Warning the emergence of ransomware DDoS attack, the scale can be up to 800Gbps

Although it is not a new form of attack, DDoS has always been considered as the leading threat to organizations and businesses globally.

Notably, both the complexity and the size of DDoS attacks are projected to increase dramatically in recent times. New records are constantly being set, and blackmail through the DDoS attack threat is on the rise, starting in August of last year.

The world-famous Internet security service provider Akamai recently released a statement saying it had to deal with the largest known, complex, DDoS-for-money attack (RDDoS). significantly more incidents of the same type have been reported in the past.

Large scale RDDoS, more complex

Akamai said that in February alone, it had to deal with '3 out of 6 largest scale DDoS attacks' it has ever recorded.

Two of these are ransom DDoS attacks that also rank among the largest known. In particular, there are new cases that take place not long ago where throughput peaks at 800Gbps. This is the RDDoS attack targeting a betting company based in Europe, and at the same time the most complicated case Akamai observed since the RDDoS ransomware DDoS attack began. is recognized.

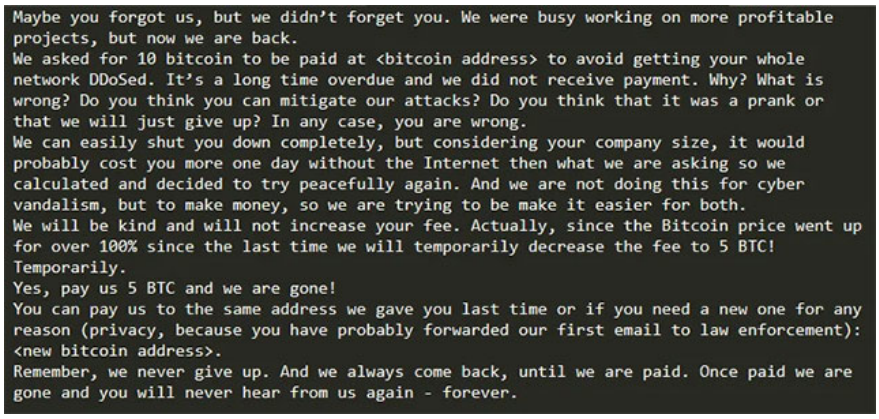
Typically, a DDoS attack is rated as high as 580Mpps and 680Gbps throughput. Cases of 200Mpps and 300 + Gbps are recorded sometimes, but the most common is below 50Mpps and 50Gbps. This is usually the result of DDoS-for-hire services. Meanwhile, the RDDoS incident Akamai recently encountered peaked at 800Gbps - showing the size of the incident that cannot be underestimated as well as the severity of the incident.

According to Akamai's preliminary investigation, the culprit used a new type of DDoS attack vector: a network protocol called the Datagram Congestion Control Protocol (DCCP), or protocol 33 for short.

Utilizing DCCP in DDoS deployments results in a mass attack and can bypass established defenses for the TCP and UDP traffic flows commonly found in these types of incidents.

Persistent and targeted

Radware, a well-known company active in the 'Anti-DDoS' field, also saw a new wave of RDDoS occurring in late 2020 and in the first week of January this year. Radware says that organizations threatened by the DDoS attack in August and September 2020 received a ransom letter demanding payment of at least 10 bitcoins to stop the attacks.


Maybe you forgot us, but we didn't forget you. We were busy working on more profitable projects, but now we are back.
We asked for 10 bitcoin to be paid at <bitcoin address> to avoid getting your whole network DDoSed. It's a long time overdue and we did not receive payment. Why? What is wrong? Do you think you can mitigate our attacks? Do you think that it was a prank or that we will just give up? In any case, you are wrong.
We can easily shut you down completely, but considering your company size, it would probably cost you more one day without the Internet then what we are asking so we calculated and decided to try peacefully again. And we are not doing this for cyber vandalism, but to make money, so we are trying to be make it easier for both.
We will be kind and will not increase your fee. Actually, since the Bitcoin price went up for over 100% since the last time we will temporarily decrease the fee to 5 BTC!
Temporarily.
Yes, pay us 5 BTC and we are gone!
You can pay us to the same address we gave you last time or if you need a new one for any reason (privacy, because you have probably forwarded our first email to law enforcement): <new bitcoin address>.
Remember, we never give up. And we always come back, until we are paid. Once paid we are gone and you will never hear from us again - forever.

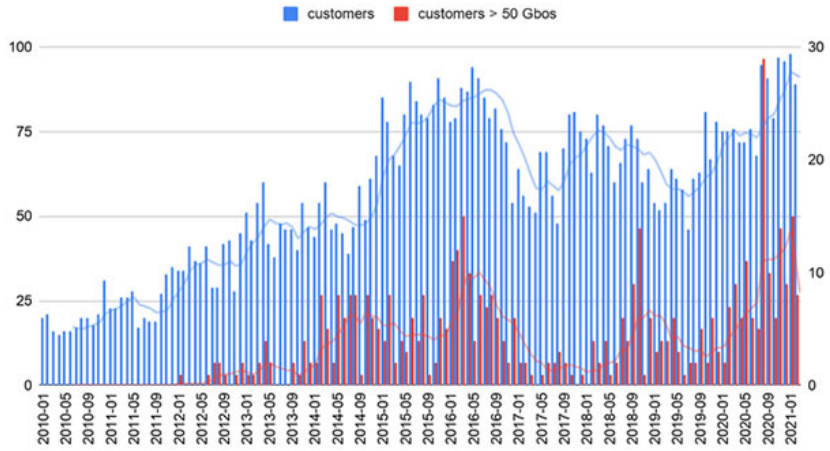
The attackers' side immediately later demonstrated that they did not pose a plain threat. Just hours after sending the ransom mail, the victims endured more than 9 hours of non-stop DDoS attack, with average throughput in excess of 200Gbps and peaking at 237Gbps.

Not only Radware, Akamai also confirmed that their customers have been through many similar cases. The company notes that 'RDDoS campaigns in 2021 appear to have become much more targeted and resilient'.

Aside from that, Akamai has also recorded multiple campaigns spanning several days and targeting a range of different IP addresses, suggesting that the attackers had been extremely well prepared.

'Attackers have been constantly looking for weaknesses in defense systems to centralize their exploits, as well as experimenting with different combinations of attack vectors. In one attack we documented, threat actors targeted close to a dozen IPs and pivoted through multiple DDoS attack vectors in an attempt to increase their ability to disrupt back-end environments' .

Another trend observed in the first three months of this year is the rapid proliferation of large-scale DDoS attacks above 50Gbps. Although it may not seem like much, this amount of junk data can cause many small and medium services to crash.



In less than three months, Akamai has recorded more attacks of this magnitude than in 2019 as a whole, and their numbers are expected to increase significantly throughout the year.