrator logs). In addition to the glaring discrepancy where "seller" appears to offer the entire Astoria dump at one specific Mega.nz url in Troia's screencap but not in the dumped logs, the Troia screencap appears to have edited two "You Bought House? Lambo?" lines to make it just one "You have lambo?" line .

3. Troia had informed DataBreaches.net that he had obtained the data set from that link in January. A check of the admin logs indicated that that screen cap with the "lambo" conversation took place on March 24 or March 25 (depending on your time zone). But Troia had published his report on March 22, so he could not possibly have first obtained the data from "Seller" or that Mega.nz link on March 24 or March 25. Troia's claims were not holding up, but there was more to check and other possible explanations[8].

4. As part of the verification process, DataBreaches.net attempted to test the Mega.nz link. Unsurprisingly it returned one of Mega's famous "no longer available" messages.



Although it is often the case that a file has been removed for violating ToS, it is also possible that a link never worked at all. DataBreaches.net decided to inquire about the link.

5. DataBreaches.net contacted Mega.nz with the url in Troia's screencap and asked them if they could provide any indication of file size that had been at that link. Mega.nz's Chief Compliance Office responded that the link this site submitted to them had never been a valid link. He commented that there had been a similar link to what this site had submitted, so maybe there had been a transcription error in what this site had sent them. DataBreaches.net doublechecked the submission and confirmed that it matched what had was in the screencap Troia provided.

At DataBreaches.net's request, Troia subsequently provided a text copy of the url in his screencap. It exactly matched the same url that DataBreaches.net had submitted to Mega and that Mega confirmed was never a working link.

[8] In response to an inquiry from this site, Troia claimed he did not know whether "Seller" was the same individual as "Seller13." In subsequent correspondence, he made it sound like they might be one and the same.

By then it appeared that Troia had given this site a screencap of a link that had never worked and a chat that, according to the administrator logs, never took place, in part, and the part that did take place occurred months after Troia claimed it took place.

DataBreaches.net contacted Troia to give him an opportunity to comment on this site's findings before we published them. With respect to the link to nowhere and a screencap that appeared doctored, Troia wrote:

> *You are making assumptions that this was the only link posted. I showed you alink specific to [name of channel -- redacted].*

I had not asked him for just any link posted on that channel. I asked him where he got the full data set. He had sent me a screencap and had claimed it showed the link he used to obtain the full dump. So, after claiming he got it from that link in January, he now tried to claim that I was making assumptions that this was the only link posted?

I confronted him about his shifting stories and dishonesty. He replied, in part:

> *As I have told you on the phone, I am under no obligation to reveal deep sources of information to you.*

He is right in one respect: he is under no obligation to reveal sources to me. That is what "no comment" is for. Rather than saying "No comment," he chose to respond dishonestly. He would later complain that I was twisting things to fit a narrative and that he had not thought he had to wordsmith his answers to me.

Troia also responded to this site's findings about the Mega.nz link. Over a series of emails, his response shifted somewhat from insisting that the link worked to acknowledging the problem. In his most recent communication about the Mega link, he wrote, in part:

> *Everything you are saying about the telegram channel and the link date is accurate. My attorney asked me to find a copy of the link. I went back to the channel and searched Astoria . Just in case there was a transcription error with the screenshot, I am attaching the plain text version:*
>
> *https://mega.nz/file/b4I1EAzQ# is-NgBua2oQfSUYOnxzEbFcXLK7fNXzy-E3fQUzS3Nw .*

> *I took a screenshot myself, it is the same screen shot I sent to my attorney a month ago, and I can confirm it has not been altered. I cannot confirm that the link was not edited after it was posted. As I mentioned in my prior email, I tested it again on April 9, that it was valid and working.*

Except that the link in his April 9 screencap could not have worked for him that day as it never worked. But DataBreaches.net does have an explanation, of sorts:

Earlier in this article, there is a text copy of an email sent to me and presumably other journalists on March 29 by Seller13. That is the same Mega.nz url as what Troia sent me, with one character difference: Seller13's url has one more character. I can now understand why Mega's Chief Compliance Office referred to the existence of a "similar" url and thought there might have been a transcription error.

But that emailed March 29th link from Seller13 was not to the full data set. That link, which did work, because I used it to obtain the data sample, was just to a sample of data in an archive called media_sample.tar that was 82.6 MB compressed. So "Seller" almost certainly would not have posted that link on the Telegram channel and claimed that it was a link to the full data set.

Troia also responded to the issue of administrator logs not supporting his claims, Troia insists that the administrator, someone with whom he has had frequent issues, had deleted all references to Astoria to cleanse the channel to remove any evidence of involvement in the Astoria breach.

DataBreaches.net put the question of retroactive purging of messages and logs to Telegram:

> *My question is whether administrator logs for a Telegram channel can be edited retroactively (e.g., months later) to leave no trace of a message that had been posted? I know admins can delete messages, but can they delete them from months earlier and leave no trace of the original message or any deletion of it?*

Telegram's reply appears below:

> *Channel admins can delete any message at any point in time, regardless of how long ago it was posted.*
>
> *The Recent Actions log will list the message for 48 hours and note that it was deleted. The Recent Actions log cannot be modified. Only channel admins can see the Recent Actions log.*
>
> *Once the 48 hours have passed, there will be no record of the post left in the logor on the channel.*

UPDATED – May 23: *Since this report was originally posted, it was suggested to me that I misunderstood Telegram's reply. I therefore removed my conclusions about whether logs could have been doctored, and I reached out to Telegram again with more detailed queries. It now seems clear that I had not misunderstood their reply and that if someone had removed an April 9 message from "Seller," it would no longer show up in recent actions log after 48 hours. So Troia was correct in arguing that messages could have been deleted and there would be no administrator logs for the channel to ever show they had appeared. But the message that Troia claimed was the source of his dataset could never have been that source as I demonstrated above, so we still have the issue of his misrepresentation and/or dishonesty about how and where he got the full data set.*

SO WHERE ARE WE?

More than two months after Troia published his report and allegations about Astoria Company, Astoria has yet to confirm his claims. If consumer data was stolen, consumers need to be notified -- particularly those whose SSN and/or bank account details may have been compromised.

But apart from the consumer protection issue, there is also the ongoing drama that seems to surround Vinny Troia. Whenever criminals/blackhats accuse him of lying or wrongdoing, Troia inevitably points out that they are criminals and therefore dishonest -- and that they are desperate to discredit him because he names them and outs them.

And now Troia is expanding his claims. TechNadu reports that Troia claims he has been able to link aliases to ShinyHunters, and that he has proof that the sellers are just a rebranding of the hacker group known as thedarkoverlord. And if that was not enough, Troia now also claims that "DonJuji," whose real identity is known to Troia and this blogger, is a part of both ShinyHunters and GnosticPlayers -- a claim he never made in his booklast year when he claimed to have identified the members of those groups.

"I KNOW [DonJuji] is working directly with seller13," Troia wrote to DataBreaches.net. " In some cases, I think [DonJuji] is sharing that account... And after you publish your story I plan on publishing my evidence, which includes Tying Seller to [DonJuji]'s home IP."

Asked to comment on those allegations, DonJuji replied:

> *I have screenshots of vinny himself saying "I work with seller13 very closely" and me asking him about who that is initially. I am not worried about any accusations that I am seller13 or that I have worked with shiny or gnostic or ranybody else and anybody doing a REAL investigation would come to that conclusion in a heartbeat. Vinny is right though. I did work with seller13.*
> *Because of course, vinny is seller13 and I used to work with vinny.*

So, it appears that Troia is accusing DonJuji of being involved in the Astoria hack, and DonJuji is pointing a finger right back at him.

DataBreaches.net will continue to follow developments in this case.

Screencaps of posts mentioned in this report can be found in the companion Appendix file.

This report was last updated May 23, 2021 to reflect follow-up with Telegram.