# Microsoft revealed the 'system crash' incident in early June was caused by a DDoS attack

During the first week of June, Microsoft unexpectedly experienced a severe outage affecting most of its services including Azure, Outlook, and Teams.

During the first week of June, Microsoft unexpectedly experienced a severe outage affecting most of its services including Azure, Outlook, and Teams. Everything has been quickly fixed by Microsoft and has not recorded any serious damage from customers. However, it is not until now, that the Redmond company has begun to disclose the cause of the problem. And as expected of many experts, the problem stemmed from a large-scale cyber attack.

In a recent blog post, Microsoft revealed details of an attack that took place in early June against network infrastructure, causing disruptions to a variety of services and taking nearly 15 hours for the company's engineers to fix. According to the Redmond giant, the company has identified a sudden increase in traffic to some of its services, and has immediately launched an investigation into the DDoS (Distributed Denial of Service) attack.

Microsoft further noted that the threat actors used multiple Virtual Private Servers (VPS), proxies, rented cloud infrastructure as well as various DDoS tools to carry out the attack. Although the case was relatively complicated, Microsoft confirmed that customer data was not accessed or compromised at all.


This recent DDoS activity targets Layer 7 and not Layer 3 or 4. Microsoft has enhanced its Layer 7 protections including tweaking the Azure Web Application Firewall (WAF) to better protect customers from the effects of similar DDoS attacks.

Microsoft also shared some technical details surrounding the attack. According to the company, a threat actor with the identifier Storm-1359 used a set of botnets and tools to launch an attack on the company's servers. These attacks include HTTP(S) overloading the system and exhausting resources through a large number of SSL/TLS requests and HTTP(S) handshakes. In Microsoft's case, the attacker sent millions of HTTP(S) requests from countless IP addresses around the globe to overload the system.

Not only that, the attacker also uses Cache bypass to bypass the CDN layer and overload the initial system with a series of queries. Finally, they continue to use Slowloris where the client requests a resource from the server but does not acknowledge receipt of the resource, forcing the server to keep the connection open and the resource in its memory.

Microsoft ends the post with a series of tips and recommendations for Azure customers to protect themselves against future Layer 7 (Layer 7) DDoS attacks. However, the company did not disclose details regarding the damage or any financial impact it suffered as a result of the attack.

Although it is not a new form of attack, DDoS is always considered the top threat to global organizations and businesses. More dangerously, both the complexity and scale of DDoS attacks are forecast to increase sharply recently, with new records continuously being set.