I Can See You! (OSINT)

I Can See You! Open Source Intelligence (OSINT)

Categories

- Announcements
- Application Security
- Best Practice Security
- Blog
- Cloud
- Cyber Essentials
- Forensics
- GDPR
- GRC
- ITHC
- Malware
- Network Security
- Penetration Testing
- Phishing

Who is looking at your information?

Welcome to no. 4 of our Breakfast Series by Perspective Risk's senior cyber security consultant Abdul Ikbal.

These posts are designed to give you some insights into the world of information security over your cornflakes. If there's no free plastic toy in your box, expect to find some goodies here.

Whether you're looking to improve your organisation's security or have an interest in working in infosec, read on. And if you missed our earlier

- Red Team
- Uncategorized

- May 2019 (1)
- March 2019 (
- November 2018 (
- October 2018
- August 2017 (1)
- July 2017 (2)
- June 2017
- May 2017 (4)
- April 2017 (4)
- March 2017 (5)
- February 2017 (4)
- January 2017 (5)
- December 2016 (6)
- November 2016 (4)
- October 2016 (4)

posts, you can catch them here: How I break into your building, Top Tips for PenTest Interview and Can I has your password?

What Public Information Could Be Risking Your Information Security?

During Red Team engagements one of my goals is to find as much information as I can about you using only publicly available resources, mostly through the Internet. This technique is referred to as OSINT, or Open Source Intelligence. *Wikipedia Open-source intelligence*.

This should probably have been the first of the breakfast series. However, it's not as cool as breaking into your office or convincing your team to give me their passwords. That said, whatever information about you is out there is potentially critical to your security.

Open Source Intelligence is done to support the later phases of a red team engagement, such as those mentioned above. At the end of this post, there's an **opportunity to obtain a free OSINT report for your organisation.**

I need to identify all available information on your company. How do I do this? Interwebs! You freely provide everything I need by posting lots of information on the Internet. And why wouldn't you? Your business model, your clients and employees demand it – that's how it is. Lucky for cyber criminals, risky for you.

- September 2016 (4)
- August 2016 (1)
- July 2016 (2)
- January 2016 (1)
- June 2015 (1)
- April 2015 (1)
- September 2014 (1)
- July 2014 (1)
- September 2013 (2)
- May 2013 (2)
- April 2013 (1)
- March 2013 (2)
- January 2013 (1)
- November 2012 (2)
- October 2012 (3)
- June 2012 (1)
- February 2012 (4)

When researching your organisation, here's what I will focus on:

Your Company Website – Rich Pickings for Cyber Criminals

Your website could be sharing details which make you vulnerable to those with nefarious intentions. When conducting OSINT intelligence, your website is my first go-to source to identify your email structure. You might make it very easy for me by listing the email addresses for many of your employees.

How can you fix this? Simple. Don't provide employee specific email addresses. Granted this may jar with the open-doors impression your sales or marketing teams seek, but there has to be a balance with your information security.

Consider the damage a hacker could do with your Head of Finance's contact details. Phishing emails are increasingly sophisticated and, considering I just need one person to click on my link, my success rate is 100%. Phishing is done by phone as well as email, so direct telephone numbers are also a bad idea.

LinkedIn / Social Networking Sites

LinkedIn is a powerful tool for professional networking and learning but it's seen an increase in the number of unprofessional posts seeking likes and shares. It's another gateway to your organisation's email structure and I can use the platform to work out who reports to who and use that as leverage.

- January 2012 (2)
- August 2011 (1)

How can you fix this? It's a tough one – you can't force your employees to hide their profiles from public view or have a partial name as opposed to their full names. You could consider a company policy stipulating that your employees don't disclose their place of work or post company details on other social networking sites.

Other websites revealing your contact details

Searching Google manually is so 2015, who does anything manually nowadays? I use the following tools that allow me to find email addresses and phone numbers for your employees with a click of a button:

- Hunter
- RocketReach

Fixing this could prove tricky. You may have some luck contacting the vendors and request them to remove your details. It will be interesting to see how these sites are affected with the introduction of the General Data Protection Regulation (GDPR).

Your Breached Data (whether you know it or not)

Once I've identified your email addresses, I will search publicly available breach records to check whether any of your details, including passwords, were compromised in the past. It's worth mentioning that if employees are in the habit of reusing passwords, it enables attackers to gain access to other systems, i.e. beyond those already breached.

This site by Troy Hunt allows me to check if your data has been breached before: have i been pwned?

Fix this by getting employees to change passwords and not reuse them. Also, Hunt is a pretty helpful chap and will remove information about your employees on request.

Your Domain Name System (DNS) records to identify your sub-domains

Using the breached accounts I have found, I would then use the passwords to login to the systems owned by your company. For example:

- email.acme.com
- remote.acme.com
- support.acme.com

And how can a determined Internet user like me find this information? With your Domain Name System (DNS) records. Your technical and web management teams should be able to make appropriate changes to your infrastructure to conceal your sub-domains.

Your Vulnerable Technologies

All technology leaks some sort of information, be it your website or your infrastructure (including sub-domains) exposing the underlying software and versions. A Google search will tell me what each technology is

vulnerable to. And guess what? If it's outdated or hasn't had patches applied for a while I may have found my way in!

Tips for Improving your Information Security

Here are steps you can take today to protect your business and your employees from the predators out there:

- Ensure that all technology in place is kept patched and remove all verbose information
- Remove personally identifiable email addresses and telephone numbers from your websites
- Ensure employees are aware of an acceptable company use policy
- Contact other website vendors to remove personally identifiable company information
- Check if your employees contact details or passwords have been breached. If so, ensure they change their passwords and contact have i been pwned? to remove their information
- Advise your technical teams to keep your technology and sub-domain leakage to a minimum; we can help them with this if needed

Request your Free OSINT Report and plug the gaps in your security

Perhaps you don't have the expertise in-house to conduct your own OSINT exercise, or you do but lack the time. A customised OSINT report identifies the sensitive or risky data you are sharing, often unknowingly. It

includes actionable information, allowing you to prioritise your risk management activities.

Take a step towards improving your organisation's resilience to cyber crime and click here to request your free OSINT report.

Category: Blog, Network Security, Red Team

- Supplier Management

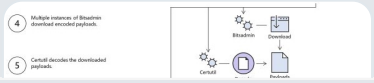
confidential information safe and your critical systems secure. We're innovative, flexible and supportive, helping you through any information security issues to deliver real business benefits and excellent value.

Tweets by @PerspectiveRisk

Perspective Risk Retweeted

Jonathan Nish
@jmnish

Fascinating read from @MsftSecIntel about how your organisation can be attacked using only legit system tools! Does your current solution protect you from these kinds of threats? @ITLabUK & @PerspectiveRisk can advise microsoft.com/security/blog/…



Embed View on Twitter

Tweets by @@perspectiverisk

Perspective Risk
an itlab company