How O_2 is responding to a sophisticated threat environment in financial services

Case Study – Banking Sector

Every minute, of every hour, of every day, a major financial organisation is under cyber attack. According to a recent report, 35% of large institutions report being the attempted targets of malware – and 33% of phishing attacks[1].

In response to this rapidly evolving threat situation, where the average cost for resolving a single, successful attack now stands at over $1 million[2], organisations are challenged with introducing capabilities for protecting against threats they know about, and speeding up detection times for those they don't.

The company

A large Spanish financial institution, with over 4500 employees deployed across an extensive global operation, engaged with Telefónica's Cyber Threat Detection Service to help augment its existing security infrastructure.

The challenge

For the customer, the principal aim of engaging with Telefónica was to gain real-time, predictive threat intelligence into the nature, direction or purpose of any potential cyber attack. These proactive insights could then be used to diagnose, classify and address any undiscovered vulnerabilities to help protect against:

- Leaks of confidential information and private customer data
- Theft of employee and customer credentials
- The existence of fake domains that could lead customers to counterfeit websites
- Malicious information and opinions posted on social networks
- Theft of credit card information by specific banking malware

Results

- Reduced reputational impact
- Early threat discovery
- Improved cost savings
- 24x7 monitoring

Telefónica

O_2 business

With Telefónica's Threat Detection Service in place, previously undiscovered attacks and malicious behaviour targeted at the organisation can now be identified and qualified – with the resulting intelligence used to address any exposed areas across the data network.

These capabilities were initially defined with support from a Telefónica Local Analyst who helped the customer analyse the full risk spectrum they faced – and the specific service modules needed. Once up and running, our Global CyberSOC monitored a vast array of different international sources 24x7 to detect any emerging threats. This intelligence was then made available for review by the customer via a customised Service Portal, with additional information and investigation available from the Local Analyst.

The results

Denying external access to confidential documents

Using the **Information Leaks module**, our investigations identified several confidential documents posted in public file sharing platforms (Pastebin, P2P link etc.), that contained private information about members of the Board – as well as details of the company's IT systems available from the metadata of the published documents. This insight allowed the customer to trace the origin of the leaked information, and to take action to avoid future occurrences – for example by changing the security controls of systems that were left open to attack. It also ensured the procedures were in place to avoid the data loss that could lead to a fine by the data privacy watchdog the ICO.

Identifying lost and stolen credentials

Another key focus area was avoiding the reputational impact of losing a customer's personal information, the theft of which continues to represent the highest external cost of cybercrime[3] (in this context, an external cost is one that is created by external factors such as fines, litigation and the marketability of stolen intellectual properties). Analysis from Telefónica quickly found approximately 200 stolen customer credentials, arranged by domain, as well as the details of more than 100 stolen employee credentials. This early discovery enabled the customer to change or take down the compromised data.

Just as importantly, users were able to identify the precise date of the theft, and from this analyse the impact of the stolen credentials – tracing impersonations as well as the overall fraud caused by that attack. This loss of employee credentials posed a significant risk to our client, given that they could enable an attacker to gain unauthorised access to internal business systems and processes. The rewards on offer to cyber criminals mean that the threat will remain constant (stolen credentials for a bank account with a balance of $70,000 to $150,000 typically have a black market value of $300 each[4]) – and only through proactive monitoring will the organisation be able to respond decisively to any future breach.

Reducing the impact of fake websites

When it came to assessing the scale of phishing activities the customer faced, our **Domain Monitoring module** was used to identify 150 fake domains relating to official websites – 20 of which were being actively used in phishing attacks. By resembling an authentic website of the organisation, these illegitimate domains attempt to trick end users into revealing confidential information such as their credentials – or to unintentionally download malware. Proactive identification helped the organisation protect their end users against phishing attacks, maintain their brand integrity, and achieve significant cost savings (the average annualised cost weighted by attack frequency was $21,094 in 2013[5]).

In addition, the **Digital Identity Monitoring module** was deployed to look for the exposure of specific identities via social networks. In particular, the customer was concerned about threats related to senior management and key personnel including fake profiles used to discredit them. With the module live, any offensive posts and

Threat Detection Service modules deployed:

Business disruption:

Information Leaks

Credential theft

Reputation and brand:

Domain Monitoring

Digital Identity Monitoring

Online fraud:

Carding

Malware

profiles can now be identified instantly, with the intelligence used to mitigate any reputational risk. In addition, the module also allows for any 'negative perceptions' of the bank be mitigated – by identifying the source and cause of the concern, alongside the intelligence to help formulate the best reaction.

Dealing with credit card fraud

With our **Credential Theft module** in place, the customer has identified on average over 200 credit card thefts per month – information available for sale via a number of black market channels. Telefónica helps identify these thefts, and provides details of the compromised cards to ensure they are quickly disabled. Armed with intelligence on which cards have been compromised, the bank is also able to proactively inform affected customers that the situation had been resolved – before they notice any impact on their personal accounts. This added level of protection has been recognised through improved satisfaction scoring as measured by the bank's customer survey, which in turn has significantly reduced the potential for any long lasting brand damage.

Proactive malware detection

By deploying the **Malware and Carding modules**, the organisation has been able to detect approximately 4700 separate references to its domains within the most common banking malware – of which Zeus is currently the best known and most active algorithm (according to the FBI, Gameover Zeus has cost businesses more than $100 million in losses, with between 500,000 and 1 million computers now infected[6]). With such proactive visibility into emerging malware threats, the customer is now using this intelligence to fix previously unseen vulnerabilities. New threats are constantly appearing, and the service continues to keep the organisation abreast of these developments, thus helping them avoid exposure to malware threats that could lead to unauthorised access or fraud.

Threat Definition

Phishing
An attempt to acquire sensitive information through fake websites or emails

Pharming
Where website traffic is redirected, causing users to unknowingly access an illegitimate domain

Malware
Including the subset of financial malware that seeks to gain data associated with specific financial transactions

Carding
The theft of credit card information, which is then used or sold on the black market.

We'd love to hear from you. To find out more about how O_2 can help your organisation, just contact your Account Manager or call us on 01235 433 507.

You can also visit o2.co.uk/enterprise

[1] http://www.forbes.com/sites/gregorymcneal/2014/05/26/banks-challenged-by-cybersecurity-threats-state-regulators-acting/

[2] 2013 Cost of Cyber Crime Study. Ponemon Institute. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

[3] 2013 Cost of Cyber Crime Study. Ponemon Institute. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

[4] http://securityaffairs.co/wordpress/19957/cyber-crime/cyber-criminal-underground.html

[5] 2013 Cost of Cyber Crime Study. Ponemon Institute. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

[6] http://www.afterdawn.com/news/article.cfm/2014/06/02/gameover_zeus-cryptolocker-malware-feds-disrupted

Telefónica

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

O2 business