The evolution of DDoS


Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Computer Fraud & Security*

Distributed Denial of Service (DDoS) attacks are an all too familiar part of the threat landscape. They gained wide public attention thanks to their use by the likes of Anonymous and are now closely associated with hacktivism and other political uses. But DDoS has its origins in criminal activity and it's there that we're seeing the technique evolve. We interviewed David Larson, CTO of Corero Network Security, about the changing nature of DDoS attacks.

Changing landscape

The earliest uses of DDoS attacks, often mounted using botnets of infected machines, were for extortion. Particularly in industries such as online gambling, firms would be threatened with disruption of their business, often at an important time such as on the eve of a major sporting event. The technique was subsequently taken up by groups with other motivations, from nuisance attacks by hacktivist groups simply trying to raise awareness of an issue through to the cyber-warfare campaigns witnessed in Estonia in 2007 and Georgia in 2008 and continuing through to current activities in Ukraine. However, political activism and blackmail are no longer the only uses of DDoS.

"The actual intent of an under-the-radar intrusion gets lost among the noise, because the logs and tools are overwhelmed by the event data that's associated with the attack"

"I think the landscape is changing," says Larson. "I think the ease with which a large-scale DDoS attack can be created and launched is making the tool more attractive to a variety of other interests. We're starting to see a much higher prevalence of hybrid, multi-vector attacks, where DDoS is being used as a distraction."

Increasingly, cyber-criminals are deploying DDoS as a way of keeping an organisation's security professionals busy while they carry out more sinister activities, such as malware insertion, data exfiltration and other forms of intrusion. It's all too easy for those people tasked with protecting the networks to misinterpret an attack as a simple nuisance – perhaps the work of a group of amateurs with an axe to grind. And it's not just the IT personnel and security analysts that can find themselves distracted.

"One of the problems with a volumetric attack is that it overwhelms the analytics tools, the log tools, that exist on all firewalls, all edge defences, even on the routers and switches and servers themselves," says Larson. "The actual intent of an under-the-radar intrusion gets lost among the noise, because the logs and tools are overwhelmed by the event data that's associated with the attack, and that all looks identical."

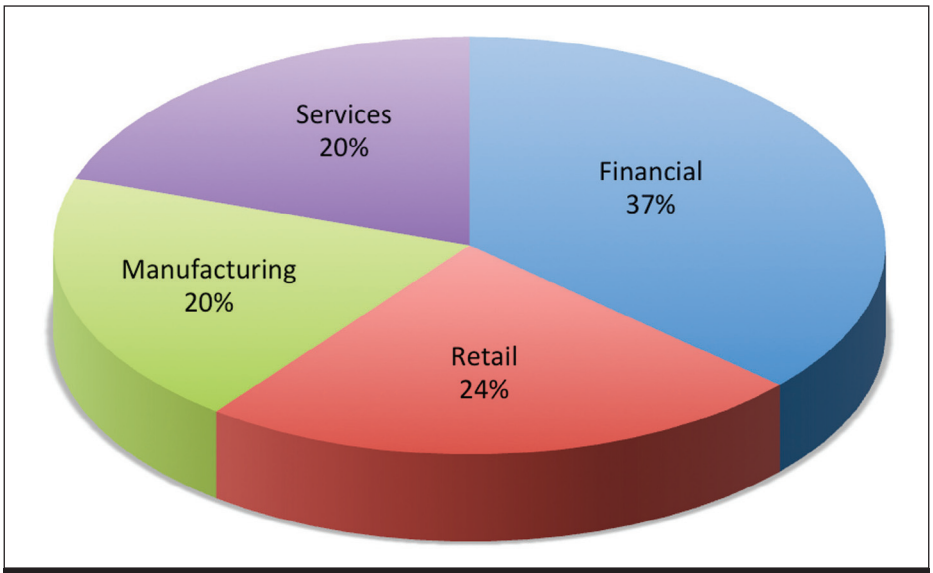

David Larson, Corero: "I think the ease with which a large-scale DDoS attack can be created and launched is making the tool more attractive to a variety of other interests."

Leaving headroom

This may sound like a strange way of going about penetrating someone's network. After all, the concept behind a volumetric DDoS attack is to bring down the system by flooding it with more traffic than it can handle. On the face of it, that would seem to leave little in the way of opportunity for an attacker to work their way into the system via the Internet. So how do they get through when legitimate visitors to the system are prevented by the DDoS assault? The answer to this is also one of the clues that such an attack is underway, explains Larson.

"We see these large attacks that are intended to be complete pipe saturation, over-saturation attacks, but we are also seeing a sweet spot attack vector that's in the 600-700Mbps range, or even 6-7Gbps range. Now, that's an odd number. Why does that matter? The reason it matters is, when we see attacks of that nature, they are intended to leave headroom on the pipe, so a 600 or a 700Mbps attack is intended to be directed at an entity that has a one gigabit link to the Internet. The reason that they use that scale is, it's enough to basically circumvent the firewall defences without taking it down, and to create enough of a distraction that other traffic is still allowed to go through."

The attackers can afford to be patient. It may take them some time to achieve a good enough connection to carry out their nefarious work, but they can do



Type of industries that typically come under DDoS attack. Source: Corero.

this in the knowledge that the defenders are likely to be looking elsewhere and won't notice the intrusion.

"We're seeing regular 100Gbps attacks, and 300Gbps isn't rare. I am of the personal opinion that, if a terabit-class attack has not already occurred, we will see it probably within the next six to nine months"

In addition to the fact that it leaves some headroom for an attack, DDoS campaigns running at, say, 700Mbps are suspicious for another reason – and that's that the attackers could easily make them bigger. According to Larson, 'instrumenting' a DDoS attack is now scarily simple. The 'traditional' botnet-based attack may require some considerable planning and resources, but there are other options. Larson points to the plethora of misconfigured servers and services running on the Internet. Notoriously, both Network Time Protocol (NTP) and Domain Name System (DNS) servers have recently been exploited for large-scale 'reflection' or 'amplification' attacks, where relatively small messages are sent to the servers, with spoofed source IP addresses matching the target system. The servers then send much larger responses to the target.

"Compromised servers and services can be used to send a totally anonymous attack at virtually any scale," says Larson, "and we're seeing regular 100Gbps attacks, and 300Gbps isn't rare. I am of the personal opinion that, if a terabit-class attack has not already occurred, we will see it probably within the next six to nine months. I think the only thing that's preventing us from seeing that class of attack is that the number of sensors and the aggregated data is not available to actually see the full dimension of some of the larger scale attacks that are occurring."

Spotting the problem

While a 700Mbps attack might be the 'hallmark' of DDoS being used to mask another form of intrusion, is it really that easy to spot that this is what's going on? In reality, it's not always so simple, but Larson claims it could be a lot easier if you are prepared for it.

"In fact, it can be easy – there are tools that will allow you to see that," he says. "You can instrument so that you are getting the proper amount of event data. You utilise the proper kinds of log management tools, or data analytics, to mine in real time, or near real time. But what we find is that the typical organisation – or perhaps the 'legacy approach' is a better way of saying this – to DDoS is to look for peaks in the flow data. Peaks are easy to see. If all of a sudden the bandwidth spikes from normal utilisation of one gig to seven or eight gig, that's readily apparent in the form of a very easy-to-set alert that can notify the IT organisation that there is an attack under way."

On the other hand, if your networks are not suitably instrumented to capture all of the metadata surrounding that attack, it's virtually impossible to extract and analyse data that will tell you exactly what went on during the attack. You may know that a DDoS attack happened, but you won't see the tell-tale trail of, for example, data exfiltration. The capability to recognise a hybrid attack has to be in place beforehand, says Larson – it's not something you can apply after the fact.

"You'd have to already have pre-positioned the ability to extract that data from the line," he explains, "to be able to look at it really quickly in the form of meaningful dashboards that are allowing you to look at a variety of different event data."

Large, forward-looking organisations, such as the big banks, are doing this kind of thing. They're correlating their edge data with application data and user data (ie, authentication) to know who's coming in and out of the network at any given time.

"It becomes a big data problem," he says. "It becomes an analytics problem. Standardising around event formats, and utilising things like syslog to great effect, are the only way that you're going to be able to tease this out, when that kind of attack is taking place."

The problem is that the vast majority of organisations don't have that expertise in house. While the biggest organisations have it, they're not the only ones coming under attack. You also have to have the wherewithal to use your logs and your analytics tools at the same time that you're busy fire-fighting the DDoS attack itself. Even if you suspect that some additional form of attack is underway, mitigating the loss of your web-based services – which

might be the lifeblood of the business – might be your top priority. Spending time and resources looking for the other thing that's going on is going to be low on your list of priorities.

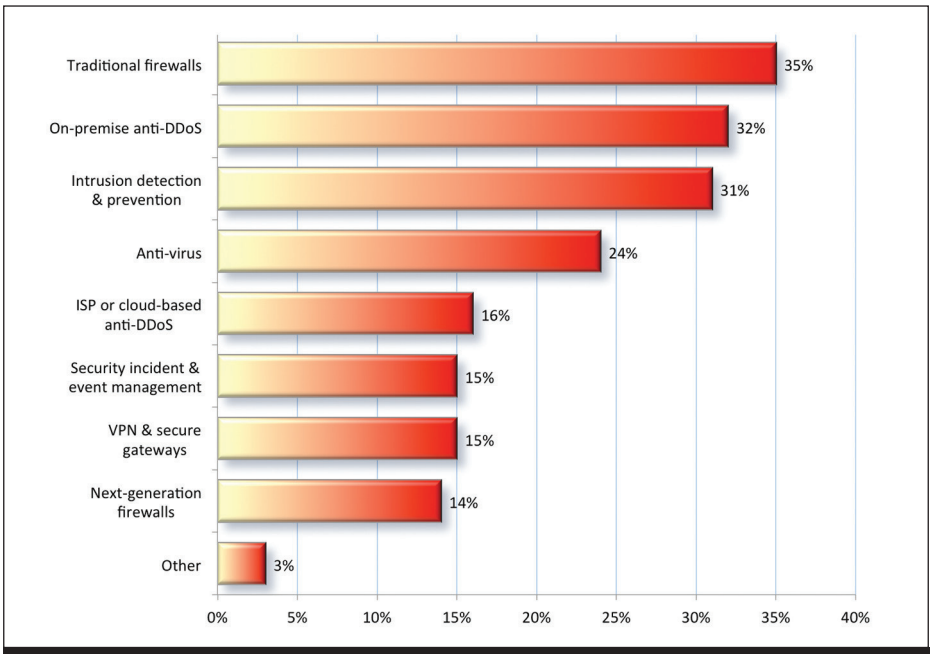
"The call centre is burning down. Your customers are complaining that they can't get through. The executive suite is saying, why is my business offline?"

As Larson describes it: "The call centre is burning down. Your customers are complaining that they can't get through. The executive suite is saying, why is my business offline? So the IT personnel are trying to solve that problem, that is being caused by the DDoS attack, and that's the whole point. It's used as a distraction, it causes a problem. It forces the IT community to take their eye off the ball, so to speak, and allow these other infiltrations to take place against the environment, which then, once they're in, they're even harder to detect. If you don't see them as they occur, you're only going to notice them once they start to cause problems, where you actually determine that you've been breached. Breaches are almost always identified by third parties, that suddenly see your data in the wild. So once you've missed the original incursion, it usually is too late to fully recover until the breach has occurred."

Mitigating the effects

In the case of hybrid attacks, your defences and mitigation strategies are not just focused on DDoS. You also need to have in place proper security geared towards more directly protecting the data.

"I would say it can be both, or it should be both," says Larson. "You need to correlate and utilise all of the information at your fingertips." And, in fact, data security is only half the problem, he insists. "Threat intelligence is the other half, and the only way to have correct

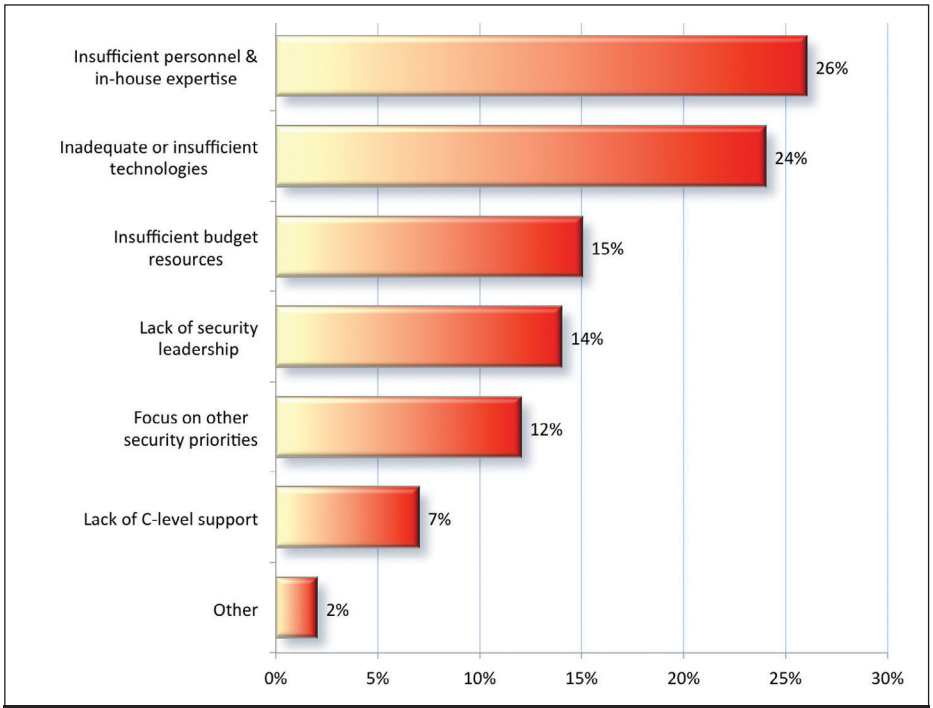


Security technologies used to prevent and detect DDoS attacks. Source: Ponemon Institute.

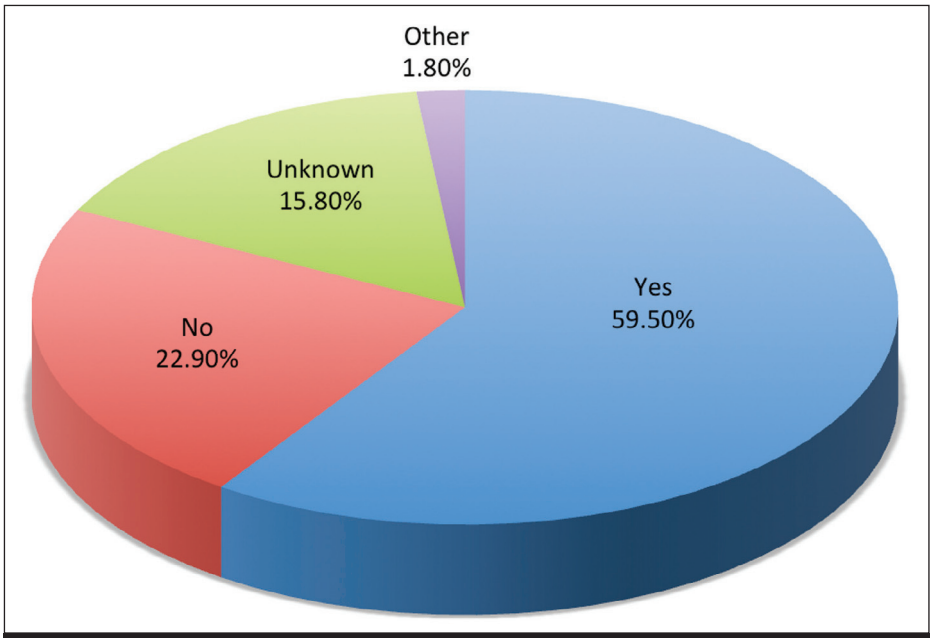
threat intelligence is to mine and utilise the event information and metadata that's provided by all of the layers of your infrastructure. So it is partly about DDoS, but it's not exclusively about DDoS."

He adds: "DDoS attacks range in a variety of dimensions, in terms of the bandwidth, the class of attack, spoofed attacks, targeted botnet attacks, multiple victims, varied frequency and variability to the attacks themselves, and a strong DDoS solution should be able to identify and isolate multiple vectors of an attack. But the other thing that the DDoS solution can do, because it's looking at network traffic, is it should be able to provide you regular network event information alongside, in the form of NetFlow or sFlow sampling, from the area where the DDoS inspection is taking place, which is usually at the edge of the network, or just in front of the server tier."

The key, says Larson, is to combine all this information with the event



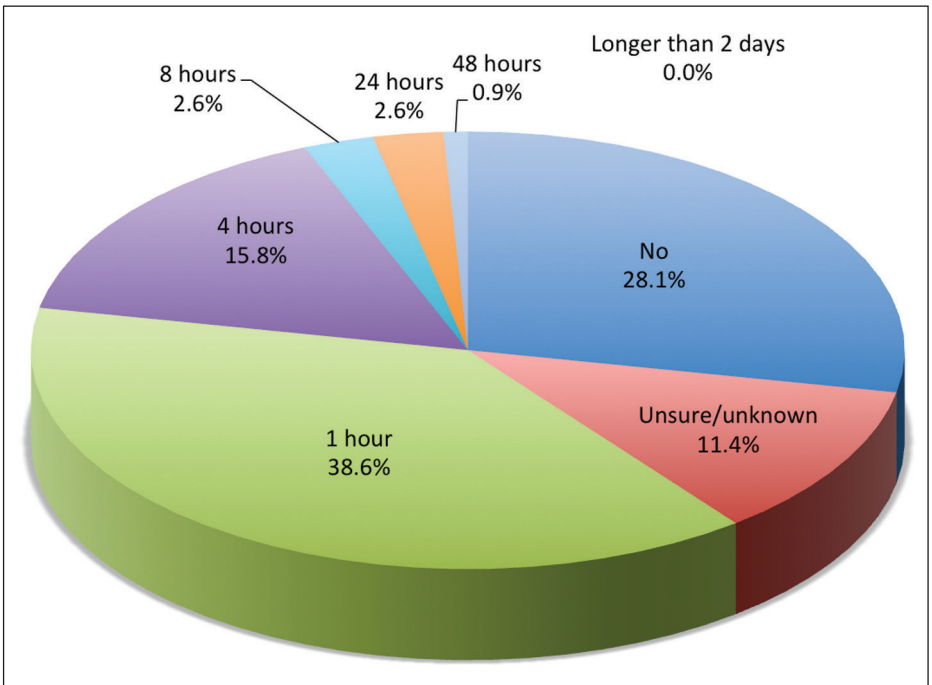
Critical barriers to preventing DDoS attacks. Source: Ponemon Institute.



Answers to the question, 'does your organisation have a plan for mitigation if it suffers a DDoS attack?'. Source: SANS Institute.

information associated with IPS devices, firewalls and next-gen firewalls, and web application firewalls. This synthesised data should be processed by an appropriate analytics engine which, he says, are readily available to and affordable by even smaller organisations now.

"Anybody can afford, and in fact should require, a good analytics capability as part of their defences," he says, "and once you have that synthesis, you should be able to tease out the information in relatively near real time. Even if you can't do it in near real time, you should be able to maintain event archives that can be used for forensic analysis after the fact, so that every time you incur a large-scale attack, your analysts should go back into the data and see if anything else was going on at the same time."



Answers to the question, 'Did the DDoS attacks cause an outage that disrupted your business and, if so, for how long was your business disrupted on average?'. Source: SANS Institute.

Network versus application

Not all DDoS attacks are about flooding the network – the classic volumetric attack. Other forms focus on the application layer – for example, by making a lot of requests for large files or by enforcing slow connections at the application level. There was a time when some specialists in the DDoS field claimed to have detected a shift from network-layer attacks to application-layer attacks. However, Larson reiterates that the large number of poorly configured servers on the Internet means that volumetric attacks using reflection methods are still highly prevalent – not least because they are virtually 'free' to mount. And these tend to be the methods favoured for massive-scale attacks.

"The bad guys have a very wide arsenal in their toolchest that they can use against any entity on the Internet, and if you don't have a good defence in-depth approach to all of those vectors, you're going to remain at risk"

In addition, he says: "On the network side, we see that there are still botnet-driven attacks that occur, that are using UDP floods. Clearly there are application-layer attacks like Slow Loris and Slow Read, that are intended to be well under the radar. They're never going to trigger a bandwidth threshold tool, and yet they're intended to occupy connections against web properties so that legitimate transactions have no place to go, and in that way you can starve out a web property with very little difficulty, and it won't even register on the radar of any of your bandwidth tools. What we see is that there are a combination of all of these tools, and legacy cross-site scripting, other forms of intrusion, other forms of malformed packet attacks. Basically, the bad guys have a very wide arsenal in their

toolchest that they can use against any entity on the Internet, and if you don't have a good defence in-depth approach to all of those vectors, you're going to remain at risk."

Threat awareness

Protecting against DDoS suffers from the same issue as any other area of information security. Buying security capabilities is like buying an insurance policy – you're paying for something that might never happen, or at least that's how a lot of people – especially at the board level – view it. And mitigation against DDoS can be expensive. Does this mean that most organisations are still woefully unprepared for a DDoS attack?

"I would say that's true," says Larson. "Part of it is lack of awareness. Often, organisations will attribute downtime to other things. They don't even realise that it's a DDoS attack that's caused the problem, that's forced the CPU utilisation of their firewall to the ceiling and thereby taking their systems offline. So part of it is an awareness thing, part of it is a cost thing.

"There are a variety of approaches to mitigation, there are cloud-based solutions, there are on-premise solutions, there are inline solutions, and there are scrubbing solutions. All are valid approaches, none are sufficient in and of themselves. So that's one of the problems with DDoS, is that you can deploy a cloud solution, or you can register with a cloud provider, so that you can have a way to move your traffic through a scrubber in the cloud when you're under attack – that's great. If you're attacked regularly, that's going to become prohibitively expensive. You're not going to be able to afford that. If it's a very rare occurrence against your environment, that's probably an acceptable approach, but even in that case, to move your traffic through the cloud organisation in order to get it scrubbed takes recognition that you're under attack, and then it takes time to move the routes or DNS updates in order to get the traffic through the scrubber."

The problem with this is that propagating DNS changes takes time – frequently an hour or more. Yet around half of all volumetric DDoS attacks last less than an hour anyway. By the time you've changed the traffic routing, the attack has ceased.

"The other problem is, you might decide that you want to have a scrubbing centre solution on your premise, so that it's out of band and you are not creating a single point of failure between the Internet and your critical services, because you don't know whether or not your DDoS solution is up to the task of staying in line," Larson says. "That's a reasonable approach. It also allows you to amortise your expense across multiple links or peering connections. So that's a legitimate way to solve the problem. But again it's only going to see what you send to it.

"And then the third way of dealing with this is to put inline solutions at every peering connection, that can block attacks as they occur. All of these approaches should be utilised in a comprehensive DDoS mitigation strategy. The inline solution will protect you from the initial spikes. The cloud solution will protect you from pipe saturation, and the on-premise scrubbing solutions allow you to amortise costs in a way that it's not going to be runaway, if you have a tremendous amount of peering connections. But sometimes the ability to actually scale to meet all of that is going to be cost-prohibitive."

The solution, he says, is to carry out a proper cost analysis that's precisely linked to your business, your industry and your risk profile.

Secondhand DDoS

There remain plenty of organisations that believe they will not come under a DDoS attack. Some think this because the nature of their business doesn't make for easy extortion. Others associate DDoS with hacktivism or politics which, they feel, are issues very remote from their world. But there's an increasingly prevalent trend which means that you can suffer from DDoS attacks even if you are not the target.

"We're seeing a tremendous amount of datacentre consolidation and the use of cloud services generally," says Larson. "So if an enterprise were to move some portion, or all, of their web presence into a hosting centre, that hosting centre is going to have some amount of finite bandwidth. Generally, it'll have more bandwidth than the enterprise itself, which is a double-edged sword. On the one hand, it allows the enterprise to have better bandwidth access to the Internet, so that their services operate better. On the other, they've now moved their services into an environment with a larger attack surface."

This can lead to what Larson calls 'secondhand DDoS'. If your systems are hosted in a multi-tenant environment, an attack against any one of the tenants – not necessarily you – can create incidental effects, secondhand damage, to all

Continued on poage 20...

...Continued from page 19

of the other tenants hosted in that environment, assuming that the solutions for DDoS mitigation are not up to the task.

"It goes back to the issue concerning a combination of the ability to absorb the original spike inline, so that the spikes themselves can be tamped down, and then the ability to move the traffic using traffic-engineering route injection principles, either into scrubbing centres or cloud services, for long-duration attacks," says Larson.

One concern is that the service providers offering multi-tenanted facilities may not even be up to the task of dealing with those initial spikes.

"A five-minute saturation attack can easily take down firewalls, routers and other equipment in the infrastructure," explains Larson. "And while that five-minute attack, if the infrastructure equipment were to stay up, is a nuisance from the perspective of the customers of that environment, if the firewalls go down, the switches go down and the routers go down and the servers fail, that's more likely going to be an outage that's going to be measured in hours, even though the attack itself was short-lived in terms of its duration."

So if you're using these kinds of cloud or datacentre services, you're going to want assurances that the service provider has mitigation capabilities in place, even if you think it's unlikely your own organisation will come under attack.

"When you create an SLA contract with your service provider or your hosting provider, you should be asking for a clean pipe, and if an outage occurs because there's pipe degradation that had nothing to do with you as a victim of an attack, you should write into the SLA that there should be some form of reimbursement, or remuneration to you," Larson says.

"The other thing is, if you instrument an appropriate defence in-depth infrastructure that includes all the metadata and analytics that I talked about before, you'll also be able to check and test multiple providers for their efficacy of their own SLA commitments to you," he adds. "So an example would be, almost all hosting providers have significant Internet peering bandwidth, and they do this using multiple providers. Well, it's very straightforward to see whether or not an attack is being propagated equally across all of those providers, or whether one particular carrier is providing a cleaner pipe than another. I would say it's in the best interests of an organisation, particularly that class of organisation – hosting providers and cloud providers – to be regularly testing the nature of the bits that they're getting from their upstream providers, and putting their investment with providers that are providing cleaner pipes. And I think the market effect of doing that will create an upstream pressure for the carriers themselves to begin to recognise that revenue is tied with not propagating attacks. So this is a long-term play; but as customers become more aware of what they're actually paying for on the line, they're going to be increasingly dissatisfied to actually pay for bandwidth that's loaded with attacks."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security and editor of Computer Fraud & Security *and its sister publication* Network Security. *He also blogs and podcasts on infosecurity issues at Contrarisk.com.*

Resources

- Pescatore, John. 'DDoS Attacks Advancing and Enduring: A SANS Survey'. SANS Institute, Feb 2014. Accessed Sep 2014. www.corero.com/resources/files/analyst-reports/Survey_DDoS_Attacks.pdf.
- 'A Study of Retail Banks & DDoS Attacks'. Ponemon Institute, Dec 2012. Accessed Sep 2014. www.corero.com/resources/files/analyst-reports/CNS_Report_Ponemon_Jan13.pdf.

EVENTS

14–16 November 2014
ISACA Information Security and Risk Management / ITGRC
Las Vegas, US
http://bit.ly/165MHQa

17 November–22 December 2014
SANS London 2012
London, UK
www.sans.org/event/london-2014

19–20 November 2014
Cloud Security Alliance Congress
Rome, Italy
www.cloudsecuritycongress.com

20–21 November 2014
DeepSec
Vienna, Austria
https://deepsec.net

25–26 November 2014
Black Hat Regional Summit
Sao Paulo, Brazil
www.blackhat.com/sp-14/

25–26 November 2014
Info-Crime 2014
London, UK
www.info-crime.com

8–10 December 2014
(ISC)^2 Security Congress Emea
London, UK
http://emeacongress.isc2.org/

26–27 February 2015
International Conference on Cyber-security for Sustainable Society
Coventry, UK
http://sustainablesocietynetwork.net/th_event/cyber-security-event-1/