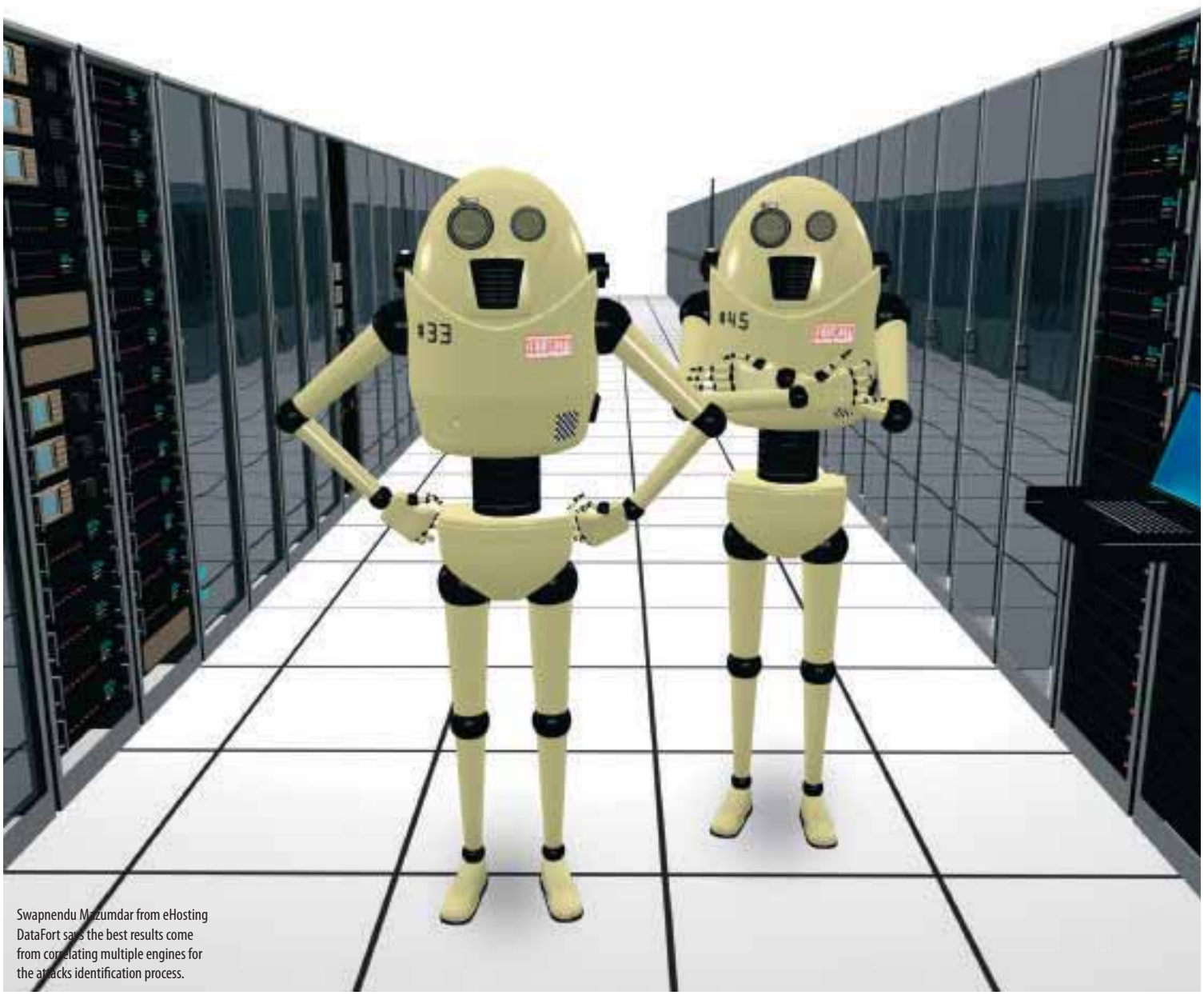
DDoS attacks: The impact

DDoS experts explain how to try to prevent DDoS attacks and what the impact is of an attack on an enterprise

The cost of a Distributed Denial of Service (DDoS) attack can continue to impact on the targeted organisation long after the event has been dealt with. It is not just the disruption to the public interface, which is damaging enough to any organisation that conducts a substantial volume of its business online. Loss of revenues while services and systems are unavailable to customers are compounded by the cost of rectifying the crisis and long-term damage to the business's reputation In some cases an organisation might even submit to extortion from the hackers, effectively paying a ransom to rid itself of the problem – until the next strike from another hacker source.

In the face of the threat, network and IT managers might be excused a constant sense of despair. The logistical and reactive challenges of anticipating and handling a threat that is all the more sinister for the apparent coordination and efficiency of its perpetrators are considerable. But that is no reason for anyone to simply hunker down and brace themselves for the next attack.

"A Distributed Denial of Service attack is a Denial of Service attack conducted by using multiple systems distributed over the internet as sources to host the attack on the same target," says Kuber Saraswat, director, strategic security consulting at Dubai-based security services provider SecureLink.



Swapnendu Mazumdar from eHosting DataFort says the best results come from correlating multiple engines for the attacks identification process.

"Most security-conscious customers already have some level of DDoS protection in place. The DDoS attacks in the Middle East have create awareness in corporate and government security strategies of the need to prepare for larger capacities to handle such events, and also to look for new attack trends and patterns.

"While every attack is dangerous, the visibility and the ability for these attacks to scale in size makes them most dangerous. The DDoS attack is focused on degrading the service quality of the target system, so that it is either unavailable or slow in response. The attack impacts business through creating delay in transmission, network outage, and has been used by organised crime for extortion, website sabotage, to incur financial losses and to block users from accessing online accounts, to reduce worker output and to cause brand and reputation damage."

> "While every attack is dangerous, the visibility and the ability for these attacks to scale in size makes them most dangerous. The DDoS attack is focused on degrading the service quality of the target system, so that it is either unavailable or slow in response."
>
> **Kuber Saraswat, director, strategic security consulting, SecureLink.**

As if that was not enough, Saraswat states that a new trend is emerging: DDoS attacks are increasingly used as a diversion to engage the target company's resources while another type of attack is launched from another access point.

IMPROVING DEFENCES

While many organisations look to comprehensive managed service systems to protect themselves as far as possible against an

Comprehensive managed service systems against DDoS attacks can be expensive for enterprises, says James Lyne of Sophos.

Nicolai Solling from help AG says that IT professionals will continuously need to battle and handle the issue of DDoS.

> "To truly defend, enterprises need to build their application or service architecture from the ground up to be resilient. You can't make a poorly-performing and secured service, so the right developing practices and architecture are key too."
>
> **James Lyne, director of technology strategy, Sophos.**

attack, this can be expensive. James Lyne, director of technology strategy at security systems specialist Sophos says that investment in a combination of software and hardware will significantly improve defences. But total prevention is a challenge for any business without substantial financial resources to maximise bandwidth and IT resources.

"That said, there are some basics that most can do," he explains. "Firstly, you should use DDoS prevention capabilities at the protocol level in your network security devices. This can filter the obvious such as a small number of systems generating basic flood packets. To really deal with the issue, however, you need to work with your service provider to ensure they can filter and handle traffic upstream from your systems. Use of a cloud provider can also help as they are likely to have significantly more bandwidth and resilient infrastructure in place."

Lyne says that DDoS preven-

tion software will help to identify a probing system or a large number of fake or malformed requests, but more traditional monitoring software – which tracks uptime and validates service availability – is also a useful source of early warnings. Armed with the information such software affords, you can work with your service provider or make configuration chances in-house to counter the attack.

"Our Unified Threat Management and network security gateways have some DDoS capabilities to help deal with certain classes of attacks or internal disruption," he said. "When combined with the right capabilities provided by the ISP or service provider, this can be an effective basis of defence against many forms of DDoS."

However, Lyne warns: "To truly defend, enterprises need to build their application or service architecture from the ground up to be resilient. You can't make a poorly-performing and secured service, so the right developing practices and architecture are key too."

Arbor Networks has been mitigating DDoS attacks on some of the world's most demanding networks for more than a decade, claims sales director Mahmoud Samy. With its Pravail Availability Protection System (APS), it advocates a layered approach that embraces the identification of threats and treats system availability as a primary indicator of an attack.

"Today, that means having purpose-built DDoS mitigation protection at the enterprise network perimeter, together with a managed security service that offers DDoS mitigation in the cloud," says Samy.

"The reason for this layered protection strategy is to address the two main types of attack. Application-layer attacks are stealthy, low and slow-type attacks that use little bandwidth. They are best mitigated with a purpose-built device deployed at the enterprise perimeter. For large flood attacks, it is too late once it has reached the enterprise perimeter as link capacity can be overwhelmed; these attacks have to be mitigated in the cloud."

Samy makes the sobering point that you cannot prevent an attack from occurring. What you must do, however, is prevent it from being successful – and for the enterprise, that means

Mahmoud Samy from Arbor Networks says enterprises must have purpose-built DDoS mitigation protection at the enterprise network perimeter.

"Application-layer attacks are stealthy, low and slow-type attacks that use little bandwidth. They are best mitigated with a purpose-built device deployed at the enterprise perimeter. For large flood attacks, it is too late once it has reached the enterprise perimeter as link capacity can be overwhelmed; these attacks have to be mitigated in the cloud.."

Mahmoud Samy, sales director, Arbor Networks.

Paul Wallace from Riverbed says it requires less of the hackers' resources to target the customer at application level, under the guise of asking it to do apparently useful work.

> "Bandwidth is only going to get higher and it will be much more difficult for hackers to gather the resources to pull together a concerted DDoS attack."
>
> **Paul Wallace, director of product marketing, Riverbed**

deploying advanced DDoS countermeasures that will identify and neutralise malware families in both the service provider and data centre environments.

THE COST

Specific DDoS cost data is hard to come by, perhaps because of the sensitivity – and even embarrassment – surrounding the experience and impact for any business that has fallen victim. But even if you consider the effect simply from the cost of downtime perspective, the benefits of a best-practice prevention strategy are clear.

"The cost of data centre downtime is a function of data centre size and business type," says Samy. "According to a Ponemon survey, 16 different industry segments with 41 business managers reporting on the costs that their operations had incurred due to unplanned data centre outages, the hourly cost of downtime per 1,000 square feet ranged from $8,500 to $201,000, with a mean of $46,000. The large fluctuation in downtime costs is mainly due to business type: companies reliant on data centres to conduct business such as financial services incur the greatest losses.

"For most enterprises, replacing highly uncertain and risky cost outcomes with the very predictable, lower cost of DDoS threat mitigation and attack protection is sound practice from a security perspective as well as a financial perspective."

Some industry watchers think the massive increase in bandwidth availability and the parallel rise in ISP service levels and capability will be good news from a DDoS perspective, but will put the focus firmly on the application layer as frustrated hackers turn on targets where they can find more chinks in the corporate network armour.

Paul Wallace, director of product marketing at application delivery software specialist Riverbed Stingray, says it requires less of the hackers' resources to target the customer at application level, under the guise of asking it to do apparently useful work. This explains why SQL injection attacks are increasing on corporate databases – with the purpose of extracting customer data.

DDoS attacks should be dealt with as part of an overall security strategy, he says, with the risk spread as thinly as possible. That means asking service providers what experience they have in dealing with attacks, how they route their services and how to do they develop applications to provide their agility in the event of an attack.

"Bandwidth is only going to get higher and it will be much more difficult for hackers to gather the resources to pull together a con-

certed DDoS attack," says Wallace. "Hence, application-level attacks will become more common."

PREVENTION STRATEGY

A combination of security measures that include proper incident response plans and an adequate business continuity/disaster recovery strategy as well as DDoS mitigation services and on-site software and hardware tools, would be the ideal solution, according to Swapnendu Mazumdar, network infrastructure manager at hosting services provider eHosting DataFort.

"The best results come from correlating multiple engines for the attacks identification process," he says, "correlating logs from multiple sources such as firewalls, intrusion prevention/detection systems, host-based intrusion/detection systems, DDoS detection/prevention systems, and from auditing desktop and server logs."

Corey Nachreiner, director of security strategy at another security systems specialist, Watchguard Technologies, says that DDoS prevention tools can detect an attack in many different ways: traffic threshold monitoring; normal DoS flood detection which might spot a distributed attack; spotting known DDoS tool signatures; analysing behaviour and statistics to spot unusual packet attributes; host or user challenge response test to make sure a visitor is human; and by using data from reputation lists or lists of infected attack victim that can block traffic from IPs with a bad reputation.

DDoS attacks are increasingly used as a diversion to engage the target company's resources while another type of attack is launched from another access point, according to Kuber Saraswat from SecureLink.

"But personally, I don't think DDoS prevention hardware or software can really 'prevent' all DDoS attacks," says Nachreiner.

"Rather, they can help mitigate some of them. In short, once the DDoS prevention control has differentiated the DDoS packets from normal traffic, it can start dropping these packets quickly, or blacklisting the IPs that are sending them through. Doing this significantly lessens the resources used on the DDoS traffic. However, even immediately dropping a packet does take a bit of resource. In huge volume attacks, certain gateway appliances or even DDoS prevention controls can become so busy dropping packets that they do not have time to handle legitimate traffic. Over the past few years, researchers have seen examples of DDoS attacks that generate 50-100GB per second of sustained traffic, which even the best DDoS prevention controls would be hard-pressed to handle. This is why a multi-layered solution is the only way to truly mitigate DDoS attacks."

There is no sign of any let-up in threat levels in the foreseeable future.

Nicolai Solling, director of technology services at security services vendor help AG, says the Middle East remains an area of great interest to attackers due to the strong economy and the political situation in the region. That is why most attacks in the Gulf have been aimed at govern-

Corey Nachreiner from Watchguard Technologies says that DDoS prevention tools can detect an attack in many different ways.

"Over the past few years, researchers have seen examples of DDoS attacks that generate 50-100GB per second of sustained traffic, which even the best DDoS prevention controls would be hard-pressed to handle. This is why a multi-layered solution is the only way to truly mitigate DDoS attacks."

Corey Nachreiner, director of security strategy, Watchguard Technologies

ment websites and the financial services sector.

"IT professionals will continuously need to battle and handle the issue of DDoS," he says. "What is worrying is that there are no network layer controls, which really is the key to avoiding DDoS attacks. We need to focus on making sure the attack is dropped as close to the source as possible. It is therefore important to understand where the sources of DDoS attacks are, which is typically the regions where the most botnet-infected machines also are.

"Over the past couple of years, this has typically been in Asia and the former eastern-bloc countries. A major reason for this is that lack of copyright laws means there is a very large number of pirated software and operating systems. Because of this, users in such regions are now more susceptible to malware and botnet agents which are the source of Distributed Denial of Service attacks."