

WebBreacher's Hacking and Hiking Blog



≡ MENU



Harvesting Whois Data for OSINT

```
Domain Name: FARRELLSWEBSERVICE.COM
Registry Domain ID: 383287028_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.enom.com
Registrar URL: www.enom.com
Updated Date: 2016-03-16T04:34:19.00Z
Creation Date: 2006-03-20T21:40:51.00Z
Registrar Registration Expiration Date: 2017-03-21T01:40:51.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Reseller: ICDSOFT.COM
Domain Status: clientTransferProhibited https://www.icann.org/epp#cli
Registry Registrant ID:
Registrant Name: KEITH FARRELL
Registrant Organization:
Registrant Street: 938 GREENWOOD ROAD
Registrant Street: NA
Registrant City: WINCHESTER
Registrant State/Province: VA
Registrant Postal Code: 22602
Registrant Country: US
Registrant Phone: +1.5407230087
Registrant Phone Ext:
Registrant Fax: NA
Registrant Fax Ext:
Registrant Email: PEZMAN1960@VERIZON.NET, KEITH.FARRELL@DHS.GOV
Registry Admin ID:
```



At work I was given the task of figuring out at least one method to find some of the domains that were registered by my company's employees but that we may not have known that they registered. Anyone can visit GoDaddy or PSI or landl and register a domain. We wanted to find out anyone that that registered a domain with

an “@MYCOMPANY.com” email in the domain registry. Once I figured out how to do this, I found some really interesting things!

Registering a Domain

In case you don't know this, when someone registers a domain name like “webbreacher.com” or “osint.ninja” they use a registrar such as Go Daddy or Network Solutions who then does the work of reserving the domain and tagging it as owned by a certain person/organization. There is some personal or business information that you must provide to the registrar for them to make the registration of the domain you want. Most will want your credit card info first 😊 and also personal information such as your name, home/business address, phone, and email(s).

Personal v. Private Registrations

When you register a domain, many times you have the choice to have the registrar “mask” your personal information that you use to purchase the domain. This is helpful to keep your personal information, well, personal. Instead of using your personal data, the registrar uses their data and then keeps track, internally, who is

the actual owner of the domain. For my purposes of finding out what employees are registering domains using our company email address, this masking of their info presents a problem.

Whois

One of the main tools that people use on unix, linux and Mac systems to look up the registration information about a domain is called *whois*. From a command line or terminal window, a user can type *whois example.com* and the registration information for that domain will be returned. This should include names, emails, phone numbers and more...unless the registrant is using the whois masking feature of their registrar.

Some caveats here are that whois data is many times stale, old, or just very wrong. Many registrars never check the information that is self-submitted when registering a domain. If I wanted to register *insertmydomainhere.info* as Barack Obama at 1600 Penn Ave, Washington, DC, there are some registrars that would be happy to take my money. Take whatever responses from whois as suspect data until verified or corroborated with other information.

Using whois is great if you want to retrieve the information about a single domain. In my case, I wanted to search ALL domains for any registration information with my company's email address domain. Using whois for my task, I'd need to request every single domain name with whois and then scrape the results for "@example.com" to complete my task. Laborious if not impossible.

ViewDNS.info

The best place I found that had a reverse whois lookup that would allow the searching of whois data using registrant information AND wildcards (such as *) was the viewdns.info site. Let's show an example using the *dhs.gov* domain. Using the ViewDNS web page at <http://viewdns.info/reversewhois/?q=%40dhs.gov> you can retrieve the first 500 hits on domains having the *@dhs.gov* string in them somewhere. Below are some of the results.

Reverse Whois results for @dhs.gov

=====

There are 88 domains that matched this search query.
These are listed below:

Domain Name	Creation Date	Registrar
applesandfriends.com	2007-11-29	GODADDY.COM, LLC
applesandgrapes.com	2007-11-29	GODADDY.COM, LLC
asisaustintx179.org	2010-03-24	DOMAIN.COM, LLC
asistxgulfcoast.org	2010-03-08	DOMAIN.COM, LLC
bethlehemcog.org	2015-11-17	MELBOURNE IT, LTD
birthonomics.com	2013-01-29	GODADDY.COM, LLC
blainemwr.com	2011-02-02	ENOM, INC.
borderlinesupply.com	2005-05-27	GODADDY.COM, LLC
bostonjrhuskies.com	2016-01-14	GODADDY.COM, LLC
bostonjuniorhuskies.com	2016-01-27	GODADDY.COM, LLC
carusconsult.com	2008-09-20	TUCOWS DOMAINS INC.
cectf.com	2011-06-29	ENOM, INC.
cectf.net	2011-06-29	ENOM, INC.
celticwarriorsmc.com	2014-03-29	GODADDY.COM, LLC
cheekrisers.com	2013-03-07	GODADDY.COM, LLC
chiectf.com	2011-06-29	ENOM, INC.
chiectf.net	2011-06-29	ENOM, INC.
crossfitpistoleros.com	2014-10-16	GODADDY.COM, LLC
dancommiato.com	2012-02-25	REGISTER.COM, INC.
dhsaapin.org	2011-12-12	NETWORK SOLUTIONS, LLC
dhsheadquarterstrainingcenter.org	2014-12-12	1 & 1 INTERNET AG
disastergypsy.com	2013-12-11	GODADDY.COM, LLC
epsmwr.org	2014-02-03	GODADDY.COM, LLC
farrellswebsevice.com	2006-03-21	ENOM. INC.

feaeep.org	2007-12-28	TUCOWS INC.
fema.net	1996-03-22	NETWORK SOLUTIONS, LLC.

This was a huge time saver for me. ViewDNS also has a great API to pull these records down in XML and JSON formats which are easily used in scripts and other programs.

So...I was happy and yet confused. I thought that there may be something wrong with the site. Looking at the bottom of the above picture, you can see that *fema.net* is a domain that has the *@dhs.gov* string in the registration somewhere. This makes sense since *fema.gov* is a DHS entity and *fema.net* is something DHS might register to prevent someone else from registering it and tricking users. But, did you see the *farrellswebservice.com* and *celticwarriorsmc.com* domains? Those do not look like DHS domains. Let's take the *farrellswebservice.com* domain and do a command line whois on it.

```
Domain Name: FARRELLSWEBSERVICE.COM
Registry Domain ID: 383287028_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.enom.com
Registrar URL: www.enom.com
Updated Date: 2016-03-16T04:34:19.00Z
Creation Date: 2006-03-20T21:40:51.00Z
Registrar Registration Expiration Date: 2017-03-21T01:40:51.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Reseller: ICDSOFT.COM
Domain Status: clientTransferProhibited https://www.icann.org/epp#cli
Registry Registrant ID:
Registrant Name: KEITH FARRELL
Registrant Organization:
Registrant Street: 938 GREENWOOD ROAD
Registrant Street: NA
Registrant City: WINCHESTER
Registrant State/Province: VA
Registrant Postal Code: 22602
Registrant Country: US
Registrant Phone: +1.5407230087
Registrant Phone Ext:
Registrant Fax: NA
Registrant Fax Ext:
Registrant Email: PEZMAN1960@VERIZON.NET, KEITH.FARRELL@DHS.GOV
Registry Admin ID:
```



Well that solves it. There was no problem with the web site. Under the red arrow is the @dhs.gov email account that the viewdns.info site found: keith.farrell@dhs.gov.

Moving into OSINT

I hear some of you saying “So what?” Well, in the world of OSINT we try to tie pieces of data together. Getting email addresses, phone numbers and addresses for people is key to furthering investigations. We can use this data as pivot points (additional search terms to use to find even more information about a target) to augment your OSINT data. In the above pic for the whois output of the *farrellsweb service.com* domain, we have all of these pieces. Keith Farrell’s name, home address, phone number, personal and business email addresses are out there in the public for anyone to harvest.

So what happened here? It seems like some people use their work emails for personal registrations. While I only use my work email for work purposes, I do know people that use their work email for non-work purposes.

Reverse Email Search

We have completed a forward search for domains that have whois data with @domain.tld (ex., @dhs.gov). Kirby (<https://twitter.com/kirbstr>) noted that we can perform a reverse whois lookup for any of the email results that we obtain from our first search.

So let's say that we performed our first wildcard domain search for @domain.tld. It returned 3 results where the contact email addresses found were:

- mary@domain.tld
- rashid@domain.tld
- quan@domain.tld

What we would then do is perform another reverse whois lookup for each of those email addresses to find out what other domains they are registered to. This widens our understanding of what domains (and possibly outside-of-work activities) the people behind these emails are participating in or care about.

Applying this Information

OK. So we can easily pull up all the domains registered with a certain email domain. Again, so what? Well, what if those domains showed interests of the employees of that company? What if they showed personal information or pictures of a person's family? In fact, if you visit some of those domains from our results above in a web browser, that is exactly what you get. Check out <http://farrellswebservice.com/> and <http://bostonjrhuskies.com/>.

So now we have:

- First and last name
- Home address
- Phone number(s) which may be work and or personal
- Email(s) which are work and may also be personal
- Personal interests
- Pictures of family
- In some cases we have much MUCH more (check out <http://www.crossfitpistoleros.com/>)

Attackers could use this information:

- For reconnaissance prior to a cyber or physical attack to gather information
- Phishing or pretexting data to better-craft emails or scripts that victims may fall for
- Social engineering
- Espionage....and so on

We can also take this data, export it to a CSV (Comma Separated Value) file and import it into a spreadsheet program or visualization app like Paterva's Casefile

(free – <http://paterva.com/web7/buy/maltego-clients/casefile.php>). Doing that, we can see connections in the data such as all domains registered on a certain date or by a specific registrar. This data can help you determine if a specific domain was registered by the organization and is most likely a work domain or if someone else may have registered it.

Automating with Python

If you would like to use the ViewDNS API (<http://viewdns.info/api/> – You need at least the \$40/month level for reverse Whois to work), then I may have a nice script you can use to automate the lookup a domain process. Check out <https://github.com/WebBreacher/emailwhois> for some code and docs.

Conclusions

How do you prevent this? Most domain registrars allow you to make your domain registrations “private” or “masked” so that, instead of your personal (or work) information being displayed when someone looks up the domain registration, it is the information of the registrar that is shown. For example, let’s look at what the whois data for the osint.ninja domain are:

```
└─> $ whois osint.ninja
Domain Name: osint.ninja
Domain ID: 63028534bbde4621a2ec4f70ad0845a0-RSIDE
WHOIS Server: www.godaddy.com
Referral URL: http://www.godaddy.com
Updated Date: 2016-05-02T00:31:23Z
Creation Date: 2016-02-07T22:48:41Z
Registry Expiry Date: 2017-02-07T22:48:41Z
Sponsoring Registrar: GoDaddy.com, LLC
Sponsoring Registrar IANA ID: 146
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhib
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant ID: cr231186803
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com 14747 N Northsight Blvd Suite 111, PMB 309
Registrant City: Scottsdale
Registrant State/Province: Arizona
Registrant Postal Code: 85260
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: osint.ninja@domainsbyproxy.com
```

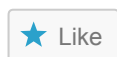
When I registered that domain, I selected to pay a little additional and have GoDaddy replace my personal information with some generic information pointing to their systems. Anyone having an issue with the domain (or network traffic coming from it) could contact GoDaddy and then they would know to contact me.

Additionally, try to limit the places where you use work information for personal purposes especially if that data is or could become public.

For all you OSINT people out there, I bought the \$20/month API access to viewdns.info's data and have scripted this process (and doing subsequent lookups). It does require an API key from the site. If this is something you do regularly, I highly recommend purchasing the API key. Oh, if you are thinking of just scraping the data from the web site...don't. Viewdns.info actively blocks IP addresses that do this. Trust me. I still cannot get to this site from home. 😞

Like this post? Tweet to me [@OsintNinja](#) or [@Webbreacher](#).


SHARE THIS:



Be the first to like this.

🕒 August 9, 2016

 infosec, osint, python

 infosec, osint, whois

 Career Days

 Mind over body

COMMENTS ARE CLOSED.

SEARCH

Search ...



TOP 5 POSTS

» [OSINT Map: A MindMap for Your Investigations](#)

- » [Videos](#)
- » [Introducing OSINT YOGA](#)
- » [Recon-ng: Profiler Module](#)
- » [Projects](#)

RECENT POSTS

- » [2020-May SANS @MIC: “Moving Past Googling It” Companion Post](#) May 20, 2020
- » [2020-March SANS @MIC: “Moving Past Googling It” Companion Post](#) March 16, 2020
- » [2019 Layer8 Conference “Getting the Good Stuff” Talk Companion Post](#) June 8, 2019
- » [Consumer Reports Article on Privacy](#) April 11, 2019
- » [It has been a while...](#) February 18, 2019

POST CATEGORIES



FOLLOW BLOG VIA EMAIL

Enter your email address to follow this blog and receive notifications of new posts by email.

Follow



FOLLOW ME ON TWITTER

Tweets by @WebBreacher



Micah

@WebBreacher



Cantaloupe with nacho chili powder and cayenne. Yes please!





1h



Micah

@WebBreacher



Tonight is the final night of my 2 week-long [#LiveOnline](#) [#SEC487](#) [#OSINT](#) class which ran 5 hrs/day Mon-Fri 8a-1p Singapore time.

We have talented students from Australia, the Middle East, North America, and Europe. Thank you students! [#sec487AroundTheWorld](#)



5h



Micah Retweeted



Jake Williams

@MalwareJake

This [@washingtonpost](#) COVID-19 analysis is amazingly awesome. But you know who I'd like to see this sort of easily usable data from? The CDC...[washingtonpost.com/politics/2020/...](#)

The good news for Trump is that, the move from Charlotte to Jacksonville like appears like a side case. More.

CATEGORY CLOUD

Backpacking boy scouts conference enumeration high school Hiking infosec job kids Moab network
Network Security Monitoring NSM osint password pentest philmont privacy python recon-ng SANS
sec487 security securityunion teaching travel Untangle Utah webapp wifi

FOLLOW BLOG VIA EMAIL

Enter your email address to follow this blog and receive notifications of new posts by email.

Follow



RECENT POSTS

- » [2020-May SANS @MIC: “Moving Past Googling It” Companion Post](#)
- » [2020-March SANS @MIC: “Moving Past Googling It” Companion Post](#)
- » [2019 Layer8 Conference “Getting the Good Stuff” Talk Companion Post](#)
- » [Consumer Reports Article on Privacy](#)
- » [It has been a while...](#)
- » [We are OSINTCurious!](#)

A WORDPRESS.COM WEBSITE.

UP ↑