White Paper

Investing in security versus facing the consequences

...implementing DNSSEC to mitigate financial and brand risks

A White Paper by Bloor Research
Author : Fran Howarth
Publish date : September 2010

The problems of DNS security have long been known, which is why DNSSEC was developed. However, it is only now that widespread deployment is possible.

Fran Howarth

Executive summary

The internet and associated electronic communications mechanisms have revolutionised the way that we handle information, connect with each other and interact with organisations. Today, organisations routinely offer services via the internet to their customers, such as online banking and ecommerce. However, the information exchanged via such services is often highly sensitive and can be used for fraudulent purposes such as identity theft or the stealing of funds from an online banking account. One key avenue for attack is via the domain name system (DNS). DNS is the directory service for the internet, ensuring that messages and website requests are directed to the intended recipient or resource. The reason for this potential vulnerability is that DNS was developed many years ago, when efficiency was a greater concern than security. It has long been known that DNS contains vulnerabilities that can be exploited by hackers, allowing them to hijack websites and other exploits. Because of this, DNS Security Extensions (DNSSEC) was developed some years ago to provide greater authentication and integrity for DNS lookups by cryptographically signing the responses that are given.

However, uptake of DNSSEC has been slow. It has been plagued by accusations that it is too complex to administer and manage and because there were few commercial products for serving the DNS lookups or for accepting the responses. It was also necessary for the 13 root servers that form the backbone of the DNS system to be cryptographically signed in order for a chain of trust to be established.

Today that situation has been reversed. The root servers have been signed, top-level domains are in the process of being signed, and products are available for efficiently automating DNSSEC implementation and management. This document discusses issues surrounding why DNSSEC is needed and how it will benefit organisations in securing their internet presence to engender customer loyalty and shield themselves from security issues caused by the lack of security in DNS. It is intended to be read by any organisation that has a significant web presence that could leave them open to the threat of an attack.

Fast facts

- Cryptographic signing of DNS servers is underway. The root zone has been signed and the signing of other domains is ongoing, including the .eu domain.
- Technology products and services are now available that automate many of the tasks involved in deploying and managing DNSSEC, taking the complexity out of implementing it.
- The widespread use of DNSSEC will significantly improve the security of the internet, providing consumers with greater levels of confidence in the services offered and organisations a better ability to protect their brands and operations. Those that act now will have a tremendous window of opportunity over their competitors as adoption of the DNSSEC label on their websites will prove that the site is safe and will guarantee that users are reaching valid services.
- DNSSEC will eliminate cache poisoning and man-in-the-middle attacks against DNS and will vastly improve the security of the infrastructure of the internet.

The bottom line

Every organisation must look to shield itself from security exploits that could lead to brand and reputational damage, and even financial loss, including the threat of fines and other sanctions for failing to adequately protect sensitive data from loss or theft. One type of attack that is currently growing is that of DNS cache poisoning, which can be used to redirect communications and website requests with serious consequences.

DNSSEC was invented to solve these issues, but its take up was plagued with issues that include the complexity of its implementation and the lack of readiness of the internet infrastructure to accept DNSSEC lookups. Those issues have now been solved and its use is likely to spread fast. It is the foundation of next-generation internet security and is part of the future. Organisations should look now at deploying DNSSEC in the near future to protect themselves, their reputations and their customers from the damage that can be caused by a DNS attack.

What DNS is and how it works

The domain name system (DNS) is essential for the efficient functioning of the internet. It is sometimes referred to as the phone directory for the internet in that it acts as a lookup service to ensure that emails are sent to the correct server and mailbox and that website requests reach the real address, rather than being directed to an incorrect website. On a technical level, computers work with binary identifiers that are used to locate and address computer resources, but strings of numbers are difficult for humans to remember. Because of this, DNS was invented to translate numerical identifiers into domain addresses that are meaningful to humans, associating the names with IP (internet protocol) addresses. For example, without DNS, a user would have to remember and type in "66.249.92.104" in order to reach popular web search engine Google.

DNS is a hierarchical system that works with a number of domains, the top-level of which comprises 13 root servers spread throughout the world. Under the root level are a number of sub-domains. The next level down is the top-level domain, examples being .com, .org and .edu, as well as country-level top-level domains, such as .ru and .nl. The next level down usually points to a company or an organisation, such as the 'Google' in www.google.com. Beneath this is the host name which is the requested resource, that is, the 'www' in website addresses. DNS works by assigning authoritative name servers for each domain in the hierarchy, which are responsible for assigning names to the IP addresses for their own domain, and in turn assign other authoritative name servers for their sub-domains.

The following is an example of how the DNS lookup system works, made freely available from Wikipedia.

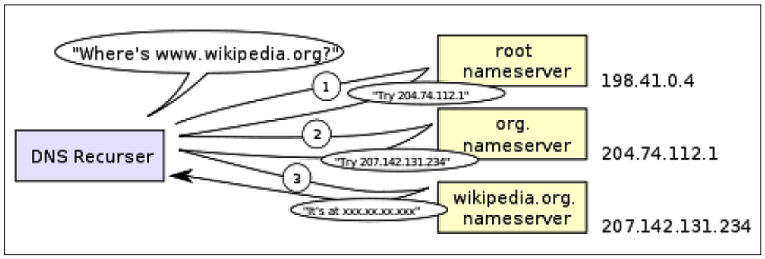

Figure 1: How the DNS lookup system works

Security issues with DNS

DNS was originally invented in 1983 and was intended to increase the efficiency of the internet. Its invention is credited with the widespread growth of the use of the internet, ushering in a whole new age of electronic communications. However, it was not originally designed with security in mind and it has a number of known security issues.

One class of vulnerabilities known to affect DNS is that of cache poisoning, which can lead to exploits such as identity theft, malware distribution and the dissemination of false information. In a DNS lookup, when a user requests an IP address for a website, the DNS request follows the chain as shown in Figure 1, starting from the root server down to the server that owns the zone for that website address. In order to make the process more efficient, the response may be cached by the local DNS server or the ISP serving the request to make the process faster for the next user requesting that same resource.

The vulnerability with cache poisoning is that a hacker can impersonate a real DNS server, which allows them to insert a different IP address onto the DNS system. This fake address will then direct the user to a spoofed copy of a real website without the user or the owner of the website realising that anything is wrong because the DNS server has been tricked into believing that it has received authentic information. As well as redirecting the user to a bogus website, the attack can be combined with malware that can steal information from victims, such as social security numbers and credit card data, or that can be installed on the device to hijack it and use it to relay spam as part of a botnet. This technique can also be used to redirect email.

The DNS cache poisoning vulnerability has been known about for some time. In 2005, security researcher Dan Kaminsky used a high-bandwidth connection to examine 2.5 million of the approximately 9 million DNS servers connected to the internet. He found that of the 2.5 million examined, 13,000 had a cache that could definitely be poisoned, 60,000 were very likely to be open to this type of attack, and 230,000 were probably vulnerable to DNS cache poisoning attacks.

Three years later, in July 2008, Kaminsky announced that he had discovered a fundamental flaw in the DNS protocol itself, allowing an attacker to easily perform cache poisoning attacks on any DNS name server, enabling a wide range of attacks to be made in addition to website impersonation and email interception, such as being able to bypass authentication controls when users use a feature common on many websites that allows a forgotten password to be supplied to them. As a temporary fix, it was recommended that source port randomisation be implemented so that an attacker would need to know the transaction ID as well as the port from which the transaction was sent. However, a determined hacker with sufficient computing resources could still defeat this fix. As a result, it is recommended that DNSSEC (DNS security extensions) be implemented to provide cryptographic assurance in the form of digital signatures that the results provided by DNS are genuine.

How DNS security issues affect organisations

Although there is not a great deal of information available on the specifics of DNS security attacks, organisations around the world have been affected, from big online retailers to the military. In January 2010, the Center for Strategic and International Studies released a report based on a survey of 600 organisations in 14 countries worldwide. One of the key findings of the report was that 57% of respondents stated that they have been the victims of DNS poisoning attacks in the past year that resulted in web traffic being redirected, with nearly half of those reporting multiple monthly occurrences of such attacks. More than 60% of those experiencing DNS poisoning attacks reported that the exploits had a significant operational impact on their systems.

Two cases received press attention in 2009. These were the Irish ISP Eircom, which reported in July 2009 that it had been the victim of a DNS cache poisoning attack that resulted in two major service outages and that led to its customers being redirected from popular websites such as Facebook to bogus websites. Earlier that year, in April 2009, one of the biggest banks in Brazil, Bradesco, suffered a DNS cache poisoning attack on its ISP that led to some of its customers being redirected to fraudulent websites that attempted to steal passwords and install malware on their computers. According to press reports, just 1% of the bank's customers were affected by the attack. However, considering that Bradesco claimed 57.1 million customers in the first quarter of 2010, that is still a considerable number of people.

The problems that an organisation involved in such an attack could face include damage to its brand or credibility, or even legal liability from customers that become victims of scams resulting from the DNS attack. In the majority of cases, the customer will not know that they have been redirected to a spoof site, where hackers could harvest passwords and user names and even siphon off funds—but then the organisation may not necessarily know either that their customers are being redirected to a bogus site that misrepresents their organisation and that they could be losing business as a result. If the organisation involved has not taken steps to secure its DNS servers, it could be held liable for any damage caused, as it has not deployed sufficient security controls. At present, there are few industry standards or government regulations that specify DNS security controls, although PCI DSS from the Payment Card Industry specifies that DNS servers must be scanned for vulnerabilities on a regular basis as these could lead to services being spoofed, which could allow credit card information to be compromised. It is mooted that controls will be beefed up further within the PCI standard to specify DNS security.

The promise of DNSSEC

DNSSEC stands for DNS security extensions. It was developed by the Internet Engineering Task Force and is a suite of security extensions that provide authentication regarding the origin of DNS records, including authenticated denial of existence for bad records and data integrity through verification that the response was not modified in transit. This integrity of the DNS response is provided using digital signatures and asymmetric cryptography using two key pairs, these being a public and a private cryptographic key, with the public key published in the DNSKEY records so that anyone can access it. In this way, cryptography is being used to provide assurance of the integrity of the DNS record, rather than to obscure a message as in the use of cryptography for encryption.

Each zone in the DNS hierarchy provides assurance for all the sub-zones beneath it to form a chain of trust. The root zone—the highest level in the hierarchy—contains the public records for all the domains beneath it, through the top-level domains such as those for a country or zones such as .com or .org, down to those owned by specific organisations. Thus, the DNS records beneath the root zone can be trusted owing to the signing of the records in the root zone. This chain of trust is depicted on the right-hand side of Figure 2.

There is a common misperception that DNSSEC in unnecessary. Many organisations argue that they are already using Secure Sockets Layer (SSL) or its successor Transport Layer Security (TLS) cryptographic protocols for managing the security of a message in transmission on the internet or to authenticate the website a user is connecting to. Both these protocols incorporate public and private cryptographic key encryption and use a digital certificate. It is used to encrypt the traffic. However, if the DNS cache is poisoned and the website is hijacked, SSL or TLS will still allow the user to be transported to the wrong site, albeit in a secure fashion. It is a relatively easy task to obtain an SSL certificate, especially as they can even be self-signed, and this is a tactic that many phishing sites deploy. Only through using DNSSEC can the integrity of the website be guaranteed.

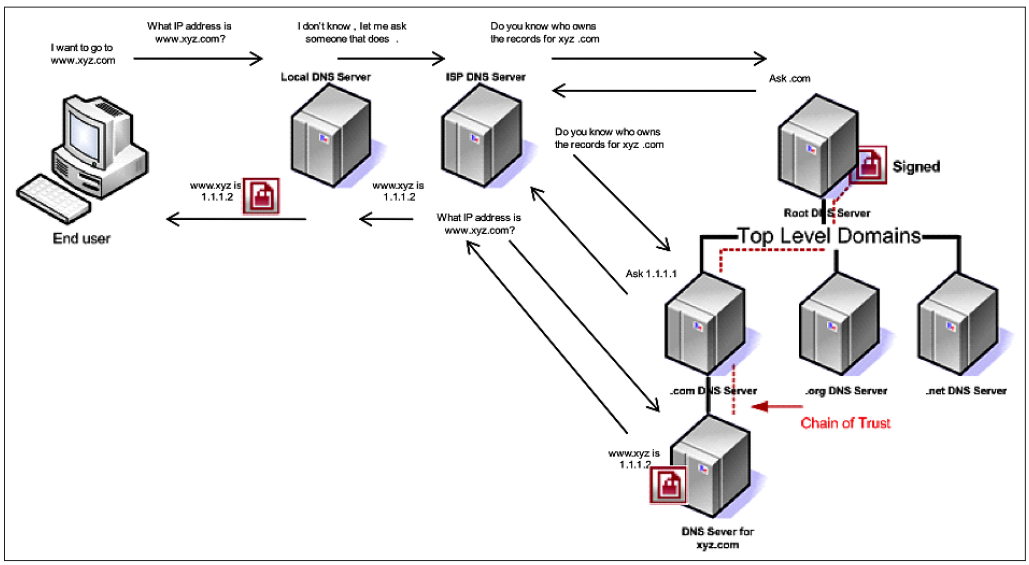

Figure 2: The DNS system 'chain of trust' Source: F5 Networks

DNSSEC deployment

DNSSEC was originally developed some 12 years ago, but its deployment has suffered many setbacks as challenges had to be overcome such as the lack of automation for processes such as key generation and management. One particular reason for the lack of take up of DNSSEC was that the 13 servers that make up the root zone at the top of the DNS hierarchy were not signed until July 2010, having been tested for some time. It was essential that the root zone be signed since all sub-zones rely on the root zone being signed. Because of this delay, technology vendors lacked the incentive to develop products for validating DNSSEC responses since there were no servers providing DNSSEC signed responses. Equally, there were no incentives to develop those servers since there were no clients accepting responses.

However, there was some level of adoption prior to the signing of the root zones. Some country-level top-level domains, including Brazil, Bulgaria, the Czech Republic, Puerto Rico and Sweden, have adopted DNSSEC and the first ISP to adopt DNSSEC was TDC in Sweden. In February 2009, VeriSign, which provides internet infrastructure services including the operation of two of the 13 root servers and top-level domains that include .com, .net, .cc, .name and .tv announced that it would deploy DNSSEC across all of the top-level domains that it operates within 24 months.

Office of Management and Budget mandate:

"The efficient and effective use of our networks is important to promote a more citizen-centered and results-oriented government. The government's reliance on the internet to disseminate and provide access to information has increased significantly over the years, as have the risks associated with potential unauthorized use, compromise and loss of the .gov domain space. DNSSEC provides cryptographic protections to DNS communication exchanges, thereby removing the threats of DNS-based attacks and improving the overall integrity and authenticity of information processed over the internet."

To spur adoption, the Office of Management and Budget of the US issued a mandate in August 2008 that all federal agencies should deploy DNSSEC as a new authentication mechanism for all websites in the .gov sub-domains by the end of 2009 in order to prevent hackers from hijacking web traffic and redirecting it to bogus sites. However, as of August 2010, many .gov domains remain unsigned, including many large federal agencies and departments. Problems cited as delaying deployments include the need to replace dated software and ageing hardware with those that support Windows 2008 DNS and BIND 9.0;BIND being one of the most commonly used DNS servers. However, the top-level .gov and .edu domains have been signed.

Although many have criticised federal agencies for not implementing DNSSEC by the deadline set, some have stated that the deadline was too tight and that end-2010 is a more realistic timeframe. Once all the .gov domains have been signed, the market is likely to receive a boost and more vendors and service providers will actively develop products and services. The federal government deployment is being used as a blueprint by vendors that are developing tools and methods to automate the processes involved, which will be used in the commercial sector to ease implementation and use, and reduce the cost of deployment. As of September 2010, the .org and .info zones have also been signed—the third and fourth largest generic top-level domains in use, and the largest, .com, will be signed soon.

Some countries, such as Sweden, have started providing incentives for their major DNS providers to support DNSSEC and clients are starting to appear for validating DNSSEC responses, including a plug-in for the Firefox browser, a test validation LDNS server from US communications provider Comcast and a DNSSEC-aware client is included in Microsoft's Windows 7 operating system. Indeed, Comcast is one of the first commercial operations to announce the deployment of the DNS root key to all of the DNSSEC trial servers that it operates in the US, allowing all of its customers to start using the trial servers by changing their DNS server IP addresses to those of its trial servers.

DNSSEC deployment

Because of the initiatives that have been taken, the pace of adoption is growing rapidly, with real growth having been seen over the past 12 months in particular. By the end of the first quarter of 2011, the .com zone will have been signed. When this has been done, more than 200 million domain names will be secured by DNSSEC—equivalent to more than half of the URLs in existence worldwide. Further adoption will also likely be spurred as further countries adopt the stance of the US government, which demands that all websites used by the US government at all levels willbe secured with DNSSEC. Governments may even go further than this and demand that all organisations handling money and customers, such as financial services and ecommerce organisations, implement DNSSEC to keep that data secure. ICANN, the Internet Corporations for Assigned Names and Numbers, which is responsible for assigning and managing IP addresses, is also spurring further adoption. It is mandating that all new top-level domains that are created must utilise DNSSEC or approval will not be granted.

Other measures taken to spur further adoption need to be taken further down the chain of trust than the root servers and top-level domains. What is needed is that more ISPs and network service providers follow the example of Comcast in the US, which offers DNSSEC to all of its customers. To spur adoption among consumers, router equipment manufacturers must ensure that they develop equipment for home users that incorporates support for DNSSEC because, at present, many older routers choke on DNSSEC traffic as they are unable to handle the higher bandwidth required for DNSSEC records, which are in the magnitude of ten times greater than ordinary DNS records. Once DNSSEC has been deployed throughout the DNS hierarchy, from the root level to end users, the internet will be a much safer place. According to Ram Mohan, CEO of Afilias and board member of ICANN, that day is just around the corner.

DNSSEC—ready for prime time

Now that DNSSEC has been thoroughly tested and most of the challenges in deployment have been ironed out, such as how encryption keys would be administered, and the root zone has been signed as well as some top-level domains, the basis for widespread deployment has finally been laid. There is a range of technology vendors that incorporate best practices learnt through the testing of DNSSEC deployments into products that automate many of the tasks involved in deployments to make DNSSEC implementation an easier task. These include tools that can be accessed through a graphical user interface that automate key generation, signing, storage and policy management, key rollover as keys expire to reduce the chance of key compromise, and global server load balancing to map the IP address against a geolocation database for more efficient operation.

> *"A big security exploit against the DNS will happen. Organisations cannot afford to sit around and wait. The pain of being behind will be the driving force. The question that will be asked at the board level is—why are we so behind on security? Those organisations that move now will have a window of 6 to 12 months, which will give them tremendous competitive positioning."*
>
> Ram Mohan,
> CEO Afilias and board member of ICANN

According to Tuscany Networks, a consultancy specialising in the DDI (DNS, DCHP and IPAM) markets, the lack of signed zones was not the only reason why take up of DNSSEC has been slow. Rather, it was the difficulty of implementing and managing DNSSEC because of its complexity, since it requires a lot of maintenance with manual processes adding to the costs of deployments. However, the products that are available on the market today remove much of the complexity by allowing all tasks to be handled through one central management interface, where policies regarding key management can be effectively enforced. This allows keys—key signing keys and zone signing keys—to be automatically generated simply and intuitively, providing choices for which cryptographic algorithms are to be used, the type and length of key, and validity, expiration and rollover periods. Most tools for managing DNSSEC provide an interface for zone lists and allow for multiple zones to be signed at the same time.

Now that tools are available to make the management of DNSSEC deployments an easier task and the root zones have been signed, the way is open for more widespread deployment. The signing of the top-level domains is progressing, helped by factors such as the federal government mandate from the US and efforts made by other countries to spur take up.

It is therefore now time for commercial organisations and other governments around the world to plan to deploy DNSSEC. Given the ease with which DNS can be hacked—the Kaminsky bug found in 2008 has led to countermeasures being developed, but they do not fix the problem, rather just making DNS harder to attack—and the damage that organisations can face in terms of brand, reputation and lost revenues from being attacked, all organisations should at least look to deploy DNSSEC for their external-facing websites. This will prevent customers from being victimised by hackers looking to steal identity, health or financial information—or any other information that is valuable—by hijacking the brand.

At the very least, organisations that have a large online presence, offer online sales, are particularly big name brands, or that handle highly sensitive information such as healthcare records should take a look at how DNSSEC can protect their brand from being damaged and their customers becoming victims of cyber crime. There are many regulations that demand that high levels of security are applied to protect information, such as the data protection acts of all countries in the EU. As more domains are signed and organisations start to take up the technology, those that have not protected their DNS records could see themselves the subject of fines or other sanctions for non-compliance. As yet, although no regulations or industry standards specifically mandate DNSSEC, it is likely that it will become a requirement of government regulations or standards, such as PCI DSS from the payment card industry, in time.

DNSSEC—ready for prime time

> *"DNSSEC represents the biggest change to DNS since its inception and is one of the most significant security updates to the internet over the past few years. DNS is the world's largest decentralised, distributed and most effective directory system. The addition of DNSSEC makes DNS a trusted directory system that will become the foundation for a much more secure and trusted internet."*
>
> Nathan Meyer,
> product manager, F5 Networks

As DNSSEC becomes more widely adopted, consumers will start to demand that their banks, health service providers and ecommerce sites have implemented DNSSEC so that they can be sure that the resource they are visiting is valid and has not been spoofed. An add-on is already available for the Mozilla Firefox browser and its use will become more widespread. This will facilitate more secure sharing of information online and will increase consumer trust in online transactions and in the brands and validity of the services they wish to access.

DNSSEC is finally moving out of early mover stage to mainstream adoption, although its take up among enterprises is, as yet, small. This creates a window of opportunity for organisations that adopt DNSSEC, which enables them to demonstrate to customers that their brand names and websites are safe, and to guarantee that when users visit their websites, they are indeed arriving at the intended destination.

DNSSEC will not mitigate all security vulnerabilities affecting organisations, but it will be a good complement to other measures being taken. Once seen as overly complex to implement and manage, automated tools are now available that make it easy and cost-effective to secure precious online estate and boost consumer confidence in the overall security of the internet.

Summary

The problems of DNS security have long been known, which is why DNSSEC was developed. However, it is only now that widespread deployment is possible as the internet infrastructure is being readied to accept DNSSEC lookups and tools are available to remove the complexity involved in its deployment. Its use will do much to improve the security of the internet, boosting consumer confidence once they can be sure that the resource they are trying to reach, such as their bank's or healthcare provider's website, are genuine and have not been spoofed by hackers looking to steal their personal information for financial gain. This will be a boost for organisations and will allow them to extend the services that they offer in a secure manner whilst protecting their brands from harm and their organisation from security exploits that could leave them unable to comply with the regulations that they face regarding the adequate protection of sensitive information. Over the coming year, the deployment of DNSSEC is set to expand rapidly. Organisations that wish to benefit from the protection that it offers their vital internet presence and electronic communications should start planning their deployments and take a look at the technology tools that are available to help them improve their overall security.

Further Information

Further information about this subject is available from
http://www.BloorResearch.com/update/2056

Bloor Research overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter "noise" and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent over two decades distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

About the author

Fran Howarth
Senior Analyst - Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.

Copyright & disclaimer

2nd Floor,
145–157 St John Street
LONDON,
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com