A CxO's guide to network resilience

White paper

Understanding and mitigating impact of distributed denial of service (DDOS) attacks.

Designing a resilient network

Computer networks play a central role in business as more organizations are becoming fully digital and heavily-reliant on technology to carry out business tasks. Connecting users to applications from anywhere to anywhere is key for business success and depends upon reliable network connections. When it comes to concern about risk management, it is not only the CIO/CTO or CISO who are focused on network resilience but it is also the CFO and CIO (and other C-level leaders) who are sensitive to the reputational, financial, and legal risks associated with network failures. Network resilience is now a strategic corporate objective.

Network architecture and design patterns take into account many options for engineering a resilient network. These include, but are not limited to, multiple network connections, path diversity, Internet service provider diversity, and use of emerging technologies like software defined wide area networks (SD WAN). However, a sound network architecture and design are insufficient unless operational resilience and security monitoring are also incorporated into the overall strategy. This is where protection against Denial of Service (DOS) attacks—and mitigating their impact—becomes crucial.

Designing for network resilience is critical, given that Distributed Denial of Service (DDoS) attacks on networks are one of the largest sources of security incidents, according to Verizon's 2021 Data Breach Investigations Report (DBIR). The 2021 DBIR shows that incidents related to denial of services account for almost half of all of the 80,000+ security incidents examined for the report. The following diagram shows the trend of DDoS incidents pattern as a percentage of all security incident data (depicted by the rising blue line).[1]

DDoS attacks, by definition, severely impact network availability and impede access to critical business applications. Also, they are highly unpredictable and unevenly distributed. These factors make DDoS resilience design challenging.

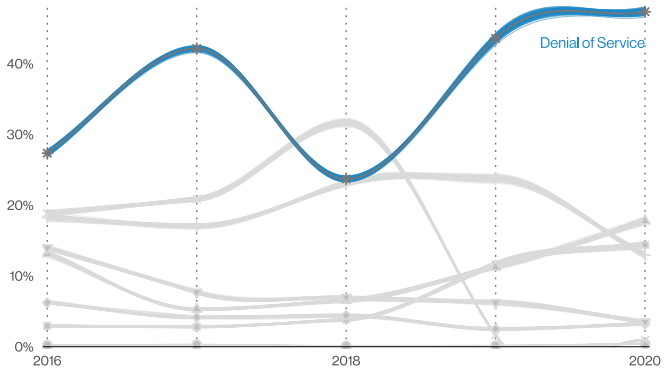

Figure 50. Patterns over time in incidents

What is a DDoS Attack?

In general, the term Denial of Service is used to describe an attack where availability of a system, network or application is impacted in such a way that legitimate users are not able to use the service. Denial of service attacks come in a variety of forms and characteristics. Understanding these attacks can help better identify which ones merit risk mitigation for a particular business as well as account for respective risk prioritization. Some common denial of services attacks are listed below:

- **Network DDoS Attacks** – A distributed denial of service attack, or commonly known as a network DDoS attack, is characterized by attackers using a large number of compromised hosts on the public Internet to send large volumes of data to a network, crippling and blocking legitimate network traffic.[2]
- **DDoS Amplification Attacks** – These are special types of DDoS attacks where an attacker sends a large number of requests to a public Internet service such as Domain Name Servers (DNS) that appear to be coming from the victim IP addresses (through a technique known as IP address spoofing). These requests result in even much larger response data going to the victim's network, amplifying the network traffic volume.

verizon

- **Telephony Denial of Service (TDoS) Attacks** – A TDoS attack targets telephony services and systems and could result from a flood of malicious inbound calls blocking legitimate callers from connecting. These attacks could be automated or in some cases launched by tricking large numbers of people using social media to call specific numbers.
- **Application Denial of Service Attacks** – In some cases attackers can exploit an application vulnerability to crash it (make it unavailable) by sending specific data packets. These attacks don't need a large volume of network traffic compared to network DDoS attacks.

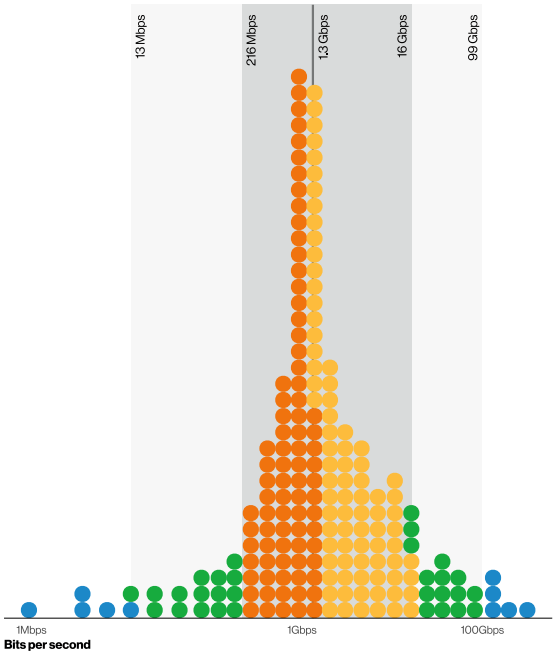

Figure 51. Bits per second in DDoS Incidents (n=11,306)
Each dot represents 0.5% of organizations

Regardless of which type of denial of service attack it is, thoughtful planning for network, systems and applications availability is necessary in the digital organization. For the purpose of this white paper, however, the focus here and forward will be solely on volumetric network DDoS attacks. While Network DDoS attacks loom large in the 2021 Verizon DBIR, it is one of the easiest threats to mitigate effectively. In fact, 95 percent of DDoS incidents in the new DBIR fell between 13 Mbps and 99 Gbps (as shown in the diagram[3]), which is a range that can be easily mitigated with a robust DDoS mitigation service.

DDoS Mitigation is all about network resilience.

Networks need to function without interruption, and protection against DDoS attacks encompasses three steps:

Planning – A number of recommendations are provided in this white paper for planning to get ready for handling DDoS attacks. Planning starts with a good network design, incident preparedness, response planning and others.

Detection – Early detection of attacks can drastically reduce the response time and save services from unavailability issues.

Remediation – Depending upon the type of denial of service attacks, remediation strategy may include DDoS mitigation services.

DDoS Business Impact is more than just network and applications issues.

The impact of DDoS attacks goes well beyond the network and applications availability issues. Some of the areas you should consider while making an assessment include:

- Reputational and brand impact.
- Operational issues in serving customers.
- Financial losses, such as resulting from unavailability of ecommerce or banking/trading applications.
- Missing service level agreements.

It is common to find organizations impacted by DDoS attacks in more than one of these ways, and failure to understand these possible impacts can exacerbate the stress experienced by incident response teams during an attack.

Network Resilience Assessment

A periodic assessment of network resilience against DDoS attacks will help keep incident response plans updated and strong. At a minimum, it is beneficial to perform periodic tabletop exercises to simulate an attack, to identify gaps in the response plan, and to improve the overall incident management process. As part of network resilience planning, be sure to:

- Perform a business impact analysis (BIA) including applications, SaaS services, and other systems that require availability of the Internet.
- Refine business continuity plans based upon the results of the BIA.
- Test your plans on a periodic basis.

A typical network resilience testing assessment should include collaboration among network, security, applications and other infrastructure teams who are responsible for systems dependent on Internet access.

Recommendations for CxO

To answer the question, "What can we do to be ready for effectively handling and responding to DDoS attacks?" we suggest C-level leaders support the following activities:

1. **Inventory all internet connections** – Create a list of all ISPs (Verizon or others), the business purposes they serve, and validate their necessity.
2. **Map business functions to all internet connections** – Identify critical connections for operating business (keeps the lights ON).
3. **Define War and Peace Situations** – Document what the normal network operations looks like and course of action when it does not. This will help you create an incident response plan.
4. **Perform annual tabletop exercise** – An incident response plan has no value and is a piece of paper until it is tested and updated on a regular basis. Tabletop exercises are common to test incident response plans. As part of the tabletop exercise, you can create a hypothetical scenario of a DDoS attack on one or more critical Internet connections and understand how different teams will react to such an attack.
5. **Define countermeasures** – Create action items to minimize the impact of DDoS attacks on critical Internet connections.
6. **Create a RACI model** – RACI (Responsible, Accountable, Consulted, Informed) is a common model to clearly define the role of all internal and external stakeholders, including the ISP, in detection and mitigation of DDoS attacks. This helps in ensuring all parties understand their roles and responsibilities.
7. **Define criteria for selecting ddos mitigation service** – When selecting a DDoS mitigation service, you should consider the following important features:
   - **Highly scalable** – A DDoS mitigation service should be able to defend against even the largest recorded DDoS traffic volumes.
   - **Carrier-agnostic** – The service should be able to protect all of your traffic regardless of carrier or ISP.
   - **24x7x365 support** – DDoS attacks don't necessarily happen during office hours and the service should be able to provide round-the-clock support when need arises.

Conclusions

With increasing Cloud and SaaS services adoption, reliance on the availability of the Internet has increased. At the same time, data shows that DDoS attacks are increasing. A comprehensive network resilience plan is needed that includes a strategy of dealing with DDoS attacks. Many organizations find themselves in a situation where they are under DDoS attacks and don't have robust plans and preparations to effectively mitigate its impact. Understanding the DDoS attacks, their impact on business, and properly planning for these is key to keep your business functioning and avoid outages that could span many days. Recommendations shared in this white paper are critical to achieving better network resilience.

The Verizon solution: DDoS Shield

Business growth means more connected devices to your network, and more bandwidth to accommodate users. It also opens the door to increased risk, where attackers move in with sophisticated distributed denial-of-service (DDoS) attacks. At Verizon, we understand DDoS attacks, having analyzed many of them in our 2021 Data Breach Investigations Report (DBIR). Verizon DDoS Shield is a cloud-based DDoS mitigation service that can tackle today's most advanced threats. This DDoS prevention solution can help lift the burden off your team by giving you the intelligence to help distinguish good traffic from bad traffic, and the capacity you need to combat large volume attacks. DDoS Shield offers a highly-scalable attack mitigation service that helps you tackle today's sophisticated and high volume DDoS attacks. It works across your enterprise environment to alleviate the burden on your network and perimeter systems, and helps maintain continued availability to your customers.

For more information about DDoS Shield, visit https://www.verizon.com/business/products/security/network-cloud-security/ddos-shield/ or contact your Verizon Sales Representative.

verizon

1 Page 36, Figure 50 of Verizon 2021 Data Breach Investigations Report (DBIR)

2 Please watch a short Verizon video about how network based DDoS attacks work: https://www.youtube.com/watch?v=z7ltWcN3mqk.

3 Page 36, Figure 51 of Verizon 2021 Data Breach Investigations Report (DBIR).