DDOS PROTECTION: KEEPING YOUR BUSINESS SAFE

January 2016

- Trends and Current Threats
- Methods and Motivations
- The Impact, Cost and Hidden Danger
- Mitigating Attacks

Whitepaper

cogeco PEER 1

CONTENTS

1. Executive Summary

Distributed denial-of-service (DDoS) attacks are one of the oldest threats on the IT security landscape. They can be used to bring down Internet-facing business services and cause general havoc for any organization and its IT security staff.

But despite having their roots in the past, DDoS attacks are still prevalent and devastating today, making the case to implement a dedicated mitigation solution to combat them stronger than it's ever been.

As the name suggests, denial-of-service (DoS) attacks are designed to deny legitimate users access to websites and services by overwhelming them with illegitimate connections, requests and traffic. A distributed denial-of-service attack is when the DoS attacks are being done by multiple attackers all trying to attack a source at once, be it from real hackers or from a single entity and their network of bots. While most DoS attacks on their own can be mitigated with existing technology, there is very little that can be done against a large scale DDoS attack without proper mitigation steps in place from the onset.

DDoS attacks are hard to trace, difficult to prevent, easy to carry out and increasingly affordable to acquire. This makes them one of the top methods of attack for extortionists, political activists (hacktivists) and disgruntled individuals/groups.

Unlike more traditional attack vectors, which look to infiltrate networks undetected, DDoS attacks are far from subtle or sneaky, and creating noticeable disruption is their main aim.

This Cogeco Peer 1 whitepaper focuses on the current DDoS threat landscape and looks at some of the current DDoS trends emerging across the security industry. It also looks at the different types of DDoS attacks being witnessed today, and the motivations behind them.

The impact to businesses and associated costs of DDoS attacks is also explored, as is the potential hidden danger that can be lurking when an attack hits. The paper concludes by outlining a seven-point strategy for better organizational DDoS defense.

2. DDoS: Latest Trends and Current Threat Landscape

According to the State of the Internet - Q2 2015 Security Report from Akaimai, the number of DDoS attacks witnessed in quarter two of 2015 hit record highs. In fact, the number of DDoS attacks grew by 7% over the previous quarter, which is cause for concern as it is. Yet more worrying is the reality that DDoS attacks in the second quarter of 2015 were up by a staggering 132% compared to the same period last year.

Even more worrying still is that Akamai's report categorizes 12 attacks that peaked at more than 100 Gigabits per second (Gbps) and five attacks that peaked at more than 50 Million packets per second (Mpps) as "mega attacks". These mammoth threats, one of which peaked at 240Gbps and lasted for more than 13 hours, are exactly the type of attack that would cause the vast majority of networks to crumble under their pressure.

Despite DDoS attacks increasing in terms of frequency and magnitude, one factor has consistently remained the same, and that's where the majority of them originate from. Incapsula's Global DDoS Threat Landscape Q3 2015 report shows that China continues to be the number one source of DDoS traffic, accounting for 37.5% globally. In fact, Incapsula found that DDoS traffic originating from China actually increased by 152% over the previous quarter.

The Incapsula report also found that the United States was the biggest target of DDoS attacks worldwide, with 45.8% of DDoS traffic aimed at websites hosted in the US.

Perhaps the most unsettling aspect of DDoS attacks is that they can impact any type of organization operating in any industry. For example, the online gaming sector was hit especially hard in the second quarter of this year, bearing the brunt of over 35% of all attacks, according to the Akamai report. This isn't a new revelation, with online gaming remaining the most targeted industry since the second quarter of 2014.

The bottom line is that if you operate online gaming services for Xbox and PlayStation owners, the threat posed by DDoS attacks and the potential impact of them is very real and severe.

The software and technology (27.74%), Internet and telecom (12.9%), media and entertainment (9.41%), and financial services (8.19%) industries made up the remainder of the top five sectors targeted by DDoS attacks in the second quarter of this year, with some of the most high profile DDoS attacks resulting in substantial data breaches within these business sectors.

One of the fastest emerging DDoS attack trends is the growing botnet-for-hire industry. With the widespread availability of these DDoS-for-hire services, even non-technical individuals and groups can carry out – or have carried out for them, as is the case – large scale DDoS attacks, sometimes for as little as $5 a go.

It's these rentable services that have caused the number of multi-vector attacks witnessed in recent times to increase. DDoS attackers today have access to more tools, vulnerable devices and a monetized framework, all of which help make DDoS-for-hire a lucrative business.

DDoS attackers today have access to more tools, vulnerable devices and a monetized framework, all of which help make DDoS-for-hire a lucrative business.

While the concept of being able to leverage customized botnets to carry out DDoS attacks is one that will inevitably fill IT security managers with dread, attacks that are conducted in this way are usually shorter and more rudimentary in their nature. Nevertheless, with some DDoS-for-hire services promising attack volumes of over 200Gbps, they remain a significant threat for under-protected networks.

In the recently published Kaspersky Lab DDoS Intelligence Report Q3 2015, a special mention was given to the rise in attacks on financial institutions over the reporting period. Major banking organizations in a variety of countries were targeted, with the hackers threatening to knock services offline unless a ransom was paid.

This trend of financial institutions being targeted by DDoS attacks was not just picked up on by Kaspersky. A separate Akamai case study paper issued in September 2015 also underlined the rise of an attack strategy by a group known as DDoS-for-Bitcoin (DD4BC) which looks to extort bitcoins from financial organizations.

A supplement to the firm's main State of the Internet Security Report, the Akamai Case Study: Summary of Operation DD4BC paper shows that enterprises in the US and Canadian financial services industries are being increasingly targeted by the bitcoin extortionist group.

Since April, Akamai estimates that there have been 114 DD4BC attacks alone, with the focus initially placed on organizations in North America and Asia. However, companies in Korea, China, Australia and New Zealand have also now become targets, underlining how rapidly attackers can shift their focus.

The Kaspersky Lab report also highlights what it calls an "unusual attack scenario", which saw a certain CloudFlare customer's site being subjected to 275,000 HTTP requests per second. The report notes that an iFrame with a malicious advert was run on the browsers of many users, causing their workstations to bombard the victim with XHR requests.

The DDoS situation has become so serious, with attacks now more powerful and prevalent than ever, that the Pentagon has recently announced plans to fund tools and researchers in an attempt to help organizations defend themselves against the increasingly risky DDoS threat landscape.

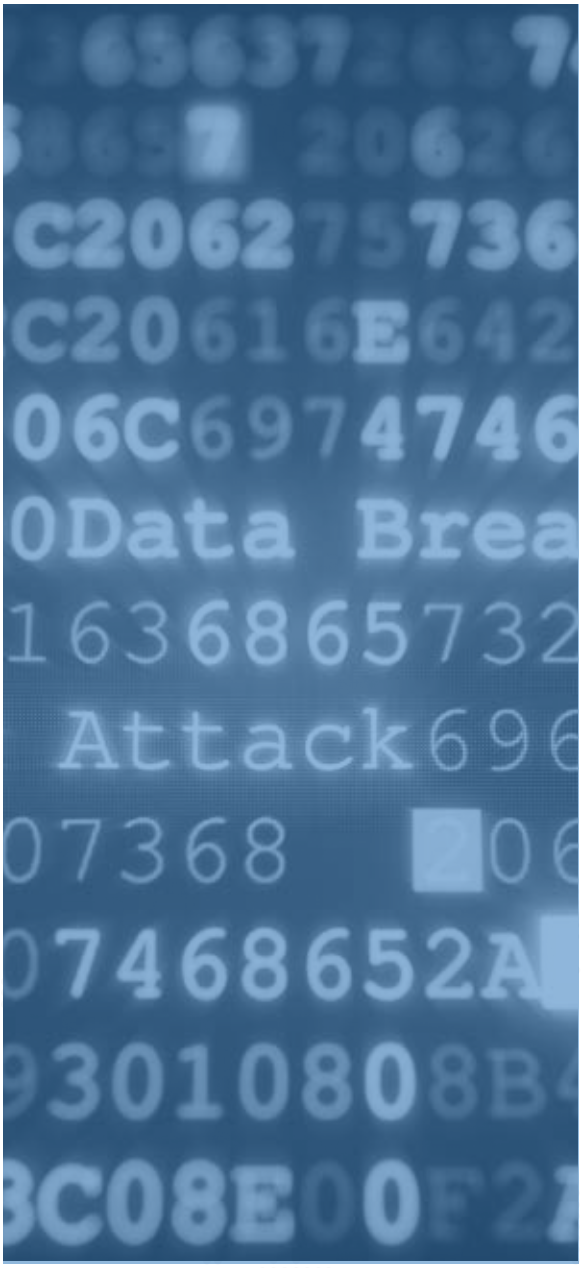
Known as Extreme DDoS Defense, or XD3, the Pentagon initiative will see military-funded researchers tasked with producing new tools that will allow affected organizations to recover from DDoS attacks within 10 seconds.

The tentative start date for the three-year program is April 1, 2016 and participating researchers will be chosen by the Defense Advanced Research Projects Agency (DARPA).

A three-pronged approach is being adopted by the XD3 program, which will look to disperse heavily consolidated cyber assets, which present a large surface area for attackers to target, change the predictable behavior of many web services to deceive the hackers and devise adaptive endpoint mitigation techniques.

The fact that the DARPA is proactively leading the fight against hackers will give many organizations some solace, but the threat remains immediate and rampant, which is why organizations must get their DDoS defenses in order in the first instance.

Malicious actors often change the rules of the DDoS game by frequently switching tactics, continuously seeking out new vulnerabilities and even resorting to old techniques that have been previously shelved as obsolete.



3. DDoS: Methods and Motivations

Types of DDoS Attacks

Despite being some of the oldest threats on the Internet – literally dating back decades – DDoS attacks aren't just occasional occurrences today, they are abundant. The main reasons for this are because they are easy to accomplish, difficult to prevent, cheap to carry out and hard to trace. This makes them a low risk, yet high impact attack strategy.

The problem for organizations today is that DDoS attacks have evolved over time and no longer come in just one variety. This makes trying to prepare for, and mitigate against, them an increasingly difficult task.

Broadly speaking, there are two main types of DDoS attack:

- **Connection based: which requires a mutual "handshake" between a server and a client using certain standard connection protocols before an attack can take place.**
- **Connectionless: which does not require a formally-established session/connection before an attack occurs.**

Unlike a denial of service (DoS) attack – in which just a single computer and Internet connection is used to hit a target with packets of data – a DDoS attack sees many computers and many Internet connections used, which are often distributed (hence the name) across a global network known as a botnet.

DDoS attacks can be further broken down into three main categories, depending on which specific part of the network infrastructure is being targeted:

Volumetric Attacks

Volumetric attacks - also known as “floods” - are typically executed using botnets and are connectionless. The main aim of this type of attack is to saturate the bandwidth of the target and cause so much congestion that the site is overwhelmed.

Botnets are commonly leveraged to generate the massive traffic volumes, and the “gang rush” nature of volumetric attacks makes them very difficult to mitigate compared to attacks that originate from a single source.

Volumetric attacks come in a variety of forms, but User Data Program (UDP) floods and Internet Control Message Protocol (ICMP) floods (ping requests) are the two most commonly seen. Their magnitude is measured in bits per second (Bps) or gigabits per second (Gbps).

According to Arbor Network’s 10th annual Worldwide Infrastructure Security Report (WISR), which was released earlier this year, volumetric attacks accounted for 65% of all DDoS attacks witnessed in 2014.

State-Exhaustion Attacks

State-exhaustion attacks or protocol attacks, as they are sometimes referred, target actual firewalls, web servers and/or load balancers, with the specific aim of exhausting their available resources.

Even high-capacity devices that are designed to maintain millions of concurrent connections can be brought down by state-exhaustion attacks.

One of the most common and perhaps the most notorious type of state-exhaustion attack is Ping of Death. This technique sees an attacker defragment and send a 65,536-byte size packet to a target as fast as possible.

Once the target server reassembles the IP fragments into the complete packet, a buffer overload usually happens. This causes the target to crash and a denial of service for legitimate packets to occur.

State-exhaustion attacks are measured in Packets per second and Arbor Network's WISR says that they accounted for 20% of all DDoS attacks witnessed in 2014.

Application-Layer Attacks

Application-layer attacks – also known as Layer 7 attacks – target a specific application or server Application-layer attacks – also known as Layer 7 attacks – target a specific application or server weakness. They look to establish a connection with the targeted resource and then exhaust it by monopolizing processes and transactions.

This type of attack usually comprises seemingly legitimate and innocent requests and can be carried out using a small number of machines, making it much harder to detect. The magnitude of application-layer attacks is usually measured in Requests per second.

Historically, HTTP and DNS services have been the primary focus of application-layer attacks, but HTTPS and SMTP are becoming increasingly popular targets too.

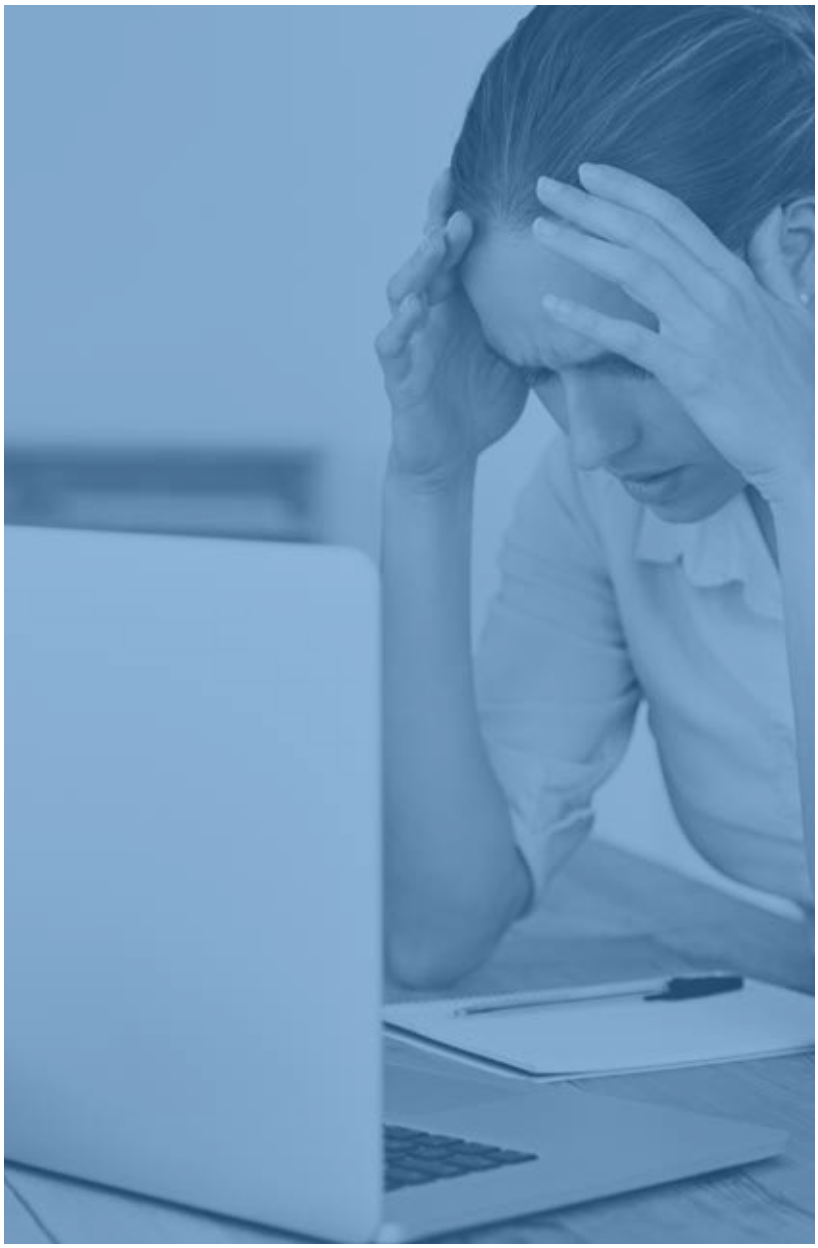
In 2014, application-layer attacks accounted for 17% of all DDoS attacks witnessed, according to Arbor Network's WISR.

In extreme cases, organizations can be hit by a combination of the three types of attack listed above, which makes DDoS defense even more challenging.

Zero-Day DDoS Attacks

While not actually a specific type of DDoS attack, zero-day DDoS attacks are worth mentioning because they are often referred to in the security world. They occur when an attacker exploits a zero-day vulnerability, which is unknown to the vendor and has had no patch released to address it.

The term “zero-day” is well-known in the hacker community and refers to the fact that the vendor has zero days (before disclosure) to fix it. Zero-day exploits are frequently traded among hackers meaning that they are often quickly spread once discovered – a reality that puts even more pressure on vendors to create and release patches.



The term "zero-day" is well-known in the hacker community and refers to the fact that the vendor has zero days (before disclosure) to fix it.

DDoS Attack Motivations

While every type of organization can find itself the target of a DDoS attack – and the most obvious consequence of a successful one is rendering a particular resource or service unavailable or unusable to their intended users – the motivations behind them inevitably vary.

Extortion and Profit

Perhaps the easiest motivation to comprehend is the desire to profit from the targeted organization. Attackers know that they can often extort money from an organization using the threat of a DDoS attack.

The attackers usually blackmail their victims via email and sometimes underline their intentions by launching a small-scale DDoS burst against the target organization. Prime targets for extortion attacks are companies that rely heavily on their online presences, such as online gambling, eCommerce and media organizations.

Perhaps surprisingly, the attackers often demand a small amount of money in the first instance. There's a chance the company will pay to save itself from the fallout of a DDoS attack, but in some instances the attackers then up the ante and ask for more money once a payment has been made.

DDoS attacks motivated by extortion and profit are often planned to cause maximum disruption, and look to hit an organization during a particular event. For example, online gambling sites may be targeted when there's a large sporting event taking place, or eCommerce stores targeted over the holiday season.

Perhaps surprisingly, the attackers often demand a small amount of money in the first instance.

Hacktivism

Hacktivism is becoming increasingly popular and DDoS attacks are often carried out by groups that want to disrupt organizations and individuals that disagree with their political, social and/or religious beliefs.

Groups like LulzSec and more recently Anonymous regularly hit the headlines for threatening DDoS attacks against organizations or movements. Their motivations are not profit-based, but more to get exposure for their cause via media attention.

Hacktivist groups often announce their plans ahead of an attack so that the event gets maximum attention and press coverage. The additional exposure also serves to cement the group's capabilities and boost its reputation in the hacktivist community.

A classic example of this type of motivation is the cyber assault that was launched against the Mumsnet website earlier this year. A group calling itself Dadsec said that it was behind the attack which knocked the site offline and was motivated by the anti-father sentiments believed to be on display on the Mumsnet site.

Disputes

It's an unfortunate sign of the times when DDoS attacks are used during disputes, but it's a reality that has emerged today. Online gamers in particular, often use short DDoS attacks to disrupt their opponents. The target is either unable to play or suffers from a severely degraded service which impacts their effectiveness.

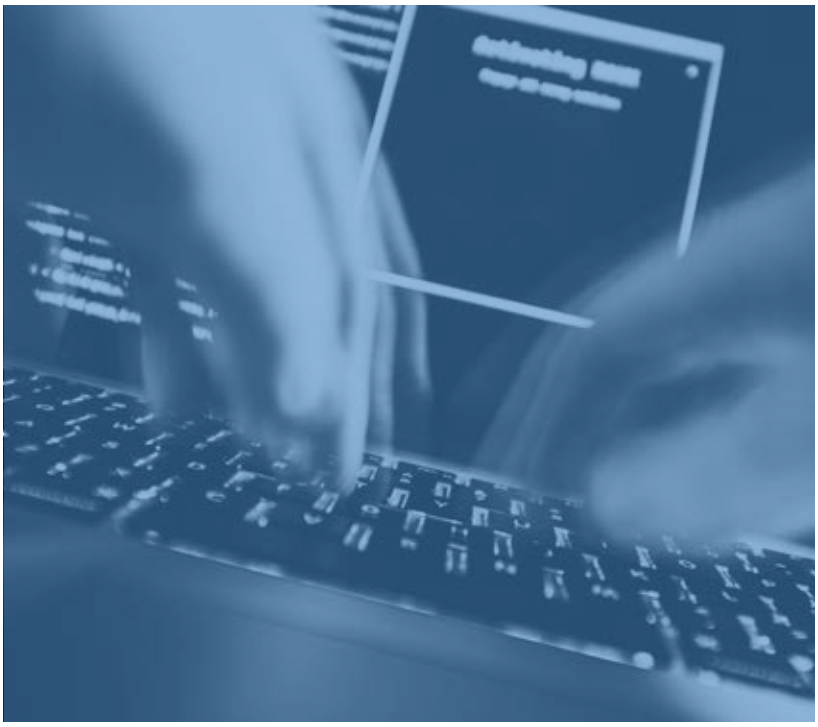
However, it's not just online gamers that can leverage DDoS attacks. Potentially anyone who holds a grudge might conduct one or pay to have one conducted. It could be a disgruntled customer or ex-worker who wants revenge against an organization.

The rise of DDoS-for-hire services has, unfortunately, enabled anyone who is willing to pay to perform attacks, and that's why they are becoming increasingly pervasive. It might even be the case that a company has hired the services of a hacker to disrupt the online operations of its competitors.

Unintentional Outages

While it can't specifically be labeled a DDoS attack, unintentional floods of traffic to a website can often have the same effect. This sometimes happens when a smaller company or organization is featured in a major piece of news, and visitors flock to their websites as a result.

The website crumbles under a spike in traffic and the abnormal pressure can be likened to an application-level DDoS outage in its subsequent impact. While nobody is necessarily to blame, these types of outage highlight just how fragile some organizations are to sudden peaks in demand. It further emphasizes the need for DDoS protection.



4. DDoS: The Impact, Cost and Hidden Danger

Impact and Cost

Any IT outage or period of downtime affects an organization's bottom line, regardless of how it is caused. That said, the severe impact and often prolonged nature of DDoS attacks makes them particularly damaging for organizations.

However, it's not only the obvious financial implications that companies need to concern themselves with when a DDoS attack hits. There are other significant ramifications to consider too.

Revenue Loss

Businesses that rely solely on their Internet-facing applications and services to generate revenue undoubtedly have the most to lose in the face of a DDoS attack. For example, if an eCommerce retailer's website is knocked offline for several hours then a direct loss of revenue will occur as customers will simply be unable to place orders.

But while a monetary figure can often be placed on downtime like this during a 'normal' business day, the impact a DDoS attack can have if it strikes at a particularly busy time of year – such as Black Friday, Cyber Monday or the holiday season – can be immense and almost immeasurable.

Customers always expect a seamless service from their favored retailers and their high expectations mean the unavailability of a website is unacceptable at the best of times, let alone when they are trying to secure a specific online deal or make holiday season purchases.

A Ponemon Institute report, titled The Cost of Denial-of-Service Attacks, released in March 2015, shows that the average total cost per year of DDoS attacks to a business is $1.5 million. The proportion of this cost attributed to revenue losses occurring because customer-facing services were not available is $491, 152, making it the number one financial consequence of a DDoS attack.

Indeed, Kaspersky Lab's Global IT Security Risks Survey 2014 – Distributed Denial-of-Service (DDoS) Attacks report, which was released at the beginning of this year, shows that the average cost of a single DDoS attack on SMBs is $52,000 per incident. Larger enterprises are hit even harder with a single incident costing as much as $444,000. These costs include lost business due to outage, as well as spending on IT to resolve the issue.

Productivity Loss

When business systems are down, an organization's workforce inevitably experiences a significant drop in productivity. This is especially true for staff whose duties and responsibilities revolve around an organization's eCommerce offering.

But DDoS attacks, according to the same Ponemon report cited above, have the ability to impact a much wider range of systems and services. In fact, 82% of respondents said that a DDoS attack shut down their entire datacenter (34%) or part of it (48%). This reality means that an organization's non-eCommerce/online departments could also be hit with drops in productivity while a DDoS attack is happening.

Ponemon found that lost user productivity as a result of a DDoS attack costs businesses $173,169 per year, on average.

Reputation Damage

Reputation damage is a much more difficult DDoS consequence to evaluate in terms of financial loss. Reputation damage is a much more difficult DDoS consequence to evaluate in terms of financial loss. Nevertheless, it is the number one consequence of a DDoS attack, according to 64% of the respondents who participated in the Ponemon study. It significantly outweighs both diminished productivity for IT staff (35%) and revenue losses (33%).

After all, a DDoS attack could see an organization's customers lose confidence in the brand and think twice before shopping there in the future. With so much competition now online, organizations cannot afford to have their brand reputation damaged.

Large-scale DDoS attacks which cause prolonged outages invariably hit the headlines; especially if the affected business is a large household name. This kind of publicity, unfortunately, sees the organization painted with the 'hacked' brush, and even though a DDoS attack has caused a website to crumble, but no customer data was compromised, the damage to an organization's reputation is already done.

The Hidden Danger

DDoS attacks are designed to disrupt organizations, cause havoc and make a statement. But while there's nothing covert about the way they are carried out, DDoS attacks are frequently used as a smokescreen to occupy an organization's IT staff and mask the real intentions of the attackers.

In August 2015, Uk-based cell phone retailer Carphone Warehouse was bombarded by a DDoS attack. At the time, the firm scrambled to recover its affected services, but after the dust had settled it was revealed that a much more sophisticated attack had taken place.

While the DDoS attack was taking place, cyber criminals infiltrated Carphone Warehouse's systems and stole the personal and banking details of 2.4 million of its customers. The theft may have been noticed and thwarted if IT security staff weren't fire-fighting the DDoS attack.

A similar case back in 2011, which is perhaps the most famous, saw Sony's PlayStation Network shut down for weeks after the personal and financial details of some 77 million customers were stolen. In a letter to the United States House of Representatives following the breach, Sony Computer Entertainment chairman Kazuo Hirai wrote: "Security teams were working very hard to defend against denial of service attacks, and that may have made it more difficult to detect this intrusion quickly."

"Security teams were working very hard to defend against denial of service attacks, and that may have made it more difficult to detect this intrusion quickly."

Using DDoS attacks as a smokescreen is a practice that's becoming more widespread, according to a Kaspersky Lab report released in September this year, titled Denial of Service: How Businesses Evaluate the Threat of DDoS Attacks.

The Kaspersky report found that almost three quarters (74%) of companies that experienced a DDoS attack also noticed a disruption to other services, which makes them believe that the attack was used to mask a more serious intrusion.

Malware infections are the main side effect of DDoS attacks (45%), but 32% of respondents indicated that they experienced network intrusions or another type of hacking incident. Overall, 26% of businesses which reported a DDoS attack said that sensitive data was lost as a result and 31% said that non-sensitive data was stolen.

This worrying and rising trend of DDoS as a decoy adds even more weight to the argument for a real-time, behavioral-based attack mitigation system.

5. DDoS: Mitigating Attacks

With DDoS attacks becoming more prolific, more sophisticated and cheaper to accomplish, the importance of a precise mitigation plan has never been greater. Adopting an 'it won't happen to us' mindset is, unfortunately, no longer good enough. Cyber criminals, hacktivists and disgruntled parties do not often discriminate between who they target, and that makes every organization potentially vulnerable to DDoS attacks.

Most importantly, organizations need to address the threat posed by DDoS attacks before they occur. Being hit by a service outage is one thing, but having corporate data stolen because of it is quite another.

So what can you do to ensure your organization remains resilient in the face of a DDoS attack? Here is a seven-point strategy for better DDoS defense:

1. Make DDoS Attacks a Core Part of Your Business Continuity Plans

DDoS attacks should undoubtedly form a part of your organization's business continuity and disaster recovery plans. But that implies that DDoS attacks are accidental or unexpected, and that's simply not the case today.

Therefore, DDoS should also be an integral and highly-defined part of your organization's incident response plan. This means key members of staff, strategic partners and their relevant emergency contact numbers need to be captured ahead of the event, so that when a DDoS attack hits, the organization knows exactly how to respond.

Annual, or even six-monthly, tests of these plans are recommended to ensure that every aspect has been covered and every individual involved understands exactly what their role is. These regular "fire drills" will not only help your organization better prepare for an attack, but could also satisfy any annual BCP test compliance obligations you may have.

2. Don't Rely Too Much on or Overestimate Your Networking Infrastructure

Under normal operation, your edge network hardware will invariably handle everything that it's been provisioned to. However, the traffic volumes that can be produced by modern DDoS attacks are enough to topple even the most advanced networking hardware.

Organizations that think their firewalls will provide adequate defense in the face of a DDoS attack will soon realize that that's not the case. Even next-generation firewalls that boast advanced DDoS protection cannot secure your critical infrastructure against every type of DDoS attack.

3. Set Benchmarks so You Can Spot a DDoS Attack More Easily

Astonishingly, many organizations do not know what kind of strain their networking infrastructure is under during 'normal' operation. So they cannot easily detect when abnormal behavior occurs. However, unusually slow network performance and website unavailability – while DDoS warning signs – do not necessarily indicate that your organization is under attack.

By increasing enterprise-wide security monitoring from edge to endpoint, organizations can increase their chances of detecting a DDoS attack when it begins. Likewise, by designing your network with flexibility and scalability in mind – and knowing where all your bottlenecks exist beforehand – you can more accurately recognize DDoS attacks in a proactive manner.

4. Think like a Hacker

Don't think that hackers are erratic and opportunistic. In fact, they're usually extremely methodical in their approaches and will look to take advantage of other weaknesses if their attempts are being thwarted. The same is true for DDoS attacks and that's why putting yourself in their shoes can pay dividends ahead of time.

Think about where they might focus their efforts in sequence and plan against all possible types of attack. Even one piece of vulnerable infrastructure could be the difference between your network holding up or being exposed.

5. Know Your Customers

Most organizations know where the majority of their customers are

located, and that means the origins of network traffic can be analyzed and understood. Of course, new customers will come onboard all the time, but if your company definitely isn't expecting interest from Eastern Europe or China, then traffic coming from those countries may indicate that something isn't right.

While blacklisting IP addresses based on their origin is a thankless and never-ending task, restricting access based on location is an option, especially if your chosen DDoS protection solution facilitates it.

6. Deploy a Dedicated DDoS Solution Ahead of Time

Emergency DDoS mitigation solutions are available and can often be deployed within an hour in most cases. These solutions tend to rely on null routing and traffic redirecting on a per-event basis, with costs associated for the event being billed to the customer. But why risk your organization's reputation, productivity and bottom line by relying on a mitigation solution that isn't proactively guarding your infrastructure?

Having a dedicated, behavioral-based DDoS mitigation system in place is not only much safer, but also affords greater peace of mind for your business. Essentially, these solutions reside in-line with your data flow and are sent through scrubbing centers that filter out the majority of suspicious traffic and delivering only genuine traffic in real time.

Forming part of your overall incident response plan, this dedicated DDoS protection should feature immediate alerts that ensure any attack is identified and acted upon.

Having a dedicated, behavioral-based DDoS mitigation system in place is not only much safer, but also affords greater peace of mind for your business.

7. Test for Every Eventuality

Your DDoS mitigation solution should be tested and validated once it has been implemented, and then at regular intervals going forward. This not only ensures that it meets your organization's expectations from the outset, but also guarantees that no vulnerabilities have been overlooked.

DDoS attacks have evolved since they first came onto the security scene all those years ago and it's inevitable that they'll evolve further in the future. It's for this reason that your mitigation solution also needs to evolve, otherwise you could find that your organization is left exposed at a later date. Building a strong working relationship with your chosen DDoS mitigation provider is also encouraged to ensure that your response to an attack is calm, rehearsed and effective.

The threat posed by DDoS attacks is very real and the intensity with which they can hit – coupled with the low prices they can be obtained for – make them an increasingly worrying security concern for organizations today.