

Advertisement



[Subscribe to RSS](#)



[Follow me on Twitter](#)



[Join me on Facebook](#)

MALWARE IS COMING
Get the right resources to protect against global cyber threats.

[VISIT THREAT CENTER »](#)

Infoblox

Krebs on Security

In-depth security news and investigation



[About the Author](#)

[Blog Advertising](#)

25

Sep 13

Data Broker Giants Hacked by ID Theft Service

An identity theft service that sells Social Security numbers, birth records, credit and background reports on millions of Americans has infiltrated computers at some of America's largest consumer and business data aggregators, according to a seven-month investigation by KrebsOnSecurity.



The Web site **ssndob[dot]ms** (hereafter referred to simply as SSNOB) has for the past two years marketed itself on underground cybercrime forums as a reliable and affordable service that customers can use to look up SSNs, birthdays and other personal data on any U.S. resident. Prices range from 50 cents to \$2.50 per record, and from \$5 to \$15 for credit and background checks. Customers pay for their subscriptions using largely unregulated and anonymous virtual currencies,

such as Bitcoin and WebMoney.

Until very recently, the source of the data sold by SSNDOB has remained a mystery. That mystery began to unravel in March 2013, when teenage hackers allegedly associated with the hacktivist group [UGNazi](#) showed just how deeply the service's access went. The young hackers used SSNDOB to collect data for [exposed.su](#), a Web site that listed the SSNs, birthdays, phone numbers, current and previous addresses for dozens of top celebrities — such as performers **Beyonce**, **Kanye West** and **Jay Z** — as well as prominent public figures, including **First Lady Michelle Obama**, **CIA Director John Brennan**, and then-FBI Director **Robert Mueller**.

Earlier this summer, SSNDOB was compromised by multiple attackers, its own database plundered. A copy of the SSNDOB database was exhaustively reviewed by KrebsOnSecurity.com. The database shows that the site's 1,300 customers have spent hundreds of thousands of dollars looking up SSNs, birthdays, drivers license records, and obtaining unauthorized credit and background reports on more than four million Americans.

Frustratingly, the SSNDOB database did not list the sources of that stolen information; it merely indicated that the data was being drawn from a number of different places designated only as “DB1,” “DB2,” and so on.

But late last month, an analysis of the networks, network activity and credentials used by SSNDOB administrators indicate that these individuals also were responsible for operating a small but very potent botnet — a collection of hacked computers that are controlled remotely by attackers. This botnet appears to have been in direct communications with internal systems at several large data brokers in the United States. The botnet's Web-based interface (portions of which are shown below) indicated that the miscreants behind this ID theft service controlled at least five infected systems at different U.S.-based consumer and business data aggregators.

guid	ip	time	Description
{5D74EE24-D79F-48F4-9DA5-5A5642745664}	158.151.200.129	2013-09-08 16:08:00	DNB2
{181B2686-A874-446E-9E1C-1FE13FF6A15C}	8.18.2.254	2013-09-08 16:07:13	CROLL CORP
{D942FF11-058C-443E-80DC-19F74E93754C}	198.185.25.201	2013-09-08 15:59:33	lex 1
{C25D66E8-A78B-43CE-B6E3-3F59C5124D57}	158.151.200.129	2013-09-08 15:52:04	DNB1
{FD986AE6-CB0A-4983-99BB-DF1A243F58C2}	198.185.24.201	2013-09-08 15:45:28	lex 2

The botnet interface used by the miscreants who own and operate ssndob[dot]ms

DATA-BROKER BOTNET

Two of the hacked servers were inside the networks of Atlanta, Ga.-based [LexisNexis Inc.](#), a company that according to Wikipedia maintains the world's largest electronic database for legal and public-records related information. Contacted about the findings, LexisNexis confirmed that the two systems listed in the botnet interface were public-facing LexisNexis Web servers that had been compromised.

The screenshot shows a web interface for a botnet. At the top, there's a header with 'Main' and 'lex 1'. Below it, a URL is displayed: [ID947FF11-058C-443E-80DC-19F74E93754C1](#). A timestamp reads '198.185.25.201 prod-gw.lexisnexis.com 2013-09-08 14:29:31 (10m 23s ago)'. A table lists several machines with columns for 'id', 'type', 'data', 'status', and 'Status Date'. The 'data' column contains 'abc.exe 91.205.96.12.441'. Below the table is a 'Run Command' dropdown menu with options like 'Set time Interval', 'Update Domain Names', 'Download File', 'Stop Service', and 'Set Description'. The main area displays system information for a host named 'psd3bweb77a', including DNS settings, IP address (138.12.88.149), and network configuration.

id	type	data	status	Status Date
87	malware	abc.exe 91.205.96.12.441	DONSE	2013-04-17 10:06:52
88	malware	abc.exe 91.205.96.12.441	DONSE	2013-04-12 22:30:42
89	malware	abc.exe 91.205.96.12.441	DONSE	2013-04-12 21:20:53
92	malware	abc.exe 91.205.96.12.441	DONSE	2013-04-11 18:18:33
91	server	2700	DONSE	2013-04-10 11:34:08
90	server	ex.1	DONSE	2013-04-10 11:31:55

Host Name: psd3bweb77a
 Primary Dns Suffix: PRODWEBD3.net
 Node Type: Hybrid
 IP Routing Enabled: No
 WINS Proxy Enabled: No
 DNS Suffix Search List: PRODWEBD3.net, lexisnexis.com
 Ethernet adapter Prod BE (138.12.88.x):
 Connection-specific DNS Suffix: PRODWEBD3.net
 Description: VMware Accelerated AMD PCNet Adapter
 Physical Address: 00-50-56-E3-39-2F
 DHCP Enabled: No
 IP Address: 138.12.88.149
 Subnet Mask: 255.255.252.0
 Default Gateway: 138.12.89.211
 DNS Servers: 138.12.88.229, 138.12.88.232, 10.172.88.121
 Primary WINS Server: 138.12.88.229
 Secondary WINS Server: 138.12.88.232

One of two bots connected to SSNOB that was inside of LexisNexis.

The botnet's online dashboard for the LexisNexis systems shows that a tiny unauthorized program called "nbc.exe" was placed on the servers as far back as April 10, 2013, suggesting the intruders have had access to the company's internal networks for at least the past five months. The program was designed to open an encrypted channel of communications from within LexisNexis's internal systems to the botnet controller on the public Internet.

[Two other compromised systems](#) were located inside the networks of [Dun & Bradstreet](#), a Short Hills, New Jersey data aggregator that licenses information on businesses and corporations for use in credit decisions, business-to-business marketing and supply chain management. According to the date on the files listed in the botnet administration panel, those machines were compromised at least as far back as March 27, 2013.

[The fifth server](#) compromised as part of this botnet was located at Internet addresses assigned to [Kroll Background America, Inc.](#), a company that provides employment background, drug and health screening. Kroll Background America is now part of [HireRight](#), a background-checking firm managed by the Falls Church, Va.-based holding company [Altegrity](#), which owns both the Kroll and HireRight properties. Files left behind by intruders into the company's internal network suggest the HireRight breach extends back to at least June 2013.

An initial analysis of the malicious bot program installed on the hacked servers reveals that it was carefully engineered to avoid detection by antivirus tools. A [review of the bot malware](#) in early September using **Virustotal.com** — which scrutinizes submitted files for signs of malicious behavior by scanning them with antivirus software from nearly four dozen security firms simultaneously — gave it a clean bill of health: none of the 46 top anti-malware tools on the market today detected it as malicious (as of publication, the malware is currently detected by 6 out of 46 anti-malware tools at Virustotal).

ASSESSING THE DAMAGE

All three victim companies said they are working with federal authorities and third-party forensics firms in the early stages of determining how far the breaches extend, and whether indeed any sensitive information was accessed and exfiltrated from their networks.

For its part, LexisNexis confirmed that the compromises appear to have begun in April of this year, but said it found “no evidence that customer or consumer data were reached or retrieved,” via the hacked systems. The company indicated that it was still in the process of investigating whether other systems on its network may have been compromised by the intrusion.

“Immediately upon becoming aware of this matter, we contacted the FBI and initiated a comprehensive investigation working with a leading third party forensic investigation firm,” said **Aurobindo Sundaram**, vice president of information assurance and data protection at **Reed Elsevier**, the parent company of LexisNexis. “In that investigation, we have identified an intrusion targeting our data but to date have found no evidence that customer or consumer data were reached or retrieved. Because this matter is actively being investigated by law enforcement, I can’t provide further information at this time.”

Dun & Bradstreet and Altegrity were less forthcoming about what they’d found so far. **Elliot Glazer**, chief technology officer at Dun & Bradstreet, said the information provided about the botnet’s interaction with the company’s internal systems had been “very helpful.”

“We are aggressively investigating the matter, take it very seriously and are in touch with the appropriate authorities,” Glazer said. “Data security is a company priority, and I can assure you that we are devoting all resources necessary to ensure that security.”

Altegrity declined to confirm or deny the apparent compromises, but through spokesman **Ray Howell** offered the following statement: “We consider the protection and safeguarding of our various systems of the utmost importance. We have dedicated significant information security resources to managing security and protecting the data and privacy of our customers. We have a range of incident response specialists and teams from both inside and outside the company investigating your allegations vigorously.”

Referring to the SSNDOB compromises, **FBI Spokesperson Lindsay Godwin** confirmed that the FBI is “aware of and investigating this case,” but declined to comment further except to say that the investigation is ongoing.

KNOWLEDGE IS POWER

The intrusions raise major questions about how these compromises may have aided identity thieves. The prevailing wisdom suggests that the attackers were going after these firms for the massive amounts of consumer and business data that they hold. While those data stores are certainly substantial, fraud experts say the really valuable stuff is in the data that these firms hold about *consumer and business habits and practices*.

The screenshot shows a botnet control interface. At the top, there's a header with 'Main' and 'DNS2'. Below it, a table lists botnet entries:

id	type	data	status	Status	Date
89	setip	2400	DONE		2013-03-27 23:44:48
88	setdesc	DNS2	DONE		2013-03-27 23:44:33

Below the table is a 'Run Command' dropdown menu with options: Run Command, Set time interval, Update Domain Names, Download File, Stop Service, and Set Description. The main area displays configuration details for a host named 'DBPWSCRAP02' on 'dabst.net'. It shows network settings for 'Ethernet adapter Local Area Connection 7', including IP address (158.151.10.149), subnet mask (255.255.254.0), and DNS servers (10.69.130.32). A 'Windows IP Configuration' section at the bottom repeats the host's basic network information.

The botnet control panel entry for a hacked Dun & Bradstreet server

Avivah Litan, a fraud analyst with **Gartner Inc.**, said most credit-granting organizations assess the likelihood that a given application for credit is valid or fraudulent largely based on how accurately an applicant answers a set of questions about their financial and consumer history.

These questions, known in industry parlance as “knowledge-based authentication” or KBA for short, have become the gold standard of authentication among nearly all credit-granting institutions, from loan providers to credit card companies, Litan said. She estimates that the KBA market is worth at least \$2 billion a year.

“Let’s say you’re trying to move money via online bank transfer, or apply for a new line of credit,” Litan proposed. “There are about 100 questions and answers that companies like LexisNexis store on all of us, such as, ‘What was your previous address?’ or ‘Which company services your mortgage?’ They also have a bunch of bogus questions that they can serve up to see if you really are who you say you are.”

According to Litan, Dun and Bradstreet does roughly the same thing, except for businesses.

“Dun & Bradstreet doesn’t do KBA *per se*, but if you’re filling out a business loan and you want to pose as that business, having access to a company like that can help,” Litan said. “Dun & Bradstreet is like the credit bureau for businesses.”

Overall, Litan says, credit applicants fail to answer one or more of the KBA questions correctly about 10-15 percent of the time. Ironically, however, those that get the questions wrong are more often legitimate credit applicants — not the identity thieves.

“These days, the people who fail these questions are mainly those who don’t remember the answers,” Litan said. “But the criminals seem to be having no problems.”

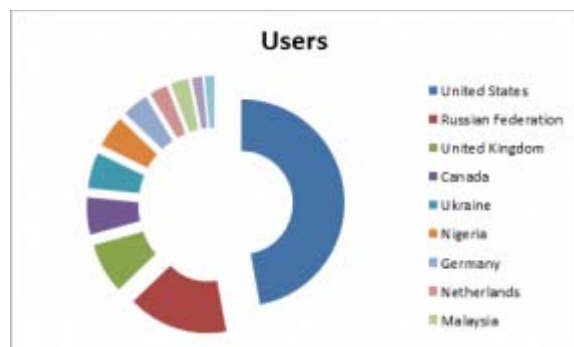
Litan related a story she heard from one fellow fraud analyst who had an opportunity to listen in on the KBA questions that a mortgage lender was asking of a credit applicant who was later determined to have been a fraudster.

“The woman on the phone was asking the applicant, ‘Hey, what is the amount of your last mortgage payment?’, and you could hear the guy on the other line saying hold on a minute....and you could hear him clicking through page after page for the right questions,” Litan said.

The Gartner fraud analyst said she has long suspected that the major KBA providers have been compromised, and [has been saying so for years](#).

“We could well be witnessing the death of knowledge-based authentication, and it’s as it should be,” Litan said. “The problem is that right now there are no good alternatives that are as easy to implement. There isn’t a good software-based alternative. Everybody in the industry knows that KBA is nearing its end of usefulness, but it’s not like you can instantly roll out biometric identifiers to the entire US population. We’re just not there yet. It’s years away. If ever.”

CUSTOMER SERVICE



Breakdown of ssn[dot]dob users by IP address

A closer examination of the database for the identity theft service shows it has served more than 1.02 million unique SSNs to customers and nearly 3.1 million date of birth records since its inception in early 2012.

Thousands of background reports also have been ordered through SSNOB. Records at the ID theft service indicate that the service was still able to order background reports via LexisNexis more than 10 days after the data aggregator disabled the infected Web servers listed in the botnet’s control panel, suggesting that the intruders still had a store of accounts that could be used to pull information from the company’s databanks.

In a written statement provided to KrebsOnSecurity, LexisNexis officials said that report was generated from a law student ID that was being misused.

“Unrelated to the intrusion you have asked about, you provided to us a LexisNexis report. We determined that that report was generated from a law student ID that was being misused. That ID accesses only unregulated public records information and was identified by our fraud detection tools and shut down by us before you brought it to our attention.”

The registration records for SSNOB show that most users registered with the ID theft service using Internet

addresses in the United States, the Russian Federation, and the United Kingdom, although it is likely that a large portion of these users were using hacked PCs or other proxy systems to mask their true location.

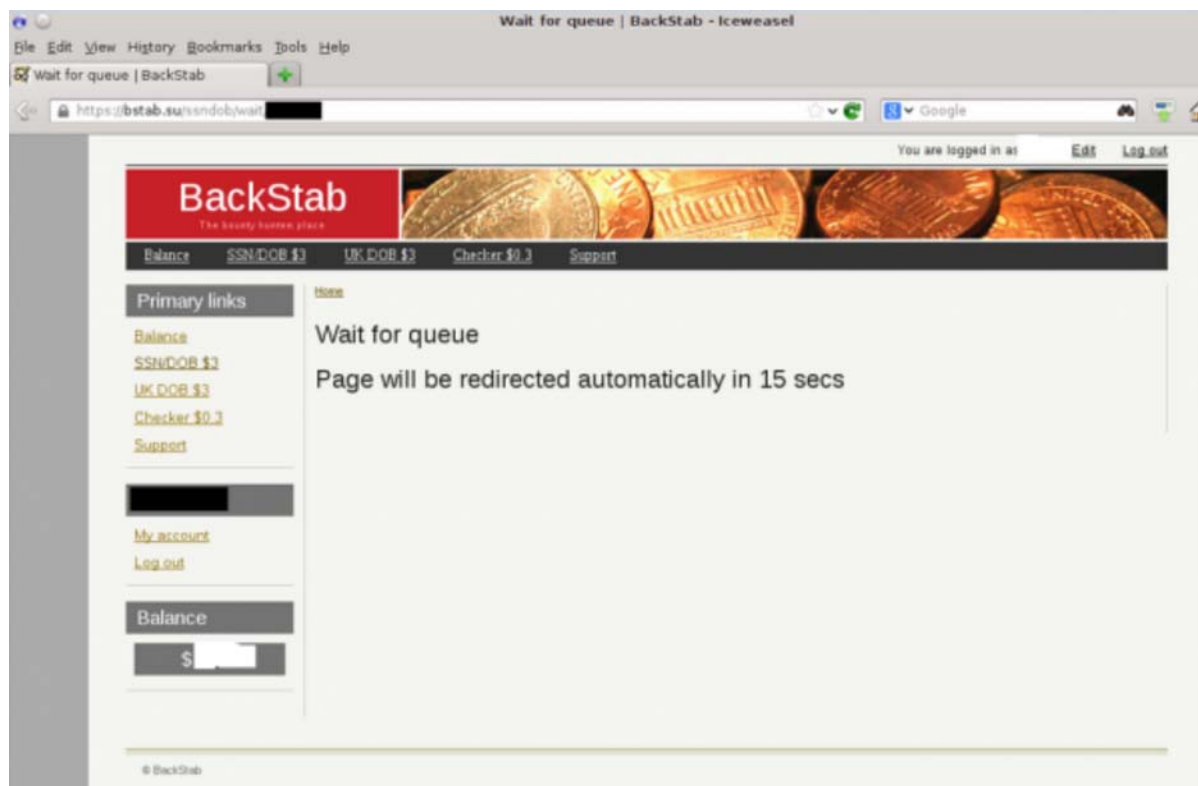
SSNDOB also appears to have licensed its system for use by [at least a dozen high-volume users](#). There is some evidence which indicates that these users are operating third-party identity theft services. A review of the leaked site records show that several bulk buyers were given application programming interfaces (APIs) — customized communications channels that allow disparate systems to exchange data — that could permit third-party or competing online ID theft sites to conduct lookups directly and transparently through the SSNDOB Web site.

Indeed, the records from SSNDOB show that the re-sellers of its service reliably brought in more money than manual look-ups conducted by all of the site's 1,300 individual customers combined.

I would like to thank **Alex Holden** of [Hold Security LLC](#) for his assistance in making sense of much of this data.

Stay tuned for Part II and Part III of this rapidly unfolding story. **Update:** See Part II of this series: [Data Broker Hackers Also Compromised NW3C](#).

Update, 2:05 p.m. ET: SSNDOB appears to be down. Also, one likely reseller of the ID theft service's data — a fraud site called bstab[dot]su, has been having trouble all morning looking up SSN data. Lookups at that service are sending paying customers into an endless loop today. See image below.



Tags: [Altegrity](#), [Aurobindo Sundaram](#), [avivah litan](#), [Dun & Bradstreet](#), [Elliot Glazer](#), [fbi](#), [Gartner Inc.](#), [HireRight](#), [Kroll](#), [Kroll Background America Inc.](#), [LexisNexis](#), [Lindsay Godwin](#), [Ray Howell](#), [Reed Elsevier](#), [ssndob.ms](#), [UG Nazi](#), [virustotal](#)

This entry was posted on Wednesday, September 25th, 2013 at 12:02 am and is filed under [A Little Sunshine](#), [Web Fraud 2.0](#). You can follow any comments to this entry through the [RSS 2.0](#) feed. Both comments and pings are currently closed.

102 comments

1.  *anymouse*

[September 25, 2013 at 5:00 pm](#)

“LexisNexis officials said that report was generated from a law student ID that was being misused”

It’s not just law students. Paralegal students are also given free subscriptions to LexisNexis. Many lawyers and paralegals have current access to it (a few still use books). LexisNexis is one of the big-two companies which sells access for online legal research to lawyers.

HireRight is one of the companies which provides background checks for companies which have outsourced their HR function. If you refuse to deal with HireRight, the employer which contracted with them will not hire you.

If you are a victim of identity theft or even data theft from a website, the most you will receive is one year’s worth of data monitoring. You will receive no compensation whatsoever for legal costs.

Victims should consider adding a credit freeze to their accounts with the big three agencies, but remember that subsequent credit checks will cost you \$10 each.

This entire subject was a predictable outcome of allowing U.S. banks to do business in all 50 states and outsource their functions to companies around the world. In the old days, one needed to visit a local banker to obtain a credit card.

○  *DefendOurFree*

[September 26, 2013 at 9:04 am](#)

This is true of online paralegal training programs too. Full online access to Lexis came with the program, as of 2010, at least.

■  *Shinki-itten*

[September 26, 2013 at 1:41 pm](#)

A user’s Lexis-Nexis account does not include access to non-public information, such as full SS# or DL, so “mis-use” of a law student or paralegal account would not account for the data leak described in the article. Voter registration records can be mined for addresses, but only after meeting statutory requirements.

■  *DefendOurFree*

[September 26, 2013 at 1:59 pm](#)

Sorry, that is not true.

2.  *George G*

[September 25, 2013 at 8:07 pm](#)

“most credit-granting organizations assess the likelihood that a given application for credit is valid or fraudulent largely based on how accurately an applicant answers a set of questions about their financial and consumer history.”

Hah ! That is a joke.

Recently I decided to get my annual free credit report from Equifax. I went the internet route.

The second page to come up was to verify my identity via questions similar to mentioned in the quote above.

It told me that my files indicated a mortgage taken out in June 2013 (I have not had a mortgage in quite a while) and asked me to select from a list of financial institutions from which the mortgage was obtained.

Never heard of any of them.

Then I was presented with a list of mortgage payment ranges.

Naturally I answered none of the above.

Then came very similar questions on a car loan. Just as inapplicable to me as the mortgage questions. I answer none of the above.

It tells me my identity could not be verified.

Now I am concerned.

I go to obtain the credit report via the mail (snail mail, that is).

Credit report arrives.

Not a word about the mortgage or car loan mentioned while my identity was being “verified”.

And businesses actually pay these credit bureaus when they use them ?

○  *Claiborne*

[September 25, 2013 at 9:53 pm](#)

Actually, this is exactly the same thing that happened to me with Equifax. It is their way of trying to keep you from getting the “free” credit report. Make it as difficult as possible.

My partner ordered his the same day, and the same response from Equifax.

Trying to get them to correct inaccurate information is next to impossible, too.

○  *IA Eng*

[September 26, 2013 at 12:31 pm](#)


The credit bureaus throw bogus questions at you in order to throw off anyone that may be posing as you. Some of the questions may be from the past, like several years or more. The important thing is knowing which questions apply to you and which ones don't.

One thing that ticks me off is that Equifax and other Credit agencies sell your creditworthiness information. If you get a bunch of credit card and financial offerings, check the back of the offer for paragraphs about “Equifax” and the creditworthiness mail spam campaign. They are in it for the money, and all I can say is they are part of the problem when they think they can simply announce to the world that you have decent credit.

All the crooks have to do is assemble enough information and they too can try to pose as you, and they may actually get approved for some stupid loan under your name.


I have been lucky – so far.

Thanks Equifax, for acting like a secure, prim and proper credit reporting agency. NOT ! Freakin Bozo’s.

3.  *TondoJondo*
[September 25, 2013 at 8:10 pm](#)

That makes a lot of sene dude.

<http://www.Got-Privacy.com>

- o  *George G*
[September 25, 2013 at 9:15 pm](#)


The URL you provided earns a “red flag” from the Web of Trust extension of my browser.

4.  *Jedi Mercer*
[September 25, 2013 at 11:24 pm](#)


@anymouse, many years ago I used to work at the law college of a major university. Not only were most of the professors lawyers and had Lexis-Nexis accounts, most of the students were granted access as well.

I wasn’t even a student at the school, merely an PC technician. Walking around the campus doing my assigned duties I would routinely find Lexis-Nexis login IDs lying around. They were pre-printed card distributed to the students.


That was decades ago, I doubt much has changed.

5.  *Clyde Tolson*
[September 26, 2013 at 8:31 am](#)


Don’t worry everyone...the FBI is on it.

- o  *QHoster*
[September 30, 2013 at 6:44 pm](#)

Yes data records already leaked over Internet, or may be a lot more. Who knows ... And the worst part whoever needed this information will be use it for not so honorable purposes.

6.  [Paul Wagenseil](#)
[September 26, 2013 at 9:09 am](#)



7.  [Algo Rythm](#)
[September 26, 2013 at 10:03 am](#)

Calling all lawyers,

When our company lost the SSNs of some of their employees, we had to purchase a couple years of credit fraud insurance.


Am irked that LexisNexis et al seem to be escaping the consequences of their crummy security attitude. For a change I see a good reason for a class action lawsuit...all three of these companies should be collectively buying us all fraud insurance.

Al

- o  [DefendOurFree](#)
[September 26, 2013 at 10:46 am](#)

There is one. Maybe you can join?

Class action lawsuit Gregory Thomas Berry, et al. v. LexisNexis Risk & Information Analytics Group, Inc., No. 3:11CV754 (E.D. Va.)

-  [IA Eng](#)
[September 26, 2013 at 12:46 pm](#)

Go to databreaches.net and look at all the failed attempts at suing some one for losing data. they fall apart in court since people suing cannot prove that the information that was just lost is causing damages to the people suing.

Then as time passes, and people's accounts get siphoned, how do you know which business leaked the information? It could be the one you are eyeballing, or it could be an establishment that got hacked years ago, or, one that has gone unreported or undetected.

The crooks know that the ways of reporting and clean up is messy, and since there is no really hard-lined defined procedures in place, the crooks can take their time with thousands of records and live life at your expense – should they be able to compromise your identity.

The way the credit reporting agencies handle the security of accounts stinks worse than an overstuffed buffalo which at a huge pile of garlic and laxatives which is just about to

have an....issue.

8.  *techvet*

[September 26, 2013 at 12:20 pm](#)

Congrats to your and the others you worked with on the excellent sleuthing. I just saw a BBC story mentioning Brian, so you know it has hit the big-time.

o  *IA Eng*

[September 26, 2013 at 12:36 pm](#)

I see Brian's Blog mentioned in the Department of Homeland daily Security Infrastructure Brief.

He was actually in there a couple of days ago.....

8. September 18, Krebs on Security – (National) Crooks hijack retirement funds via SSA portal. The Social Security Administration (SSA) and financial institutions reported a rise in identity theft cases where criminals register an account on the SSA Web portal in the name of a retiree and then divert the benefits to themselves in the form of prepaid debit cards. Source: <http://krebsonsecurity.com/2013/09/crooks-hijack-retirement-funds-via-ssa-portal/>

o  *Bikebrains*

[September 27, 2013 at 12:32 pm](#)

SOURCE: <http://www.bbc.co.uk/news/technology-23502300>

30 July 2013

“A respected US-based internet security expert says he has foiled an attempt to frame him as a heroin dealer.”

9.  *Just Me*

[September 26, 2013 at 4:47 pm](#)

Call me cynical but what I wonder is if these computers were really hacked and if the botnet existed at all. I can easily imagine that either the companies themselves or individuals within the company sold their data to the black market as a way to enhance profits or skim off some retirement funds. Of course these people are going to claim “hack” but maybe it wasn't a actual hack at all.


10.  *nikol*

[September 27, 2013 at 7:13 am](#)

I was going to make a comment on how.... even the pentagon gets hacked.And your article sent me to check my credit report.....The Fair and Accurate Credit Transactions Act and the Fair Credit Reporting Act require each of the three major credit bureaus (Experian, Equifax and TransUnion) to provide you with access to a free credit report once a year.I thought this website would be bulletproof.....but a check with QUALYS SSL LABS at <https://www.ssllabs.com/ssltest>

[/analyze.html?d=annualcreditreport.com](#) and WTFall servers have a grade F!!!!


Damn ,I don't even want to make this information available.Unbelievable! But I'm fairly certain the crooks already know this.

11.  [Carol Kayes](#)
[September 27, 2013 at 4:32 pm](#)

And now they will have a new source of information. The Congress has told the IRS to release all of our tax and income information to the online Health Insurance Exchanges – and who knows how insecure that will be. Thank you Obamacare for making it even easier to get the data all in one place.

-  [DefendOurFree](#)
[September 27, 2013 at 4:37 pm](#)

They IRS has been hacked, <http://www.scmagazine.com/irs-leaks-tens-of-thousands-of-social-security-numbers/article/302212/> . Even the Pentagon has been hacked. This article is about LexisNexis. Let's not make Brian read Dr. Seuss to us, ok?

12.  [DefendOurFree](#)
[September 27, 2013 at 5:08 pm](#)

This article covering Brian's research is interesting:

<http://phys.org/news/2013-09-lexisnexis-breach-earlier-year.html>

“LexisNexis’ wide-ranging databases, which are built from public records and proprietary sources, are used for identity checks, employee screenings, debt collections and more. Its clients include government agencies, insurers, banks, media companies, corporate personnel offices and private investigators. ”


One of LexisNexis's resellers actual trains and certifies Private Investigators for their state licenses.

<http://defendourfreedom.net/2012/11/15/did-you-know—101.aspx>

<http://defendourfreedom.net/2012/11/16/did-you-know—102.aspx>

<http://defendourfreedom.net/2012/11/17/did-you-know—103.aspx>

Kinda like a fox guarding the hen house affect to ensure access to it's next meal.

-  [kavinmoore](#)
[October 7, 2013 at 1:32 am](#)

Yeah, actually I am impressed the way they research and investigate of this cause absolutely amazingly. So, I am also impressed to read above article.



13. *DefendOurFree*

[September 28, 2013 at 9:47 am](#)

These domains are doing redirects now to do look ups:

search-ssn.com

SSNRecords.net

ssnlookup123.com



14. *Ryan Baron*

[September 28, 2013 at 6:09 pm](#)

I think we are all going to need to proactively attempt to protect our identity in the future with services like lifelock.com or <http://legalshieldassociate.com/hub/ryanbaron> . Over the past years I have submitted personal information to countless websites, even if I stopped giving my information out today, which isn't realistic, I don't know who has my information already.



o *Shinki-itten*

[September 28, 2013 at 11:28 pm](#)

A credit service, if reasonably priced, may be helpful. Legal Shield sells the services of Kroll on a monthly payment basis. If the customer has a credit theft, Kroll will take many steps to repair credit. However, Kroll requires that the hack victim give Kroll an extraordinarily comprehensive power of attorney to use as it tries to repair the credit. Ironically, Brian's article identifies a hacked Kroll server as one of the sources these criminals used to steal credit information. Even though Brian's article was picked up by USA Today, I haven't seen any explanation from Kroll or Legal Shield about the breach and whether accounts of any Legal Shield customers were breached.



15. *Doug*

[September 28, 2013 at 7:41 pm](#)

The report says "obtaining unauthorized credit and background reports" but the three data providers listed do not have credit reports. Which of the bureaus was compromised?




o *Brian Krebs*

[September 28, 2013 at 10:48 pm](#)

I believe SSNDOB sold credit reports by taking advantage of the services offered via the three major credit bureaus via the congressionally-mandated annualcreditreport.com. See:

<http://krebsonsecurity.com/2013/03/credit-reports-sold-for-cheap-in-the-underweb/>

16.  *Deer Caught in the Headlights*
[September 30, 2013 at 7:04 pm](#)

First, great work. Nice to see someone telling aggregate data miner emperors they have no clothes on.

Similar story with the credit rating services. Why would they want to fix their integrity problems? They have created a new business opportunity; charging monthly fees to concerned consumers to project themselves against the industry's own folly. Ah yes, and I can purchase insurance from one of their friends in the financial services sector, to protect myself, just like I can get insurance to protect myself from an uninsured drunk driver.


Truly a sad state for consumers.

17.  *Chris*
[October 1, 2013 at 10:50 am](#)

Folks commenting that they had access to Lexis/Nexis during law school, etc. should bear in mind that “Lexis/Nexis” the company has a variety of products, only some of which, eg. Accurant, are PII-related.

Lawyers, for example, are likely to have accts limited to obtaining legal citations, articles, and the like. Other persons, for example those offering credit, are likely to have very different access, including access to PII.


Unsurprisingly, Lexis/Nexis offers this variety on an a la carte basis, presumably to maximize their revenue. As a former user of the Accurant public records product, I can assure you that even though all the data sources in it are “public”, it is amazingly juicy. It was somewhat sobering to see what it had on me!

18.  *Micheal Bian*
[October 5, 2013 at 5:21 am](#)

Great article.....Thank you for sharing this one...

19.  *Marc Schultz*
[October 16, 2013 at 9:02 am](#)

I am still amazed at how little publicity there has been on this. Has anyone heard any updates on who is doing what notifications if any?

20.  *Will*
[October 22, 2013 at 5:11 pm](#)

This design is spectacular! You most certainly know how to keep a reader amused. Between your wit and your videos, I was almost moved to start my own blog (well,

almost...HaHa!) Fantastic job. I really enjoyed what you had to say, and more than that, how you presented it. Too cool!

21.  [Jedi Mercer](#)

[October 22, 2013 at 7:52 pm](#)

Note that commentors “Will”, “Micheal Bian”, and “kavinnmoore” are just bots/spammers making generic comments in order to direct traffic to websites.

(Full disclosure: my own entry redirects to my website, but it’s actually related to me AND the Information Security profession).

I’m amused by it, but Brian you should probably turn off the website link option. it could easily be abused to deliver malware, drive-bys, etc. You have a lot of people gunning for you, stay safe and keep up the good work!

[← Older Comments](#)

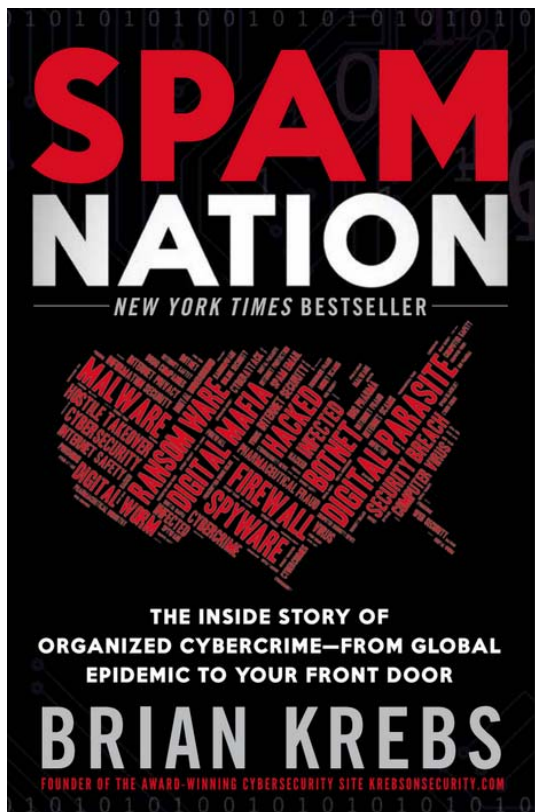
Advertisement



The advertisement features a blue and orange color scheme. At the top, there is a circular logo with the text "CIS SECURITY BENCHMARKS CERTIFIED" and a stylized "S" symbol. Below this, the text "NNT WORKPLACE SOLUTIONS" is displayed next to the word "WEBINAR" in large, bold letters. Underneath "WEBINAR" is the phrase "NOW AVAILABLE". The main body of the ad contains the text "MODERNIZING YOUR CYBER SECURITY APPROACH WITH THE CENTER FOR INTERNET SECURITY". At the bottom, there is a prominent orange button with the text "WATCH NOW >" in white.

• 

• **My New Book!**



A New York Times Bestseller!

Buy at Amazon

Donate with PayPal

Recent Posts

- [Exclusive: Dutch Cops on AlphaBay ‘Refugees’](#)
- [After AlphaBay’s Demise, Customers Flocked to Dark Market Run by Dutch Police](#)
- [Trump Hotels Hit By 3rd Card Breach in 2 Years](#)
- [Experts in Lather Over ‘gSOAP’ Security Flaw](#)
- [Porn Spam Botnet Has Evil Twitter Twin](#)

Subscribe by email

Please use your primary mailbox address, not a forwarded address.

Your email:

Enter email address...

Subscribe

Unsubscribe

• All About Skimmers



Click image for my skimmer series.

• The Value of a Hacked PC



Badguy uses for your PC

• Tools for a Safer PC



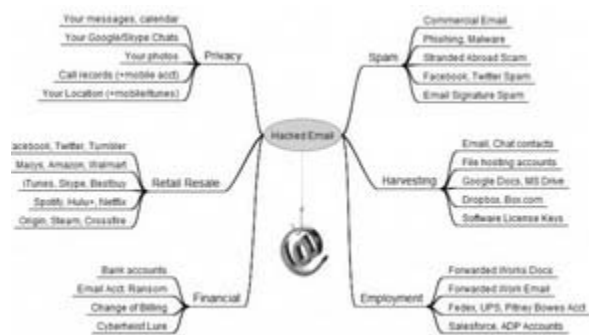
Tools for a Safer PC

• The Pharma Wars



Spammers Duke it Out

• Badguy Uses for Your Email



Your email account may be worth far more than you imagine.

• eBanking Best Practices



eBanking Best Practices for Businesses

• Most Popular Posts

- [Online Cheating Site AshleyMadison Hacked](#) (798)
- [Sources: Target Investigating Data Breach](#) (620)
- [Cards Stolen in Target Breach Flood Underground Markets](#) (445)
- [Reports: Liberty Reserve Founder Arrested, Site Shuttered](#) (416)
- [Was the Ashley Madison Database Leaked?](#) (376)
- [True Goodbye: 'Using TrueCrypt Is Not Secure'](#) (363)
- [Who Hacked Ashley Madison?](#) (360)
- [Following the Money, ePassporte Edition](#) (353)
- [U.S. Government Seizes LibertyReserve.com](#) (315)
- [Extortionists Target Ashley Madison Users](#) (310)

• Category: Web Fraud 2.0



Innovations from the Underground



-

ID Protection Services Examined

- **Is Antivirus Dead?**



The reasons for its decline

- **The Growing Tax Fraud Menace**



File 'em Before the Bad Guys Can

• Inside a Carding Shop



A crash course in carding.

• Beware Social Security Fraud



At each stage of your life, **my Social Security** is for you. Your personal online **my Social Security** account is a valuable source of information beginning in your working years and continuing throughout the time you receive Social Security benefits.

If you receive benefits or have Medicare, you can:

Use a **my Social Security** online account to:

- Get your **benefit verification letter**;
- Check your **benefit and payment information** and your earnings record;
- **Change your address** and phone number; and
- **Start or change direct deposit** of your benefit payment.

Sign up, or Be Signed Up!

• How Was Your Card Stolen?



Finding out is not so easy.

- **Krebs's 3 Rules...**



...For Online Safety.