TALION

OSINTGlass

Understand your organisation's digital footprint and risks it could pose

29% of breaches involve stolen credentials.

Verizon, May 2020

80% of hacking related breaches are tied to passwords.

NetSec, May 2020

46% of organisations see careless or unaware employees as a risk.

Kaspersky Daily, October 2020

TALION.NET

e. hello@talion.net

t. +44 (0) 800 048 5775

OSINTGlass

Challenge

How attractive are you to a hacker?

Are you an easy target?

Are your or your employees' passwords exposed on the Internet?

We all have a digital footprint, but what is it, where is it and to what risks could such openly accessible information expose us to?

The cyber threat is growing. Companies must defend themselves against nation states, organised criminal groups and lone wolf opportunists seeking to steal, disrupt and extort. Even the best resourced businesses are suffering.

If businesses do not know which vulnerabilities an attacker will exploit, how can they protect themselves?

Threat intelligence will help you to identify the most likely ways you will be attacked and arrange your defences to deter or repel them.

What is OSINT?

Open-source intelligence (OSINT) is data collected from publicly available sources that is used by attackers to damage your company and its reputation, and by competitors to gain competitive insights.

Collecting and analysing OSINT to identify the digital threats you face requires expertise, experience, and time - commodities that are in short supply in many companies. **What if this challenge was removed?**

What is OSINTGlass?

OSINTGlass from Talion keeps you one step ahead of the attackers by revealing what information they can obtain about your company and its employees, that could increase risk to your business.

For over a decade, our Threat Intelligence team has been trawling the huge volume of openly available data sources, distilling what could be used by an attacker to target your company.

Using your company's digital footprint, our team will advise you on the techniques that attackers are most likely to use and how best to defend against them.

How Does the Service Work?

Our expert Threat Intelligence team provides a security intelligence service that identifies potential sources of information leakage, planned attacks, defamatory messages and password dumps within the public domain that could be used to specifically target your organisation or its employees (including executives).

OSINTGlass

We review the following core business interests:

- IT estate (including external internet footprint)
- Information about major projects, key personnel and suppliers
- Exposure to key threats and vulnerabilities based on observation of their tools and techniques, and historic incidents
- Key intelligence sources including website and internet facing IT assets
- Social media and RSS feeds
- Surface Internet (indexed websites)
- Exposure sites such as 'Pastebin'
- Your own threat sources

What will you receive?

- A regular report (frequency to be agreed), highlighting online footprint and key risks
- Expert advice on reducing your risk exposure
- Access to skilled professionals to train your employees
- Advice on security controls that you can introduce to limit this exposure

Case Study

The Challenge: A world leading legal organisation manages critical and sensitive services to global corporations. The need to understand external threats is imperative to protect their customers, staff, and reputation.

How we helped: Talion deliver OSINT Glass to provide a regular view of intelligence that could be used against the client. OSINT Glass looks for leaks, identifies weaknesses, defamatory messages and negative actions that might target the client.

Outcome/Benefits: Talion exposed an imminent threat to the Head Office and were able to identify the threat group and a significant risk to staff at that location. Working with law enforcement the law firm was able to protect their premises and take proactive action to protect employees.

e. hello@talion.net
t. +44 (0) 800 048 5775

OSINTGlass

What is included in an OSINTGlass review?

Component	Description
Domain typo-squatting	Enumerating all non-corporate linked domains that appear to be targeted at the main domain
Insecure infrastructure	Insecure login pages, vulnerable infrastructure, open SFTP sites
Uploaded sensitive documents	Company sensitive information/files found on malware repositories/open upload sites/paste sites
Domain hygiene	Exploring the registration record of the main domain as well as other linked domains that we can pivot to
Credentials	Corporate credentials found in password lists
Online sentiment	Recent public sentiment towards the company in question, highlighting any particularly brand damaging issues as well as groups/individuals
Exposed company details	Detailed and useful information found about the company which could be useful for an attacker. E.g. photo uploaded of an employee with an ID badge, or platform technical information on a person's CV
Individual footprint	Explores the open-source footprint of an individual. Requires a consent form to be completed by the individual

About Talion

At Talion, we're changing the way organisations interact with their Managed Security Service Provider. Born out of BAE Systems, our service is built on first-hand knowledge of military engineering and defence-grade security, together with an in-depth understanding of the threat landscape facing the commercial world today.

When it comes to cyber security, we believe every organisation deserves full visibility and complete control over how threats are monitored, how decisions are made, and how their business is protected. That's why we prioritise transparency and collaboration across our service lines, implementing security programs that give businesses the control and freedom to pursue ambitions and realise goals, safe in the knowledge that we've got their back, 24 hours a day, 7 days a week.

HQ
The Hub, Fowler Avenue
Farnborough GU14 7JF

Security Operations Centre
Marshall's Mill
Marshall Street
Leeds LS11 9YJ

Engineering Centre
Unit 32-01, Level 32
The Vertical Corporate Office
Tower B, Avenue 10
Bangsar South, No 8
Jalan Kerinchi, 59200
Kuala Lumpur, Malaysia