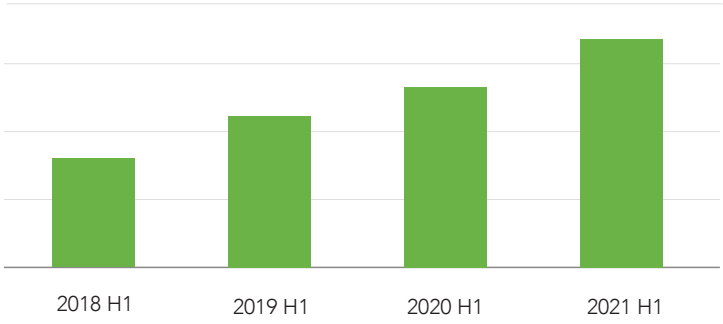
2021 Mid-Year DDoS Attack Landscape Report

NSFOCUS | 腾讯安全 Tencent Security

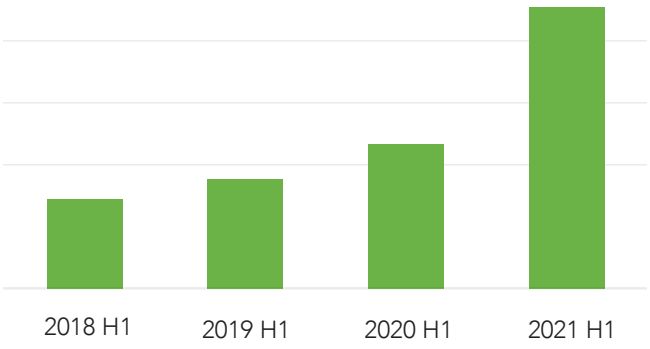
01 DDoS Attacks Witnessing a Rapid Increase for Four Consecutive Years

As COVID-19 pandemic sweeps the world, much of our everyday lives, work, recreation and entertainment have moved online. It contributes to the development of online services but also attracts attackers' attention and fuels attack increases.



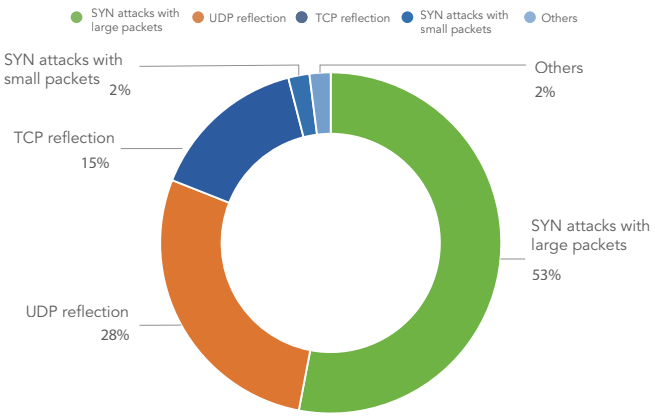
02 Volumetric Attacks Posing an Increasing Challenge

Volumetric Attacks over 100 Gbps

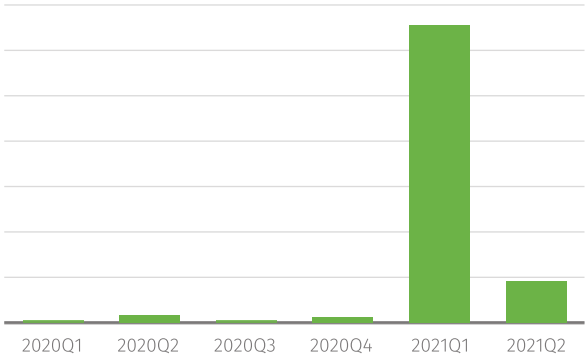


As network bandwidth keeps increasing, threat actors, by fully tapping new attack resources, are launching much more volumetric attacks over 100 Gbps. The growth rate of large DDoS attack is even higher than the growth rate of overall attacks. Especially, TCP reflection attacks featuring an extreme high packet rate can cause devastating effects on target networks. Arguably, volumetric TCP reflection attacks pose a severe challenge to defenders.

Type Distribution of Volumetric Attacks over 100 Gbps



Trend of TCP Reflection Attacks over 100 Gbps



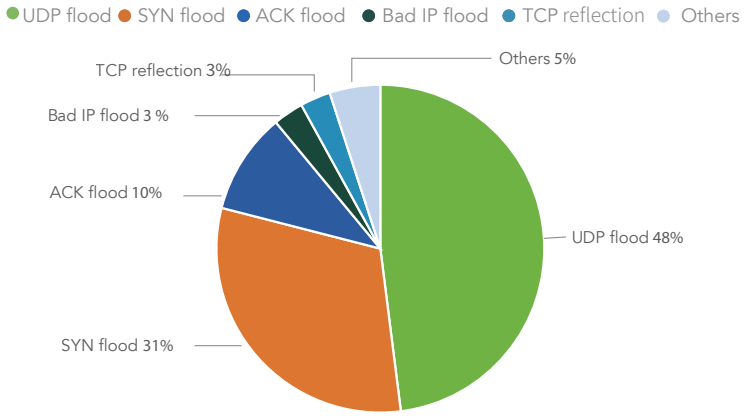
NSFOCUS | 腾讯安全 Tencent Security

03 UDP Reflection Attack as the Most-Favored Attack Means

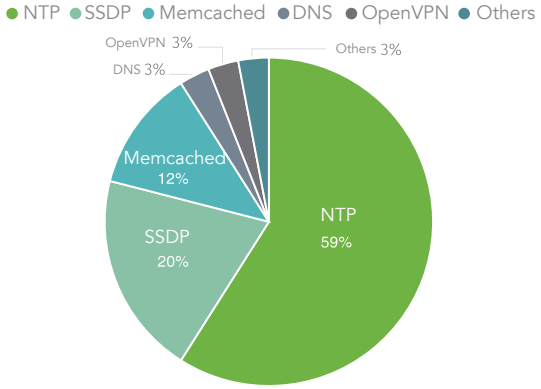
Reflective UDP amplification attacks are characterized by ample attack resources, big amplification factors, and difficulty in traceback. What's worse, the underground industry chain properly encapsulates reflective UDP amplification attacks to make it easier to execute. Therefore, it is not surprising that reflective UDP amplification attacks are the most popular with attackers. NTP reflection is the most popular vectors amongst amplification attacks.

As the COVID-19 accelerates the trend toward telecommuting, more OpenVPN traffic is observed in customers' business. However, with over 1,000,000 attack sources, the attack exploiting the OpenVPN service has become the "dark horse"of new vectors for amplification attacks.

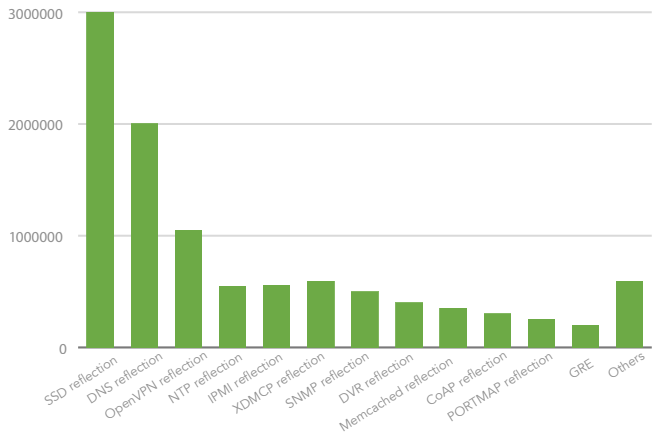
DDoS Type Distribution



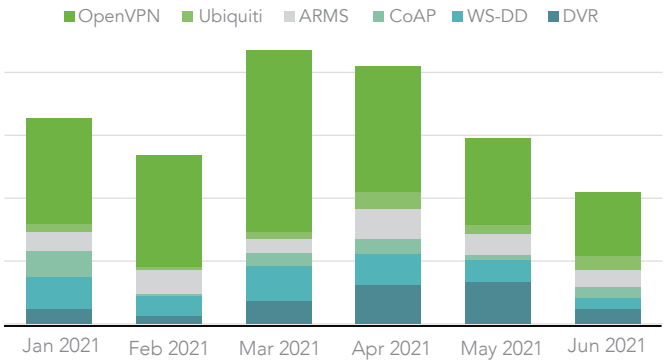
Type Distribution of Reflective UDP Amplification



Distribution of UDP Reflection Attacks by Attack Source



New Vectors Used for Reflective UDP Amplification Attacks



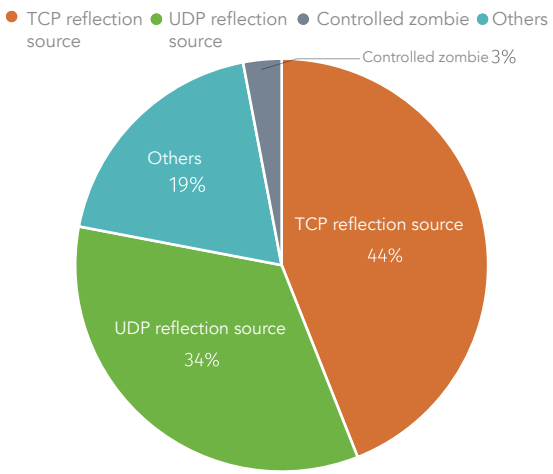
2021 Mid-Year DDoS Attack Landscape Report

NSFOCUS | 腾讯安全 Tencent Security

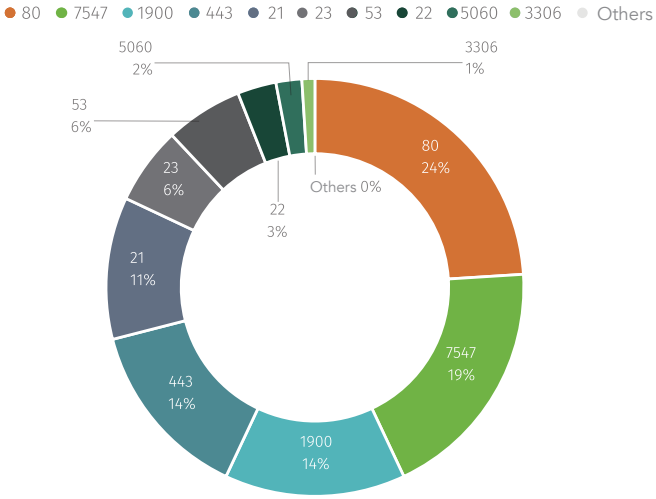
04 TCP Reflection Attacks Favored by Hackers

By virtue of considerable and widespread attack resources, TCP reflection attacks are finding increasing popularity among worldwide hackers. There is a tendency for the attacks to increase in size and quantity and new service ports (such as TCP port 7547/3306) are also targeted. In 2021, TCP attacks over 100 Gbps traffic are not a rare sight, with some even reaching Tbps magnitude, posing a severe challenge to upstream and downstream network devices, protection devices, and cloud-delivered cleaning services.

Attack Resource Distribution

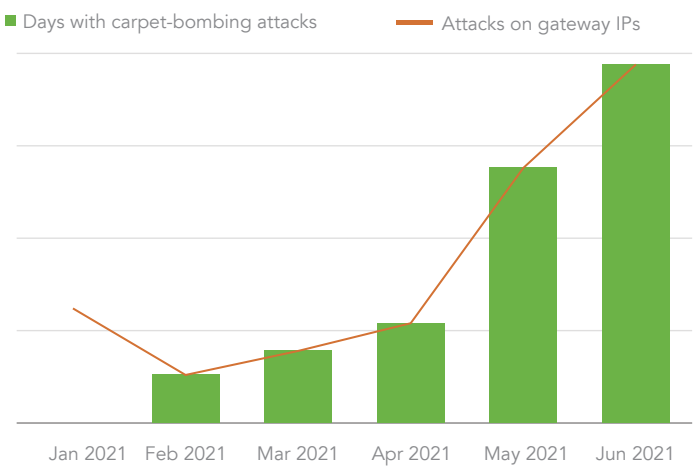


Distribution of TCP Reflection Attack Sources by Port



05 Growing Security Concerns for ISPs, IDCs, and PaaS Providers

Carpet-Bombing Attacks in 2021



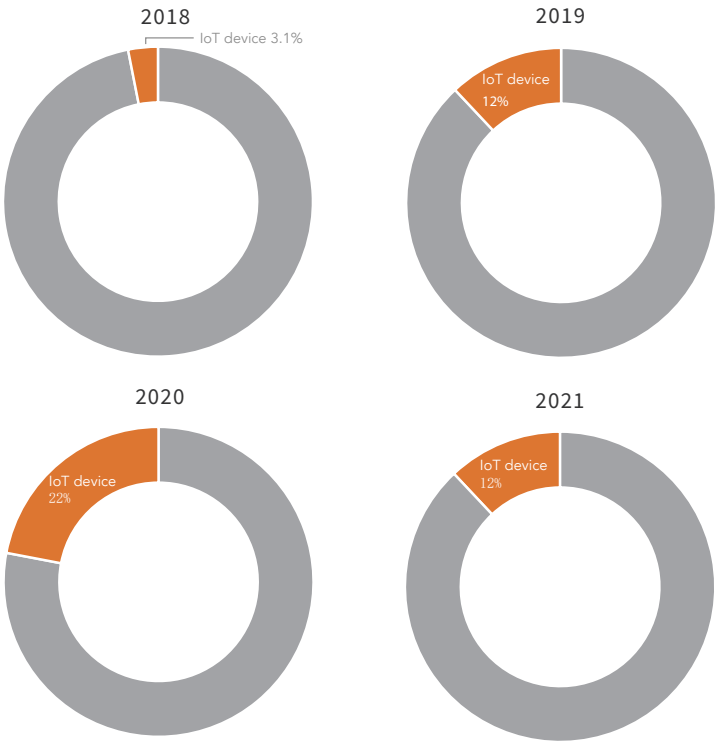
Besides constantly looking for new attack methods, attack groups also keep finding and exploiting vulnerable targets by the existing means craftily. The carpet-bombing DDoS attack and the attack on gateway IP addresses targeting ISPs, Cloud services, data centers and PaaS providers are two typical vectors.

2021 Mid-Year DDoS Attack Landscape Report

NSFOCUS | 腾讯安全 Tencent Security

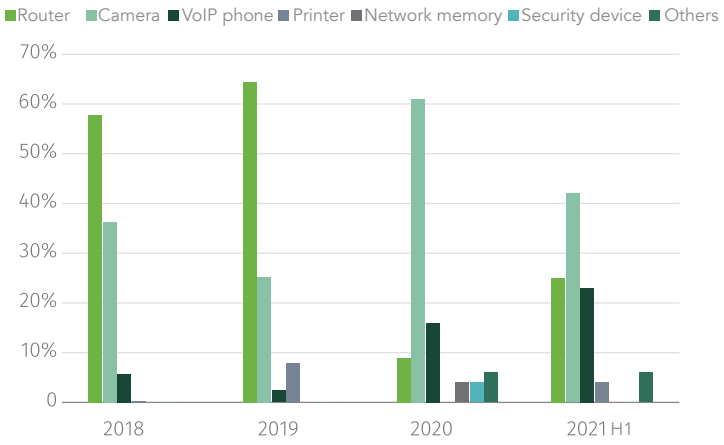
06 IoT Devices

Percentage of IoT Devices Among Long-Term Active Attack Sources



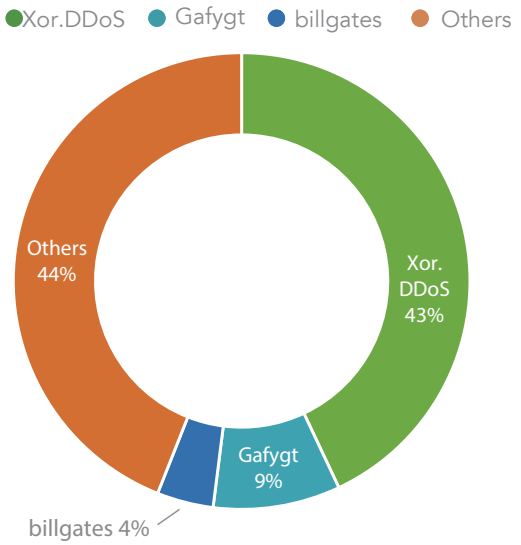
Note: According to active duration of the IP addresses, attack sources that remain active for more than 10 days are deemed highly active and vulnerable.

Type of IoT Devices Deployed in DDoS Attacks

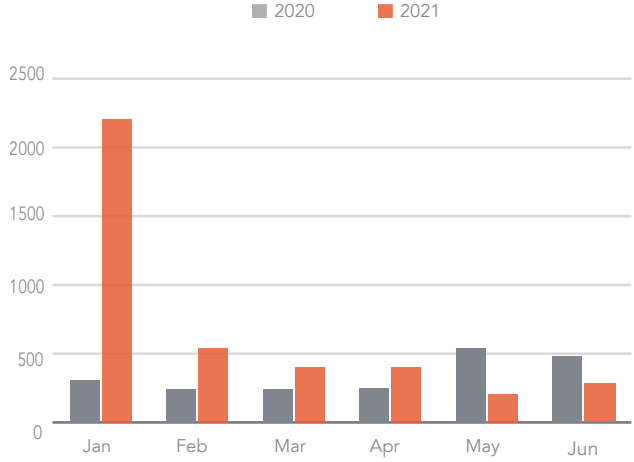


07 Botnets

Bot Distribution



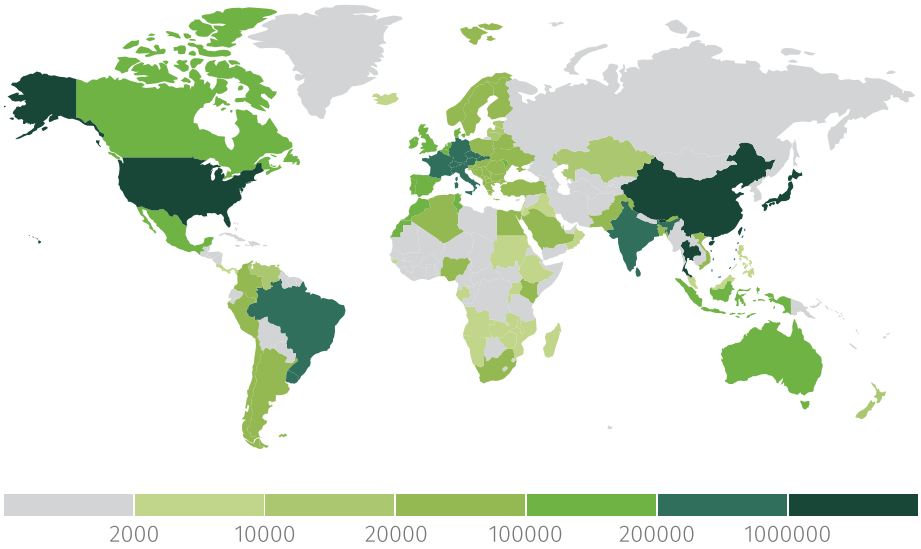
Trend of Attacks by XOR DDoS

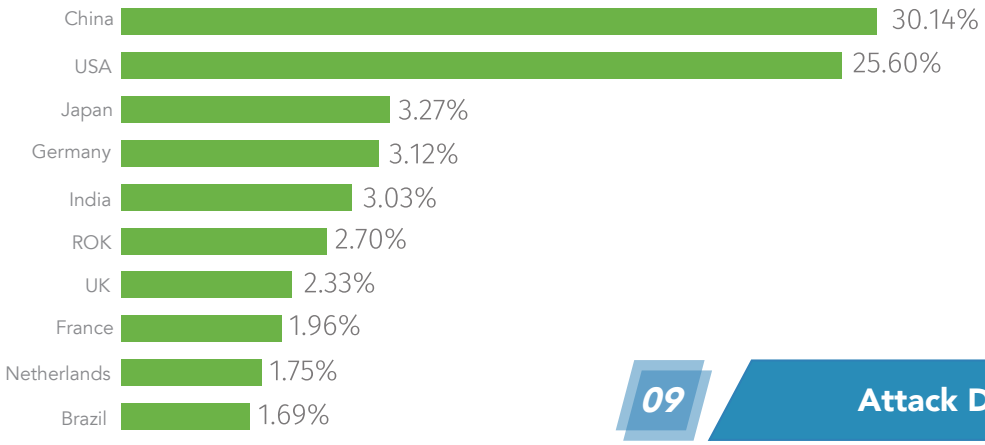


2021 Mid-Year DDoS Attack Landscape Report

NSFOCUS | 腾讯安全 Tencent Security

08 Geographic Distribution of Active Attack Sources





09 Attack Duration Distribution