

Forum:[Hack Forums](#)

Thread: [WLI DB Lookup Has Been Seized](#)

Pronouncer - January 15, 2020, 3:42 pm

Edit: To anyone who thought it was fake here u go

<https://www.justice.gov/usao-dc/pr/weleakinfocom-domain-name-seized>

edit 2: arrests made

<https://www.nu.nl/tech/6024433/arnhemmer-aangehouden-voor-rol-bij-zoekmachine-met-miljarden-wachtwoorden.html?redirect=1>

<https://www.psnipolice.uk/news/Latest-News/170120-weleakinfo.com-site-hosting-stolen-credentials-taken-down-after-international-operation/>

Dunno if u noticed but the domain no longer points to a-records.

If you go to the www. (Insert WLI) . com you will see its been seized RIP boys no more DB lookups

Evading - January 15, 2020, 3:43 pm

No doubt another one will pop up soon :)

Nachfolger - January 15, 2020, 3:45 pm

My boy, the DOJ, out there doing God's work.

Bless their hearts.

SIM-3205632 - January 15, 2020, 4:01 pm

Couldnt afford a subscription anyway.

Thrift - January 15, 2020, 4:02 pm

Another will be made soon without a doubt.

Mr. Robot - January 15, 2020, 4:29 pm

There are like 50 others anywho, just use haveibeenpwned my dudes.

The only good thing about WLI was they had a few more DBs that haveibeen don't have so it's hard to keep track of what's been breached.

dedsec - January 15, 2020, 4:31 pm

Well, another one bites the dust. Hopefully another similar search engine pops up soon, someone let me know if you find one.

Mr. Robot - January 15, 2020, 4:35 pm

I'm still on the fence about it though tbh, never seen a page be taken down with red outlines rather than red bar behind the main title.

Disc channel also is just removed rather than the normal 'under investigation' page.

Twitter was still live 3 hours ago too.

Pronouncer - January 15, 2020, 4:36 pm

(Jan 15, 2020 05:35 PM)Mr. Robot Wrote: [\[CITE\]](#) I'm still on the fence about it though tbh, never seen a page be taking down with red outlines rather than red bar behind the main title.

Disc channel also is just removed rather than the normal 'under investigation' page.

Twitter was still live 3 hours ago too.
all the signs of it being legit are there too

SIM-4033767 - January 15, 2020, 4:38 pm

(Jan 15, 2020 04:42 PM)Pronouncer Wrote: [\[CITE\]](#) Dunno if u noticed but the domain no longer points to a-records.

If you go to the www. (Instert WLI) . com you will see its been seized RIP boys no more DB lookups

What's this?

Mr. Robot - January 15, 2020, 4:40 pm

(Jan 15, 2020 05:36 PM)Pronouncer Wrote: [\[CITE\]](#) all the signs of it being legit are there too
Such as?

There are many possibilities with the way it's being played out.

The website was hijacked.
The owners have decided to take it down.
The feds did take it down.

The thing is right, usually shit doesn't all go down and offline in the same couple of minutes. It generally takes a bit of processing to do, it looks like a fast sloppy job IMO

? Soufian ? - January 15, 2020, 4:43 pm

Well f*ck me...
I used it yesterday...
This was one of my top tools for doxing

Mr. Robot - January 15, 2020, 4:44 pm

The only thing I can guarantee -
>> If it's legit and was seized, it was done so by EU not US. Just in co-operation with a US led investigation.

18 U.S. Code § 981.Civil forfeiture
18 U.S. Code § 982.Criminal forfeiture

(982 is only applicable if //)
18 U.S. Code § 1956.Laundering of monetary instruments
18 U.S. Code § 1957.Engaging in monetary transactions in property derived from specified unlawful activity
18 U.S. Code § 1960.Prohibition of unlicensed money transmitting businesses

All of which are viable options, but we see that across pretty much any site related.

Inter alia:

"among other things"

Pronouncer - January 15, 2020, 4:50 pm

(Jan 15, 2020 05:44 PM)Mr. Robot Wrote: [\[CITE\]](#) The only thing I can guarantee -

>> If it's legit and was seized, it was done so by EU not US. Just in co-operation with a US led investigation.

18 U.S. Code § 981.Civil forfeiture

18 U.S. Code § 982.Criminal forfeiture

(982 is only applicable if //)

18 U.S. Code § 1956.Laundering of monetary instruments

18 U.S. Code § 1957.Engaging in monetary transactions in property derived from specified unlawful activity

18 U.S. Code § 1960.Prohibition of unlicensed money transmitting businesses

All of which are viable options, but we see that across pretty much any site related.

Inter alia:

"among other things"

Considering the UK police and Netherland and Irish being involved probably eu

Evading - January 15, 2020, 4:53 pm

(Jan 15, 2020 05:44 PM)Mr. Robot Wrote: [\[CITE\]](#) The only thing I can guarantee -

>> If it's legit and was seized, it was done so by EU not US. Just in co-operation with a US led investigation.

18 U.S. Code § 981.Civil forfeiture

18 U.S. Code § 982.Criminal forfeiture

(982 is only applicable if //)

18 U.S. Code § 1956.Laundering of monetary instruments

18 U.S. Code § 1957.Engaging in monetary transactions in property derived from specified unlawful activity

18 U.S. Code § 1960.Prohibition of unlicensed money transmitting businesses

All of which are viable options, but we see that across pretty much any site related.

Inter alia:

"among other things"

<https://hackforums.net/showthread.php?tid=5819287>

Your thread from 2018, could be them pulling another prank.
Time will tell, I'm 50/50 as to whether it's real or fake atm.

? Soufian ? - January 15, 2020, 4:56 pm

(Jan 15, 2020 05:53 PM)Zine????????????????? Wrote: [\[CITE\]](#)
<https://hackforums.net/showthread.php?tid=5819287>

Your thread from 2018, could be them pulling another prank.
Time will tell, I'm 50/50 as to whether it's real or fake atm.
Pretty sure it aint.
What I find strange tho.. is the fact that they have a different style of seizing pages everytime.

Sometimes they host the image as a file, and link to it.
Now they've encoded it as base64 and embedded it in-line.

Sometimes they center it, sometimes it covers the full page etc

genesiseher - January 15, 2020, 4:58 pm

funny if true but looks fake asf to be honest as the actual domain would show it and the crop job is pathetic lol

Pronouncer - January 15, 2020, 4:59 pm

(Jan 15, 2020 05:58 PM)genesiseher Wrote: [\[CITE\]](#) funny if true but looks fake asf to be honest as the actual domain would show it and the crop job is pathetic lol
not true. do u know how many times actual sites have been raided and the police have only ever had domain or www.domain
working. The amount of times only one worked is insane

? Soufian ? - January 15, 2020, 5:00 pm

Plot twist: This is a media stunt.
Everyone talking about WLI again and media posting news.
Inb4 it'll be up again tomorrow.

Evading - January 15, 2020, 5:00 pm

(Jan 15, 2020 05:56 PM)? Soufian ? Wrote: [\[CITE\]](#) Pretty sure it aint.
What I find strange tho.. is the fact that they have a different style of seizing pages everytime.

Sometimes they host the image as a file, and link to it.
Now they've encoded it as base64 and embedded it in-line.

Sometimes they center it, sometimes it covers the full page etcYea it just looks off to me.
Spoiler ([Click to View](#))

genesiseher - January 15, 2020, 5:01 pm

(Jan 15, 2020 05:59 PM)Pronouncer Wrote: [\[CITE\]](#) not true. do u know how many times actual sites have been raided and the police have only ever had domain or www.domain
working. The amount of times only one worked is insane
ya could be true was just saying wtf is the image not covering whole page lol. looks like someone got it off shutterstock and tried to cut out the watermarks lol

Pronouncer - January 15, 2020, 5:02 pm

(Jan 15, 2020 06:01 PM)genesiseher Wrote: [\[CITE\]](#) ya could be true was just saying wtf is the image

not covering whole page lol. looks like someone got it off shutterstock and tried to cut out the watermarks lol
thats normal too

Mr. Robot - January 15, 2020, 5:04 pm

Right now if I had to put money on it, they looked at the IP addresses of their most used users - made sure to include those locations in the block to get attention.

I mean, could be wrong but i've seen a lot of sites go down in the past and this aint it chief.

Could also be they just want out.

? Soufian ? - January 15, 2020, 5:10 pm

What's also strange is the fact that their nameservers are still pointing to cloudflare.

Which means cloudflare gave away the backend. The domain registrar has no way to get the backend ip. So cloudflare could be the one to blame for this.

Pronouncer - January 15, 2020, 5:18 pm

(Jan 15, 2020 06:10 PM)? Soufian ? Wrote: [\[CITE\]](#) What's also strange is the fact that their nameservers are still pointing to cloudflare.

Which means cloudflare gave away the backend. The domain registrar has no way to get the backend ip. So cloudflare could be the one to blame for this.

Meh no a records

? Soufian ? - January 15, 2020, 5:23 pm

(Jan 15, 2020 06:18 PM)Pronouncer Wrote: [\[CITE\]](#) Meh no a records

Surely has NS records tho

Pronouncer - January 15, 2020, 5:24 pm

(Jan 15, 2020 06:23 PM)? Soufian ? Wrote: [\[CITE\]](#) Surely has NS records tho

whatsmydns.com

? Soufian ? - January 15, 2020, 5:24 pm

(Jan 15, 2020 06:24 PM)Pronouncer Wrote: [\[CITE\]](#) whatsmydns.com

genesiseher - January 15, 2020, 5:26 pm

(Jan 15, 2020 06:10 PM)? Soufian ? Wrote: [\[CITE\]](#) What's also strange is the fact that their nameservers are still pointing to cloudflare.

Which means cloudflare gave away the backend. The domain registrar has no way to get the backend ip. So cloudflare could be the one to blame for this.

if cloudflare is subpoena'd they have no choice but to give up the info they would have as in IP's, registration.

? Soufian ? - January 15, 2020, 5:26 pm

Right now only www. is working, and that one is on Cloudflare as well.

Omniscient - January 15, 2020, 5:47 pm

I call bullcrap because DNS is Cloudflare. Anyone know of any similar seizures we can review the DNS? I really doubt that the government bothers with having a CF account and redirects to it.

Domain seizure means they grab it at the registrar and take DNS control. What was DNS before? If it didn't change then domain was not seized.

Registrar not changed either.

It's publicity stunt.

Pronouncer - January 15, 2020, 6:56 pm

(Jan 15, 2020 06:47 PM)Omniscient Wrote: [\[CITE\]](#) I call bullcrap because DNS is Cloudflare.

Anyone know of any similar seizures we can review the DNS? I really doubt that the government bothers with having a CF account and redirects to it. Domain seizure means they grab it at the registrar and take DNS control. What was DNS before? If it didn't change then domain was not seized.

Registrar not changed either.

It's publicity stunt.

That would be a horrible horrible publicity stunt. It would hurt their image more than benefit them. Only the next few days will tell

(Jan 15, 2020 06:47 PM)Omniscient Wrote: [\[CITE\]](#) I call bullcrap because DNS is Cloudflare.

Anyone know of any similar seizures we can review the DNS? I really doubt that the government bothers with having a CF account and redirects to it. Domain seizure means they grab it at the registrar and take DNS control. What was DNS before? If it didn't change then domain was not seized.

Registrar not changed either.

It's publicity stunt.

From what it looks like it used to be ns1.weleakinfo.com and ns2

Moxxi - January 15, 2020, 7:05 pm

that screen looks so fucking fake and like something a memer or script kiddie would put onto a website to deface it or troll lol

Mr. Robot - January 15, 2020, 7:37 pm

(Jan 15, 2020 08:05 PM)Moxxi Wrote: [\[CITE\]](#) that screen looks so fugging fake and like something a memer or script kiddie would put onto a website to deface it or troll lol

tbh it actually resembles what they do actually use lmao someone would be mad if they read this.

sdsa8d7a - January 15, 2020, 7:43 pm

It was quite the run if it has come to this

Moxxi - January 15, 2020, 9:28 pm

(Jan 15, 2020 08:37 PM)Mr. Robot Wrote: [\[CITE\]](#) tbh it actually resembles what they do actually use lmao someone would be mad if they read this.

pretty funny though how script kiddie it looks lol

Party Parrot - January 15, 2020, 10:56 pm

i wonder what the process of all these agencies taking over a site actually consists of

genesiseher - January 16, 2020, 12:57 am

(Jan 15, 2020 11:56 PM)Party Parrot Wrote: [\[CITE\]](#) i wonder what the process of all these agencies

taking over a site actually consists of

1. FBI contacts cloudflare
2. cloudflare gives up all info they have on you.
3. the domain is then seized. with a cute image as you see it has now.
4. FBI contacts interpol to come arrest your ass.

done

as looks pretty dam legit if u notice cloudflare has kicked them to curb as no longer is on cloudflare DNS

<https://mxtoolbox.com/SuperTool.aspx?action=a%3aweleakinfo&run=toolpage>

Shisho - January 16, 2020, 2:38 am

(Jan 15, 2020 06:47 PM)Omniscient Wrote: [\[CITE\]](#) I call bullcrap because DNS is Cloudflare. Anyone know of any similar seizures we can review the DNS? I really doubt that the government bothers with having a CF account and redirects to it. Domain seizure means they grab it at the registrar and take DNS control. What was DNS before? If it didn't change then domain was not seized.

Registrar not changed either.

It's publicity stunt.

(Jan 15, 2020 06:26 PM)? Soufian ? Wrote: [\[CITE\]](#) Right now only www. is working, and that one is on Cloudflare as well.

<https://webcache.googleusercontent.com/search?q=cache:lhM3RkDmrlwJ:https://subdomainfinder.c99.nl/scans/2020-01-06/weleakinfo.com+&cd=4&hl=en&ct=clnk&gl=us>

<https://subdomainfinder.c99.nl/scans/2020-01-06/weleakinfo.com>

I found this cached result of a subdomain brute force done fairly recently on 01/06/2020 suggesting that their original name servers were actually CNAME records pointing at Cloudflare.

I'm currently scanning for any web page containing a portion of the base64 encoded seizure image to narrow down a netblock to scan for the original WeLeakInfo homepage.

? **Soufian ?** - January 16, 2020, 2:39 am

(Jan 16, 2020 03:38 AM)Shisho Wrote: [\[CITE\]](#)
<https://webcache.googleusercontent.com/search?q=cache:lhM3RkDmrlwJ:https://subdomainfinder.c99.nl/scans/2020-01-06/weleakinfo.com+&cd=4&hl=en&ct=clnk&gl=us>

<https://subdomainfinder.c99.nl/scans/2020-01-06/weleakinfo.com>

I found this cached result of a subdomain brute force done fairly recently on 01/06/2020 suggesting that their original name servers were actually CNAME records pointing at Cloudflare.

I'm currently scanning for any web page containing a portion of the base64 encoded seizure image to narrow down a netblock to scan for the original WeLeakInfo homepage.

That's actually my site ?

Scans don't get deleted, no need for cache:

<https://subdomainfinder.c99.nl/scans/2020-01-06/weleakinfo.com>

However,

It seems that this might be real.

As the following nameservers which they used:

ns1.weleakinfo.com

ns2.weleakinfo.com

Are not pointing to any A record anymore. Doubt that could be a part of a publicity stunt.

I believe the government might actually have their own Cloudflare account made just for seizing websites.

But the other strange thing is that the IP of the CF nameservers they use, is linked to many shady/malicious sites and files:

<https://www.virustotal.com/gui/ip-address/104.31.69.28/relations>

Which could mean they've been forced to deface themselves?

Shisho - January 16, 2020, 2:50 am

(Jan 16, 2020 03:39 AM)? Soufian ? Wrote: [\[CITE\]](#) That's actually my site ?

Scans don't get deleted, no need for cache:

<https://subdomainfinder.c99.nl/scans/2020-01-06/weleakinfo.com>

However,

It seems that this might be real.

As the following nameservers which they used:

ns1.weleakinfo.com

ns2.weleakinfo.com

Are not pointing to any A record anymore. Doubt that could be a part of a publicity stunt.

I believe the government might actually have their own Cloudflare account made just for seizing websites.

But the other strange thing is that the IP of the CF nameservers they use, is linked to many shady/malicious sites and files:

<https://www.virustotal.com/gui/ip-address/104.31.69.28/relations>

Which could mean they've been forced to deface themselves?

Cloudflare does serve traffic for millions of websites and generally does not vet them before providing service. This means that if a website is seen serving malicious content then the Cloudflare IP will be what shows up in a DNS lookup and, consequently, on a website that reports those findings.

? **Soufian** ? - January 16, 2020, 2:53 am

(Jan 16, 2020 03:50 AM)Shisho Wrote: [\[CITE\]](#) Cloudflare does serve traffic for millions of websites and generally does not vet them before providing service. This means that if a website is seen serving malicious content then the Cloudflare IP will be what shows up in a DNS lookup and, consequently, on a website that reports those findings.

I know CF serves traffic for millions of sites, but that's not the point.

But when I lookup the IP of the CF nameservers my sites are using, I come across a shitload of different sites, but I also see a few other projects of mine passing by, which are on the same CloudFlare account.

But having so many shady sites, literally almost only shady sites connected to these nameservers.. is quiet strange. But it could just be a coincidence which I want to assume it is.

Shisho - January 16, 2020, 3:05 am

(Jan 16, 2020 03:53 AM)? Soufian ? Wrote: [\[CITE\]](#) I know CF serves traffic for millions of sites, but that's not the point.

But when I lookup the IP of the CF nameservers my sites are using, I come across a shitload of different sites, but I also see a few other projects of mine passing by, which are on the same CloudFlare account.

But having so many shady sites, literally almost only shady sites connected to these nameservers.. is quiet strange. But it could just be a coincidence which I want to assume it is.

As much as I'd hate to disagree with you, based on information I've found online these particular name servers and the configuration they were using suggests a Business or Enterprise Cloudflare account:

<https://support.cloudflare.com/hc/en-us/articles/200169006-Setting-up-Custom-Nameservers-at-Cloudflare>

It's like saying Tech Featured is a shady site because they use 162.159.9.158 as a name server:

Code shisho@shisho:~\$ dig a server2.techfeatured.com

```
; <<>> DiG 9.11.14-1-Debian <<>> a server2.techfeatured.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53527
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;server2.techfeatured.com.    IN      A

;; ANSWER SECTION:
server2.techfeatured.com. 900    IN      A      162.159.9.158
```

SUI-3183372 - January 16, 2020, 7:07 am

Someone look up what other domains use BOTH of the name servers JOCELYN and PLATO. That will give a hint of the other domains associated with that CF account and could help verify if it's LE controlled or WLI controlled. If you search only one NS at a time, you'll have millions of results returned. But if you refine that search to domains using BOTH of those nameservers, you'll get a much smaller list of domains that could be associated.

Gashi - January 16, 2020, 7:50 am

Not surprised if it were to happen.

Pronouncer - January 16, 2020, 8:06 am

(Jan 16, 2020 01:57 AM)genesiseher Wrote: [\[CITE\]](#) 1.FBI contacts cloudflare
2. cloudlare gives up all info they have on you.
3. the domain is then seized. with a cute image as you see it has now.

4. FBI contacts interpol to come arrest your ass.

done

as looks pretty dam legit if u notice cloudflare has kicked them to curb as no longer is on cloudflare DNS

<https://mxtoolbox.com/SuperTool.aspx?action=a%3awebleakinfo&run=toolpage>

Yeah no that's a dumb way.

1. Arrest
2. Seize

Why would they seize then be like hey we are coming to arrest you.

Chances are they made no arrests because they couldn't find the owners however they did get access to servers and domains.

Cooligan - January 16, 2020, 8:38 am

Holy shit, it's crazy that that amount of countries wants their piece of the WLI pie lol.

NCA = National Crime Agency UK (there's actually even an official HF account for them as well)
PSNI = Police Service of Northern Ireland (UP THE IRA!!!)
FBI = Federal Bureau of Investigations (US)
DOJ = Department of Justice (US)
Politie = Netherlands Police
Bundeskriminalamt = Federal Criminal Police Office of Germany

Omniscient - January 16, 2020, 8:45 am

Quote:1.FBI contacts cloudflare

2. cloudflare gives up all info they have on you.
3. the domain is then seized. with a cute image as you see it has now.
4. FBI contacts interpol to come arrest your ass.

Again, a domain seizure happens at the registrar level and with the registry. If someone can find a legit site seized by FBI you can probably figure this out.

Looking at the list from Wikipedia wasn't too helpful.

https://en.wikipedia.org/wiki/Category:Seized_domain_names

But the BackPage you can see their Registrar Whois data and DNS for the domain were changed to something more LE like.

<http://whois.domaintools.com/backpage.com>

Just don't see FBI using CF unless they suddenly got smart and tired of DDOS attacks. :) Maybe. CF does have the best infrastructure around right now.

Well, if this isn't a stunt then the site is gone. Oh well. BTW, where is the FBI/DoJ press release on this? If it's legit why has it not been publicized by them?

flavoral - January 16, 2020, 8:50 am

(Jan 16, 2020 09:45 AM)Omniscient Wrote: [\[CITE\]](#) Well, if this isn't a stunt then the site is gone. Oh well. BTW, where is the FBI/DoJ press release on this? If it's legit why has it not been publicized by

them?

Same question. I keep checking for articles on Google or even Press releases on FBI's site, but there's none. The most recent/top article on Google even mentioning WLI is from OCT 2019.

Shisho - January 16, 2020, 8:55 am

(Jan 16, 2020 09:38 AM)Cooligan Wrote: [\[CITE\]](#) Holy Clay Davis, it's crazy that that amount of countries wants their piece of the WLI pie lol.

NCA = National Crime Agency UK (there's actually even an official HF account for them as well)

PSNI = Police Service of Northern Ireland (UP THE IRA!!!)

FBI = Federal Bureau of Investigations (US)

DOJ = Department of Justice (US)

Politie = Netherlands Police

Bundeskriminalamt = Federal Criminal Police Office of Germany

According to a few big, bad internet lawyers they are accessory to numerous crimes that have not yet been committed in basically every country because they're selling passwords and that's illegal.

The seizure notice looks like alphabet soup.

V?rt - January 16, 2020, 9:02 am

That sucks. I think it's pretty funny that they tried to make the page look cool, like a font text at the top, some cool "matrix hacking" lines in the back and all that

Cooligan - January 16, 2020, 9:03 am

(Jan 16, 2020 09:55 AM)Shisho Wrote: [\[CITE\]](#) According to a few big, bad internet lawyers they are accessory to numerous crimes that have not yet been committed in basically every country because they're selling passwords and that's illegal.

The seizure notice looks like alphabet soup.

It really does lol, they normally do honestly.

Like I said, everyone always wants a piece of the pie no matter what, especially in this day in age.

PrivateAlps - January 16, 2020, 9:37 am

(Jan 15, 2020 04:42 PM)Pronouncer Wrote: [\[CITE\]](#) Dunno if u noticed but the domain no longer points to a-records.

If you go to the [www. \(Instert WLI\) . com](http://www.(Instert WLI) . com) you will see its been seized RIP boys no more DB lookups

<https://ghostproject.fr>

?

Pronouncer - January 16, 2020, 9:39 am

(Jan 16, 2020 09:45 AM)Omniscient Wrote: [\[CITE\]](#) Again, a domain seizure happens at the registrar level and with the registry. If someone can find a legit site seized by FBI you can probably figure this out.

Looking at the list from Wikipedia wasn't too helpful.

https://en.wikipedia.org/wiki/Category:Seized_domain_names

But the BackPage you can see their Registrar Whois data and DNS for the domain were changed to something more LE like.

<http://whois.domaintools.com/backpage.com>

Just don't see FBI using CF unless they suddenly got smart and tired of DDOS attacks. :) Maybe. CF does have the best infrastructure around right now.

Well, if this isn't a stunt then the site is gone. Oh well. BTW, where is the FBI/DoJ press release on this? If it's legit why has it not been publicized by them?

Theres numerous reasons it could still be pointed to cloudflare. They could have gained access to the cloudflare and domain. Rather than just domain.

Often when domains are seized people have the idea that the police transfer the domain which is not true. EG When a domain was seized on ghandi they didnt move it or change registrar simply take access of the domain. The same can be said for cloudflare. The shitty style of the seize page is typical of the police being unable to have both www. and domain.tld working at the same time. Thats typical police fashion if looked at previous raids you will see that they never send tech people to a raid rather some braindead officer who tries and changes the a-records or cname records.

The reason there may not be a press release is because there could be no arresests. Normally the route goes Arrest then Seizure. However in the case there is no arrest there is very rarely any press release because they know they have only temporarily halted operation.

(Jan 16, 2020 09:55 AM)Shisho Wrote: [\[CITE\]](#) According to a few big, bad internet lawyers they are accessory to numerous crimes that have not yet been committed in basically every country because they're selling passwords and that's illegal.

The seizure notice looks like alphabet soup.

See compared to beenpwned they do many illegal things. Providing a DB search itself isnt illegal aslong as the DB's are from publicly available breaches however WLI have had numerous big private Databases.

The thing that also backs up the legitimacy was the website used to say "Operates under UK law" Thats not a normal location to choose, unless ofcourse you're from the UK which would explain the abundance of EU police forces including northern ireland which isnt a common one to see ever.

(Jan 16, 2020 10:37 AM)PrivateAlps Wrote: [\[CITE\]](#) <https://ghostproject.fr>
?

Also that site looks like utter dogshit. Did you really think using a french tld was a smart idea? or us9ing bookmyname was smart.

I swear this is how a bunch of HF kids get arrested every year trying to do shit out of their league without understanding basic principals

Evading - January 16, 2020, 10:38 am

(Jan 16, 2020 10:39 AM)Pronouncer Wrote: [\[CITE\]](#) See compared to beenpwned they do many illegal things. Providing a DB search itself isnt illegal aslong as the DB's are from publicly available breaches however WLI have had numerous big private Databases.

The thing that also backs up the legitimacy was the website used to say "Operates under UK law" Thats not a normal location to choose, unless ofcourse you're from the UK which would explain the abundance of EU police forces including northern ireland which isnt a common one to see ever.

Seeing the PSNI on there is so weird and if this is real the owner or one of the owner(s) must be living in Northern Ireland, otherwise it would have just been UK involvement and not Northern Ireland.

Pronouncer - January 16, 2020, 10:41 am

(Jan 16, 2020 11:38 AM)Zine????????????????? Wrote: [\[CITE\]](#) Seeing the PSNI on there is so weird and if this is real the owner or one of the owner(s) must be living in Northern Ireland, otherwise it would have just been UK involvement and not Northern Ireland.

i mean it would make sense that northern ireland be involved considering the site was stated to complyw ith UK law before they removed the snippet. Which includes northern ireland.

Considering they went out to remove the complying by UK law statement if they faked it why would they re-enforce something they hid? bit weird to give ur approx location away for a joke. Especially including ireland is a very very rare one to ever see

Evading - January 16, 2020, 10:51 am

(Jan 16, 2020 11:41 AM)Pronouncer Wrote: [\[CITE\]](#) i mean it would make sense that northern ireland be involved considering the site was stated to complyw ith UK law before they removed the snippet. Which includes northern ireland.

Considering they went out to remove the complying by UK law statement if they faked it why would they re-enforce something they hid? bit weird to give ur approx location away for a joke. Especially including ireland is a very very rare one to ever see

But if it's real there's definitely one of them living in Northern Ireland, if they were living in the UK the PSNI logo wouldn't have been on the site.

Pronouncer - January 16, 2020, 11:09 am

(Jan 16, 2020 11:51 AM)Zine????????????????? Wrote: [\[CITE\]](#) But if it's real there's definitely one of them living in Northern Ireland, if they were living in the UK the PSNI logo wouldn't have been on the site.

Kinda but not really. Even if they live in england or wales the Irish department would have been heavily involved with the raid so they would still appear. Its obvious who ever owns it is EU from the fact there is so mayn EU firms

? **Soufian ?** - January 16, 2020, 2:24 pm

(Jan 16, 2020 09:45 AM)Omniscient Wrote: [\[CITE\]](#) Again, a domain seizure happens at the registrar level and with the registry. If someone can find a legit size seized by FBI you can probably figure this out.

Looking at the list from Wikipedia wasn't too helpful.

https://en.wikipedia.org/wiki/Category:Seized_domain_names

But the BackPage you can see their Registrar Whois data and DNS for the domain were changed to something more LE like.

<http://whois.domaintools.com/backpage.com>

Just don't see FBI using CF unless they suddenly got smart and tired of DDOS attacks. :) Maybe. CF does have the best infrastructure around right now.

Well, if this isn't a stunt then the site is gone. Oh well. BTW, where is the FBI/DoJ press release on this? If it's legit why has it not been publicized by them?

Every seize is different and shouldn't necessarily look like another seize.

This is what I discovered after checking the source code of many sites that have been seized (booter providers).

Just like the link you've sent right now, they show an actual screenshot of the website as a background and the image is clickable.

While many other simply have this black seized page and non-clickable centered image.

So I'm not really sure what game they're playing over at the FBI or whether it's a different organization behind every seize (since they work together with Interpol etc.)

skipmaster82 - January 16, 2020, 2:54 pm

DOJ website - <https://www.justice.gov/usao-dc/pr/weleakinfo-com-domain-name-seized>

So ya.. it's legit.

Nyx - January 16, 2020, 3:04 pm

Most of the Dbs they used were public dumps or semi public ones that could be purchased off the darknet.

No doubt another lookup will come around. Anyone who bought lifetime on WLI has more than likely made there money back (illegaly) so I do not want to hear any complaints about people being scammed. You signed up for a lookup tool that was not strictly being used for whitehat users. Sure they "presented" themselves as that, but lets be realisitic, most users of WLI had malicious intent.

Pronouncer - January 16, 2020, 3:08 pm

(Jan 16, 2020 03:24 PM)? Soufian ? Wrote: [\[CITE\]](#) Every seize is different and shouldn't necessarily look like another seize.

This is what I discovered after checking the source code of many sites that have been seized (booter providers).

Just like the link you've sent right now, they show an actual screenshot of the website as a background and the image is clickable.

While many other simply have this black seized page and non-clickable centered image.

So I'm not really sure what game they're playing over at the FBI or whether it's a different organization behind every seize (since they work together with Interpol etc.)

The clickable image isnt too common when it comes to EU based raids. Backpages for example was heavily us based in terms of LE. However from this we can see its heavily EU based.

saianne - January 16, 2020, 3:26 pm

(Jan 16, 2020 04:11 PM)-Scrub Wrote: [\[CITE\]](#) Plenty of others out there . Just one gone .

It had many private databases.

I mean... at least our data is safe. Didn't they just seize the domain? Otherwise, I don't think they'd be asking for information on the owners, lol.

(Jan 16, 2020 04:04 PM)Nyx Wrote: [\[CITE\]](#) Most of the Dbs they used were public dumps or semi public ones that could be purchased off the darknet.

No doubt another lookup will come around. Anyone who bought lifetime on WLI has more than likely made there money back (illegaly) so I do not want to hear any complaints about people being scammed. You signed up for a lookup tool that was not strictly being used for whitehat users. Sure they "presented" themselves as that, but lets be realisitic, most users of WLI had malicious intent.

Yeah true.

I made hella off WLI, at least 15k usd

Voxi - January 16, 2020, 3:31 pm

I actually new the two founders years ago on their old aliases. It was eventually going to happen like the website before it (forgot the name), wonder if arrests were made?

Evading - January 16, 2020, 3:36 pm

Now that we know it's real, unlucky for them I guess.

Pronouncer - January 16, 2020, 3:39 pm

(Jan 16, 2020 04:31 PM)Voxi Wrote: [\[CITE\]](#) I actually new the two founders years ago on their old aliases. It was eventually going to happen like the website before it (forgot the name), wonder if arrests were made?

Arrests where not made. But considering how many people had contact with the owners and the owners having HF accounts it is only a matter of time till someone gives information on them.

Voxi - January 16, 2020, 3:39 pm

(Jan 16, 2020 04:39 PM)Pronouncer Wrote: [\[CITE\]](#) Arrests where not made. But considering how many people had contact with the owners and the owners having HF accounts it is only a matter of time till someone gives information on them.Deleted :P

Pronouncer - January 16, 2020, 3:54 pm

(Jan 16, 2020 04:39 PM)Voxi Wrote: [\[CITE\]](#) I know at least one of them has been arrested by the NCA before anyways on another alias although he is not from the UK.

Edit: I even have a photo of him on my old hard drive.
probably shouldnt be saying that stuff on a public forum when there is an open investigation on them.

Mr. Robot - January 16, 2020, 5:33 pm

(Jan 16, 2020 03:54 PM)skipmaster82 Wrote: [\[CITE\]](#) DOJ website - <https://www.justice.gov/usao-dc/pr/weleakinfo-com-domain-name-seized>

So ya.. it's legit.
Looks like it, took them long enough to publish

Zeffor - January 16, 2020, 7:11 pm

Damn, RIP. But like Silk Road, I believe another will come

Evading - January 16, 2020, 7:14 pm

(Jan 16, 2020 08:11 PM)Zeffor Wrote: [\[CITE\]](#) Damn, RIP. But like Silk Road, I believe another will come

And that's a fact.
There's a gap to fill and whoever fills it will make serious fuggin money.

Chilled - January 16, 2020, 9:50 pm

(Jan 16, 2020 04:31 PM)Voxi Wrote: [\[CITE\]](#) I actually new the two founders years ago on their old aliases. It was eventually going to happen like the website before it (forgot the name), wonder if arrests were made?Apparently they're yet to make any arrests and are asking for anyone with information to contact the FBI.

(Jan 16, 2020 04:39 PM)Voxi Wrote: [\[CITE\]](#) I know at least one of them has been arrested by the NCA before anyways on another alias although he is not from the UK.

Edit: I even have a photo of him on my old hard drive.
For their sake, and yours, I'd delete this comment. Silly thing to be flexing.

Cooligan - January 16, 2020, 10:00 pm

(Jan 16, 2020 12:09 PM)Pronouncer Wrote: [\[CITE\]](#) Kinda but not really. Even if they live in england or wales the Irish department would have been heavily involved with the raid so they would still

appear. Its obvious who ever owns it is EU from the fact there is so mayn EU firms
This and not to mention Northern Ireland is technically still under British rule so even if it was "just in Ireland" the Brits would still be involved if it happened in that part of Ireland.

#free the fookin' North

Accord - January 16, 2020, 10:05 pm

Theres still db look up but why fbi doesnt seized them, some db look up service has this tagline
Quote:is trusted by experts from law enforcement to major worldwide companies.

WANT3D - January 16, 2020, 10:51 pm

I won't say I am not fully shocked for it to turn out to be real. It didn't really seem like a true seizure at first glance, but hey, it is what it is.

Slim - January 16, 2020, 11:32 pm

OP, can you talk a little about why this was even seized? What's so special about it? Was it around for a long time? Was it a legal? What is a scenario in which this website would have been useful for white/grey/black hat individuals?

Bluffer - January 17, 2020, 12:32 am

Seems like others have said, a new one will popup immediately.

Surprised they don't just use the dark web for this.

Grim - January 17, 2020, 12:57 am

(Jan 17, 2020 01:32 AM)Bluffer Wrote: [\[CITE\]](#) Seems like others have said, a new one will popup immediately.

Surprised they don't just use the dark web for this.

They do and there's still hundreds just by googling not sure what they accomplished lol. There's even some on hf people sell

Mr. Robot - January 17, 2020, 1:06 am

(Jan 17, 2020 12:32 AM)Slim Wrote: [\[CITE\]](#) OP, can you talk a little about why this was even seized? What's so special about it? Was it around for a long time? Was it a legal? What is a scenario in which this website would have been useful for white/grey/black hat individuals?

Scenario:

I'm teaching websites and companies about digital security.

I use the website to enter their company domain.

I pull up results of vulnerable employees using the same passwords in multiple places, leading to vulnerable employees which can be used as leverage up a business.

Especially effective against lawyers.

//

Blackhat:

Well obvious.

//

Greyhat:

Useful for exploiting websites with password reuse attacks - then finding or making exploitable code in websites to then 'offer to patch' for others. Extremely effective.

Just some examples.

Credential reuse is extremely effective. Too many people don't know the basics.

1. Never use the same password in multiple places, not matter how strong you think it is. If one website doesn't use an encryption that's hard to break especially one without a salt - even worse if in plaintext - it can be found fairly fast.

2. Never use password permutations. Such as 123Google / 123Facebook or something people can figure out based on other website passwords.

Nate - January 17, 2020, 2:05 am

Not surprised, another one will pop up soon enough

Pronouncer - January 17, 2020, 3:18 am

(Jan 16, 2020 11:00 PM)Cooligan Wrote: [\[CITE\]](#) This and not to mention Northern Ireland is technically still under British rule so even if it was "just in Ireland" the Brits would still be involved if it happened in that part of Ireland.

#free the fookin' North
2 ARRESTED

<https://www.psni.police.uk/news/Latest-News/170120-weleakinfo.com-site-hosting-stolen-credentials-taken-down-after-international-operation/>

<https://www.nu.nl/tech/6024433/arnhemmer-aangehouden-voor-rol-bij-zoekmachine-met-miljarden-wachtwoorden.html?redirect=1>

(Jan 16, 2020 04:31 PM)Voxi Wrote: [\[CITE\]](#) I actually new the two founders years ago on their old aliases. It was eventually going to happen like the website before it (forgot the name), wonder if arrests were made?

yes

(Jan 16, 2020 08:14 PM)Zine????????????????????? Wrote: [\[CITE\]](#) And that's a fact. There's a gap to fill and whoever fills it will make serious fuggin money. there is no gap. There is hundreds of alterntives including leakedsource snusbase etc

LoRemIpsum - January 17, 2020, 3:25 am

(Jan 17, 2020 04:18 AM)Pronouncer Wrote: [\[CITE\]](#) 2 ARRESTED

<https://www.psni.police.uk/news/Latest-News/170120-weleakinfo.com-site-hosting-stolen-credentials-taken-down-after-international-operation/>

<https://www.nu.nl/tech/6024433/arnhemmer-aangehouden-voor-rol-bij-zoekmachine-met-miljarden-wachtwoorden.html?redirect=1>

A guy from Belgium as well as a guy from Ireland got arrested as I can say by the "nu.nl" link. \$2 to use the website for 24 hours is amazingly cheap. There are worse websites out there, like

pedophiles who hunt at innocent children, which I find 100x worse, but I assume some of the 'high class' are afraid to be exposed with their passwords being leaked.

More and more 'hackers' are caught, arrested or fined, while the real 'bad guys' are still out there. Pedophiles, black mailers, (child) human traffickers and much more. Anyway, leaking passwords could be harmful for many people and companies I assume, so that's where the priority is?

Pronouncer - January 17, 2020, 3:33 am

(Jan 17, 2020 04:25 AM)LoremIpsum Wrote: [\[CITE\]](#) A guy from Belgium as well as a guy from Ireland got arrested as I can say by the "nu.nl" link.

\$2 to use the website for 24 hours is amazingly cheap. There are worse websites out there, like pedophiles who hunt at innocent children, which I find 100x worse, but I assume some of the 'high class' are afraid to be exposed with their passwords being leaked.

More and more 'hackers' are caught, arrested or fined, while the real 'bad guys' are still out there. Pedophiles, black mailers, (child) human traffickers and much more. Anyway, leaking passwords could be harmful for many people and companies I assume, so that's where the priority is?

You say that and i dont disagree there are worse out. But think the amoubnt of damage this site has done, the amount of financial fraud that can be done because of all the information made accessible to random kids that think they are cool

Mr. Robot - January 17, 2020, 3:41 am

Honestly tempted to wipe my drive because of the DMs I get tbh, I access/accessed the website plenty and shared an account with someone else.

Mainly for tracking down pedos/scammers and helping people on HF and other places remove information from the internet. Otherwise it was for business use, helping companies secure themselves.

More concerned about the fact the account was shared.

>>Just feel like I was probably one of the most active users so if they did target the top usage i'd be in it with IP and all.

Accord - January 17, 2020, 3:43 am

(Jan 17, 2020 04:39 AM)Shkreli JGT Wrote: [\[CITE\]](#) Assuming you're referring to Snusbase, the difference between them and WeLeakInfo is that WLI were selling passwords. Snusbase just sells access to their website, which at least in the context of U.S. law is not a crime. Don't know about the United Kingdom.

Thank you for giving the differences about these two services, i didnt know what wli offer but i know theyre both db lookup.

Voxi - January 17, 2020, 4:26 am

(Jan 16, 2020 10:50 PM)Chilled Wrote: [\[CITE\]](#) Apparently they're yet to make any arrests and are asking for anyone with information to contact the FBI.

For their sake, and yours, I'd delete this comment. Silly thing to be flexing.
You quoted me so it doesnt make a difference now :/

Silent Uprising - January 17, 2020, 4:38 am

(Jan 17, 2020 05:26 AM)Voxi Wrote: [\[CITE\]](#) You quoted me so it doesnt make a difference now :/
I was gonna say that too lol. I mean likee both of you can remove your posts in regards to that

topic.

I did read on the news website thing that anyone who knew them or has extra evidence to come forward like the Ireland police. So yea maybe y'all should just delete posts XD

Chilled - January 17, 2020, 5:07 am

(Jan 17, 2020 04:41 AM)Mr. Robot Wrote: [\[CITE\]](#) Honestly tempted to wipe my drive because of the DMs I get tbh, I access/accessed the website plenty and shared an account with someone else.

Mainly for tracking down pedos/scammers and helping people on HF and other places remove information from the internet. Otherwise it was for business use, helping companies secure themselves.

More concerned about the fact the account was shared.

>>Just feel like I was probably one of the most active users so if they did target the top usage i'd be in it with IP and all.

Same here, bud. What's the legality surrounding looking up something? I'm sure that isn't a crime.

saianne - January 17, 2020, 5:33 am

(Jan 17, 2020 02:06 AM)Mr. Robot Wrote: [\[CITE\]](#) Scenario:

I'm teaching websites and companies about digital security.

I use the website to enter their company domain.

I pull up results of vulnerable employees using the same passwords in multiple places, leading to vulnerable employees which can be used as leverage up a business.

Especially effective against lawyers.

//

Blackhat:

Well obvious.

//

Greyhat:

Useful for exploiting websites with password reuse attacks - then finding or making exploitable code in websites to then 'offer to patch' for others. Extremely effective.

Just some examples.

Credential reuse is extremely effective. Too many people don't know the basics.

1. Never use the same password in multiple places, not matter how strong you think it is. If one website doesn't use an encryption that's hard to break especially one without a salt - even worse if in plaintext - it can be found fairly fast.

2. Never use password permutations. Such as 123Google / 123Facebook or something people can figure out based on other website passwords.yea true
weleakinfo helped me business wise

i definitely made a decent amount off it
some companies used databases to find chargebackers and stuff
idc if i get search warranted again

ToxicInfliction - January 17, 2020, 5:54 am

Damn I can't believe that it's legit. When I the web domain and the image it looked like something a person who used photoshop for 2 minutes created.

But, now that it is officially confirmed. R.I.P.

Also word of advice on passwords. I would use something of an auto generator to update your passwords. And if you keep the same password for even close to a month that is too long. I change my passwords often across things. I try to keep up with everything I have accounts on/for. But the number one way to prevent doxxing/hacking is keeping yourself low on activity and your names out of shit.

As for another site coming up I'm sure someone will prioritize filling that gap. As they will want to strive to make the money that's in it. So only a matter of time really.

? Soufian ? - January 17, 2020, 5:59 am

(Jan 17, 2020 04:41 AM)Mr. Robot Wrote: [\[CITE\]](#) Honestly tempted to wipe my drive because of the DMs I get tbh, I access/accessed the website plenty and shared an account with someone else.

Mainly for tracking down pedos/scammers and helping people on HF and other places remove information from the internet. Otherwise it was for business use, helping companies secure themselves.

More concerned about the fact the account was shared.

>>Just feel like I was probably one of the most active users so if they did target the top usage i'd be in it with IP and all.

I highly doubt they'll hunt the users. The providers are most important.
For the same matter you simply are a security researcher.

Arizonalce - January 17, 2020, 6:52 am

First leakedsource now WLI - sad times both HQ sites with good dumps. I don't think any site right now is on the same level as WLI.

Hopefully someone will step up soon - with good opsec this time

Gashi - January 17, 2020, 6:55 am

I do think it's strange how they got taken down. There are numerous of websites which police struggles talking down.

Where was it even hosted? Sounds like onshore.

Bambi - January 17, 2020, 6:57 am

Wait, how it works?

Do authorities just close down the website or they first need to find the owner, and tell him to shut it down ?

SIM-1729678 - January 17, 2020, 6:59 am

(Jan 17, 2020 07:55 AM)Gashi Wrote: [\[CITE\]](#) I do think it's strange how they got taken down. There

are numerous of websites which police struggles talking down.

Where was it even hosted? Sounds like onshore.

Check out the Irish article, New Zealand and some other country.

Gashi - January 17, 2020, 7:27 am

(Jan 17, 2020 07:59 AM)ScreemS Wrote: [\[CITE\]](#) Check out the Irish article, New Zealand and some other country.

Yeah as I thought, not the smartest location to host it at. Oh well, I've personally used that service my self to see databases I am connected to.

Description - January 17, 2020, 7:52 am

well, they lasted awhile didn't they?

Evading - January 17, 2020, 7:54 am

(Jan 17, 2020 04:41 AM)Mr. Robot Wrote: [\[CITE\]](#) Honestly tempted to wipe my drive because of the DMs I get tbh, I access/accessed the website plenty and shared an account with someone else.

Mainly for tracking down pedos/scammers and helping people on HF and other places remove information from the internet. Otherwise it was for business use, helping companies secure themselves.

More concerned about the fact the account was shared.

>>Just feel like I was probably one of the most active users so if they did target the top usage i'd be in it with IP and all.

Did they ever go after any customers from leakedsource or any of the other alternatives?

Maxorg - January 17, 2020, 8:14 am

There seems to be a lot of seizures recently.

Evading - January 17, 2020, 1:45 pm

(Jan 17, 2020 09:14 AM)Maxorg Wrote: [\[CITE\]](#) There seems to be a lot of seizures recently.Such as?

Pronouncer - January 17, 2020, 2:23 pm

(Jan 17, 2020 04:39 AM)Shkreli JGT Wrote: [\[CITE\]](#) Assuming you're referring to Snusbase, the difference between them and WeLeakInfo is that WLI were selling passwords. Snusbase just sells access to their website, which at least in the context of U.S. law is not a crime. Don't know about the United Kingdom.

Snusbase is illegal too

(Jan 17, 2020 07:55 AM)Gashi Wrote: [\[CITE\]](#) I do think it's strange how they got taken down. There are numerous of websites which police struggles talking down.

Where was it even hosted? Sounds like onshore.

Germany and some other country I forgot

sdsa8d7a - January 17, 2020, 2:49 pm

(Jan 17, 2020 04:41 AM)Mr. Robot Wrote: [\[CITE\]](#) Honestly tempted to wipe my drive because of the DMs I get tbh, I access/accessed the website plenty and shared an account with someone else.

Mainly for tracking down pedos/scammers and helping people on HF and other places remove information from the internet. Otherwise it was for business use, helping companies secure

themselves.

More concerned about the fact the account was shared.

>>Just feel like I was probably one of the most active users so if they did target the top usage i'd be in it with IP and all.

I can't find any instance of leak base or leaked source customers getting targeted.

Mix - January 17, 2020, 5:30 pm

Give it a week or two and they will release a new site called WeDontLeakInfoWeSwear

Mr. Robot - January 17, 2020, 7:14 pm

(Jan 17, 2020 06:30 PM)Mix Wrote: [\[CITE\]](#) Give it a week or two and they will release a new site called WeDontLeakInfoWeSwear

Not even going to lie, all the time I have used their site - I never actually clicked "We Leak Info"

I'm stoopid

SIM-4033767 - January 18, 2020, 11:27 am

(Jan 15, 2020 04:42 PM)Pronouncer Wrote: [\[CITE\]](#) Edit: To anyone who thought it was fake here u go <https://www.justice.gov/usao-dc/pr/weleakinfo.com-domain-name-seized>

edit 2: arrests made

<https://www.nu.nl/tech/6024433/arnhemmer-aangehouden-voor-rol-bij-zoekmachine-met-miljarden-wachtwoorden.html?redirect=1>

<https://www.psni.police.uk/news/Latest-News/170120-weleakinfo.com-site-hosting-stolen-credentials-taken-down-after-international-operation/>

Dunno if u noticed but the domain no longer points to a-records.

If you go to the www. (Insert WLI) . com you will see its been seized RIP boys no more DB lookups

SHIEEEEEEEEEET ?