Case Study – Media Industry

Protecting brand, reputation and intellectual property from cyber criminals

Cyber security has become increasingly important for media companies, as their business models shift from print to digital consumption. Today, monetising intellectual property is predominantly an online endeavour – and one that brings with it a whole new threat landscape.

The company

For one client, an international media company specialising in traditional and electronic publishing, this expanded risk demands an early warning system for identifying any activities that could impact either its brand reputation or sales revenues. The organisation therefore engaged with Telefonica's Cyber Security Threat Detection Service to ensure the predictive intelligence was available to help identify and prevent any cyber risks across their extended operation.

The objective of the engagement was to strengthen internal security measures with enhanced capabilities for detecting, classifying and reporting on any suspicious activity. Now, with the service operational, the company's in-house IT teams can better predict emerging threats, and use their understanding on the nature of a planned attack to implement effective counter-measures.

The solution

Defence against a concerted attack

With our **Network Hacktivism, Activism and DDoS prevention module** in place, the main influencers and discussion topics associated with the client can be monitored around the clock – as well as all online activity and 'mentions'. This information is gathered and analysed to identify trends and uncover any planned attacks aimed at the company's assets.

Safeguarding customer information

The client also wanted to ensure that everything is being done to protect their own customers' data, particularly in relation to stolen credentials. To help, we introduced our **Credential Theft module** – with the initial assessment recovering 114 credentials from 16 official websites. Armed with this intelligence, the organisation can now proactively reach out to notify customers of any suspected breach.

The cyber security challenges

- Restrict the potential for network hactivism, activism and DDoS attack – to protect the company against any activity that would affect their brand or ability to trade
- Gain early warning of any credential theft – to quickly identify and plug any gaps responsible for leaked information assets
- Identify any instances of counterfeiting or non-authorised use of brand – to maintain a reputation for quality products and to defend sales margins

Maintaining brand equity

Telefonica also deployed the **Non-authorised Use of Brand module**. With this in place, we've been able to detect a number of fake and suspicious social network accounts and domains that directly impersonate the customer's brand. During our analysis, it was discovered that only 26% of these were either official or belonged to employees.

A further 65% involved some form of illegitimate brand usage – but unrelated to the client and therefore deemed benign to their interests. Of greater concern was the 3% of accounts considered suspicious in nature. By identifying these risks, the customer now has a clear target for future investigation, and the opportunity to take action against these profiles or mitigate their brand damage.

Minimising revenue loss

This same risk also manifested itself through the appearance of unofficial domains, as detected by our **Domain Monitoring module**. This service helps detect unauthorised websites that impersonate various brand characteristics of a 'master' organisation to promote separate products and services. Our aim is to identify any such activity, and investigations have already uncovered 451 domains that were associated with the client – of which only 16 were directly owned and legitimate.

Ensuring the highest standards for quality

Another key objective set during the engagement was to reveal the existence of any counterfeit products being sold through non-authorised channels. This is where our **Counterfeit module** came into its own, helping detect illegal copies of the client's digital intellectual property. In addition, we also helped identify the availability of fake content – typically inferior quality products that if considered 'official' would create further reputational damage.

Responding to negative assertions

The client also wanted to maintain visibility of any negative views of its operation being shared through various online channels. To help, our **Offensive Content module** was included in the service. Once this went live, we were able to detect several insulting references to the company and its management team posted on public blogging platforms. This knowledge allowed our client to identify the sources of the material, and to take the action required to prompt a cessation of the activity – and to prevent further abuse.

Measuring public opinion

The last service we introduced was the **Digital Identity Monitoring module**. This was put in place to help the client understand the public perception associated with each of its brands, and how this is affected by both their off-line and on-line behaviour. As a result of this capability, the client is able to monitor their brand equity as viewed by the online community. The value of such insights is that they enable the organisation to not only appreciate any emerging threats or negative perceptions produced by the company's activities – but also to measure the impact of 'positive actions' on market opinion.

We'd love to hear from you. To find out more about how O₂ can help your organisation, just contact your Account Manager or call us on 01235 433 507.

You can also visit o2.co.uk/enterprise

Threat Detection Service modules deployed:

Business disruption:

Network Hacktivism, Activism and DDoS Prevention

Reputation and brand:

Domain Monitoring

Offensive Content

Non-authorised Use of Brand

Digital Identity Monitoring

Online fraud:

Counterfeit and Credential Theft

Published in August 2014. All information is correct at time of going to print.
Telefónica UK Limited Registered in England no. 1743099. Registered Office 260 Bath Road Slough SL1 4DX