KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks

microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/

March 17, 2023

In the last year, geopolitical tension has led to an uptick of reported cybercrime events fueled by hacktivist groups. The US Cybersecurity and Infrastructure Security Agency (CISA) published an advisory to warn organizations about these attacks and teamed with the FBI on a distributed denial-of-service (DDoS) response strategy guide. KillNet, a group that the US Department of Health and Human Services (DHHS) has called pro-Russia hacktivists, has been launching waves of attacks against western countries, targeting governments and companies with focus on the healthcare sector. DHHS published an analyst note on KillNet's threat to the health sector, mentioning that the group compromised a US healthcare organization that supports members of the US military.

KillNet uses DDoS as its main protest tool. DDoS attacks are a relatively easy and low-cost method of disrupting online services and websites and can be a powerful way to draw attention, making them a popular choice among hacktivist groups. In addition, DDoS attacks can be launched anonymously, which could make it difficult for authorities to track down perpetrators.

In this blog post, we provide an overview of the DDoS attack landscape against healthcare applications hosted in Azure over three months. We then list a couple of recent campaigns from KillNet, describe their attack patterns, and present how we mitigated and protected customers from these attacks. Finally, we outline best practices for organizations to protect their applications against DDoS attacks.

DDoS attacks against healthcare in Azure

We measured the number of attacks daily on healthcare organizations in Azure between November 18, 2022 and February 17, 2023. We observed an incline from 10-20 attacks in November to 40-60 attacks daily in February.

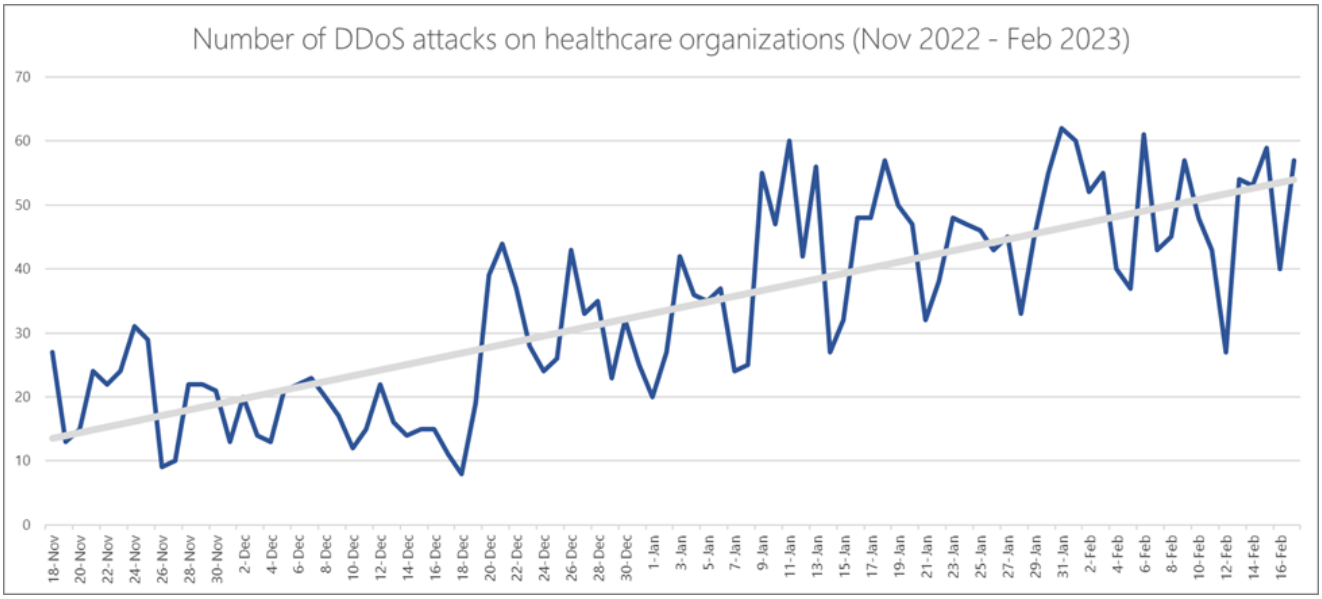

Figure 1. Number of daily DDoS attacks on healthcare applications in Azure

We tracked attack statistics through the same time period and observed that DDoS attacks on healthcare organizations didn't demonstrate severely high throughput. There were several attacks hitting 5M packets per second (pps), but majority of attacks were below 2M pps. These attacks, although not extremely high, could take down a website if not protected by a network security service like Azure DDoS Network Protection (see guidance at the end).

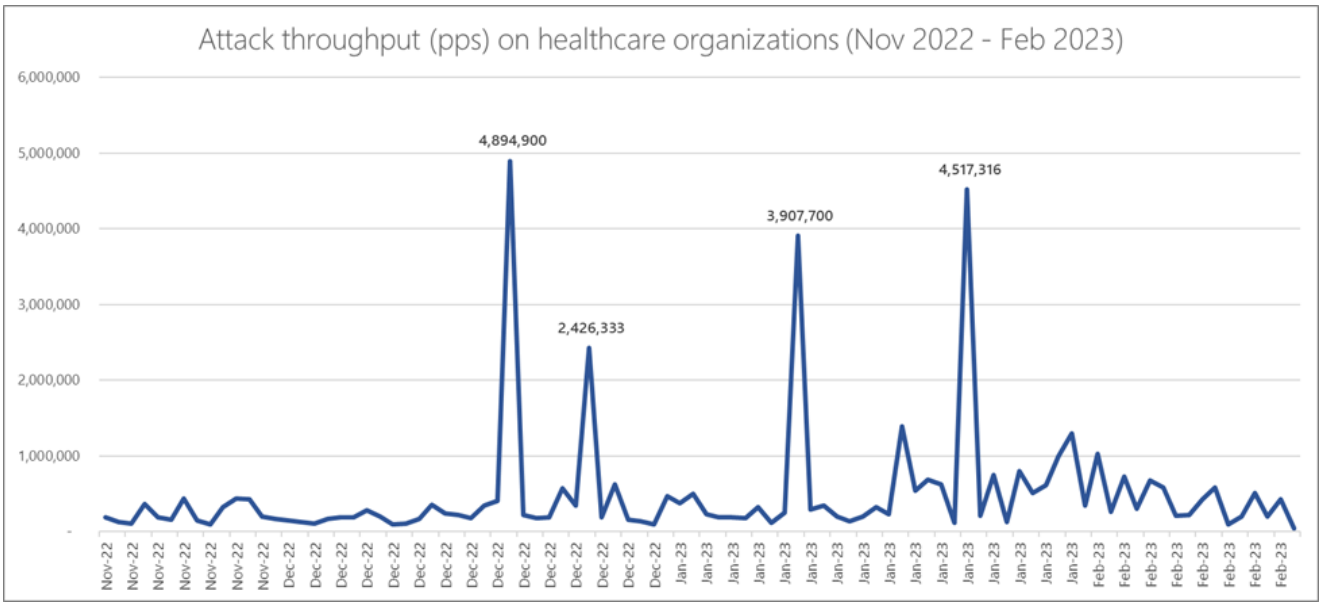

Figure 2. Attack throughput (pps) on healthcare organizations

The types of healthcare organizations attacked included pharma and life sciences with 31% of all attacks, hospitals with 26%, healthcare insurance with 16%, and health services and care also with 16%.

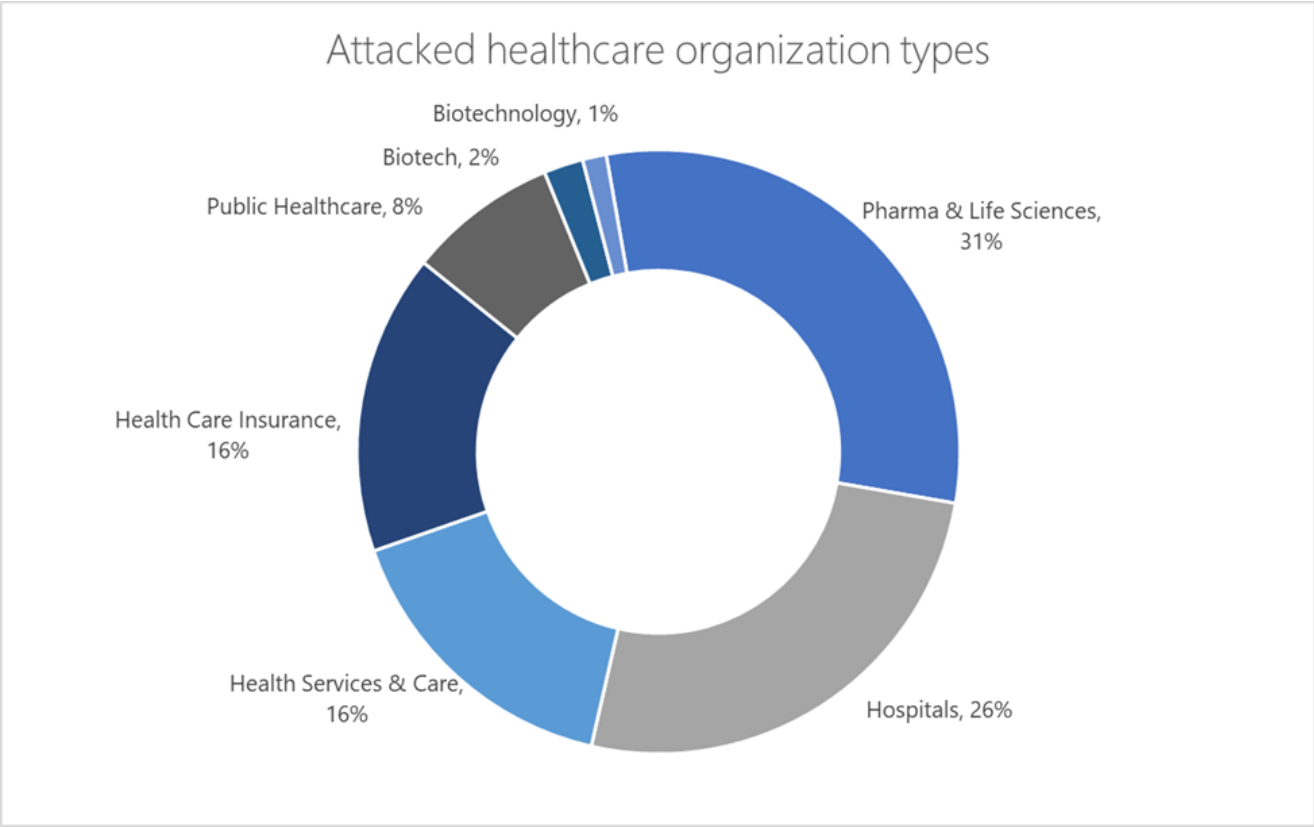

Figure 3. Types of healthcare organizations targeted by DDoS attacks

We also observed a combination of multi-vector layer 3, layer 4, and layer 7 DDoS attacks. Attacks are primarily targeting web applications, and intertwined TCP and UDP attack vectors. We observed layer 7 DDoS attacks consuming many TCP connections and keeping them alive long enough trying to deplete memory state resources to render the application unavailable. This is a repeated pattern noticed in several cases for attacks attributed to KillNet. Another common attack pattern tries to establish many new TCP connections over short intervals to hit CPU resources.

In contrast to overall DDoS attack trends for 2022, in which TCP was the most common attack vector, 53% of the attacks on healthcare were UDP floods, and TCP accounted for 44%, reflecting a different mixture of attack patterns used by adversaries on healthcare.

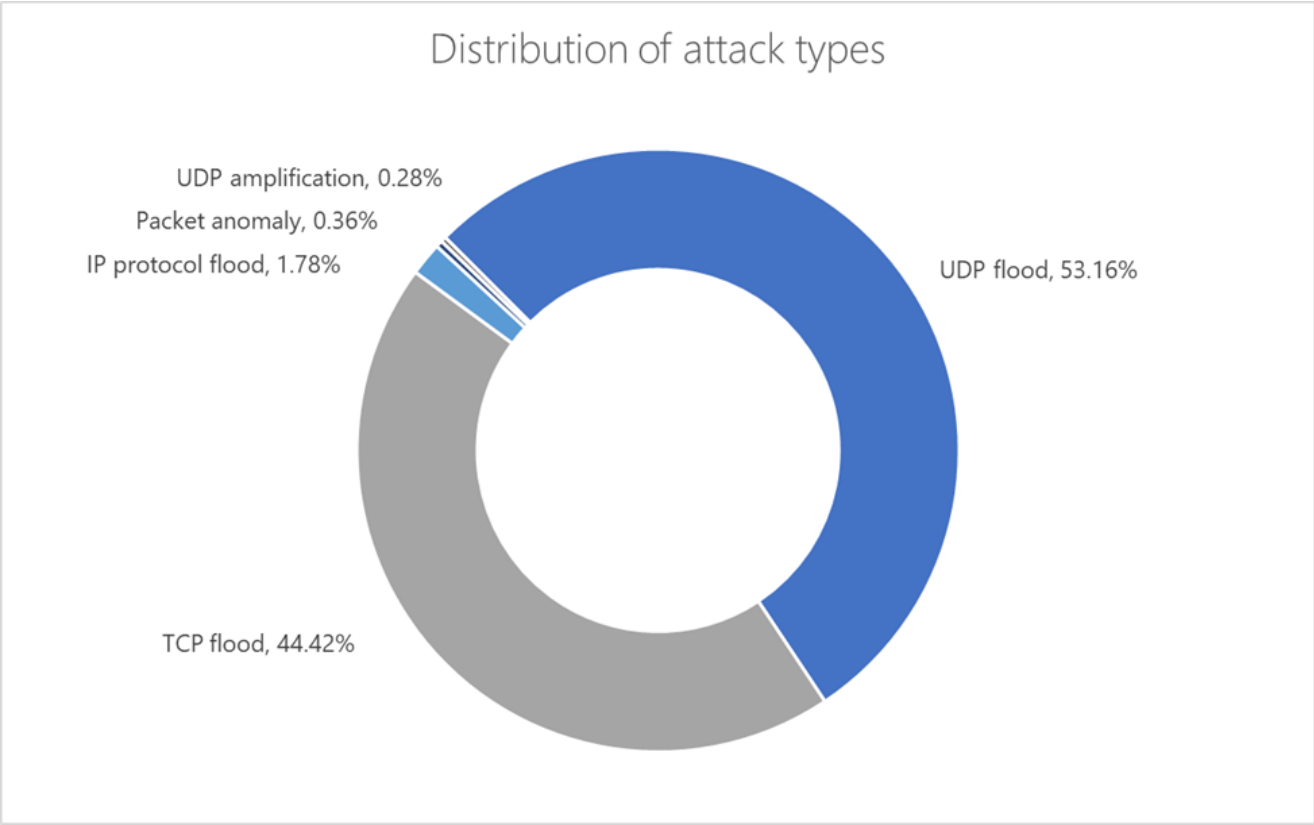

Figure 4. Distribution of DDoS attack types targeting healthcare

Out of the UDP attack vectors, 38% are UDP spoof flood attacks, followed by 29% of DNS amplification attacks. UDP reflected amplification attacks consumed 52% of all attacks. This is in line with other public reports on KillNet, where amplification and spoofed sources are used, among other attack vectors. Although majority of attacks are on web applications, adversaries used multi-vector UDP spoof and reflected amplification attacks alongside TCP attacks to saturate the network and impact the attacked application.

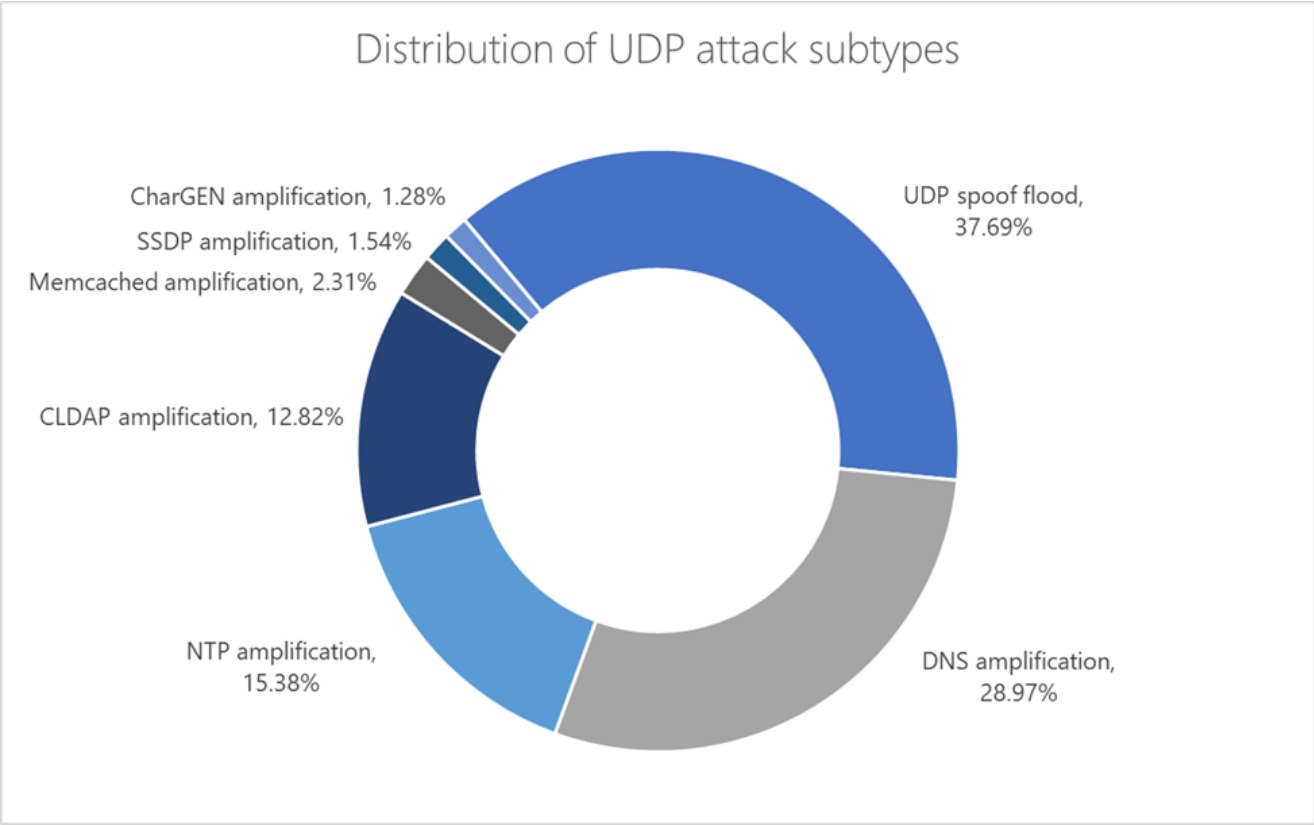

Figure 5. Distribution of UDP attacks on healthcare

Attack campaigns

In this section, we outline a couple of attack campaigns launched by KillNet or its affiliated hacktivist groups targeting customers in Azure. These attacks had no impact on Azure services and customers were protected by our Azure DDoS Network Protection service.

The first customer is a healthcare provider that was hit by a DDoS attack recently. The attack throughput wasn't very high, peaking at 1.3M pps. The organization protected its service with Azure DDoS Network Protection, and the attack was successfully mitigated. Such attack throughput demonstrates why it's crucial to protect applications against DDoS attacks. Similar attacks may target an application with low enough volumes that evade infrastructure-level DDoS protection, as they don't impose a risk to Azure services or to other customers but may still take down an application. With Azure DDoS Network Protection, we learn normal baseline patterns specific to an application and detect traffic anomalies effectively.

Attack vectors included TCP SYN, TCP ACK, and packet anomalies. The attack lasted less than 12 hours, and the adversary likely launched it using DDoS scripting tools, spoofing large numbers of source IP addresses.

Another attack targeted a multinational industrial company. The attack lasted several days and included layer 4 TCP SYN and ACK, as well as layer 7 HTTP request attacks on the company's website. It was launched from a botnet comprising 22,000 attack sources. The

attack volume was similarly not very high, hitting 250K pps, and each attack source sent a relatively small amount of HTTP traffic to the attacked website. Majority of the traffic pattern appeared as if it was legitimate client traffic. However, the number of connections created aimed to consume state and CPU resources.

The top three countries from which the adversary launched the botnet attack were the US, Russia, and Ukraine.

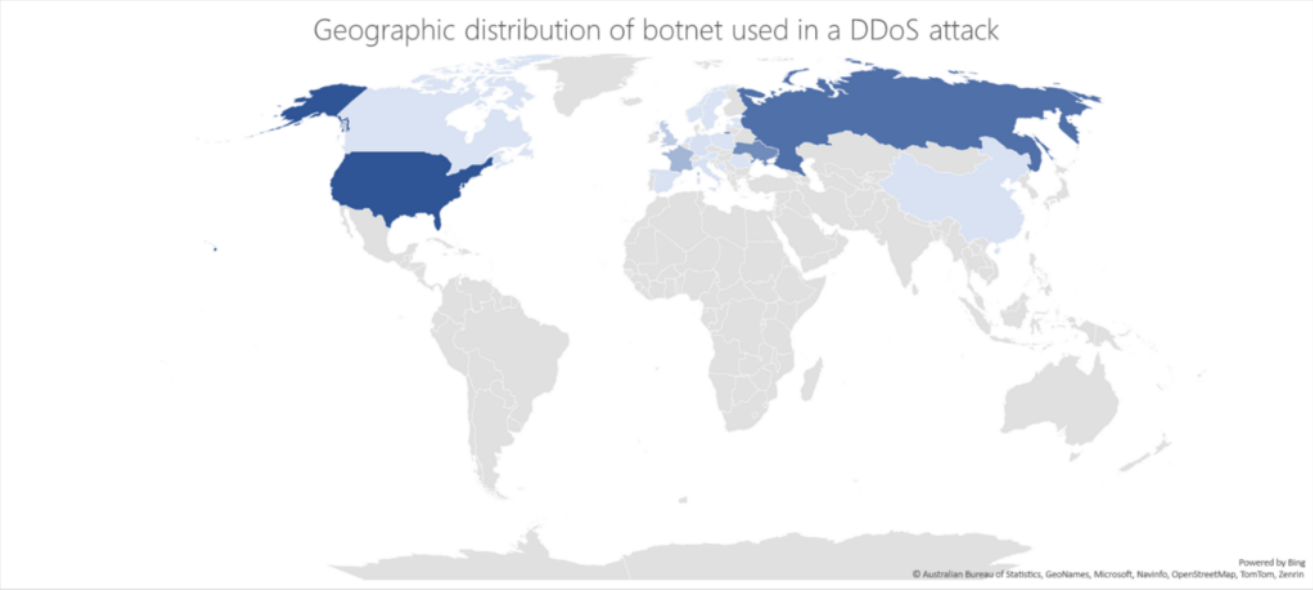

Figure 6. Global distribution of botnet used to launch the attack

These attacks were successfully mitigated for customers enrolled in Azure DDoS Network Protection and Web Application Firewall services.

Mitigating DDoS attacks from KillNet and other adversaries

KillNet and its affiliated adversaries utilize DDoS attacks as their most common tactic. By using DDoS scripts and stressors, recruiting botnets, and utilizing spoofed attack sources, KillNet could easily disrupt the online presence of websites and apps. KillNet attempted to evade DDoS mitigation strategies by changing their attack vectors, such as utilizing different layer 4 and layer 7 attack techniques and increasing the number of sources participating in the attack campaign.

Azure DDoS Network Protection helps to protect apps and resources with a profile automatically tuned to expected traffic volume. Customers can defend themselves against even the most sophisticated attacks with an Azure global network that provides dedicated monitoring, logging, telemetry, and alerts.

Azure DDoS Network Protection not only detects and mitigates DDoS attacks, but also minimizes the impact on legitimate traffic, such as in cases where botnets are harnessed to carry out attacks. We employ various mitigations to minimize false positives, including utilizing authentication, foot printing, and connection and rate-limiting countermeasures. With

DDoS Rapid Response, DDoS Network Protection customers can leverage a hotline to a DDoS service team that helps in attack mitigation, which is important when attack campaigns are highly coordinated. The combination of Azures DDoS Network Protection and Web Application Firewall (WAF) provides protection for layer 3, 4, and 7 DDoS attacks.

Steps to protect against and respond to DDoS attacks

To defend against DDoS attacks, organizations hosting web applications in Azure are recommended to take the following steps:

1. **Enable DDoS Network Protection.** Enabling DDoS Network Protection takes only a few steps, and customers don't need to change their network architecture. Include Azure WAF to protect your application against layer 7 DDoS attacks and other application attacks. Use Azure Front Door CDN to minimize the threat of DDoS attacks by distributing and balancing web traffic across Azure's global network.
2. **Design your application with DDoS best practices in mind, and ensure it's protected before an attack occurs.** Design your DDoS Protection strategy based on fundamental best practices. Make sure you test your application readiness, and DDoS Protection by simulating DDoS attacks with one of our partners.
3. **Create a DDoS response plan.** Having a response plan is critical to help you identify, mitigate, and quickly recover from DDoS attacks. A key part of the strategy is a DDoS response team with clearly defined roles and responsibilities. This DDoS response team should understand how to identify, mitigate, and monitor an attack and be able to coordinate with internal stakeholders and customers.
4. **Reach out for help during an attack.** During attacks you need to count on experts that will help you to mitigate the attack while ensuring no downtime and keeping the application up and running. Azure DDoS Network Protection customers have access to the DDoS Rapid Response team, who can help with investigation during an attack as well as post-attack analysis.
5. **Learn and adapt after an attack.** While you'll likely want to move on as quickly as possible if you've experienced an attack, it's important to continue to monitor your resources and conduct a retrospective after an attack. You should apply any learnings to improve your DDoS response strategy.

Amir Dahan *and* ***Syed Pasha,*** *Azure Network Security Team*