The trouble heading for your business

Targeted attacks and how to defend against them

February 2013

For years businesses have striven to keep malware, spam and unwanted intruders at bay with varying degrees of success. Much of the protection they have put in place assumes that most of these attacks will be random and that, if an organisation’s defences are too hard to breach, the attacker will seek an easier victim.

That situation is changing fast with the rise of targeted attacks (or advanced persistent threats/APTs), where both cyber-criminals and hacktivists are targeting selected organisations and persisting until they achieve their goals.

New research presented in this report underlines the scale and real impact of the problem, the measures being taken to defend against targeted attacks and how effective they are. It should be of interest to anyone charged with defending their businesses against contemporary cyber threats or who wants to better understand their organisation’s vulnerability.

Bob Tarzey
Quocirca Ltd
Tel: +44 7900 275517
Email: bob.tarzey@Quocirca.com

Louella Fernandes
Quocirca Ltd
Tel: +44 7786 331924
Email: louella.fernandes@quocirca.com
The trouble heading for your business

Targeted attacks and how to defend against them

In the past, businesses that invested in effective IT security could reasonably expect that random attacks would pass them by and leave their mark on less well-defended organisations. However, this is no longer the case. The growing aspirations of cyber-criminals to seek greater profits and the rise of hacktivism have led to more targeted attacks. If it’s your business attackers are after, they are more determined than ever to find a way in.

**European businesses say they are concerned about targeted attacks**

New research presented in this report shows the high level of concern amongst European businesses with regard to targeted attacks; 75% say they have been a concern for some time or that they are an increasing concern. This is partly due to the media reporting some of the more high profile attacks but also because the majority of respondents believed that their organisation had been the victim of a targeted attack, with 30% reporting a significant business impact.

**The most common impact of targeted attacks was the loss of regulated financial data**

Financial data is the asset that cyber-criminals most want to get their hands on, so it is unsurprising that it tops the lists of impacts of targeted attacks. Second was lost business, which is one of the primary aims of hacktivists and will also be a likely result of the clean-up effort that takes place after any successful attack. Just behind these were the loss of regulated personal data and intellectual property, both of which can be costly and may damage competitiveness.

**A range of techniques are being used to perpetrate targeted attacks**

Zero-day and polymorphic malware, concealing malware and the seeking out of zero-day vulnerabilities in commercial software are all techniques used to perpetrate targeted attacks. Attackers also try and dupe individuals using clever social engineering to get them to disclose access details or open attachments that carry malware. Another technique is to install command and control servers within an organisation’s network so that the traffic generated is harder to detect by network edge defences.

**Undetected malware is almost certainly running on most networks**

The majority of organisations admit they have discovered malware running on their networks that had not been detected by existing security measures. Most think they have malware running undetected on servers, mobile devices and PCs. It is clear that traditional anti-malware defences are not defending business in the way they would expect as the threat landscape is evolving. Given the damage that can result, this apparent complacency is worrying.

**There is better awareness of the problems than the solutions**

When asked to describe the technology being used specifically to defend against targeted attacks, respondents often listed the same anti-malware and firewall tools that are demonstrably failing to counter the advanced techniques being used. Just under half said that they were taking action and had either installed or were evaluating technology to counter targeted attacks. However, the evidence shows they are often not looking at some of the more advanced options, suggesting better awareness of the problems than the solutions.

**Advance protection measures are having an impact, but not a big enough one – yet**

Although many respondents say they have deployed technologies to help defend against targeted attacks, for many this was quite recent. These include tools for sandboxing, file integrity monitoring, network traffic inspection/deep packet inspection and behavioural analysis. Once such a technology was deployed, the number saying they had blocked attacks rose considerably, but it could be a lot higher. It seems probable that many are still at the evaluation stage or are overestimating the capability of existing traditional security products.

**Conclusions**

Cyber-criminals use targeted attacks to steal regulated data and/or intellectual property, while hacktivists use them to damage a given business in some way. Whatever is thought of the individuals behind such attacks, they tend to be technically competent and are finding it easy to outwit existing IT security measures. Most businesses are currently lagging behind their attackers in an ongoing arms race and need to do more to ensure they avoid the damage that such attacks can cause: lost business, potential financial costs, lost competitiveness and, in the worst case, the collapse of businesses. There are advanced security tools available that are specifically designed to combat the techniques used to perpetrate targeted attacks; however, too few organisations are deploying them effectively.
The trouble heading for your business

Introduction

In 2011 a row broke out over figures published by the UK’s Office of National Statistics that showed car crime had fallen dramatically over a fifteen-year period. The main reason, it was claimed, was improved general security built-in to all cars up-front. However, motoring interest groups have pointed out that, hidden in the good news was another telling statistic; whilst house burglaries had also decreased over the same period a specific type of crime had increased – the theft of car keys from houses. The reason? To steal a car these days it is much easier if you have the keys, and if you are going to make the effort and risk to steal car keys, it may as well be for a vehicle worth having. So, car thieves are targeting the homes of individuals with expensive cars and striking at the right moment.

This change in car crime is a good analogy for what is happening with cybercrime. As general cyber security is increasingly being built into basic IT infrastructure and the end users of IT systems are becoming more aware of how they should behave online, random attacks have become less effective. However, if high value information can be identified, then a targeted attack is proving to be an effective way of reaching it. Unlike cars that generally have a one-to-one relationship with an owner, valuable data has many custodians; targeting vulnerable individuals can be an easy way to get a foot in the door. Adding to the problem is the rise of hacktivism, where organisations are attacked in cyberspace to undermine their business for political purposes.

This report presents new research into the awareness of targeted attacks among 300 respondents from enterprises in a range of business sectors across Europe. It looks at the various security measures that are being put in place and their effectiveness. The report should be of interest to business managers worried about the damage such attacks can cause, not just through the loss of data assets but also from lost productivity, regulatory fines, loss of competitive advantage and reputational damage. The report should also be of interest to those IT managers charged with the security of IT systems who want to ensure that their organisation does not fall victim to one of these increasingly sophisticated targeted attacks.
What is a targeted attack?

In the early days of the widespread use of email, cyber-criminals could make a living by hiring a botnet (a group of hijacked computers running malware) and using it to send out millions of emails to random users asking them to hand over their credit card details on some pretence. Generally, enough people would be taken in to make the effort worthwhile. For businesses, at least, random attacks are no longer the headache that they were, having become less effective as general cyber security has improved and user awareness has increased.

However, cybercrime has certainly not disappeared; random attacks are being displaced by more insidious techniques. Rather than trying to persuade thousands of users to hand over personal information, it is better to target and steal whole databases with millions of such records. For such crimes, the best sectors to target are retailers, banks and public sector organisations; they go where the money and/or personal data (payment card details are still the most commonly stolen data item\(^1\))

Cyber-criminals also extend their efforts to stealing intellectual property (IP) such as product blueprints, industrial processing information and other secrets they can sell on – high value manufacturers and pharmaceutical companies are common targets.

Thieves have been joined by a new breed of online menace, the hacktivist, hackers who target an organisation’s IT infrastructure not necessarily to steal information (although they might do, to expose what they see as corporate malevolence), but simply to disrupt its ability to carry on business. National governments are now also thought to have entered the fray; for example it is now widely believed that the US and/or Israeli governments perpetrated the STUXNET attacks on Iranian nuclear facilities.

For the purposes of this research the type of malware that is commonly used to perpetrate targeted attacks was described to the participants as follows:

"Unknown and undetected malware residing on a network with the goal of gathering and stealing data for financial gain or commercial espionage; such malware is often bespoke and solely used to target a single organisation and, as a result, it is usually missed by traditional anti-malware defences."

Another widely used term for a targeted attack is an advanced persistent threat (APT). Overall, the respondents in this research were equally familiar with both terms. This is reflected by their general awareness. Their views are summarised in Figure 1 (after they had just been given the above definition); overall 75% were at least “concerned” about targeted attacks.

Of course, the awareness is driven to some extent by both the general and IT-specific media who are prone to talk things up. However, the sectors most likely to be targets – those that manage regulated data (financial services and retail) or have high value intellectual property (pharmaceuticals) – show some of the highest levels of concern. This suggests that some of the awareness is down to experience, which is borne out by further data where respondents were asked to report if their organisation had ever been the victim of a targeted attack (Figure 2).
Care needs to be taken in interpreting such data. The reason for reporting higher levels of attacks could be because that is really the case or it could be that certain organisations have invested in better technology and are therefore better able to detect targeted attacks. What is certain is the organisations that were most concerned were more likely to have taken action and started to put defensive measures in place, specifically to defend against targeted attacks. Once bitten, twice shy.
The impact of targeted attacks

The impact of a targeted attack will depend to some extent on the aims of the perpetrator. A hacktivist may want to undermine an organisation’s reputation or stop it trading for a period of time; they may want the results of their efforts to be high profile. A thief simply wants to get access to valuable data and, if they do so invisibly, may be able to return later for more.

According to Verizon’s 2011 data breach report, cyber-criminals launch more attacks whilst hacktivists steal more data. There are a number of reasons for this; hacktivists often target large organisations where there is more data in the first place and, whilst they are there, they will likely take anything that looks interesting that might add fuel to the fire they are trying to light. Cyber-criminals want to steal quite specific data that can monetised, to make sure their efforts are worthwhile. They need to be sure they have found what they need and they may avoid disturbing uninteresting data and systems to avoid detection. Thus many of the breaches they perpetrate go unnoticed, unreported and un-investigated.

Overall 72% of organisations interviewed confirmed they had been hit by a targeted attack. Of these, two thirds said there had been some sort of impact, over half of which said it was serious. The nature of the damage caused is shown in Figure 3. Most common was the loss of regulated financial data. Second was lost business, which could be the aim of hacktivists but it could equally be the result of business disruption whilst clearing up after a targeted attack had been identified.

The theft of IP was fourth on the list. If stolen IP was to fall into the hands of a competitor then that could damage competitiveness. Any organisation with a modicum of principles would be wary of buying such material on the open market, not least for the damage it could cause to its own reputation if found out. However, for hacktivists, just putting it in the public domain using a leaking site may be enough to achieve their goal.

Low on the list are the secondary impacts of reputational damage and negative press coverage. That these are often the aims of hacktivists does not mean that attackers are failing, just that such attacks are fewer in number. Furthermore, the use of targeted attacks to help drive politically or ethically motivated campaigns is relatively new compared to cybercrime.

Across all respondents, the loss of data is the primary concern, regardless of whether they know themselves to have been a victim to date (Figure 4). Whilst the actual reputational damage incurred by organisations that have already been a victim may not yet be too severe, many worry about what might happen in the future. Concern about reputational damage ranks above concerns about fines and remediation costs, although, as Figure 4 shows, concerns about the latter are increasing the fastest. So they should be; the size of fines is set to increase when the new EU Data Protection Regulation is introduced, probably in 2014. In its draft form it recommends that maximum fines be set at 2% of global turnover.
The concern about impacts varies both geographically and by sector. For example UK-based organisations are more concerned about both the loss of regulated data and fines (Figure 5). This could be because, for many cyber-criminals operating from overseas, it is easier to comprehend the systems and data of English-speaking organisations.

Figure 6 shows that, when it comes to intellectual property (IP), retailers worry the most; if details of a planned marketing or discounting campaign are leaked into the public domain a competitor could respond more quickly. Manufacturers worry about IP too, not wanting their designs, blueprints and processes to be made public. Many organisations indicate that they have “increased concern” about IP, although pharmaceutical companies, with a lot of high value IP, are the least worried, perhaps because of many years of experience protecting it.

Retailers and financial services organisations also worry most about reputational damage (Figure 7). Both have a high level of direct online interaction with customers and, for retailers in particular, business could drop off very quickly if shoppers are put off a given online retailer due to a nasty incident and click elsewhere. Both sectors also worry most about fines, due to the highly regulated personal financial data they deal with (Figure 8).
How are targeted attacks perpetrated?

Before looking at how to defend against targeted attacks it is necessary to understand how they are perpetrated in the first place. There is no one vector of attack; attackers will use multiple methods together to achieve their goals. Table 1 lists some of the main ones. Many of these use advanced techniques for distributing malware, others use social engineering, for example befriending individuals via social media to establish trust.

<table>
<thead>
<tr>
<th>Table 1 – targeted attacks: methods used</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Zero-day malware:</strong> new versions of malware that have not been used before and for which signatures in anti-malware products do not exist. Zero-day malware will often be an adaption of known malware, so although individual files may be hard to detect, their behaviours may not. For a targeted attack, it is worth the effort of the attacker to prepare malware variants specific to the chosen target.</td>
</tr>
<tr>
<td><strong>Encrypted malware:</strong> known malware can still be smuggled in to an organisation by encrypting it. This method was cutting edge when it was first introduced, although some anti-malware vendors have been catching up, often by focusing on the component of the malware that does the encryption/decryption, which usually remains constant. Organisations need to make sure the malware protection they use is capable of this.</td>
</tr>
<tr>
<td><strong>Polymorphic malware:</strong> if malware is designed to change its form each time it executes then it will always be zero-day as far as traditional signature detection is concerned. File detection signatures alone are no longer sufficient, advanced techniques that focus on behaviour are required.</td>
</tr>
<tr>
<td><strong>Embedded malware:</strong> the hiding of malware in other more innocuous-looking files such as spreadsheets and PDFs, which recipients are more likely to open, however they are received.</td>
</tr>
<tr>
<td><strong>Zero-day exploits:</strong> these are newly discovered, and therefore unpatched, vulnerabilities (software bugs) in commercial infrastructure or applications. Whilst such vulnerability is only known to a hacker it can be exploited multiple times. Of course, that activity may make the target aware of the vulnerability, which may lead to the vendor providing a fix. This means there is a thriving market in zero-day vulnerabilities on underground forums as vendors, hackers and even government organisations will pay premiums to get first access to them.</td>
</tr>
<tr>
<td><strong>Command and control (C&amp;C) servers:</strong> C&amp;C servers are used to manage devices and groups of devices (botnets) that have been infected with malware. Botnets are used for certain types of high volume targeted attacks such as distributed denial of service campaigns (flooding networks/servers with traffic). If a C&amp;C server is at an external location, then software, designed to thwart an attack it controls, can block traffic from its location. A recent development is to configure C&amp;C servers inside a victim's own network, thus reducing the amount of C&amp;C traffic that must cross the network perimeter, making it harder to detect.</td>
</tr>
<tr>
<td><strong>Social engineering:</strong> software vulnerabilities are one way into an organisation's network; another is to take advantage of employees' curiosity, natural willingness to help or simply to do their job. Social engineering takes many forms; for example:</td>
</tr>
<tr>
<td>- <strong>Pretexting:</strong> victims are engaged, usually by telephone, with a hoax story that persuades them to part with sensitive information (e.g. login credentials of privileged users)</td>
</tr>
<tr>
<td>- <strong>Phishing:</strong> forged, but realistic-looking, emails persuade targets to part with sensitive information</td>
</tr>
<tr>
<td>- <strong>Baiting:</strong> duping an employee in to loading malware, e.g. by leaving a USB stick in the company car park</td>
</tr>
<tr>
<td>- <strong>Tailgating:</strong> obtaining access to a physically secure area by following an authorised individual through a security gate</td>
</tr>
<tr>
<td><strong>Spear-phishing:</strong> a form of phishing where a malicious email or social media communication is tailored to target a specific individual and appears a lot more credible than it would as part of a volume campaign. Spear-phishing aims to persuade the target to open malicious files attached to emails or to click on an infected web link. Micro blogging sites, with their shortened URLs, are becoming a danger here.</td>
</tr>
</tbody>
</table>

One of the first questions each respondent to the survey was asked was whether their organisation had been a victim of any of these techniques in the last 12 months. At this stage in the survey, they were not aware that the research was specifically about targeted attacks. Figure 9 shows that the majority felt they had been exposed to
most of these techniques; zero-day malware and social engineering are increasing the fastest and both are key techniques when it comes to perpetrating targeted attacks.
Protecting your organisation against targeted attacks

As would be expected, most respondents said that traditional defences were in place such as firewalls, intrusion prevention systems (IPS) and anti-malware on servers/user end-points (this included over 50% saying it was now installed on smartphones). However, 58% said they had still discovered previously undetected malware (Figure 10). Even those that had not discovered such malware still suspect it is running somewhere, especially on end user PCs (Figure 11). Clearly hackers are getting their malware packages through current defences and there appears to be an element of complacency, which is a concern as it only takes one piece of well-placed malware to compromise a lot of data.

The responsibility for putting protection in place is most likely to lay with a specialist IT security team, although quite a few still rely on the general IT team (Figure 12). Some even had a specialist team in place to deal with targeted attacks whilst others turned to managed security service providers (MSSP).

A third of respondents said they had deployed specific technology to deal with targeted attacks; this was slightly truer of larger organisations (Figure 13). However, when asked to specifically describe the technology selected much of it was ill suited to the specific aim of combating targeted attacks, with anti-malware and firewalls topping the list. This suggests a yawning gap between the levels of understanding; respondents seemed to know what targeted attacks are but had less knowledge about types of protection technologies available and their relative effectiveness.
Big business might be more likely to have protection in place, but smaller ones are spending more on the problem (Figure 14). This is probably due to economies of scale; the larger an organisation is the more users it can protect per unit of investment in IT security. The focus of this spending is critical; as has been said, most organisations have traditional defences in place, but the majority still admit to finding malware or suspecting compromises of their systems somewhere. Many may be under the impression that they are protected, but clearly it is often the case that they are not.

Most organisations seem to be extending the range of protection they put in place to include technologies that are more focussed on detecting and stopping targeted attacks (Figure 15). Only a minority have been using such technology for “some time”. Some may mistakenly believe traditional technologies of being capable of providing advanced detection techniques; others may just not be using newer technologies effectively. Those that say they have had certain capabilities for some time are more likely to block attacks, but this is by no means certain (Figure 16).

<table>
<thead>
<tr>
<th>Table 2 – Targeted attacks: advanced defence techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated sandboxing</strong>: technology installed on network appliances, servers or end-points that enables any file, and certainly those of dubious reputation, to be tested in a safe isolated environment before being run on a live system, to ascertain if it has any malicious intent or suspicious behaviour.</td>
</tr>
<tr>
<td><strong>Whitelisting/application control</strong>: limiting the files that can execute on a given device to those of known integrity. Most useful for the devices of transactional workers, such as those in call centres, who should have little need to use anything beyond a limited range of applications.</td>
</tr>
<tr>
<td><strong>File integrity monitoring</strong>: a system that examines files accessed by users, with the capability to assess their reputation and integrity. If a file, service or application has been modified in any way the signatures will no longer match; this can be evidence of attack-related activity.</td>
</tr>
<tr>
<td><strong>Network traffic inspection and analysis/deep packet inspection (DPI)</strong>: the thorough inspection of network traffic, including the headers of, and data within, network packets and the re-composition and inspection of files from the different packets within network flows. This ensures they are consistent with relevant network protocols and application behaviours in order to decide whether they should pass through, be blocked or redirected.</td>
</tr>
<tr>
<td><strong>Behavioural analysis</strong>: even if a suspicious file has never been identified before as malware, its behaviour still provides important clues; for example, the resources it tries to access or the traffic it tries to send outside of the network. This is an important component of sandbox analysis (see above).</td>
</tr>
<tr>
<td><strong>Advanced correlation</strong>: the real-time correlation of events happening on a network with existing log information and external feeds. For example, a login attempt using a given identity consistent with previous login attempts and usual user behaviour.</td>
</tr>
<tr>
<td><strong>Heuristics</strong>: aside from traditional blacklisting technologies where files are compared against a list of known bad files, heuristics looks for specific commands or instructions that are not usually present in legitimate executable files.</td>
</tr>
<tr>
<td><strong>Mobile device protection</strong>: not an advanced technology per se, however the volume of malware targeted at mobile device operating systems and malicious apps is increasing rapidly. Attention needs to be paid to securing these devices and their users on a wide range of networks. This needs to take into account the fact that they will often be owned by the user themselves (bring your own device/BYOD).</td>
</tr>
</tbody>
</table>

There is no silver bullet for protecting against targeted attacks. Whilst whitelisting may be good for ensuring call-centre workers don’t open and run dangerous email attachments, it will not stop an administrator being duped into disclosing their login credentials via social engineering. File integrity monitoring is good for understanding the nature of changes being made to critical files and systems, but it will not stop a hacker from exploiting zero-day vulnerabilities.

When it comes to new technologies no single one will be completely effective, multiple layers of defence are required. Only a minority of businesses seem to be using them effectively, with the majority misunderstand them, are experimenting or are yet to invest.

© Quocirca 2013
Conclusions

Targeted attacks are real and are here to stay. Organisations need to put in place an effective defensive strategy, which includes the use of advanced security techniques. Some organisations may feel that they already have such technology in place; however, the results of this new research suggest that many organisations are overestimating the effectiveness of their current defences and expecting too much of existing technology, which was designed to protect more against random, rather than targeted, attacks.

Whatever is thought of the individuals behind such attacks, they tend to be technically competent and are finding it easy to outwit existing IT security measures. Most businesses are currently lagging behind their attackers in an ongoing arms race and need to do more to ensure they avoid the damage that such attacks can cause: lost business, potential financial costs, lost competitiveness and, in the worst case, the collapse of businesses. There are advanced security tools available that are specifically designed to combat the techniques used to perpetrate targeted attacks; however, too few organisations are deploying them effectively.

Failure to protect is starting to have dire consequences for many organisations. This starts with the scale of fines and even prison sentences that can now be imposed for the poor protection of regulated data and the regulatory regimes are only going to get tougher; for example with the introduction of the new EU Data Protection Directive in 2014. However, it goes well beyond this; the cost of clear up, reputational damage and subsequent loss of business and competitiveness have already taken a severe toll on some high profile organisations that have fallen victim to targeted attacks in the last few years.

Imagine waking up one morning and finding thieves had entered your house, stolen the car keys and then your car. It dawns on you that you and your car had been picked out and the thieves had to attack whilst you were at home, when the keys and car would be there. They may have chosen a night when they knew your family was away and you were alone in the house – you and your property had been staked out. That would feel very personal. This is exactly what is happening to businesses; cybercrime, and its hacktivism cousin, have become direct and personal. Someone somewhere is probably staking out the organisation you work for – if not now they will be soon.
References

1 – 2012 Data Breach Investigations Report, Verizon

2 – 2011 Data Breach Investigations Report, Verizon
The trouble heading for your business

Demographics

The following figures show the distribution of the research respondents by country, size, sector and job role:

**Figure 17: Countries**

- France: 100%
- Germany: 100%
- UK: 100%

**Figure 18: Countries by business size**

- UK: 60% (2500 to 5000 employees), 40% (More than 5000 employees)
- Germany: 59% (2500 to 5000 employees), 41% (More than 5000 employees)
- France: 61% (2500 to 5000 employees), 39% (More than 5000 employees)

**Figure 19: Sectors by country**

- Utilities: France 22%, Germany 18%, UK 15%
- Public sector: France 3%, Germany 4%, UK 8%
- Other commercial: France 10%, Germany 12%, UK 12%
- Dist, log and trans: France 8%, Germany 13%, UK 10%
- Pharmaceuticals: France 10%, Germany 14%, UK 10%
- Manufacturing: France 10%, Germany 26%, UK 14%
- Financial services: France 12%, Germany 25%, UK 25%
- Retail: France 5%, Germany 9%, UK 13%

**Figure 20: Countries by job role**

- UK: CISO 25%, Infosec director/manager 36%, Senior IT director/manager 39%
- Germany: CISO 26%, Infosec director/manager 52%, Senior IT director/manager 22%
- France: CISO 32%, Infosec director/manager 44%, Senior IT director/manager 24%
About Trend Micro

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server, network and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge – from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

For more information about Trend Micro and our products and services please visit TrendMicro.co.uk. Or follow us on Twitter at @TrendMicroUK.
REPORT NOTE:
This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today’s dynamic workforce.

The report draws on Quocirca’s extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation’s environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca’s mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca’s clients include Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh and Symantec, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca’s work and the services it offers can be found at http://www.quocirca.com

Disclaimer:
This report has been written independently by Quocirca Ltd. During the preparation of this report, Quocirca may have used a number of sources for the information and views provided. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in information received in this manner.

Although Quocirca has taken what steps it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data and advice.

All brand and product names are recognised and acknowledged as trademarks or service marks of their respective holders.