corero
FIRST LINE OF DEFENSE

Tackling the growing threat of DDoS in telecoms

telecoms.com
INTELLIGENCE

SYNOPSIS

In a digital age, for which telecoms service providers are the life-blood, modern consumers are perennially connected to internet services of one form or another. Be it online or mobile banking, video-on-demand, social media, music streaming services or live news aggregators; large enterprise organisations and telecoms companies are under pressure like never before to maintain a 24 hour a day service availability.

DDoS, or distributed denial of service, is well appreciated as a growing threat to online connectivity. A simple search of the 'DDoS' acronym will yield thousands of news articles describing network outages impacting businesses of all sizes and stories of organisations quietly paying ransoms to nefarious hacktivist groups to stop the attacks and get back online.

While DDoS-caused outages are costly in themselves, there is a deeper threat emerging related to DDoS attacks. If one looks beyond mere connectivity and the consumption of content, it has become increasingly apparent that users are storing more confidential and financial details in cloud and internet services than ever before. As a consequence, it is inevitable that DDoS techniques are being utilised by hackers and would-be evil-doers to compromise data security perimeters and access personally identifiable information details. In some industries, personal data breaches and theft can result in potentially catastrophic regulatory impositions and fines; and telcos, as internet connectivity and security managed service providers, are therefore under further obligation to protect both their networks and their customers.

DDoS is a rudimentary form of cyber-attack which has grown in frequency and sophistication over the last 10 to 15 years; a simple attack by nature but one of brute force which can be potentially devastating to enterprise companies and service providers alike if not appropriately managed. DDoS attacks have grown in scale, ferocity and diversity of end goals. It is no longer safe to assume that DDoS attacks are simply an online availability threat. DDoS vectors are being incorporated into ready-made breach kits and this evolution is bringing with it a need for a review of traditional threat mitigation.

DDOS: AN EVOLVING THREAT

In 2015's Annual Industry Survey, run by Telecoms.com Intelligence, 29% of more than 2,000 respondents said their organisation had fallen victim to a DDoS attack and network breach in the past year alone. Narrowly behind malware and fraud as the most common security incidents, DDoS was seen by a significant percentage of the survey's audience as a major threat to their organisation and its revenue streams.

DDoS refers to a "distributed denial of service" attack. The "distributed" element of DDoS comes from the use of techniques like botnets - infected internet-connected computers which send a set of requests to a large number of vulnerable open internet services via a spoofed IP address. In return, all of those vulnerable services respond with records of data, which hit the intended victim simultaneously, thus amplifying attacks by 10 or 100 fold. It has been known for even larger amplification to occur thus causing significantly larger DDoS attacks, all stemming from seemingly legitimate servers or services – such as domain name services (DNS), network time protocol (NTP), or simple service discovery protocol (SSDP), which is integral to the operation of all retail consumer plug and play network devices. All of those are notoriously vulnerable and widely available services. There are many thousands of vulnerable devices which can be tricked into responding against a victim's IP address.

The "denial of service" aspect comes from the intention of using said techniques to achieve the aim of knocking the victim off the internet for a period of time. If vulnerable devices are grouped together, network operators can be faced with a torrent of incoming data, unsolicited from the victim's point of view, which cannot be handled by their networking environment and, as previously explained, can effectively shut them off the network.

However, more recently, DDoS methods are increasingly being incorporated into sophisticated, multi-vector, pre-packaged attack tools. The reasons for this are fairly straightforward: DDoS can be used to redirect security professionals away from other potential attacks being readied; it can also be used quite effectively to degrade firewalls and intrusion prevention systems (IPS); or it can be used for its initial purpose of denying service, distracting a would be victim from the greater threat of infiltration.

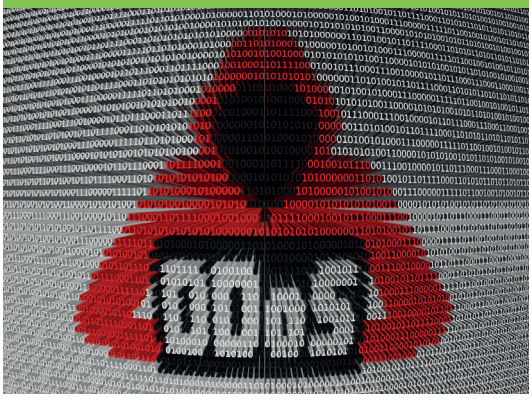
Another major form of information security threat, the Trojan appears innocuous, and is let into the networking environment unwittingly, potentially as malware guised as an email attachment. DDoS, however, is not that; in many cases it is not a subtle tool. It is a brute-force attack originating from outside the network to fill up bandwidth and deny service, and it can be used to overwhelm both compute and human resources. But make no mistake, low-level, sub-saturating DDoS can be an indicator of even greater concern.

DDoS can easily be utilised to distract information security teams; if an attack is sent in, security staff immerse themselves in diagnosing and resolving it as soon as possible. Such distraction has the potential to pave the way for more aggressive attacks with the intention of harvesting customer, financial or personal information. More importantly, while originally intended to be a denial of service attack in web-facing properties, DDoS has evolved to the extent that attackers have now taken to using it as a means of degrading firewalls and intrusion prevention systems. Fundamentally therein, a potentially enormous information security threat lies.

If DDoS is used to degrade a firewall or cause an intrusion prevention system to fail, then further exploits can occur once the attacker has made it through the security tier. At that point, Trojans, advanced persistent threats (ATPs) and other vulnerability or zero-day exploits can be implemented in the application layer.

29%

had fallen victim to a DDoS attack and network breach in the past year.



NATIONAL SECURITY MEETS REGULATION

One of the main threats of DDoS to the telco network, like any very large-scale attack, is collateral damage. If an evil-doer were to launch a several hundred gigabit DDoS attack in an attempt to take an operator offline; there is almost certainly going to be an effect on customers who co-reside or are reliant on the infrastructure transporting the attack. It is therefore important for telcos to appropriately handle and resist a DDoS attack from that perspective. Ironically, the telcos operate many of the services that come under attack or are utilised in a DDoS attack, such as NTP or DNS; so it could be argued that the telecoms industry has an even greater need to protect their infrastructure from being exposed.

Furthermore, telcos themselves can be a vector through which geographically large outages are created. If a service provider is attacked and the services allowing them to operate their network (like DNS) are compromised; a regional environment can effectively be taken out. From a nationwide point of view, operators in a region can be taken out through DDoS attacks, thus disabling local internet and potentially allowing the manifestation of national security threats in the case of further, more advanced exploits.

Considering the potential national security implications of a telecoms operator or ISP being stunned by a large-scale DDoS attack, it could stand to reason that national and international telecoms authorities could be investigating the potential implementation of information security-related regulations. At present, DDoS mitigation features at an organisational level as part of business risk and strategy planning; large-scale attacks hit reputations, finances and customer trust, but so far there's been little sign of regulators like Ofcom or the FCC throwing the book at the telecoms community regarding DDoS events.

That's not to say regulators wouldn't get involved should a large or severe enough incident occur. If a human, societal or significant financial risk emerged as a consequence of a DDoS attack, it wouldn't be surprising to see stricter rules levied upon the telco industry. Attacks are already happening on a large scale, and have been for a while; and along the way there have been terabit-levels of DDoS attack emerging, indicating the growing threat facing telco networks today.

Beyond regulatory and financial implications, the damage to the customer relationship as a consequence of suffering a heavy and sustained distributed denial of service attack can't be underestimated. Reputation damage in the public eye can take a very long time from which to recover; and trust between the affected

If a service provider is attacked and the services allowing them to operate their network (like DNS) are compromised; a regional environment can effectively be taken out.

customer and its telco has the potential to lead to irreparable churn. How a service provider deals with DDoS is of significant importance, as monthly connectivity for an enterprise is hardly an inexpensive proposition, with which comes the expectation of consistently managed and reliable internet traffic. Ineffectively handling DDoS traffic and not protecting enterprise customers appropriately can therefore lead to the churn of high-value customers.

CARPHONE WAREHOUSE, DDOS AND CUSTOMER DATA

As previously alluded to, DDoS can be utilised to achieve a selection of three primary outcomes – to distract analysts, to degrade security and/or to deny service. But what happens when a company becomes the victim of a substantial attack? In August 2015, UK mobile phone retailer Carphone Warehouse (CPW) publically revealed it had been hit by a huge denial of service attack, which resulted in the loss of more than 2.4 million customer records, including credit card information and personal details.

The attack on CPW utilised DDoS as a distraction event while other activity was taking place; resulting in the theft of user data. Not only does DDoS have the potential to distract security personnel, but it also jams up security logs and creates an environment whereby the vector used to effect the breach is totally obfuscated and made theoretically invisible. In the case of credit card information being stolen, all organisations carrying said information are required to comply with what is referred to as the PCI-DSS, a regulatory standard intended to protect and secure confidential credit and debit card information for customers of retailers or financial institutions conducting digital and credit card transactions. PCI-DSS refers to the Payment Card Industry Data Security Standard, and has 10 major categories for compliance – none of which relate directly to DDoS protection. It does, however, maintain requirements for firewalling, intrusion prevention systems, and logging capabilities. As noted previously, these security tiers have been shown to be vulnerable to DDoS as an evasion technique. Surely, any security professional that is intent on complying with the true spirit of this regulation should be examining their DDoS defense capabilities to ensure that their security perimeter is configured to avoid compromise in this way. Presumably, DDoS protection regulation won't be far away having seen major breaches associated with DDoS cause the loss of vast amounts of customer credit card data.

THE EVOLUTION OF DDOS MITIGATION

DDoS protection has evolved over the past decade as organisations play catch-up in developing resistance techniques to a potentially devastating form of information security attack. In early days, DDoS mitigation began with the ability to see an attack happening; once it could be detected, operators could advertise a null-route for the IP address of the victim in a practise known as black-holing. Black-holing effectively means any traffic associated with the victim's IP is dropped, effectively fulfilling the desired outcome of the DDoS attack from the perspective of the attacker: taking the victim off the network altogether. From the operator's point of view, black-holing prevents the DDoS attack from worsening or becoming more exacerbated against unintended victims, but it would be fair to say that this methodology presents the least desirable outcome in terms of DDoS protection with such disruption to the network.

A more common approach to DDoS protection today involves a more active method of mitigating potentially disruptive traffic overloads. Instead of black-holing the victim's route, DDoS-generated traffic is instead rerouted through a dedicated facility called a scrubbing centre; where the DDoS is removed from the flows and legitimate traffic is forwarded on. Scrubbing centres are designed on existing technology principles, and work on a best-effort basis, operating in the cloud.

Utilising scrubbing centres as a means of DDoS protection appears to come with both its benefits and drawbacks in equal measure. It's at its most effective detecting and mitigating large scale DDoS attacks in the range of 40Gbps. Once the system

Black-holing prevents the DDoS attack from worsening or becoming more exacerbated against unintended victims, but presents the least desirable outcome

has detected a DDoS event beyond pre-set thresholds, the traffic is rerouted and isolated within a scrubbing centre, DDoS traffic is removed and legitimate traffic is forwarded back on to the original destination. In this scenario the affected IP address can be back up and running in about 30 minutes.

However, in today's perennially connected digital age, 30 minutes of downtime for any organisation can cost thousands, if not millions, of dollars in revenue generation. Reputations can be damaged; headlines made and trust of the customer nullified. Scrubbing centres are a reasonably reactive means of managing DDoS attacks, and require hands-on analysis by infosec professionals, expensive in both time and resources.

By extension, recent advances in automation and proactive DDoS mitigation have the potential to pose a financial and resource optimisation proposition for service providers. Legacy DDoS prevention systems have generally been costly in nature due to the high volumes of traffic being passed through DDoS scrubbing centres; and are traditionally intended for large telcos dealing with high-volume traffic flows. Additionally, DDoS detection mechanisms rely on coarse sampling techniques that can result in less responsiveness to lower threshold levels of DDoS-generated traffic, meaning some attacks have the potential to go unnoticed for longer periods of time.

It stands to reason that the next generation of DDoS mitigation techniques will likely take the shape of automated threat detection and mitigation.

As networks become more sophisticated and intelligent, it stands to reason that emerging DDoS mitigation techniques are taking the shape of automated threat detection and mitigation, distributed across the network and capable of identifying and managing potential attacks before they cause disruption to the customer.

SPONSOR'S COMMENT

Corero Network Security believes that the modern threat of DDoS requires an equally modern approach to address the problem. Telcos and their enterprise customers require DDoS solutions with increased scale and effectiveness in order to meet the escalating challenge posed by perpetrators of DDoS attacks. Moreover, they require solutions that are economically viable in terms of acquisition and operating costs and that can potentially create new forms of services revenue to justify their deployment.

To that end Corero has developed the SmartWall® Threat Defense System (TDS), a highly distributed system of automated DDoS detection and mitigation engines that delivers always-on, line-rate DDoS defense within a highly disruptive economic model that can deliver full telco edge protection at a similar price point to traditional scrubbing centre technologies.

The Corero SmartWall Network Threat Defense Appliance provides First Line of Defense® protection against DDoS attacks and cyber threats. It delivers the industry's highest performance in a compact, energy efficient form factor for scalability in 10Gbps to 1Tbps in a single rack (1Gbps capabilities also available).

DDoS attacks against Internet-facing online services can cripple operations, impact customers, overwhelm security services and result in major economic losses. The SmartWall TDS is an intelligent, always on platform that inspects traffic, detects threats and blocks attacks against protected network resources. It allows Telecommunication, Internet Service Providers, Hosting Providers, and Managed Security Service Providers (MSSPs) to deploy centralized or distributed threat defense solutions on behalf of their customers via purpose-built network security appliances that provide advanced Layer 3-7 cyber threat protection.

The SmartWall Network Threat Defense Appliance provides continuous visibility and security policy enforcement so that organizations can establish a proactive First Line of Defense for inspecting traffic, detecting threats and blocking attacks. It is capable of mitigating a wide range of DDoS attacks (including volumetric, multi-vector, layers 3-7, etc.) while maintaining full service connectivity and availability to avoid degrading the delivery of legitimate traffic. In addition, Providers can leverage scale-as-you-grow deployments of SmartWall TDS to create incremental service revenue streams by offering high-value DDoS threat protection services to their enterprise or hosted customers.

Dave Larson, CTO, Corero Network Security

About Corero

Corero Network Security, an organization's First Line of Defense® against DDoS attacks, is a pioneer in global network security. Corero products and services provide Online Enterprises, Service Providers, Hosting Providers and Managed Security Service Providers with an additional layer of security capable of inspecting Internet traffic and enforcing real-time access and monitoring policies designed to match the needs of the protected business. Corero technology enhances any defense-in-depth security architecture with a scalable, flexible and responsive defense against DDoS attacks and cyber threats before they reach the targeted IT infrastructure allowing online services to perform as intended.
For more information, visit www.corero.com