WHITEPAPER

DDoS: The Threat that Won't Go Away

Who is doing them? How do they work? How can you stop them?

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction

Distributed Denial of Service (DDoS) attacks are a growing threat. Defined generally, they are when an adversary directs a large torrent of traffic - or traffic that's ill-formed - against a service in order to render it unavailable.

They're also fundamentally misunderstood. There are so many misconceptions about DDoS attacks. Perhaps the biggest is that victims needn't worry when it happens to them. Far too many people believe that DDoS attacks are less-than-severe, due to the fact that they don't result in any data lost or stolen, or a bad actor gaining unauthorized access to a system.

This erroneous belief is amplified by the fact that DDoS attacks are often transient. They can be over in just a few hours, or even a few minutes. Particularly damaging DDoS attacks can last a few days. It's uncommon - but certainly not unheard of - for one to endure much past this point.

But this widespread failure to recognize DDoS attacks as a threat is a critical mistake. One can cause significant losses - not just in terms of productivity and money, but also in reputation.

They're also indicative of something much more troubling. If someone has gone to the effort and cost (indeed, DDoS attacks can be expensive to execute) to launch one against your institution or enterprise, it shows that there's an external bad-actor with a grudge against you. They can be the overture of something worse.

This belief also ignores the fact that DDoS attacks aren't just undertaken against websites and API endpoints anymore. Anything connected to the Internet - be it a car, or a 'smart' insulin pump - is at risk. The consequence of someone disrupting the proper function of these devices can be fatal.

There is now a Distributed Denial of Service industry, and business is booming.

And while many of these attacks used to be performed by politically motivated, but nevertheless bored teenagers, the DDoS threat landscape has evolved to encompass motivated and well-equipped organized criminals. There is now a Distributed Denial of Service industry, and business is booming. These adversaries boast powerful digital weapons, consisting of millions of insecure systems.

And these systems are no longer infected desktop computers. They now include vulnerable Internet of Things systems. Your smart fridge might well be dominated by a criminal gang in Saint Petersburg.

Akamai's State of the Internet report provides some fascinating, but undeniably troubling, insights into the DDoS problem.

First, the worst news: they are increasingly common. Between Q3 2015 and Q3 2016, the rash of DDoS attacks soared in frequency by 71 percent. Perhaps more concerning, attacks against Level 3 and Level 4 infrastructure increased by 77 percent, showing a pivot from attacks targeting websites and endpoints, to the underlying systems.

The scale of the attacks has also changed. In general, DDoS attacks are more powerful. More damaging. They consist of more hosts. Per Akamai, the number of attacks where an attacker was transmitting over 100 gigabits per second has soared 138 percent, from 8 incidents to 19.

As DDoS attacks have soared in frequency and potency, it's increasingly important to understand them. This paper aims to explore the methodologies of DDoS attacks and their consequences, as well as the mitigation strategies that institutions and enterprises can adopt to defend against them.

We believe that those currently in a CSO, CTO, CISO and CIO role will find it most useful. However, it may also be of value to those working in a network or systems administration, or information security role.

The Staggering Costs of Distributed Denial of Service Attacks

Far too often, businesses plan their security measures based on how much they think it'll cost them. Most enterprises, for example, are often well prepared against external and internal threats that may see confidential and personal data exfiltrated.

Businesses are prepared to invest the money, because the cost of getting it wrong can be so much more expensive. Take Yahoo's tumultuous 2016, for example, which saw the disclosure of two different major security incidents, both believed to have taken place earlier.

$300,000

A short DDoS attack lasting just one hour can cost $300,000 per hour or $5,600 per minute

The first saw an external threat gain access to hundreds of thousands of users accounts The second attack was measured in the billions of accounts.

Even smaller incidents have proven to be crushingly expensive, as the victims have had to make good with both regulators, as well as their customers.

But the same concern isn't shown for DDoS attacks. As previously mentioned, this is due to the transient nature of them, and the fact that they seldom result in any data leakage.

But this is a mistake. Industry research shows that even a short DDoS attack lasting just one hour can cost $300,000 per hour. This measures to $5,600 per minute, according to Gartner's The Cost of Downtime paper.

This cost can be even higher, as it depends on a number of factors, including the vertical of the business, the size of the business, and any service-level-agreements that might be in place.

Even traditional brick-and-mortar establishments are vulnerable to DDoS attacks as they become reliant on digital processes for the day-to-day running of the business, such as Stripe and iZettle for card payment processing.

Other industry figures estimate the total cost of DDoS attacks to be lower, although still troublingly expensive. An Incapsula study from 2014 estimated that the average cost of a DDoS attack is around $40,000 per hour.

Incapsula also estimated that the average DDoS attack ranged in duration from 6 hours to 24 hours, and stated that the average cost is $500,000 per incident, with the potential to be even more expensive.

2016 Was the Year of the DDoS

For several reasons, most being out of the realm of information security, 2016 has come to be regarded as an annus horribilis. But it’s also worth recognizing it as the year in which the true potency of the DDoS attack was demonstrated.

2016 saw three of the most powerful DDoS attacks of all time. The targets - an influential information security journalist, a French web hosting company, and DynDNS - were all different. But what the attacks held in common was they all featured an inordinate number of zombified computers, and saw a truly incredible quantity of data transferred.

Krebs on Security

Former Washington Post journalist Brian Krebs is one of the most respected voices in information security journalism. But his coverage of cybercriminals has earned him some powerful enemies. As a result of his courageous work, he has been 'swatted' (where a hoax call is made to local law enforcement in order to summon a SWAT team to a property), received death threats, and even had a kilogram of heroin mailed to his address, in order to cause him legal problems.

Towards the end of 2016, his award-winning blog, Krebs On Security, was the victim of a colossal DDoS attack. According to Krebs, his web host, Akamai, described it as "nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed."

Per the KrebsOnSecurity blog, the attack commenced around 8 PM on September 20, 2016. The total amount of traffic transmitted per second varies by accounts. Initial reports said that it was approximately 665 Gigabits of traffic per second, while later analysis suggests it was closer to 620 Gbps.

As noted by Krebs, this is more than enough to take a website offline.

It's believed that this attack against Krebs was a retaliation to his coverage of vDOS - a DDoS-for-hire service that was dismantled by Israeli law enforcement, with the arrest of two of its founders

While Krebs wasn't prepared to definitively say that this was the case, he noted that some of the POST requests directed to his server included the string 'freeapplej4ck', which he noted was a reference to the nickname used by one of the vDOS founders. Hardly definitive, but certainly indicative.

OVH

But it's not just award-winning journalists who have found the ire of the criminal gangs operating DDoS botnets. Last year, French web hosting company OVH was forced off the Internet, as its servers buckled under the strain of a 1 Terabit per second DDoS attack. At the time, this was described as the "largest DDoS attack ever observed."

Nearly 145,000 connected systems were zombified in order to bring the company [OVH] to its knees

But the attack against OVH wasn't merely notable because of the vast quantity of traffic aimed at it's systems. It also represented a troubling turning point in the DDoS threat paradigm, as nearly 145,000 connected systems were zombified in order to bring the company to its knees.

The idea of an Internet-connected toaster being hacked and used in a DDoS attack is undeniably amusing, but for OVH it was anything but.

Although IoT devices are generally vastly underpowered, especially when compared to the mobile device or computer you’re reading this white paper on, they pose several advantages to anyone wishing to use them in a DDoS attack.

Firstly, unlike your computer, these devices are rarely monitored for security, and are seldom (if ever) turned off. Many IoT devices are based on Linux, or other embedded operating systems, and contain many unpatched security vulnerabilities, thereby providing an attacker with an entry point. And crucially, while someone might notice their desktop computer getting slow as the result of a malware infection, the same isn’t true of most Internet of Things devices, which aren’t performance-critical systems.

The fundamental issues with the IoT device ecosystem that resulted in the OVH attack remain just as true in 2017 as they did in 2016. There has been no meaningful attempt to resolve them.

As a result, it’s only a matter of time until we see another significant attack against a service where the zombified hosts consist mostly of IoT, connected and ‘smart home’ devices.

DynDNS

The backbone of the Internet is the DNS system, which is used to resolve human-readable domain names (like ‘Google.com’ or ‘NopSec.com’) to IP addresses. It also represents a single point of failure. By disabling a major DNS provider, it’s possible for there to be a contagion, as sites dependent on it become unavailable.

This is what happened to Dyn - one of the biggest DNS providers - towards the end of 2016. An attacker, who is yet to be identified, flooded its servers with 1.2 terabits per second of traffic.

The attack initially targeted Dyn’s Managed DNS endpoints in several major geographic locales - namely the Asia Pacific, South America, Eastern Europe, and US-West regions. As Dyn responded to these broad and disparate attacks, it adapted to focus its attention entirely on the the US-East region.

The consequences of this were significant. Multiple well-known online properties were brought down by the attack, including Amazon, Visa, Spotify, Twitter, CNN, and Reddit. These companies had no tangible connection to Dyn, other than the fact that they used its service.

The attack against Dyn is believed to be linked to the previous DDoS attack against Brian Krebs. One theory states that the services were targeted because of the assistance Dyn provided to Krebs in identifying the two Israeli criminals behind the vDOS DDoS-on-demand group.

Whether this is true or not remains to be seen. Although it was an unfriendly reminder that DDoS attacks aren't just aimed at websites. They can also target the critical infrastructure of the Internet, with devastating consequences.

Diversity in Damage

Although the aim of each DDoS attack is the same - to prevent others from accessing a website, connected device, or service - the methodologies can vary significantly. DDoS attacks can be categorized as either volume-based attacks, protocol attacks, and application attacks.

Volume-based Attacks

The goal of volume based attacks is to saturate the bandwidth of a target service. Therefore, you can measure the potency of such an attack in bits-per-second.

Volumetric attacks are simple to understand. Suppose you've got a web server with a 1Gbps connection. Should an attacker bombard it with 10 Gbps of traffic, the web server will quickly be unable to serve legitimate users.

Although this attack paradigm is relatively straightforward, there are several innovations that amplify their effect. Attackers can use IP address spoofing in order to obfuscate the origin of attack, as well as avoid blacklisting-type countermeasures. They also take advantage of common network protocols like Domain Name Systems (DNS) and Network Time Protocol (NTP) in order to amplify the attack.

Protocol Attacks

The goal of protocol-based DDoS attacks are to impair the targeted server by consuming its limited resources.

Many of these attacks take advantage of flaws found in common protocols used by the internet. The most well-known of these is known as a “SYN flood”, which exploits a fundamental shortcoming in the Transport Control Protocol (TCP) system.

The TCP protocol is built around something called the three-way handshake, which is the component used to establish a connection between the server and the client. This three-step process sees both the server and client exchange SYN and ACK packets before any data is actually transferred.

But it can be exploited. If an external attacker floods a server with SYN packets, but never completes the transaction, the server is overwhelmed. Legitimate users are unable to establish a TCP connection, thereby rendering the service completely unavailable.

Other protocol-level attacks worthy of note include the so-called ‘Ping of Death’, and UDP flooding, which attacks the User Datagram Protocol commonly used in real- time applications.

The brilliance of protocol attacks is twofold. Firstly, they take advantage of flaws in standard protocols. Because the Internet relies on everyone adhering to these predefined standards, they can be hard to mitigate against.

But worse, they don’t require the attacker to have much capacity. They’re not contingent on there being a large volume of traffic, making them relatively affordable to perform.

Application Attacks

These attacks take advantage of fundamental design flaws that are present either within a website, or within a service. As such, they require a more detailed knowledge of the target, and are therefore less common than volume-based attacks.

A common example of an application attack is the HTTP GET attack, where an attacker floods a web server with bogus GET requests. These tell the server to request something - be it a file, an image, or the results of a database query. Each time this happens, a piece of the server’s finite resources is consumed.

Make enough of these requests, and the server’s ability to process legitimate requests is fundamentally impaired, or even eliminated.

Botnets: The Unstoppable Force That Powers Most DDoS Attacks

The cost of a successful and prolonged DDoS attack to the victim can easily register in the millions of dollars. They're usually performed for two reasons. In the case of Brian Krebs and Dyn, it's believed that the attack was driven by a desire for revenge.

But often, attacks are accompanied by a ransom note demanding that the victim pay up, or else.

A notable example of this dates back to 2005 when entrepreneur Alex Tew launched the Million Dollar Homepage - a homepage consisting of one million squares, each measuring ten pixels by ten pixels. Tew sold each of these for a dollar. Quite quickly, the website gained the attention of Russian cybercriminals who launched a prolonged DDoS attack, which would be stopped if Tew paid a ransom.

Tew stood steadfast, and with the assistance of his ISP, the FBI, and Wiltshire Constabulary, he was able to restore access his site.

This financial imperative is amplified by the fact that botnets are extremely expensive, both to create and to hire (there is a thriving botnet rental market, where systems consisting of tens-of-thousands of zombified hosts can be rented by the hour). As such, the person using the botnet has an impetus to make a profit.

Mirai: A Masterclass in Sophistication

The Mirai botnet evolved into a vast network of enslaved, yet fundamentally disparate devices.

The Mirai botnet emerged in August, 2016. The term itself is Japanese, meaning 'future', which is rather apt for a system that contained several novel innovations, and unleashed attacks, the ferocity of which had never been seen previously.

Quite quickly, Mirai started to rack up several high-profile casualties. Among the first were 900,000 customers of German ISP Deutsche Telekom. The Mirai software, which is designed to infect and propagate through Internet of Things devices, disabled Internet, TV, and telephony services.

It also struck consumers in the UK, with over 2,300 routers belonging to customers of ISP Talk Talk infected. Mirai spread by searching for internet-connected devices, and then trying to access it through known default or hard-coded passwords. Hacked machines are then infected with software that places them under the thumb of a command-and-control server.

Gradually, the Mirai botnet evolved into a vast network of enslaved, yet fundamentally disparate devices.

It's hard to pinpoint how many hosts Mirai came to dominate. Research from Dyn published in October, 2016, estimates that it encompasses over 100,000 different compromised devices. These were used in the attack against it, which ultimately disrupted much of the internet. It also added that this was out of a total of 168,000 potentially vulnerable devices worldwide.

Later last year, the source code to the malware was released publicly by its creator, purportedly in response to increased interest in the software from the legitimate - or ‘white hat’ - security industry.

This has been a mixed blessing. Whilst it has given researchers a closer insight into its inner workings, it’s also placed it into the hands of more people. This has simply amplified the troubling phenomenon that’s emerged in recent years, where botnets are available as a rentable service.

Botnet-as-a-Service

There are those that wish to launch DDoS attacks. But not all of them have the resources, nor the technical know-how, to launch them. This has lead to a veritable industry of botnets-for-hire.

Remarkably, some of these cost just $5.

Fiverr is a website that allows individuals to sell goods and services for a flat fee of just $5, with the possibility of optional extras. In May, 2016, Incapsula security researchers Igal Zeifman and Dan Brenslaw discovered that several vendors were offering “DDoS testing services” on the platform. These were masked as “website stress testing services”, but with few questions asked.

One provider of such services said, “Honestly, you [can] test any site. Except government state websites, hospitals.”

That was the low-end of the market. Larger attacks cost significantly more. Research by Brian Krebs into the vDOS hacker group suggested that during its short lifetime, it was able to earn as much as $600,000.

Conclusion

It's not just those who may fall victim to DDoS attacks that must take action. An immense burden of responsibility falls upon the shoulders of Internet of Things device manufacturers. The widespread security malpractices in this industry simply must stop.

In light of what we've learned throughout 2016, it's vital that IoT manufacturers cease the practice of using default or generic passwords on their products. Once deployed, they must force the user to establish a new password that is distinct to the device, and adheres to industry best practices for passwords.

Similarly, it's important that manufacturers continue to support older devices with security updates, and ensure that these updates are actually installed, and not simply left to the user.

There are other, more fundamental steps that can be taken. Manufacturers should consider if their devices require DNS access, while owners should determine whether they need remote (WAN) access. Indeed, in many cases, they do not.

Business Readiness

As mentioned at the start of the White Paper, there is a fundamental lack of readiness when it comes to DDoS attacks. Few businesses are willing to invest the time and money, until it's too late.

This must change. Businesses need to drop their reactive approach to this threat, and instead adopt a more proactive philosophy. They need to stop rolling with the punches, and instead start throwing them. It's vital that businesses recognize that prevention is better than a cure, and therefore should invest in their defenses accordingly.

The best defense isn't a strong offense, but the ability to identify and preempt an attack. Therefore, it would be wise to invest in threat intelligence, as well as DDoS monitoring services. Businesses can also invest in DDoS mitigation services. While there are a lot of charlatans in this space - some operated by DDoS-for-hire gangs themselves - there are some legitimate and reputable companies. One of the most widely-known players in this space is Akamai.

Any of these steps required to mitigate against DDoS attacks can be taken by recruiting the services of external companies. But it's also true that they can be done internally, with the right training and the right hardware and software procurement. Often resilience can be built into systems by considering DDoS attack scenarios and architecting infrastructure accordingly.

Finally, it is worth considering non-technical solutions to keep your business running if it is a victim of a DDoS attack. The value of a DDoS attack lies in how much it can disrupt your business and impact your customers. If that is taken away by other means, for example processing payments offline, or having telephone support available, then attackers will begin to lose their leverage in this war of attrition.

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com