+44 345 094 0945
www.waterstons.com

Article

Jul 2021

How good enumeration and a little Open Source Intelligence can lead to a deep compromise

HIC SUNT DRACONES - Here Be Dragons

Image Credit: https://unsplash.com/@clintbustrillos

Old maps would inscribe unexplored seas with HIC SUNT DRACONES to indicate the presence of unknown dangers. Specifically, dragons. While my history teacher may be glad to know I retained something from his lectures, this serves as a good analogy for the infrastructure that has fallen off most organisation's maps. One thing that has always stood true for me is that, if I can't immediately find an exploit path into an infrastructure, I simply haven't looked hard enough.

This rings true for almost every organisation I have performed Open Source Intelligence (OSINT) on. While many organisations are beginning to see the value in rigorously testing and monitoring the security of their infrastructure, still we see attackers finding entrance through old secondary links with different firewall rules, web servers that were spun up for a trade show in 2015 and forgotten, employee computers outside of their corporate environment etc. I really could go on.

However, it is exactly that which lead to the LinkedIn breach of 2012. This was one of those big nasty breaches that generated a LOT of conversation around both the importance of seasoning password hashes stored in a database with 11 herbs and spices and employee password reuse. Suddenly an entire database of industry professionals and their crack-able passwords were in the public domain and of course, this was the basis for most news and conversation. However, there is a more interesting conversation to be had here that was largely overlooked; exactly how was the perimeter breached?

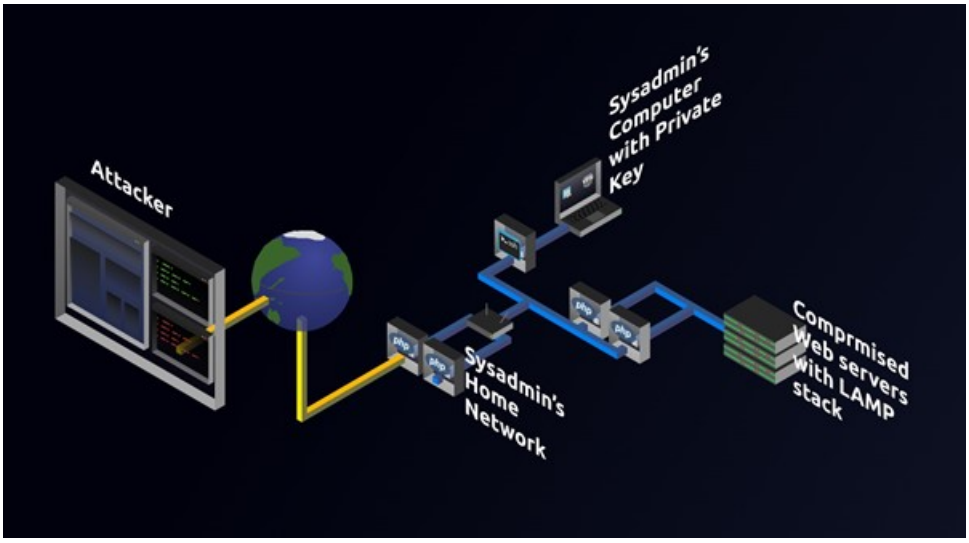
> **"It's like stalking a person or a business on Facebook or Instagram, but if Law Enforcement or Debt Collectors were doing it."**

Being a social media giant, you would expect LinkedIn to have excellent security. Given their size, excellent talent, and capability, they absolutely did, and still do. So surely it took a master hacker to pull this off. Simply put, it didn't take a genius, it only took some OSINT or Open-Source Intelligence.

When I need to describe OSINT to a layman, my typical example is "It's like stalking a person or a business on Facebook or Instagram, but if Law Enforcement or Debt Collectors were doing it."

In the case of LinkedIn's 2012 breach, our attackers used LinkedIn itself to find people who worked there that would likely have privileged access. That is, system administrators, engineers, database administrators etc. With a list of these users, they then began searching for any information they could find. In this case, one of the System Administrators had been hosting web servers from his house.

One of these webservers was vulnerable to a simple PHP upload attack and attackers were able to breach it, getting full control. This gave them access to a computer in this System Admin's internal home network. From there it was simply a matter of searching for the computer this employee used to work remotely and brute-forcing his password. From here, they were able to acquire his private key and other LinkedIn VPN/Server related information. Now, for brevity's sake, this is a super simplified version of this story, I would highly recommend giving Episode 86 of Darknet Diaries a listen if you would like to hear the events in their entirety.



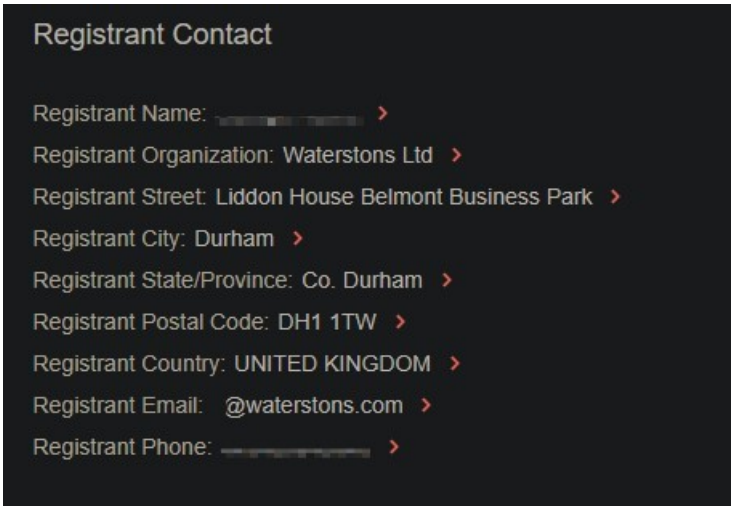
My point however stands that regardless of the talent or money poured into security systems, monitoring etc, the attacks that occurred in this example were completely off LinkedIn's map. Not even a blip on their radar. But what is stopping these things from being picked up? Especially when more and more organisations are engaging penetration testers and others with these abilities to review their infrastructure. Simply put, the scope is outlined when they are engaged. There is a specific thing being tested and nothing else.

What does a test like this look like though? What is the process for performing something like this? I teach it as "the iteration and transformation of information". Simply put, take a single piece of information, see what can be gleaned from it, transform it, and then repeat. For example. Say I want information on Waterstons Australia. How do I begin? First up, simply google the name.

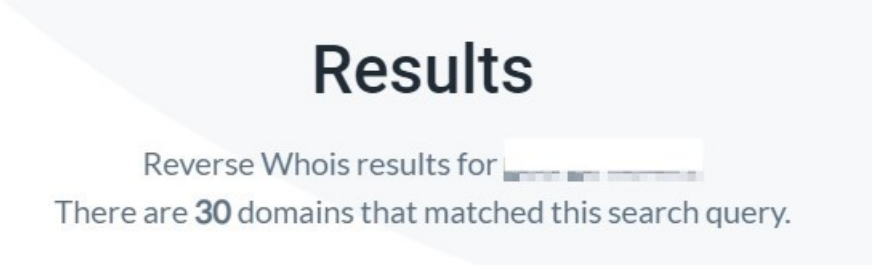
Immediately I have the office location, operating hours, a domain, etc. So now I have more information to iterate on. Let's start with the domain. If I take waterstons.com and check who owns it, what do I get?

```
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Co. Durham
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: GB
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
```

A lot of redacted information. Not super useful. Likely it wasn't always redacted though, what happens if I look at the historical records?



I find that the details were published earlier this year. Far more information than is currently available. We have a name, a location of our UK office, an E-mail address, a phone number, etc. From here we iterate onwards with new information. For example, the registrant's name, what other websites has this person registered?



I now have 30 websites that may have been registered by that contact. Now this is just 3 iterations from the domain name. Sure, I have some tools and experience at my disposal, however, this information is essentially freely available and in the public domain. Imagine if I scraped LinkedIn for all staff, searched all the subdomains, found related domains (waterstons.co.uk etc) and subdomains (mail.waterstons.com), looked at every port that was open on every IP address owned by the organisation, looked through the domain history etc.

You start to get the picture. This is how an attack surface is mapped out. And while scary it may be, that's kind of my point. A map of your organisation shouldn't simply be drawn from the inside out, it should be from the outside in. Here be dragons.

If you'd like to learn more about our offering or have a chat about what we could do to help secure your organisation, please don't hesitate to reach out to Andrey, our APAC Head of Customer Success who is always keen to understand your business and it's needs andrey.derevyanko@waterstons.com. Or even drop a line through to info@waterstons.com