Database with 191 Million US voters' personal data exposed online

December 28, 2015 By Pierluigi Paganini

G+1 6
My Page Like 241

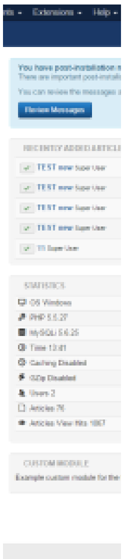
The security expert Chris Vickery has discovered a misconfigured archive exposes the personal details of 1 million U.S. voters.

A misconfigured database is the root cause of the exposure of around 191 Million voter records. Th records include voters' full names, unique voter IDs, unique voter IDs, date of births and phone numbers.

The database was discovered by the security expert Chris Vickery, the same expert that recently confirmed that information exposed in over 650 terabytes of MongoDB data was associat f the OS X

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. Accept Read More

MORE S



CVE-2

Attacks

servers

Experts a

hackers c

2015-85

comprom

The database containing voters' information was discovered on December 20th, Vickery provided all the details about his disconcerting discovery to DataBreaches.net. The archive includes over 191 Million Americans' *personal identifying information (PII).*

Vickery has found also his own information in the database containing 300GB of voters' data.

"My immediate reaction was disbelief," Vickery said. "I needed to know if this was real, so I quickly located the Texas records and ran a search for my own name. I was outraged at the result. Sitting right in front of my eyes, in a strange, random database I had found on the Internet, were details that could lead anyone straight to me. How could someone with 191 million such records be so careless?"

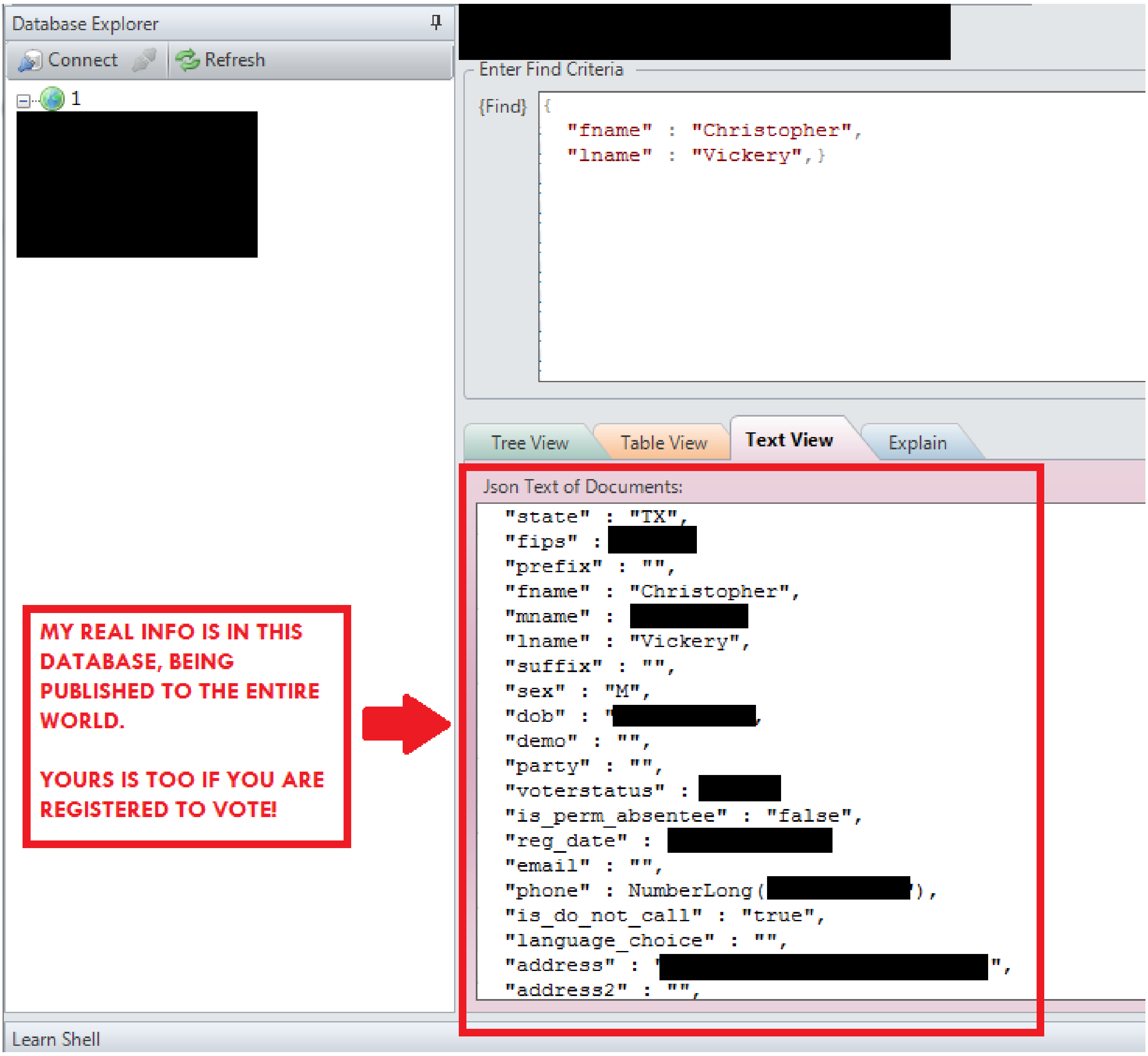
Below the detailed list of attributes stored in the leaked database.

- *Full name (first, middle, last)*
- *Residential address*
- *Mailing address*
- *A unique voter ID*
- *State voter ID*
- *Gender*
- *Date of birth*
- *Date of registration*
- *Phone number*
- *Political affiliation*
- *A detailed voting history since 2000*
- *Fields for voter prediction scores*

Vickery confirmed to have found in the voters' database the records belonging to a number of police officers in his city, he has also verified the authenticity of the information.

The database doesn't include Social Security Numbers, driver license numbers, or financial data, but the information it includes could be attractive for both cybercriminals and nation-state actors.

The principal media agencies are trying to identify possible responsible for the accidental exposure of so important data, but it is not clear who has misconfigured the archive.



[redacted]

[redacted]

```
{
  "fname" : "Christopher",
  "lname" : "Vickery",}
```

```
"state" : "TX",
"fips" : [redacted]
"prefix" : "",
"fname" : "Christopher",
"mname" : [redacted]
"lname" : "Vickery",
"suffix" : "",
"sex" : "M",
"dob" : "[redacted],
"demo" : "",
"party" : "",
"voterstatus" : [redacted]
"is_perm_absentee" : "false",
"reg_date" : [redacted]
"email" : "",
"phone" : NumberLong([redacted]),
"is_do_not_call" : "true",
"language_choice" : "",
"address" : "[redacted]",
"address2" : "",
```

MY REAL INFO IS IN THIS DATABASE, BEING PUBLISHED TO THE ENTIRE WORLD.

YOURS IS TOO IF YOU ARE REGISTERED TO VOTE!

1
2
3
4
5
6
7
8

Vickery and DataBreaches.net tried to contact voter information companies and various political groups, but all have denied any involvement in the incident.

"Salted Hash reached out to several political data firms in an effort to locate the owner of the exposed database. Dissent (admin of Databreaches.net) did the same thing. However, none of our efforts were successful." reported *Salted Hash. "The following firms were contacted by Salted Hash for this story: Catalist, Political Data, Aristotle, L2 Political, and NGP VAN. Databreaches.net reached out to Nation Builder. Speaking to Dissent, Nation Builder said that the IP address hosting the database wasn't one of theirs, and it wasn't an IP address for any of their hosted clients. As for the firms contacted by Salted Hash, each of them denied that the database was theirs, and in the case of NGP VAN, the technical aspects of the infrastructure (Linux vs. Windows) ruled them out because they're a Windows shop and the data is housed as part of a Linux build. A later attempt to contact i360, another political data firm, was unsuccessful."*

Vickery also reported the issue to the FBI and Internet Crime Complaint Center, let's hope the information will be removed as soon as possible.

Pierluigi Paganini

(**Security Affairs** – US voters database, hacking)

Share it please ...

1. Password Management

2. Detect Spyware

Hacking | data breach | database | US voters database

SHARE ON

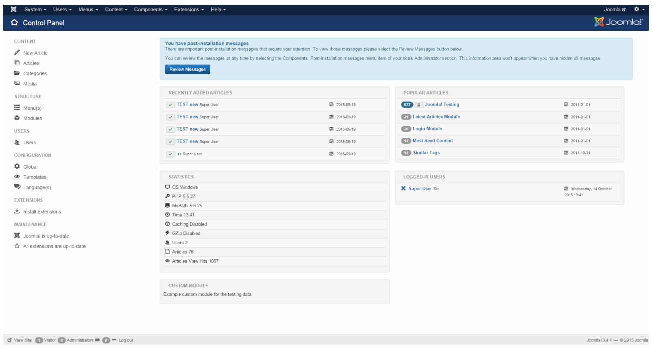
Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

‹ PREVIOUS ARTICLE
CVE-2015-8562 - 16,000 Daily Attacks on vulnerable Joomla servers

NEXT ARTICLE ›
Security Affairs newsletter Round 40 – News of the week

YOU MIGHT ALSO LIKE



Joomla! is up-to-date.
All extensions are up-to-date.

You have post-installation messages
There are important post-installation messages that require your attention. To view those messages please select the Review Messages button below.

You can review the messages at any time by selecting the Components, Post-installation messages menu item of your site's Administrator section. This information area won't appear when you have hidden all messages.

RECENTLY ADDED ARTICLES

TEST new Super User	2015-09-19
TEST new Super User	2015-09-19
TEST new Super User	2015-09-19
TEST new Super User	2015-09-19
TT Super User	2015-09-19

POPULAR ARTICLES

677	Joomla! Testing	2011-01-01
21	Latest Articles Module	2011-01-01
20	Login Module	2011-01-01
17	Most Read Content	2011-01-01
17	Similar Tags	2013-10-31

STATISTICS

OS Windows
PHP 5.5.27
MySQLi 5.6.25
Time 13:41
Caching Disabled
GZip Disabled
Users 2
Articles 76
Articles View Hits 1067

LOGGED-IN USERS

Super User Site	Wednesday, 14 October 2015 13:41

CUSTOM MODULE
Example custom module for the testing data.

Joomla! 3.4.4 — © 2015 Joomla

CVE-2015-8562 – 16,000 Daily Attacks on vulnerable Joomla servers

December 28, 2015 By Pierluigi Paganini

Darkweb, a look back at 2015 events and 2016 predictions

December 28, 2015 By Pierluigi Paganini

Copyright 2015 Security Affairs by Pierluigi Paganini All Right Reserved.

Home | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence | Laws and regulations |

|