Service providers: the gatekeepers of Internet security


Sean Newman

Sean Newman, Corero Network Security

Against a backdrop of the huge Internet of Things-based DDoS attacks we've seen in the last few months, some commentators have warned of the impending 'death of the Internet'.[1] Security expert Bruce Schneier recently warned that "over the past year or two, someone has been probing the defences of the companies that run critical pieces of the Internet."[2] There is now little doubt that if someone really wants to take down the Internet, they will direct their attacks at service providers. How can service providers protect themselves and their customers, from these giant attacks?

The DDoS landscape changed dramatically in 2016 as the power of attacks generated by Internet of Things-driven botnets began to emerge. The attack against DNS service provider Dyn in October, exploiting the Mirai malware, demonstrated a marked gear-shift in terms of the increasing scale of botnet-driven attacks, by taking offline a series of the most popular sites on the web, including Netflix, Twitter, Spotify, CNN and Fox News.

In all likelihood, botnets like Mirai will become even more powerful in the coming years as hackers take advantage of the billions of poorly secured, Internet-connected devices currently in use around the world. Such attacks are also likely to grow in complexity as additional new attack vectors are discovered and then made available for others to leverage.

So how might attacks evolve next? For hackers, a key lesson from the major DDoS attacks of 2016 was that size is everything. High-impact, high-volume attacks, such as that on Dyn, attract media attention and raise notoriety among hacking groups. Just as Dyn was an attractive target due to its capacity to knock so many well-known websites offline through a single source, a similar effect could be gained through attacks on the wider backbone of Internet service providers. This may be why Deutsche Telekom found itself the target of attacks at the end of November, as hackers attempted to recreate the success of the earlier Mirai-led attacks. So let's first examine why this threat poses a risk to the enterprise and what can be done to defend against it.

The datacentre risk

As enterprises around the world increasingly rely on hosted critical infrastructure or services, they also place themselves at greater risk from falling victim to being an indirect target of future devastating cyber-attacks. This is because the multi-tenant nature of cloud-based datacentres offers attackers the ability to knock a variety of organisations offline through a single source.

A DDoS attack, volumetric in nature against one tenant, can lead to disastrous repercussions for others – a domino effect of latency issues, service degradation and potentially damaging and long-lasting service outages. 'Secondhand DDoS' is a term originally coined to explain how the excessive amount of malicious traffic bombarding a single tenant during a volumetric DDoS attack can have adverse effects on other tenants within a datacentre, as well as the overall datacentre operation. It is increasingly common that attacks on a single tenant or service can completely choke up the shared infrastructure and bandwidth resources, resulting in the entire datacentre being taken offline or severely slowed. But when the target is not just an individual tenant but the entire datacentre operation itself, everyone is put at risk.

"It's no longer enough for customers to rely on their provider to take care of the problem – a full understanding of the process is required to ensure that they are sufficiently protected against this type of malicious activity"

As a result, enterprises that rely on hosted infrastructure or services need to start asking some tough questions of their hosting or datacentre providers, such as how they will be protected when a DDoS attack strikes. It's no longer enough for customers to rely on their provider to take care of the problem – a full understanding of the process is required to ensure that they are sufficiently protected against this type of malicious activity and prepared for the increasingly large and complex attacks that we are likely to see in the coming years.

Attacks against large providers seemed almost unfathomable just a few years ago, but the tendency for attackers to spread powerful software for free puts such attacks within the reach of many. Developing malware like Mirai takes time and skill – something that previously ensured it was the preserve of only the most experienced and well-funded

attackers – but once capabilities like this are made open source, anyone can utilise them, to devastating effect. In addition, the potential scale of such attacks is unrecognisable from even a few short years ago. Analysts at Gartner expect the number of Internet of Things-connected devices to increase to 21 billion by 2020 – as a result, we can expect the scale of DDoS attacks to increase massively in the same timeframe.[3]

Defence strategies

As large network operators have succeeded and grown, the sheer size and scale of their infrastructures and their massive customer base presents an incredibly attractive attack surface due to the multiple entry points and significant aggregate bandwidth that acts as a conduit for damaging and disruptive DDoS attacks. The combination of these trends is now driving the need for an even more sophisticated approach to DDoS mitigation that utilises purpose-built technology.

"Solutions appropriate for today need to be always-on and instantly reactive. It's clear they also need to be adaptable and scalable so that defences can be quickly and affordably updated"

As we approach the modern day DDoS threat, with advanced mitigation techniques that have evolved over the past decade, innovative protection, sophisticated visibility and scalable deployment options are emerging. Inline deployments of mitigation technology at the Internet or transit and peering points offer much needed relief from the frequent and damaging attacks that providers are dealing with on a regular basis. Alternatively, many providers prefer a scrubbing-lane approach, but require enhanced visibility into the traffic patterns as well as the need to scale the scrubbing operation for increased bandwidth.

The weaknesses of old methods – being slow to react, expensive to maintain and unable to keep up with shifting and progressive threats – tell us that solutions appropriate for today need to be always-on and instantly reactive. It's clear they also need to be adaptable and scalable so that defences can be quickly and affordably updated to respond to the future face of DDoS threats – whatever those may be.

The increasingly popular method of fulfilling these aims is dynamic, inline DDoS mitigation bandwidth licensing. With this technique, an inline DDoS mitigation engine is employed but the operator pays for only the bandwidth of attacks actually mitigated. The benefit of this approach is that it delivers full edge protection for locations in the network that are most affected by DDoS, at a fraction of the cost of traditional scrubbing centre solutions. The desirability of these tools is due to the fact that they can be constantly on, with no need for human intervention and they provide non-stop threat visibility and network forensics.

Case study: Liquid Web

Liquid Web is a privately held managed web hosting and datacentre company founded in 1997. It operates three wholly owned datacentres in Lansing, Michigan, and a fourth location in Scottsdale, Arizona. The company fills a niche in the public cloud space focused on providing premium web hosting capabilities upmarket from traditional shared hosting. It currently has 25,000-30,000 customers and has been named one of the Inc 5000 fastest-growing companies for the past 10 years.

Over the past few years, Liquid Web found that distributed denial-of-service (DDoS) attacks had become significantly more prevalent in the public cloud space, thereby affecting its core business. These attacks could be either volumetric or non-volumetric in nature. The company had an existing solution in place from a security provider, but it was not sufficient to deal with mounting DDoS problems.

When DDoS attacks were made on the Liquid Web network, incidents needed to be identified, isolated and mitigated. Using legacy DDoS mitigation solutions, such attacks were routinely detected but not prevented. Another challenge was that 'innocent bystanders' (ie, other customers on the network) could be impacted by a network slowdown even though they weren't the specific target of a DDoS attack. This was more likely to occur if they were sharing the same switch or the same section of the datacentre.

The Liquid Web management team and IT team were concerned about the impact of these attacks on both larger and smaller customers. It seemed clear that the company needed to develop a more proactive approach to avoid customers having a poor overall experience with the services they subscribed to. The best way to achieve this was to use an automatic, inline DDoS mitigation solution that provided full visibility across the network and could detect and mitigate attacks in real-time.

After implementing this solution, Liquid Web saw some dramatic improvements. In terms of metrics, the most critical improvement was the decrease in the outage minutes associated with large volumetric attacks. Multiple incidents in the past had raised the possibility of the company losing groups of customers as a result of DDoS security issues. But by implementing an effective, automatic mitigation solution, these concerns were addressed.

Case study: htp

Founded in Hanover in 1996, htp has since become one of the largest regional carriers in Germany, with more than 200 employees. The company product range includes telephone and DSL connections with different bandwidths, mobile communications offers and a range of network services as well as scalable data and infrastructure solutions offered by high-availability and high-security in-house computer centres. The firm serves more than 9,600 business customers and approximately 88,800 private customers in the Hanover region, Brunswick and the districts of Hildesheim, Peine and Wolfenbüttel.

While DDoS protection technologies have developed in leaps and bounds over the years, most solutions are only reactive to the threat and valuable time is lost as a result. After a careful analysis of

its bandwidth peaks, the company realised that it had already suffered a series of 'hidden' DDoS attacks that had not previously been detected. These attacks were generally UDP (User Datagram Protocol) amplification attacks that posed an immediate danger to its infrastructure, typically using one of the DDoS attack vectors that exploits publicly accessible systems such as poorly configured DNS servers or routers and other vulnerable points. This posed a significant threat to the organisation, given the reputational risks involved if customers were to lose data or a website was no longer accessible as a result of a DDoS attack.

As a result, the provider decided to adopt a different strategy, which involved real-time detection and mitigation of attacks. By deploying these solutions across the network, htp has achieved effective protection from all volumetric, application layer and multi-vector attacks, even those lasting less than five minutes and utilising only a small amount of bandwidth.

Next steps

The head of the UK's new National Cyber Security Centre caused uproar in the press recently by suggesting that UK Internet service providers could restrict DDoS attacks across their networks by rewriting Internet standards around spoofing. Ian Levy, technical director at the cyber defence arm of Britain's GCHQ, told the Sunday Telegraph newspaper that if ISPs made changes to the Border Gateway Protocol (BGP) and Signalling System 7 (SS7) standards that have been in place for decades, the trivial re-routing of UK traffic would be eliminated and eventually the Government could claim that UK machines would be prevented from taking part in DDoS attacks.[4]

The suggestions were met with shock and surprise in corresponding news articles, with the UK Internet Service Providers Association (ISPA) suggesting that Levy's approach fails to highlight the complexity of the issue.[5,6] But while these methods aren't a quick fix and they certainly can't protect against the full spectrum of modern DDoS threats, they could be a vital first step in speeding up our global response to attacks.

More importantly, the announcement should indicate to the service provider community that regulatory pressure could be introduced in the future to enforce such changes, if they are not achieved voluntarily. And in the long run, that could be in everyone's best interests. After all, there is a valuable business benefit for ISPs to position themselves as leading the charge against DDoS attacks, both in protecting their own networks and enabling them to offer more comprehensive solutions to their customers as a paid-for, managed service.

"There is a valuable business benefit for ISPs to position themselves as leading the charge against DDoS attacks, both in protecting their own networks and enabling them to offer more comprehensive solutions to their customers"

ISPs are likely to find themselves at an important crossroads in the coming year. By working together with governments and the international community, they can strengthen the underpinning infrastructure of the Internet and significantly reduce the volume of malicious traffic flowing across their networks. If they do nothing, they could find themselves subjected to expensive litigation claims if disgruntled customers try to recoup losses suffered as a result of their businesses being taken offline. Surely the best approach is for service providers to position themselves as the gatekeepers of Internet security, by protecting customers from the next-generation threats through the use of automatic, inline, DDoS mitigation positioned at the edge of their networks. It is only through this complete visibility that the worst threats can be identified and ultimately defeated.

About the author

Sean Newman is director of product management for Corero Network Security. He has worked in the security and networking industry for 20 years, with previous roles including network security global product manager for Cisco, which he joined as part of its acquisition of cyber-security vendor Sourcefire, where he was security evangelist and field product manager for EMEA. Prior to that Newman was senior product manager for endpoint and network security vendor Sophos, after having spent more than 12 years as an engineer, engineering manager and then senior product manager for network infrastructure manufacturer 3Com.

References

1. Vaughan-Nichols, Steven. 'Death of the Internet: GIF at 11'. ZDNet, 6 Oct 2016. Accessed May 2017. www.zdnet.com/article/death-of-the-Internet-gif-at-11/.
2. Schneier, Bruce. 'Someone Is Learning How to Take Down the Internet'. Schneier on Security, 13 Sep 2017. Accessed May 2017. www.schneier.com/blog/archives/2016/09/someone_is_lear.html.
3. Eddy, Nathan. 'Gartner: 21 billion IoT devices to invade by 2020'. InformationWeek, 11 Oct 2015. Accessed May 2017. www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081.
4. McGoogan, Cara. 'GCHQ wants Internet providers to rewrite systems to block hackers'. The Telegraph, 5 Nov 2016. Accessed May 2017. www.telegraph.co.uk/technology/2016/11/05/gchq-wants-Internet-providers-to-rewrite-systems-to-block-hacker/.
5. Neal, Dave. 'GCHQ thinks ISPs can solve DDoS by taking a good look at themselves'. The Inquirer, 7 Nov 2016. Accessed May 2017. www.theinquirer.net/inquirer/news/2476614/gchq-thinks-isps-can-solve-ddos-by-taking-a-good-look-at-themselves.
6. Spadafora, Anthony. 'GCHQ encourages ISP to rewrite their software to stop DDoS attacks'. ITProPortal, 8 Nov 2016. Accessed May 2017. www.itproportal.com/news/gchq-encourages-isps-to-rewrite-their-software-to-stop-ddos-attacks/.