NETSCOUT

| WHITE PAPER |

There is No Peacetime from Advanced DDoS Attacks

SECURITY

Distributed Denial of Service (DDoS) attacks used to be more episodic and Availability protection was typically given a lower priority when compared to the Confidentiality and Integrity sides of the Information Security CIA Triad. The DDoS threat was thought to be significant only for specific organizations, such as big banks, gaming vendors, ISPs, Cloud and SaaS companies, those whose very existence would be threatened by successful denial of services.

Well the world has changed. As business operations move online, the industries targeted, as well as the size, frequency and sophistication of DDoS attacks have increased commensurately. There is no longer any peacetime from DDoS attacks. Also greater: the financial risk of unavailable services, or worse, the compromise of sensitive data. Any business that is connected through networks to its customers, partners, supply-chain or employees – and that is EVERY business – is at risk from advanced DDoS attacks.

Any business that is connected through networks to its customers, partners, supply-chain or employees – and that is EVERY business – is at risk from advanced DDoS attacks.

Did You Know

- Average DDoS attack sizes are now above 1Gbps, a key threshold in that *an average attack can saturate the Internet connectivity of many enterprises*[1].
- Low and slow, harder to detect application-layer attacks *increased from 25 percent to 32 percent in 2017*[1].
- *48 percent of the enterprises observed a multi-vector DDoS attack;* up from 40 percent the previous year[1].
- Stateful security devices such as Next Generation firewalls, IPS devices and load balancers *are susceptible to state-exhaustion attacks.* NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report (WISR) found that *52 percent of enterprise respondents had firewalls that experienced a failure or contributed to an outage during a DDoS attack*[1].
- It has become *absurdly easy to launch effective attacks*. Recent DDoS attacks that impacted major Dutch banks Rabobank, ING, and ABN Ambro appear to have been launched by a teenager who bought a ready-made "boot stresser" DDoS package on the dark web". He paid €50 a week to send 50-100 Gb/s of attack traffic to his targets[2].

48 percent of the enterprises observed a multi-vector DDoS attack; up from 40 percent the previous year.

Business relies on a complex, growing web of data and application services. A more inter-connected business also presents more threat surfaces. A DDoS attack targeting an organization's Internet facing infrastructure can impact their ability to reach their customers, and their ability to transact business. Equally damaging can be an attack against a third-party's infrastructure if it supports, directly or indirectly, critical business services. For example. In October 2016, DNS service provide DYN was that target of a DDoS attack. The intended victim(s) of the attacks was not DYN, but rather the many key Internet brands that relied upon DYN's DNS services to maintain the availability of their services.

[1] NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report.

[2] Teenager suspected of crippling Dutch banks with DDoS attacks Tijs Hofmann, Feb 2018

What's New with Advanced DDoS

In reality, DDoS is now weaponized. Bad actors can launch multiple, coordinated attack vectors at the same target at the same time - at the push of a button. As you read this sentence attacks are happening around the world to all types of organizations, some looking to saturate connectivity, some looking to cripple or disable specific target applications. In today's connected economies, you are as vulnerable as the 'weakest link' in your extended network. And remember, recovery takes longer than just bringing targeted systems back online.

According to NETSCOUT Arbor's August 2018 Threat Intelligence report, DDoS campaigns now involve hundreds of thousands–even millions–of victims who are used to amplify the attack, or end up as collateral damage. Just two examples of the size and sophistication of advanced DDoS attacks:

- Reflection/amplification attacks based on Simple Service Discovery Protocol (SSDP) have been used since 2015. Yet in 2018 the NETSCOUT Arbor team uncovered a new class of SSDP abuse where naïve devices respond to SSDP attacks with a nonstandard port. The resulting flood of UDP packets uses fleeting source and destination ports–known as SSDP diffraction. Mitigating SSDP diffraction requires inspecting packet content, something traditional, cloud-only based DDoS protection service may not offer.
- Vulnerabilities in misconfigured Memcached servers open to the Internet can be used to launch enormous DDoS attacks. Indeed, NETSCOUT Arbor confirmed a 1.7 Tbps reflection/amplification attack exploiting Memcached servers on March 5th, 2018, a record event.

The new tactics, techniques and procedures (TTPs) of DDoS now rivals that of Advanced Persistent Attacks (APT). Advanced DDoS botnets can be directed in real-time with inbound and outbound control communications. In fact, DDoS attacks have become a core component of many orchestrated campaigns attempting to steal data and/or extort payment. Targeted DDoS attacks can disrupt call center operations or ecommerce processes and then extort bitcoin. Even the threat of a disruption, timed around a product launch, major marketing initiative, or merger/acquisition can serve as a powerful extortion tool.

Advanced DDoS attacks are cheap to deploy and can be launched by virtually anyone with the click of a button. There are malware downloaders for sale, e.g. Kardon Loader, which offers the ability to tweak the bot, making it harder to detect. And it is not just hactivists. Nation States and crimeware organizations now include DDoS attacks as part of their TTPs and use them in coordination with other attack vectors during well-orchestrated attack campaigns. For example, Hidden Cobra is a North Korean APT group that actively targets corporations, with a heavy emphasis on financials. Hidden Cobra's TTPs include DDoS botnets, keyloggers, remote access Trojans (RATs), and wiper malware – just to name a few.

As you read this sentence attacks are happening around the world to all types of organizations, some looking to saturate connectivity, some looking to cripple or disable specific target applications. In today's connected economies, you are as vulnerable as the 'weakest link' in your extended network.

Nation States and crimeware organizations now include DDoS attacks as part of their TTPs and use them in coordination with other attack vectors during well-orchestrated attack campaigns..

The Role of IoT Botnets

Billions of connected Internet of Things (IoT) devices present a tremendous opportunity for DDoS attackers because they:

- are usually always on and connected at high-speed;
- typically contain hard coded or default credentials;
- are susceptible to buffer overflows;
- contain little or no built in monitoring or security.

Corralled together by botnet malware compromised IoT devices can quickly drive significant volumes of traffic, use different protocols, propagate automatically, and be controlled remotely. One example is the Mirai malware used in the attacks on Dyn. The original Mirai malware code was published in 2016, and NETSCOUT Arbor has seen modified versions of Mirai wreaking havoc ever since. Variants include:

- Satori leveraged remote code execution (RCE) exploits to enhance the Mirai code;
- JENX removed several features from the code and instead relies on external tools for scanning and exploitation;
- Wicked targets Netgear routers and CCTV-DVR devices that are vulnerable to specific RCE flaws.

Another variant, OMG, adds an HTTP and SOCKS proxy. Depending on how the device is connected, the bot author can scan and pivot to internal, private networks connected to the infected IoT device. Internal devices can then be used to launch attacks from within. This is a fundamental change and shifts the way we need to think about DDoS detection and defense – specifically intercepting command and control (C2) communications leaving an organization.

The point is the sophistication of DDoS attacks is on the rise. Unfortunately, DDoS attack protection, when compared to other forms of cyber protection, is often neglected.

The original Mirai malware source code was published in 2016, and NETSCOUT Arbor has seen modified variants of Mirai such as Satori, JENX, Wicked and OMG, wreaking havoc ever since.

The Importance of Contextual Threat Intelligence

For security practitioners inundated by alerts, false positives and false negatives, spotting the real threat is a constant challenge. Adding context to an Indicator of Compromise (IoC) allows security professionals to better prioritize their efforts. Context can include recent activity, likely targets and relevant TTPs. Armed with this data security professionals can more quickly answer critical questions such as:

- Is this IoC unique to my organization or is this something my industry peers or organizations within this region are experiencing now?
- What threat actor is this IoC attributed to? And what TTPs are they known for?
- How have those TTPs been used during various stages of an attack?
- What data from the contextual threat intelligence can I use to proactively hunt for signs of breach?

As the lines between DDoS and other cyber threats start to converge, the value of contextual threat intelligence grows. Because organizations face more threats than just DDoS attacks, advanced DDoS attack security tools must protect them from more than just DDoS attacks. Because of the close interrelationship between DDoS attacks and other advanced threats, advanced DDoS attack protection solutions should offer more contextual intelligence for threats they detect.

Contextual intelligence can provide specific data to look for, e.g. IP addresses used for C2. A broader context can help identify how this threat is likely to try and compromise your infrastructure. For example, what vulnerabilities it may try to exploit or what protocols it may use to communicate. The better threat intelligence can even suggest steps for detection.

Advanced DDoS Requires Updated DDoS Defense

The potential impact from advanced DDoS attacks has become far more consequential. Best practices in DDoS protection already calls for layered on-premise and upstream, service provider components.

- On-premise protection to automatically detect and mitigate the more stealthy, application layer attacks targeting business services, and the TCP-state exhaustion attacks targeting stateful devices such as Next Generation firewalls (NGFW), IPS and load balancers;
- Stateless protection deployed at the very edge of the network – before stateful firewall, IPS and load balance devices; which will protect them from DDoS attacks.
- Upstream protection from your internet service provider or MSSP to stop large volumetric attacks, before they overwhelm local Internet connectivity;
- The ability for on-premise components to intelligently and automatically re-route traffic to your internet service provider's cloud-based mitigation or your MSSP.

But protection from advanced DDoS requires more. Advanced DDoS protection requires quick identification and blocking of inbound and outbound communications that may indicate risk from internal DDoS, or from another form of advanced DDoS botnet. Reputational threat intelligence (IP addresses, domains and URLs), is just the baseline. Contextual threat intelligence has become critically important for quickly, and more efficiently detecting and mitigating advanced DDoS attacks that are increasingly being used as vectors in well-coordinated attack campaigns against an organization.

Advanced DDoS protection requires quick identification and blocking of inbound and outbound communications that may indicate risk from internal DDoS, or from another form of advanced DDoS botnet.

Advanced DDoS represents more risk to the organization. Therefore DDoS protection solutions must do more than just stop DDoS attacks – Advanced DDoS attack protection solutions must contribute to the larger security posture. Advanced DDoS attack protection should be:

- Backed by continuous, highly curated contextual threat intelligence that provides insights on more than just DDoS attacks.
- Automated, using combinations of rate-based, behavioral and intelligence based mechanisms.
- Easily integrated into the existing security stack by supporting standards such as STIX, TAXI and REST APIs.
- SDN/NFV ready with available integrations into tools such as OpenStack, Heat, Tacker, Ansible, Nokia Cloudband, Cisco NSO, and other ONAP or ETSI NFV management and orchestration technologies.

Advanced DDoS represents more risk to the organization. Therefore DDoS protection solutions must do more than just stop DDoS attacks – Advanced DDoS attack protection solutions must contribute to the larger security posture.

The reality is there is no longer any peacetime from advanced DDoS attacks. Have your DDoS attack defenses kept pace?

To find out how your DDoS protection compares to industry best practices take this online DDoS Attack Assessment Survey.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECWP_008_EN-1801 09/2018