Security in the data centre
DDoS impact, awareness and attitudes
October 2014
About Megabuyte

Megabuyte is the UK’s definitive source of independent corporate and market intelligence covering the Software, IT Services and Telecoms sectors.

Our intelligence is accessible through a variety of subscription, pay-as-you-go, project or retainer-based options designed to meet the differing requirements of our customer base. www.megabuyte.com

I S Research Ltd
The Blade, Abbey Square, Reading, RG1 3BE
+44 (0)118 948 5850
info@megabuyte.com

Contents

Introduction 3
Key findings 4
What is Denial of Service (DDoS)? 5
Impacts 7
Defences 9
Vendor Viewpoint 11
Responsibility 12
Opportunity 13

Corero is dedicated to improving the security of the Internet through the deployment of its innovative First Line of Defense® solutions. Corero products and services provide customers with protection against a continuously evolving spectrum of DDoS attacks and cyber threats that have the potential to impact any Internet-connected business.

Contact us:
For further details on how Corero Network Security could help your business, please contact:
Corero Network Security
Regus House
Highbridge, Oxford Road
Uxbridge UB8 1HR, UK
Email: info_uk@corero.com
Telephone: 01895 876579
www.corero.com

Published by the team at Megabuyte

Author
Hannah Finch hannah.finch@megabuyte.com © Megabuyte 2014
Introduction

For today’s internet-driven businesses, any service degradation or outage can have a detrimental impact on brand, customer loyalty and the bottom line. Increasingly, such incidents are being caused by Distributed Denial of Service (DDoS) attacks. In recognition of this growing trend, Megabuyte is interested to understand how companies are dealing with the growing threat of cyber-attacks and how the market opportunities are developing for vendors that provide protection against these threats. When cyber-attacks grab headlines in mainstream media, it is often as a result of an online enterprise, entertainment service or government organisation that has been forced offline, typically resulting in significant business loss and reputation damage.

Fueling the apparent increase in the scale and sophistication of DDoS attacks is the criminal monetisation of the DDoS attack method. This means that a wider spectrum of organisations stand to suffer in the future as they become victims of this trend. Companies and Government organisations alike are calling for service providers to provide help and answers. We aim to investigate this trend in our report, as we assess the impacts, awareness and attitudes towards DDoS security in the datacentre.

NATHAN MARKE
CTO DAISY GROUP

Objectives and methodology

In preparing this report we have sought the views of over 30 UK-based CEOs, CTOs and decision-makers on the impacts of, and attitudes towards, DDoS attacks and the available mitigation strategies. We have combined an in-depth survey and follow-up interviews with selected companies to feed our analysis. This has helped us gain valuable insight into how service providers are not only responding to the threat of DDoS attacks but also assessing the opportunity for offering DDoS-monitoring and mitigation services to customers.

The companies surveyed include thirteen data centre and hosting providers, nine network services providers, eight managed data services providers and one ISP. They were represented predominantly by their CEOs and Managing Directors, but responses also came from a broad spectrum of CIO/CISOs, CFOs and Technical staff. In turn, the customer base of the surveyed companies spanned large enterprises, SMEs and other service providers including several data centre and hosting provider customers.

“Security is a constantly learning and evolving landscape”

NATHAN MARKE
CTO DAISY GROUP

“Our DDOS platform alerted us to the attack”

CTO
DATA CENTRE & HOSTING PROVIDER

With thanks

Our introduction would not be complete without acknowledging our research sponsor Corero Network Security. As well as sponsoring the report, we are pleased to include a vendor viewpoint discussion with Corero’s CEO Ashley Stephenson, who offers insights on the latest emerging threats and the available defences. The Corero First Line of Defense® solutions provide advanced DDoS and cyber threat protection for hosting providers, service providers and enterprises alike. The Corero SmartWall® Threat Defense System (TDS) is a purpose-built family of network security appliances that is configurable to meet the needs of the individual business. This technology is coupled with sophisticated security event analysis for actionable DDoS attack intelligence leveraging Splunk software for big data analytics and advanced visualisation capabilities.
Key findings

DDoS is targeting and impacting service providers and their customers

- All of the companies we surveyed believe that DDoS attacks are occurring at least as much, if not more than, they have in the past.
- PC botnets are being replaced with much higher bandwidth commercial servers and attackers are targeting service providers due to their extensive customer networks.
- Just over half of the companies in our survey have been impacted by DDoS in the last year, 1-2 years or 2+ years.
- While service providers and their customers are both impacted by DDoS attacks, the latter typically suffers to a greater extent.

Multiple defences are required for comprehensive security

- DDoS mitigation tools are helping detection, but customer complaints about service issues remain one of the main ways that service providers become aware of an attack.
- Network appliances are the most used and most popular method for future adoption amongst the service providers in our study.
- The majority of service providers have at least one DDoS mitigation tool installed, while four companies told us that they utilise all of the three proposed mitigation methods.

DDoS mitigation and monitoring is a high priority

- The companies we spoke to said that DDoS mitigation is either more important than or as important as other types of IT security.
- Five companies said they believe that DDoS mitigation is more important than other security tools for both themselves and their customers.

Service providers feel responsible for DDoS mitigation

- The vast majority of service providers said that they feel they have a responsibility to implement tools or services to protect themselves and their customers from DDoS.
- However, there are some service providers that feel that customers should take care of their own DDoS mitigation.

DDoS business opportunities exist

- There is a premium placed on security services of all types and more enterprises are turning to their internet and network service providers for help in mitigating DDoS.
- The majority of the companies in our study said that they perceive a modest business opportunity for offering DDoS mitigation and monitoring services.
- However, we received a variety of responses, ranging from companies that see no business opportunity through to those that see a very significant opportunity.

“The outage only affected a tiny percentage of overall customers but was highly significant to those who were out.”

GROUP STRATEGY DIRECTOR
MANAGED NETWORK AND DATA SERVICES PROVIDER

“The impacted by DDoS between 10 and 50 times a day”

TECHNICAL DIRECTOR
DATA CENTRE & HOSTING PROVIDER
What is Denial of Service?

Denial of Service (DoS) is a general name given to any kind of attack that impacts the availability of services or data, essentially denying access to the service. In the current environment, DoS has become synonymous with DDoS or Distributed Denial of Service. The latter term is the most frequently used acronym and no longer implies a specific type of attack. DDoS attacks typically take advantage of vulnerabilities in the online service applications or infrastructure and cause them to slow down, stop responding or even "crash". Although this type of attack does not explicitly give attackers any elevated privileges or access to the target's data, it can cause serious financial damage by interrupting the normal operations of the websites, services, or applications under assault. It should be noted that DDoS has been reported to have been used in combination with breach attempts that are intended to comprise customer data.

There are many different DDoS attack types. It is helpful to review by these categories:

- Volumetric attacks – saturate internet bandwidth and computing resources.
- State exhaustion attacks – target infrastructure components such as firewalls, load balancers and servers.
- Application-layer attacks – more stealthily target a specific aspect of an application or service.

Both volumetric and application-layer denial of service attacks aim to disrupt availability, but they go about it in different ways. Volumetric attacks, which include flooding, reflection and amplification tactics, remain the predominant type of denial of service, most likely because they are simpler to implement and require no knowledge of the victim's service. These types of attacks are now readily available and relatively cheap to purchase as-a-service on the so-called "dark web". Meanwhile, application-layer attacks establish connections to the victim service and pose as legitimate traffic, with the intent of exhausting finite resources. These attacks, which are often equally devastating, have steadily risen in use over the last few years.

- Multi-vector attacks – as the name suggests use combinations of different denial of service tactics. These types of attacks are also on the rise.

Recently, DoS attacks have changed in size, scale and sophistication. Now, they are more likely to be complex multi-level assaults that combine high-bandwidth floods directed at the network, with low-bandwidth attacks on specific target applications. Multi-vector attacks also lend themselves well to reconnaissance, enabling attackers to probe the target's service for mitigation tools and infrastructure protection. These types of custom-crafted denial of service attacks are also growing in number, which suggest that as attackers become increasingly familiar with the available protection methods, they are continuously looking for new ways to bypass them.

“While the frequency of attacks on the whole seems to be fairly constant, the size of attack is significantly growing, and we have seen our first 20Gbps+ attacks this year, against relatively small private company targets”

COO, DATA CENTRE & HOSTING PROVIDER

Denial of service attacks are often labelled ‘distributed’ or DDoS because attacks come from many ‘distributed’ computers. Collections of compromised computers are known as robot networks or Botnets, which can be used to launch DDoS attacks on the demand of an attacker. Increasingly, with the growth of the Cloud and the demise of the desktop PC, attackers are moving to use commercial servers attached to high-bandwidth connections rather than large groups of consumer PCs. This has resulted in the recent growth of reflection and amplification attacks where the legitimate services of the Internet infrastructure itself are hijacked to attack victim networks and services.
DDoS occurrence, impact and awareness increasing...

Like many other types of cyber-attack, DDoS was originally used by computer-savvy hobbyist hackers for fun. It has since evolved into a powerful tool for cyber-crime, cyber-protest and even cyber-warfare; the same attacks can be used to cripple online businesses, advance ideological agendas, extort ransoms or even battle with nation states. Once a phenomenon that was particular to online gaming, it has recently made headlines for attacks on financial organisations and government websites. These attacks are increasing in number and are spreading across verticals, with e-commerce, entertainment and other internet-driven industries more recent DDoS targets.

This trend has been echoed in our investigation, with not a single company stating that they believe DDoS is occurring less frequently. Rather, the majority of the directors that we have spoken to believe that DDoS is occurring more frequently and even those companies which have not been impacted by DDoS in the last year believe that, on the whole, it is increasing in occurrence. With more businesses aware of the rising threat of denial of service attacks and no shortage of denial of service attacks in the media, organisations of all shapes and sizes are questioning their current strategies and are turning to their service providers for DDoS detection and mitigation.

Unfortunately, the size and scale of data centre, hosting, network and infrastructure service providers and their extensive customer bases in itself offers an attractive target for DDoS attackers, due to the multiple entry points and significant aggregated bandwidth. Indeed, a large proportion of the different service providers involved in our investigation have been impacted by DDoS in recent years.

**FIGURE 1: “Has the company you represent been impacted by DDoS attacks?”**

<table>
<thead>
<tr>
<th>Data centre &amp; hosting providers</th>
<th>Managed data service providers</th>
<th>Network service providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impacted in the last year: 38%</td>
<td>Impacted in the last year: 54%</td>
<td>Impacted in the last year: 33%</td>
</tr>
<tr>
<td>Impacted in the last 1+ years: 54%</td>
<td>Impacted in the last 2+ years: 50%</td>
<td></td>
</tr>
<tr>
<td>Not impacted: 8%</td>
<td>Not impacted: 12%</td>
<td>Not impacted: 67%</td>
</tr>
</tbody>
</table>

Source: Megabuyte Security in the data centre survey

...And IT security budgets are reacting

Traditional First Line of Defence tools, such as firewalls, are not capable of providing complete protection against the various types of denial of service, while in-house developed tools are typically slower to combat DDoS than what is deemed appropriate for the majority of internet-dependent businesses. Meanwhile, as the threat landscape has expanded and developed, IT security has increasingly become a mainstream operational consideration that is drawing increased board-level attention and therefore a larger portion of IT budgets. Almost three-quarters of the companies we surveyed said that their IT security budget is increasing over time, while an equal number indicated that the size of the budget was specified each year as indicated that it was unspecified. Surprisingly, a handful of respondents said that an IT security budget was unavailable, suggesting that security may not yet be a top ongoing priority on every company’s agenda.

"We have automated tools along with procedures to black-hole routes with all of our carriers... Plus, we have lots of bandwidth to swallow most attacks while we identify and mitigate!"  
MANAGING DIRECTOR  
DATA CENTRE & HOSTING PROVIDER
Impacts

Impact divided across service providers

In the last year alone, global DDoS attack targets have ranged from high-profile social media companies such as LinkedIn, to banks including Citizens Bank and RBS, to major hosting websites, to Nato-operated websites, to World of Warcraft online gaming and even Hong Kong’s referendum voting websites. Clearly, there are a number of industries that are more likely to attract hacktivist-type DDoS threats, including government and financial institutions, but while these industries remain under fire, recent attacks show that e-commerce, gaming and social media are also now targets.

It is fairly common for service providers to have diverse customer bases and so the majority of them are also likely to experience DDoS attacks. For example, in our investigation, the customers of the companies we spoke to were typically spread across multiple verticals; only a fifth of the companies we surveyed focused on two or fewer industries. Interestingly, an equal number of the companies that we surveyed said that they had been impacted in the last year, as said that they had not been impacted by DDoS in any of the time scales that we listed. A small number of companies said that they had been impacted in either the last 1-2 years or the last 2+ years.

The clear divide between the companies that have and have not been impacted could suggest that some of these companies have already implemented successful DDoS protection and have therefore seen little impact from denial of service attempts. Some of the service providers that we spoke to also suggested that they do not operate at the level at which DDoS would be a concern, although others noted that they can be subject to DDoS attempts between 10 to 50 times each day.

“No impact due to our DDoS service”

NATHAN MARKE
CTO DAISY GROUP

From our discussions, we have found that service providers’ customers have experienced mostly modest or significant impacts from the worst DDoS attack in the period, while the majority of service providers themselves also suffered some minor impacts.

FIGURE 2: “How do you rate the impact of the (worst) attack?”

Tools to help detection

The majority of attacks witnessed by the companies we spoke to were brought to the attention of the respondents by their existing DDoS platforms or tools that displayed high bandwidth spikes. Some were also affected by infrastructure outages and application outages. Unfortunately, a number of respondents also said that they were alerted to the attack by their customers, who complained of service issues, suggesting that the service provider may not have tools in place to quickly mitigate these attacks before their customers are negatively impacted.
We spoke with the CIO at a leading pan-European provider of managed network, communications and hosting services to better understand who stands to be impacted by denial of service attacks, what defences are available and why, in this business, every minute matters.

Q. Which types of companies are commonly targeted by DDoS attacks? Where is the major pain being felt?
“There are of course certain types of businesses that invite denial of service attacks simply because of the industry they operate in. However, as market trends have shifted towards shared infrastructures such as public Cloud, I actually believe that the real victims of these attacks are the innocent bystanders that can suffer performance issues as a side effect of multiple companies being hosted on shared infrastructure. The very nature of these services enables DDoS attacks to propagate.”

Q. So how do service providers typically become aware of a DDoS attack taking place?
“For us, if it gets to the point where we hear complaints from our customers, it means we have almost failed. Because of this, we use a combination of technologies and monitoring to identify potential DDoS attacks, as well as use black-holing and other mitigation strategies if an attack is underway. Transmitting network telemetry over an out-of-band network can help to determine sudden surges or signpost the preparation stages of an attack, just like how a car thief may test the handle on a car to size up what is available. Changes to traffic patterns, such as an elevated number of incomplete transactions, can help to indicate that a DDoS is on the way before it is fully launched.”

Q. Have the tools that you use to counter DDoS attacks changed over time?
“For several years we used an in-house developed and maintained DDoS mitigation tool, which did a good job at defending but was somewhat slower than what is available commercially today. Because of this, relatively recently we implemented a purpose-built DDoS solution which, although at reasonable cost to us, fit our brief and provided an overall better use of our IT resource. You have to remember that this is an industry where the difference between a one minute outage and a five minute outage is a really big deal to our customers, particularly those, such as online-retailers, whose website is absolutely business critical.”

Q. How would you describe the overall awareness of DDoS attacks? Are companies willing to pay a premium for DDoS protection from a managed service provider?
“I think that there are really three types of companies that have a good awareness of DDoS. Firstly, of course, there are those companies that have been directly targeted by denial of service attacks and therefore understand first-hand the importance of DDoS mitigation. There are also, as I mentioned previously, the bystander victims that have experienced performance issues due to DDoS attacks aimed at other companies. Thirdly, any company that has half an eye on the media should certainly be aware of the impact that denial of service attacks can have. DDoS now makes the front cover, not just technology section and so I believe that, at the very least network managers, infrastructure managers and IT directors will have an awareness of the importance for DDoS mitigation. From our perspective, customers that have either been impacted by DDoS directly, or understand that it is probably only a matter of time until they are impacted themselves, are willing to take premium services.”
Defences

Multi-vector attacks require multiple defences

The combination of different denial of service attack methods can create a smokescreen for other malicious activity. For instance, a DDoS attack may create noise and divert attention from a data breach attempt. This multi-vector attack technique has led to a similarly multi-vector defence portfolio, including network appliances to handle infrastructure exhaustion and stealthy application-layer attacks and on-demand scrubbing centres or Cloud-based DDoS mitigation to defend against volumetric attacks that may be too large to be mitigated on-premise.

Black-holing a common but crude defence

A black-hole route can be used by a Cloud, data centre or hosting provider to discard excess traffic as it enters the network. This method is very straightforward to implement, which makes it an efficient (and commonly used) way to relieve a saturated network and help prevent customers other than the victim from experiencing service issues as collateral damage of the attack. However, the issue with black-holing is that the victim IP address(es) under attack are made unavailable from the internet; in effect, the attackers objective of denial of service to the target has been successfully completed.

When asked about preferred defence methods, the service providers in our study indicated that DDoS monitoring and mitigation network appliances were both the most used method out of three choices (Figure 3) and the method that the largest number of companies have plans to adopt in the future. When deployed in line, appliances are capable of inspecting, analysing and responding to threats in near real-time; this clearly makes them a good choice for DDoS mitigation.

Interestingly, there were still four respondents that have no plans to adopt any of the three defences and one service provider said that it does not operate at the level at which it would require DDoS protection.

Managed security services on the rise

There has been a general trend that has seen outsourcing move up the food chain to more mission-critical activities such as security. Now, a number of managed security service providers (MSSPs) offer DDoS monitoring and mitigation amongst other security services. Indeed, the companies involved in our survey include service providers that utilise DDoS mitigation from another service provider as well as those which offer managed DDoS mitigation services to their customers. In our study, managed DDoS mitigation was the second most popular tool.

“We have adequate tooling to contain DDoS attacks”

Technical Director
Data Centre & Hosting Provider
Cloud-based mitigation to combat high-volume attacks

Cloud-based mitigation is often complementary to on-premises appliances and used specifically for volumetric attacks that are greater than the size of the Internet access pipe. In these cases, traffic is lost due to congestion within the network of the end-users’ Internet service provider. Typically, Cloud-based mitigation services are called in to play when a customer premises appliance detects pipe saturation. This triggers a reroute of all victim traffic to a remote ‘scrubbing’ centre, from which only the scrubbed traffic is then forwarded on. Cloud-based DDoS mitigation was the least utilised mitigation choice amongst the service providers we spoke to, with only six companies indicating that they already have this employed. It also appears to be the most unpopular of the three types, as almost half of the companies we spoke to said that they currently have no plans to adopt this.

“We always look to improve and learn”

NIGEL SHAW, COO PULSANT

DDoS perceived as a high priority

As mentioned previously, it is increasingly the case that service providers are targets for denial of service attacks. Reports suggest that the attacks have also continued to grow in size to the point that entire service provider networks may be disrupted. The vast majority of companies that we spoke to believe that DDoS defences are either more important than or as important as other types of security defences. Only two companies believed that other security defences were more important. Service providers also feel that DDoS protection is high on their customers’ list of priorities, as a similar number stated that DDoS defences are of more or equal importance here. Five of the respondents believe that DDoS is more important to both the company they represent and their customers, compared to other security tools.
"The statements from the individuals that have participated in this study drive home the fact that DDoS attacks and cyber threats can be catastrophic for any Internet-connected business. It illustrates the increased awareness and value of taking proactive steps for protection against these sophisticated attacks.

"As enterprises increasingly rely on hosted critical infrastructure or services, they are at an even greater risk from these devastating cyber threats – potentially even as an indirect target"

Ironically, the size and scale of hosting or data centre operator network infrastructures and their massive customer base results in an expansive attack surface due to the multiple entry points and significant aggregate bandwidth made available as a conduit for a damaging and disruptive DDoS attack. As enterprises increasingly rely on hosted critical infrastructure or services, they are at an even greater risk from these devastating cyber threats – potentially even as an indirect target.

Cyber-attackers know no boundaries when it comes to targeting their next victim, and the drivers for launching attacks are far-ranging and difficult to predict—anyone can become a victim at any time. As the attacks continue to become larger, longer and more sophisticated, businesses that rely on their online service and web presence as a revenue source cannot remain complacent.

"Anyone can become a victim at any time."

The findings in this report strongly underscore the importance of including a First Line of Defence against DDoS attacks as a vital component of your network security architecture. With comprehensive visibility into the DDoS-related security events taking place on your network and the ability to respond in real-time to block them, you are proactively protecting your customers from one more category of damaging cyber threats directed at your network and their services.

"Any organisation that has not taken the appropriate steps to protect against these types of attacks, will be at serious risk."

Any organisation that has not taken the appropriate steps to protect against these types of attacks, will be at serious risk. I believe we have seen ample evidence of that need with the data points and analysis captured in this report.”

ASHLEY STEPHENSON
CEO CORERO NETWORK SECURITY
Responsibility

It’s not you, it’s me
As the size, complexity and regularity of denial of service attacks on organisations continues to rise, it increasingly seems the case that service providers have an obligation to their customers to protect against these attacks. The vast majority of the service providers that we spoke to believe that they have a responsibility to implement tools or services to protect themselves against DDoS attacks, while 23 different companies also said that they have a responsibility to do so for their customers’ protection. Surprisingly, three companies indicated that while they felt that they needed to implement DDoS mitigation for their own protection, they did not feel responsible to do so for their customers.

“Very minor impact for us due to our scale, capacity, and automated tools, but customers not taking a clean feed from their service provider can be significantly impacted until their routes are black-holed”

NIGEL SHAW
COO PULSANT

Attacks trigger DDoS investment
Despite being a prime target, service providers are in fact well-placed to deliver solutions to combat the majority of attacks on availability and our study suggests that many of them are already implementing DDoS mitigation and monitoring services. The multi-vector features of DDoS mean that multiple layers of defence are required for comprehensive protection and some service providers have said to us that they believe ongoing investment is needed to update the platform, improve their monitoring and analysis of attacks and to understand steady-state traffic flows.

Perhaps unsurprisingly, the service providers whose customers experienced a significant impact from the worst DDoS attack in the period, all made at least some changes to their defences following the attack. In total, out of the seventeen services providers that said in our survey that they had been impacted by DDoS, nine companies said that they made some changes to their defences following the attacks. Two companies implemented entirely new defences while one company was unsure of any changes. There were also five companies that made no changes to their mitigation strategy following the DDoS, although each of these companies noted either minor or no impact from the worst attack in the period, suggesting that they were not convinced of the need to improve their defences.

 “[We] added extra diversity, upgraded some hardware and migrated customers away from legacy networks to our NGN.”

GROUP STRATEGY DIRECTOR
MANAGED NETWORK AND DATA SERVICES PROVIDER

“We provide managed DDoS services for our clients that mitigate these attacks”

NATHAN MARKE
CTO DAISY GROUP
Opportunity

Service providers well-placed to offer DDoS protection

The evolution of denial of service attacks and the increasing importance of the Internet to all businesses today suggest that there is a sound opportunity for service providers to offer DDoS protection to their customers. Certainly, the premium placed on all types of cyber security is becoming increasingly attractive as a driver for new service offerings. In this case, not only do customers stand to benefit from improved attack protection and access to more effective, faster defence technologies but the service providers who are in a unique position to provide the managed monitoring and protection services will be able to generate incremental revenue streams.

“We provide proactive DDoS monitoring for our network, along with having significant upstream bandwidth to be able to swallow most attacks”

MANAGING DIRECTOR
DATA CENTRE & HOSTING PROVIDER

“Even when customers have had a DDoS, there is a real reluctance to spend any money on this.”

COO
DATA CENTRE & HOSTING PROVIDER

Contrasting views on business opportunity

However, there currently seems to be a disconnect between this apparent opportunity and the perceived business benefits for offering DDoS mitigation services among the service providers that we spoke with. The majority (Figure 4) said to us that they see just a modest business opportunity from DDoS and a large proportion see minimal opportunity. Delving a little deeper, some service providers believe that customers still do not want to invest in DDoS protection — whether internally or from their service providers — even after they have been impacted by a denial of service attack.

FIGURE 4: “How do you rate the business opportunity for offering DDoS/Cyber-threat protection to your customers?”

Source:
— Megabuyte Security in the data centre survey

This view is in stark contrast to the handful of companies that we spoke to which do believe that there is a significant opportunity to offer cyber threat protection to their customers. Most of these companies currently offer managed DDoS services and believe that customers are willing to pay a premium for protection, particularly when they already receive other managed security services.
Disclaimer

IS Research Ltd will not accept any liability to any third party who for any reason or by any means obtains access or otherwise relies on this report. IS Research Ltd has itself relied on information provided to it by third parties or which is publicly available in preparing this report. While IS Research Ltd has used reasonable care and skill in preparing this report, IS Research Ltd does not guarantee the completeness or accuracy of the information contained in it and the report solely reflects the opinions of IS Research Ltd.

The information provided by IS Research Ltd should not be regarded as an offer to buy or sell securities and should not be regarded as an offer or solicitation to conduct investment business as defined by The Financial Services and Markets Act 2000 ("the Act") nor does it constitute a recommendation. Opinions expressed do not constitute investment advice. Any information on the past performance of an investment is not necessarily a guide to future performance. IS Research Ltd operates outside the scope of any regulated activities defined by the Act. If you require investment advice we recommend that you contact an independent adviser who is authorised by the Act to conduct such services. IS Research Ltd does not have any direct investments in any companies contained in the report and has compiled this report on an independent basis.