The smart solution to cyberattacks

Intelligent protection is needed to guard the financial services industry from cyberattacks. President of **Corero Network Security** Andrew Lloyd outlines the threats facing the sector, the issues with traditional methods of defence and the need for organisations to take a proactive stance in their approach to online security.

Distributed denial-of-service (DDoS) attacks pose a serious and increasingly sophisticated threat to online services. The target is flooded with requests from numerous sources, with the intention of inhibiting the success of legitimate requests. In early 2018, GitHub suffered a 1.3Tbps attack, the largest in history – a record that was quickly broken by a 1.7Tbps assault on an unnamed provider.

The 'Half year 2018 DDoS trends report' published by Corero, a DDoS defence solutions provider with 20 years' experience, shows that these attacks are rising in number and mutable in approach. Using data from Corero customers, the report concludes that, year over year, the number of DDoS attacks has increased by 40%, with one in five victims receiving a second attack within 24 hours. Plus the attacks are changing, becoming shorter and more frequent – 82% lasted under ten minutes.

> "I think the real issue is whether banking executives believe that it is happening to them, and if non-IT executives are equipped to have this discussion with their IT colleagues."

The risks are particularly acute for the financial services industry, as Corero's president, Andrew Lloyd, explains. "Banks and financial services at large are undoubtedly one of the most attacked types of organisations, simply because if the attack is successful, then the criminals who are perpetrating them stand to either gain financially or cause financial harm to the victim," he says.

A breach of trust

A cyberattack such as DDoS, which results in a loss of functionality, can have serious consequences. If a successful attack becomes public knowledge it can result in an erosion of trust, reputational damage and a long-term loss of business. "There's only so many TSB-style outrages that any customer can tolerate," Lloyd says, referring to the IT upgrade that went wrong in April 2018, which resulted in customers being locked out of their bank accounts for weeks. In addition, compromised defences can lead to data exfiltration, allowing perpetrators to gain access to extremely sensitive information.

Check and double-check

While Lloyd does not doubt that banking executives are cognisant of the seriousness of the threat the industry faces from DDoS, he questions whether they have the necessary understanding to interrogate and assess their own protection provision. "I think the real issue is whether they believe that it is happening to them, and if non-IT executives are equipped to have this discussion with their IT colleagues," he says, explaining that receiving a simple assurance that DDoS protection is in place and active is not enough.

Executives need to discover whether the protection they have is adequate, and how long it would take to mitigate a DDoS attack. Should the response indicate that the defence time would be anything more than a few seconds, the next question must inevitably determine how much damage could be inflicted in those seconds, minutes or tens of minutes. "The only credible answer to that will be either 'a lot', or 'I don't know'," Lloyd points out.

Many of the products available to the industry are not sufficient to deal with the threat. Internet gateway solutions such as firewalls are not designed to repel DDoS. Manual DDoS mitigation – in which traffic deemed to be an attack is automatically detected and then manually redirected to a scrubbing centre, which separates out legitimate and fraudulent traffic – is too slow to deal with quick-fire attacks, typically needing minutes before it begins to work.

The approach taken by the majority of the financial services industry is to use a cloud-based 'always on' solution. However, the extremely high costs of this method means that banks may choose to only protect the assets that are most sensitive or vulnerable to attack, opting for an on-demand service or even no protection at all for the rest. "I think even that level of insight is going to be a revelation to some executives who presumed that all of their assets were protected," Lloyd observes.

Defend smart and fast

Corero's SmartWall Threat Defense System (TDS) offers an alternative, providing cost-efficient, fully automated and real-time DDoS protection, which allows services to remain online and functional while under attack. The defence architecture includes real-time layer 3–7 mitigation against volumetric attacks for IPv4 and IPv6 traffic, and also boasts built-in protection to counter zero-day network DDoS attacks. Always-on and scrubbing solutions can also be employed according to specific requirements.

> "It's lunacy to say that it is inevitable that you're going to be taken offline and therefore all your focus should be on recovering from going offline. There are many technologies out there – and we're not just talking DDoS – that can give you the proactive real-time defence that would stop you going offline in the first place."

A flexible architecture means the Corero TDS is extremely cost-competitive. "In comparison to having always-on in the cloud, Corero can be an order of magnitude less expensive," Lloyd says. The SmartWall TDS is available in increments of 10–100Gbps, and scales to terabits-per-second of overall protection, allowing a solution that fits the cost requirements of each client.

Let the right ones in

Corero resolves the need of allowing legitimate traffic to continue to reach the service provider. "If the DDoS protection stops legitimate traffic – a so-called false positive – that is arguably the worst thing it can do," Lloyd says. "The key mantra is 'do no harm'."

Corero's "do no harm" mantra favours allowing a tiny amount of attack traffic to pass through, ensuring accurate automatic attack detection, rather than blocking genuine requests. Furthermore, this is done without adding unnecessary latency. Employing Corero's always-on solution adds only a few tens of microseconds – a tiny fraction in terms of the transit times across the internet. "Those are the two main things that we do, and that we are genuinely world class at," Lloyd says.

Turning to Corero also mitigates a significant problem: a concentration of risk caused when numerous institutions choose the same DDoS protection provider, and the current reality in the UK and European banking industry. "If everybody's using the same defence and that defence fails to protect against a zero-day threat, then everybody fails at the same time," Lloyd says. "That means there is no UK banking for however long those attacks are launched."

Focus on prevention

Corero's products respond to a growing movement in the industry that expects companies to take responsibility for resisting rather than simply responding to cyberattacks.

"It's lunacy to say that it is inevitable that you're going to be taken offline and therefore all your focus should be on recovering from going offline," Lloyd says. "There are many technologies out there – and we're not just talking DDoS – that can give you the proactive, real-time defence that would stop you going offline in the first place."

This is evident in the stance taken in the Bank of England's June 2018 'Financial stability report', reproduced in the discussion paper 'Building the UK financial sector's operational resilience' released by the Bank of England, the Prudential Regulation Authority and the Financial Conduct Authority, which states that "Firms have primary responsibility for their ability to resist and recover from cyber incidents."

"The emphasis is that they must be able to resist and maintain a normal service in all but the most extreme cases," Lloyd says. "That really is a sea change."

Corero's always-on SmartWall technology has excellent visibility of the network traffic arriving at their customers' businesses. Through the use of the company's SecureWatch Analytics, this data can be used to provide information on the cyberthreats facing their customers, allowing them to take a more active approach. "Being proactive – threat hunting – is very much the stance that progressive businesses want to take," Lloyd says. "Our analytics, and the threat intelligence that we're able to provide through those analytics, is certainly an area of ongoing investment for us."

Corero is exploring means of detecting and mitigating threats much further upstream, before they reach enterprise customers such as banks. A global reselling agreement with Juniper Networks has led to a new product known as Threat Defense Director, which sits at the ingress edge for service providers. "As with any supply chain, the more upstream you can go in terms of nipping this in the bud, the better," Lloyd explains.

This development is consistent with Corero's mission to provide security for its customers. "Fundamentally, we're here because we believe that the internet should be a safe place to conduct business," Lloyd says. ■

Further information
Corero Network Security
www.corero.com