Why DDoS Makes for Risky Business – And What You Can Do About It

Defending organization's networks against DDoS attacks and other threats has long been a daunting challenge–but now cybercriminals are making it even more so.

Consider the following facts:[1]

- The **size** of DDoS attacks is decreasing. In 2019, the largest reported DDoS attack was 622 Gbps, a 36% decrease in size over 2018. However, attacks between 100 Gbps and 200 Gbps increased 15% as adversaries learned to stay under the radar and avoid the unwanted attention of larger attacks.
- The **complexity** of DDoS attacks is increasing. The modern-day DDoS attack, more routinely being executed by IoT based botnets, is a dynamic combination of volumetric, TCP-state exhaustion and application layer attack vectors. Attackers are weaponing new and common UDP reflection/amplification attack vectors, combining new variations of well-known attack vectors, and making them stronger than the sum of their parts by combining TCP reflection/amplification attacks with carpet-bombing techniques.
- The **frequency** of DDoS attacks is also staggering. NETSCOUT® Arbor's ATLAS®, which tracks DDoS attacks on a worldwide basis, observed 8.4 million DDoS attacks in 2019, a 16 percent increase in attack frequency over past years. That equates to 23,014 attacks PER DAY, 959 attacks PER hour, and 16 attacks PER minute.
- Evidence also shows that DDoS attacks are not independent events, but closely related to or may be **part of complex advanced threat campaigns** against organizations and used as a diversionary tactic in multiple phases of the Kill Chain and extortion.

Yet even in today's dynamic threat landscape, many organizations still believe that a dedicated DDoS protection solution is not important–or that the one they adopted a few years ago still provides adequate protection from modern day DDoS attacks. In these instances, organizations are gambling with their network. It's time to debunk some outmoded misconceptions about DDoS.

5 Common Misconceptions About DDoS Protection

Let's take a look at five common mistakes organizations make when addressing DDoS and shed some light on these failed practices.

Misconception #1: Firewalls, IPS or Content Delivery Networks Are the Answer

The evolution of IT infrastructures and the dependency on third-party clouds have created a complex environment that no longer has a perimeter. Traditional "perimeter" security solutions such as firewalls and IDS/IPS are still vital parts of an integrated security posture. However, because these devices conduct stateful inspection of network connections, they are susceptible to some DDoS attacks which can make matters worse. According to NETSCOUT's 14th Annual Worldwide Security Report, TCP-state exhaustion attacks now make up 31% of all DDoS attacks - that's two times more than the prior year. Impact of these attacks are evident as 54% of firewalls or IPS fail as a result of a DDoS attack.[2]

5 COMMON MISCONCEPTIONS

1. Firewalls, IPS or CDNs can stop all DDoS attacks.
2. A single layer of DDoS protection is enough.
3. The odds are we will not become a target, so it's worth the risk.
4. The impact of a DDoS attack does not justify the cost for protection.
5. DDoS attacks are not advanced threats.

[1] NETSCOUT Arbor's 14th Annual Worldwide Infrastructure Security Report (2019).

[2] Ibid

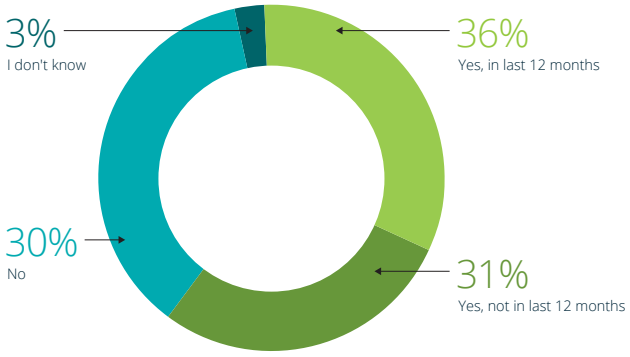

Figure 1: Multi Vector DDoS Attacks.
Source: NETSCOUT 14th Annual Worldwide Security Report (2019)

And the best place to stop stealthy application-layer attacks is on the customer premises, closer to where key applications or services reside.

Many organizations also erroneously believe that Content Delivery Networks provide a solution to stopping DDoS attacks. The truth is that a CDN merely addresses the symptoms of a DDoS attack. By absorbing these large volumes of data, a CDN actually lets all the information into and through the network—providing an "all are welcome" approach. In addition, most CDN based DDoS protection solutions only focus on absorbing HTTP/HTTPS DDoS attacks ignoring all others such as NTP/DNS amplification attacks which are very common.

Misconception #2: A Single Layer of DDoS Protection is Enough

Because modern day DDoS attacks use a dynamic combination of volumetric, TCP state exhaustion and application-layer attack vectors industry best practices recommend that organizations take a layered approach to protection. That is, the best place to stop large flooding attacks is upstream in a service provider's cloud before they overwhelm local internet connectivity or on-premises DDoS protection systems. And the best place to stop stealthy application-layer attacks is on the customer premises, closer to where key applications or services reside. Just as importantly, you must have an intelligent form of communication between these two layers backed by up-to date threat intelligence to stop dynamic, multi-vector DDoS attacks.

Unfortunately many organizations choose only a single layer of protection resulting in an incomplete DDoS protection solution.

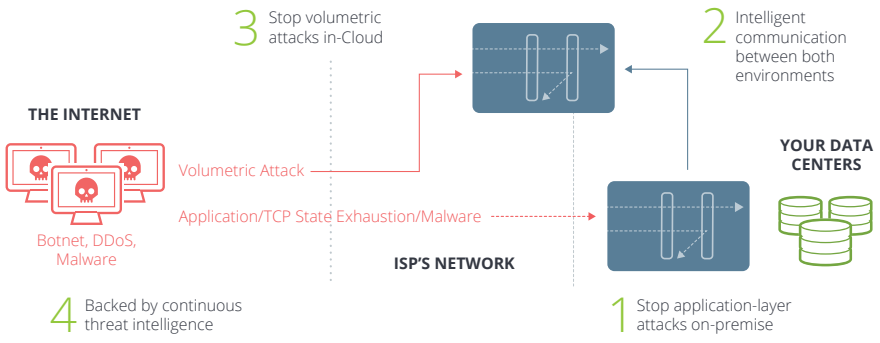

Figure 2: Layered DDoS Attack Protection.
Source: NETSCOUT

Misconception #3: The Odds Are We Will Not Become a Target, So It's Worth the Risk

Then dramatic rise in the number of DDoS attacks is due to two main factors.

1) Ease of launching an attack and 2) Multiple motivations behind attacks.[3] It's never been easier in history to launch a DDoS attack. Anyone can simply download a Do-It-Yourself DDoS attack tool for free or pay a small fee to third-party to conduct a DDoS attack as a service. And while the price for launching an attack is in the tens of dollars, the losses for organizations can be in the tens of millions. The motivations behind DDoS attacks are plenty. No longer are DDoS attacks motivated by financial gain or conducted by state sponsored organizations.

Today, all it takes is for someone to simply disagree with your opinion, political affiliation or stance on a topic to launch a DDoS attack using the plethora of tools or services available to them. To make matters worse, if your services are housed in a shared cloud environment, you don't even have to be the target of the DDoS attack to be impacted by the collateral damage. So you have to ask yourself, "Do I feel lucky?"

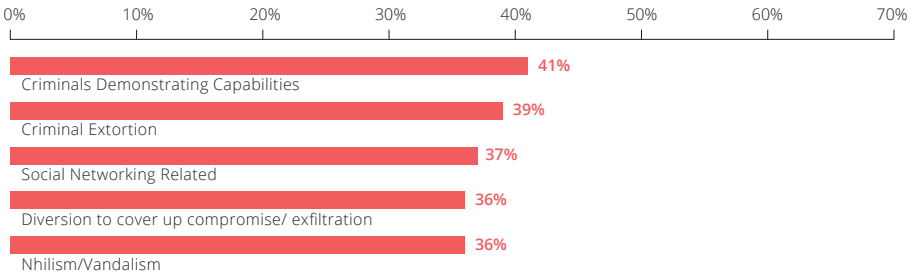

Figure 3: Top 5 DDoS attack motivations.
Source: NETSCOUT 14th Annual Worldwide Security Report (2019)

Misconception #4: The Impact of a DDoS Attack Does Not Justify the Cost for Protection

The impact of a DDoS attack can be immediate and severe. The fact is that many organizations do not conduct the proper risk and countermeasure analysis to help justify the purchase of a comprehensive DDoS protection solution. Sure, calculating the cost of downtime for a revenue generating service may be a no brainer; but have you consider all the other costs that are associated with a DDoS attack?

According to Arbor, 39% of Enterprises cite Cost of specialized IT security remediation and investigation services as the number one impact of DDoS attacks.[4] But there are many other indirect costs that are routinely overlooked such as SLA credits, legal/regulatory fees, PR costs for brand repair, customer churn, increase in cyber insurance premiums, extortion etc. There are even documented cases where executive or board members have been fired due to their organizations not being adequately prepared to stop DDoS attacks and other threats.

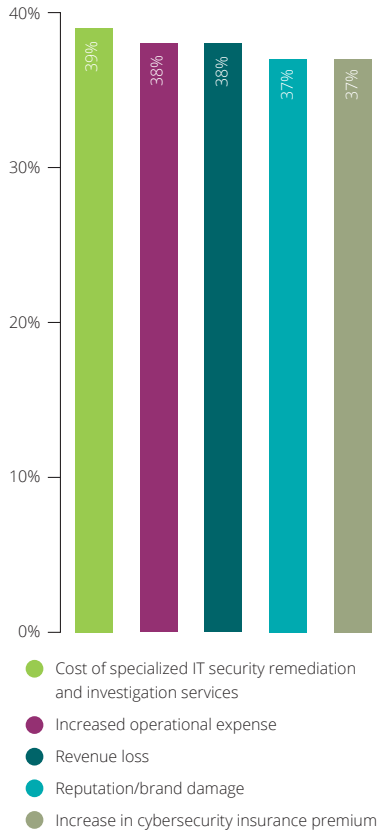

Figure 4: Top 5 Impact of DDoS Attacks
Source: NETSCOUT 14th Annual Worldwide Security Report (2019)

50%

reported the cost at $1000 to $10,000 per minute, up significantly from the previous year.[4]

[3] Arbor 14th Annual Worldwide Infrastructure Security Report (2019).

[4] Arbor 14th Annual Worldwide Infrastructure Security Report (2019).

Misconception #5: DDoS Attacks Are Not Advanced Threats

Gone are the days where a single bot offered a simplistic DDoS attack type. In today's DDoS threat landscape, attackers increasingly add diversification into their bots, allowing a wide variation of attacks and protocols to take down networks. NETSCOUT's ATLAS Security Engineering and Response Team's (ASERT) 18 years of global research into botnets and DDoS attacks has determined that they are very closely related to advanced threats such as malware, RATs, etc. In fact, they may all be used together in what's known as the Cyber Attack Kill Chain.

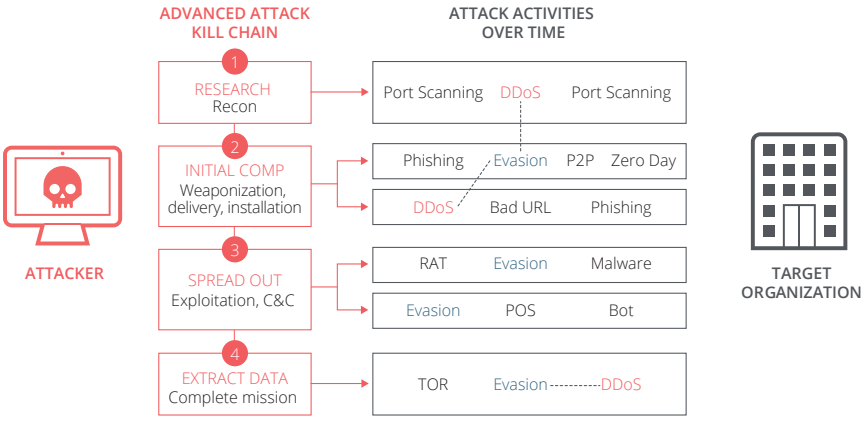

Figure 5: DDoS Used During Various Stage of Attack Kill Chain. Source: NETSCOUT

For example, there have been documented cases where DDoS attacks were used during:

- The early reconnaissance stage to test an organization's ability to respond to a DDoS attack which will be used as a diversionary tactic later in the kill chain.
- The weaponization or malware delivery stage, where they were used to fill security forensic product log and data files; making the search for the planted malware much more challenging.
- The data extraction stage where the attacks where used as a diversionary tactic. According to Arbor's last Worldwide Infrastructure Security Report, respondents cited "Diversion to cover compromise/data exfiltration" to be the motivation behind DDoS attacks.

According to NETCOUT's Threat Intelligence Report Advanced Persistent Threat (APT) groups are increasingly adding DDoS attacks to their many Tools, Tactics and Procedures (TTPs). For example, Hidden Cobra is a North Korean APT group that actively targets corporations, with a heavy emphasis on financials. As shown by the graphic to the right they deploy a variety of TTPs including DDoS attacks that are used to take out services and serve as a diversionary tactic during well-orchestrated attack campaigns.

Botnets themselves are becoming multi-use. The Emotet botnet for example is used for multiple purposes. Research has shown the C&C server is responsible for sending modules used for SPAM, Network Worms, Mail and Browser Password Viewing, and malware that can add the infected machine to a botnet to carry out DDoS attacks.

The reality is the line between DDoS attacks and other forms of cyber threats is starting to blur.

36%

of Enterprises cite "diversion to cover compromise/data exfiltration" to be the motivation behind DDoS attacks, according to Arbor.

HIDDEN COBRA APT

Country of Origin
North Korea

Primary Targets
Financial Institutions primarily in South Korea and U.S.

Known Techniques
DDoS Botnet, Disabling Security Products, Brute Force Lateral Movement, SMTP Data Exfiltration, Bootkit, Access Token Manipulation, remote Access Trojan, Keylogger, Destructive Malware, Custom C2 Protocol, Timestomping, Persistent Shortcuts

As the lines between DDoS attacks and other forms of cyber-attacks blur, organizations need cyber threat protection solutions that stop all types of inbound threats and intercept outbound communication to C2 from compromised internal devices.

It's Time for an Intelligent, Multi-Layered Approach to DDoS Protection That Can Do More Than Just Stop DDoS Attacks

As the lines between DDoS attacks and other forms of cyber-attacks blur, organizations need cyber threat protection solutions that can do more than just stop specific types of attacks. These solutions need to be able to detect and stop all types of inbound threats (i.e. DDoS attacks, malware, etc.) and intercept outbound communication from compromised internal devices to command and control infrastructure.

NETSCOUT offers such a comprehensive solution. Our solution is a fully managed, intelligently automated, combination of on-premise and in-cloud DDoS attack protection; continuously backed by global threat intelligence, making it capable of stopping threats beyond DDoS.

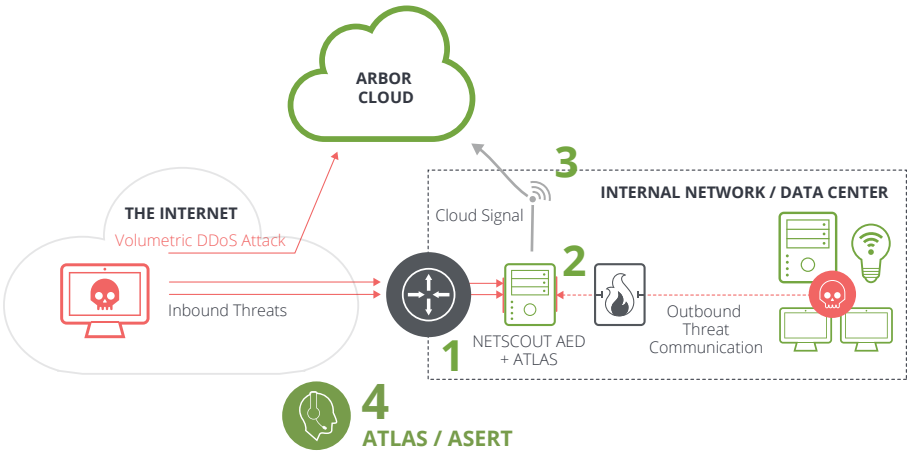

Figure 6: Arbor's DDos Protection Solution.
Source: NETSCOUT

1. On the premise, the NETSCOUT Arbor Edge Defense (AED) product is an in-line, always on product that can automatically detect and stop all types of DDoS attacks.
2. Armed with reputation-based threat intelligence from Arbor's ATLAS® Intelligence Feed and or 3rd party threat intelligence, and using stateless packet processing technology, NETSCOUT AED can also detect and block inbound IoCs AND outbound communication from compromised internal devices.
3. In the event of a large volumetric DDoS attack, NETSCOUT AED's Cloud Signaling will intelligently route attack traffic to an appropriate Arbor Cloud scrubbing center. Arbor Cloud is a 24x7, fully managed DDoS attack protection service offering over 14Tbps of mitigation capacity via 12 worldwide scrubbing centers.
4. During and post attack, a comprehensive set of reports are automatically generated detailing all attack activity. For blocked IoCs, additional Contextual Threat Intelligence is provided, enabling cybersecurity teams to determine risk and hunt using their arsenal of other security tools.

So as the lines between DDoS attacks and other forms of cyber-attacks blur, organizations can rely upon NETSCOUT's solutions to help protect themselves. To learn more about NETSCOUT's solutions visit: https://www.netscout.com/products/netscout-aed

KEY FEATURES & BENEFITS

First Line of Defense
Deployed at the network perimeter, using stateless technology and armed with millions of IoCs, AED detects and blocks inbound cyber threats at internet scale, thus taking pressure off of stateful devices such as Next Gen Firewalls.

Last Line of Defense
AED can detect and block outbound communication to hacker command and control (C2), domains and URLs; thus helping stop the further proliferation of malware with an organization and avoid a data breach.

Contextual Threat Intelligence
AED leverages the global threat intelligence of NETSCOUT ATLAS to provide more context related to blocked IOCs, thus helping security teams determine risk and/or hunt using their other tools.

Best of Breed Hybrid DDoS Protection
AED can automatically detect and stop inbound application layer, TCP-state exhaustion and DDoS attacks as large as 40 Gbps. In the event of even larger DDoS attacks, Cloud Signaling automatically reroutes traffic to Arbor Cloud or a MSSP's cloud-based mitigation center.

Integration with Security Stack
AED's robust REST API, support for CEF and LEEF Syslog formats and STIX/TAXII enables AED to integrate with existing security technologies and processes.

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

SECSB_010_EN-2001 06/2020