Nokia Deepfield Network Intelligence Report

DDoS in 2021

Distributed Denial of Service (DDoS) activity and trends in 2021

Contents

Introduction

In the era of the cloud, the Internet of Things (IoT) and 5G, networks matter more than ever. And even more so during the COVID-19 pandemic, when our work, learning and entertainment have shifted online.

The COVID-19 pandemic has changed online behavior and internet traffic patterns. We covered some of these changes and their impact on the internet and service provider networks in the Nokia Deepfield Network Intelligence Report 2020.

Unfortunately, the pandemic has also generated significant growth in traffic that corresponds to distributed denial-of-service (DDoS) attacks.

DDoS threats and attacks have become more frequent and impactful over the last decade, especially during the last two years. Attacks now come from outside and inside service provider networks and are aimed at internet hosts and servers, customers, users and network infrastructure.

This report provides our perspectives on DDoS traffic and trends in 2021, as captured by our Deepfield research team.

> “The pandemic generated significant growth in traffic that corresponds to distributed denial-of-service (DDoS) attacks.

DDoS attack types

DDoS attacks can be classified into three general categories:

- Volumetric DDoS attacks
- Flooding attacks using spoofed IP addresses through IP header modification (IPHM)
- Application-level attacks

Volumetric DDoS attacks present the greatest danger because of their immense impact on networks, services and users. In terms of bandwidth, volumetric DDoS attacks made up the majority of all DDoS traffic until the second half of 2021.

Volumetric attacks appear as high-bandwidth attacks that are characterized by their total bandwidth expressed in bits per second (b/s). They aim to exhaust transmission capacity by generating a high volume of traffic.

Volumetric attacks can also can also appear as high packet rate attacks that are characterized by their packet intensity expressed in packets per second (p/s). They aim to exhaust the processing capacity of network hosts and other network elements such as firewalls.

The most common volumetric attacks are amplification DDoS attacks, where attackers send small packets (e.g., 40-byte requests). These attacks can exploit about 40 distinct types of internet servers, including DNS servers, time servers and CLDAP servers. A misconfigured server will send a response that is 10 to 1,000 larger to the target system. As a result, the target system gets a very large traffic volume that often originates from many different points on the internet, each of which acts as distributed amplifier.

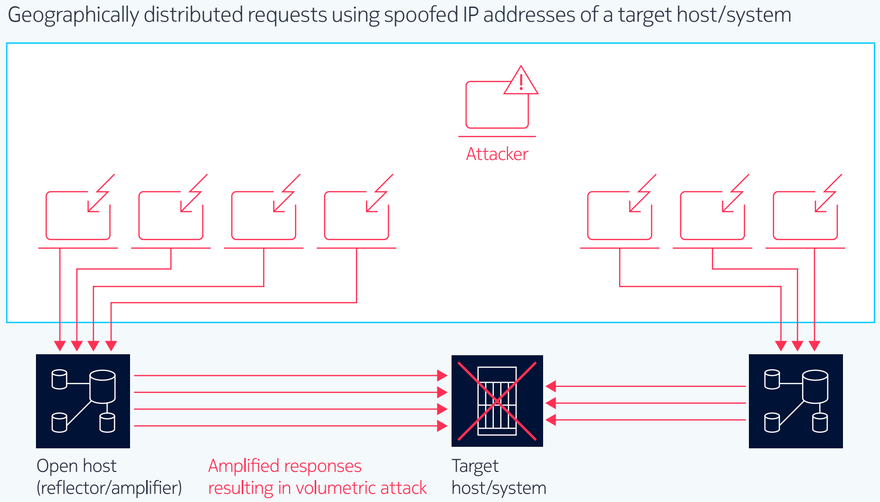


Figure 1. Volumetric DDoS attack created using reflection and amplification

Volumetric DDoS attacks, especially amplification and reflection attacks, generally require IP address spoofing, which is a form of IPHM. Spoofing the source IP address(es) hides the originator's IP address(es) and allows the attacker to pretend to use the IP address(es) of the targets. For example, the attacker might send traffic to regular internet servers (e.g., Google, Akamai or Microsoft) with a spoofed IP address. These servers will respond (e.g., with SYN-ACK packets) to the spoofed IP address(es), sending millions of packets to the target systems.

Amplified responses of spoofed IP traffic can lead to a high volume of traffic going to targets' systems.

Spoofing is also used in traffic **flooding attacks** that send high volumes of TCP, UDP and ICMP requests to targeted servers. In this case, the DDoS attacks take the form of irregular protocol message exchanges that confuse and saturate servers. Examples include synchronization packet (SYN) floods and fragmented packet attacks. The extraordinary amount of flooding traffic exhausts state information on (stateful) firewalls, load balancers or on different parts of the infrastructure. As a result, end users experience significant delays and are eventually disconnected from the service.

Application-level DDoS attacks aim to disrupt or crash target systems by causing state exhaustion at the application level. These can include low-and-slow attacks, GET/POST floods and other forms of attacks that target specific servers, applications or hosts.

Most application-level attacks are driven by **botnets**, which are compromised devices or systems that have been exploited and can be remotely controlled by a bot master (also called a bot herder).

DDoS techniques such as carpet bombing use an extended range of IP addresses as targets (instead of an IP address of a single host) or hide the "real" attack in a range of simultaneous attacks (e.g., a bits-and-pieces attack).

In 2021, we saw significant growth of botnet DDoS traffic. At times the attacks came in the form of a "ransom DDoS." Victims were asked to pay a ransom in cryptocurrency to make the attacks stop or not have them escalate further - potentially to terabit levels.

> 2021 brought a significant growth of botnet DDoS traffic.

Impact and damage from DDoS attacks

DDoS attacks spare no one. Targets range from individual users to service providers, cloud builders and large digital enterprises.

While most DDoS attacks are a nuisance, the bandwidth represented by high-bandwidth and high-packet-intensity volumetric attacks is cause for concern. With volumetric amplification DDoS, attackers simply need bandwidth and connectivity. They can then launch attacks that leverage millions of servers and unsecured and compromised IoT devices across the internet to overwhelm interfaces, routers, load balancers, firewalls and network hosts. These attacks reduce the performance of the targeted systems, and services are degraded or stopped.

Large-scale DDoS attacks are particularly dangerous to network routers and infrastructure. These attacks can disrupt connectivity and service availability for tens of thousands of enterprises and millions of consumers. They can result in losses that range from thousands to millions of US dollars.

On May 4, 2021, a network provider supplying connectivity services to the Belgian government was hit by a DDoS attack that originated from 257,000 IP addresses in 29 countries. The attack left many customers without vital connectivity and disrupted online schooling and the Belgian COVID-19 vaccination reservation system.

While some big attacks make headlines, many attacks go unreported because service providers do not want to expose details about their security capabilities or vulnerabilities.

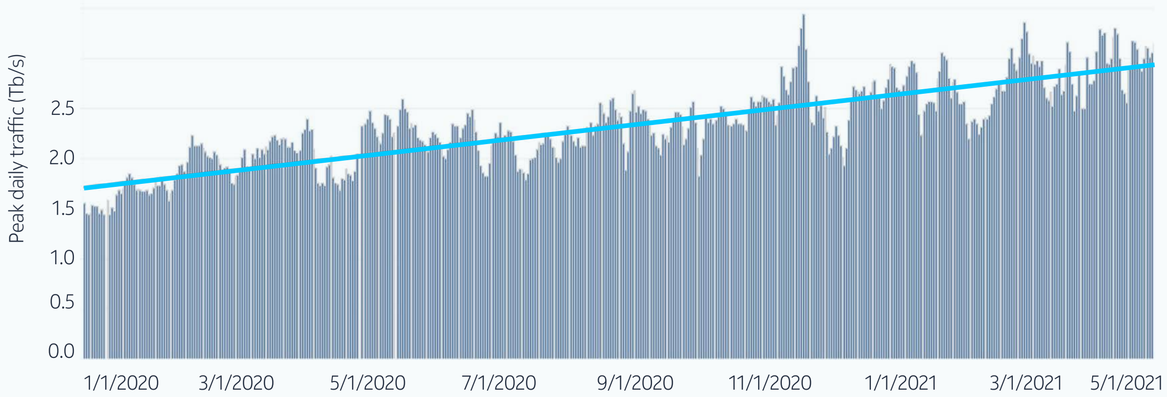
Even worse, many attacks go undetected.

> Large-scale DDoS attacks can disrupt connectivity and service availability for tens of thousands of enterprises and millions of consumers.

DDoS in the time of the COVID-19 pandemic

DDoS attacks have increased in recent years. Around 2016, we saw the first terabit-level DDoS attacks. Today, DDoS attacks are a reality for most networks. In the **Nokia Deepfield Network Intelligence Report: Networks in 2020**, we showed how, in the short period from early February to late May 2020, aggregate DDoS volume levels in the United States rose by more than **40 percent**.

The situation appeared even worse when we looked at global DDoS traffic in May 2021. As shown in Figure 2, daily DDoS peaks had more than doubled in a little more than a year. In January 2020, the average daily 5-minute peaks were around 1.5 Tb/s. By the end of May 2021, these peaks exceeded 3.0 Tb/s.



Source: Nokia Deepfield, May 2021.

Figure 2. Peak daily DDoS traffic January 2020–May 2021 across select service providers

> Daily DDoS peaks doubled between January 2020 and May 2021.

DDoS in 2021

In mid-2021, we completed our multi-year Nokia Deepfield research project, which looked at the internet as a whole and significant number of Tier-1 service provider networks, encompassing thousands of network routers. This research represented the most comprehensive study of DDoS traffic ever conducted, tracing DDoS back to its origins. We continue to monitor DDoS globally, collecting detailed information about every DDoS attack.

Our research uncovered several key DDoS trends for 2021:

- Spoofing was a major contributor to the number of DDoS attacks for the first half of 2021. However, spoofing DDoS attacks originate from fewer than 50 hosting companies and regional providers.
- The rapidly growing number of open and unsecured internet services and IoT devices means there is a threat potential for DDoS attacks over 10 Tb/s. This is **four to five times** the scale of the largest attacks reported so far.
- In the second half of 2021, botnet DDoS has become a major source of DDoS traffic, both in the frequency and volume of attacks. For example, on December 29, 2021, we recorded the largest botnet DDoS attack. The attack peaked at **4.4 Tb/s** (429.7 million p/s) and involved 5,270 unique IP addresses.
- The number of ransom DDoS incidents also grew significantly. A 2021 Neustar study shows that enterprises reported ransom DDoS attacks as more common than ransomware attacks.

> The largest botnet DDoS attack, recorded on December 29, 2021, was at 4.4 Tb/s (429.7 million packets per second).

Spoofed DDoS

Most DDoS analyses stop at amplifiers because they seem to be the source(s) of the DDoS attack traffic. Tracing spoofed traffic beyond amplifiers and reflectors typically requires a lot of manual tracing and investigation, and for a long time it was considered an impossible task.

In 2021, for the first time ever, our Deepfield research team was able to track spoofed DDoS back to its origins on the internet.

We used fingerprinting techniques to identify DDoS traffic. Adding other techniques and tools, such as tracking time-to-live (TTL), allowed us to trace the DDoS traffic back from victims to the closest internet entry point.

This combination of techniques also enabled us to identify the specific hosting providers from which about 40–50 percent of DDoS traffic originated. We performed additional analytical steps to find the origins of the remaining 50 – 60 percent of the traffic.

The first step was to obtain account information and other details on every DDoS-for-hire service we could find. We spent a lot of time collecting information from many sources, including darknet lists as we negotiated paid access to some of these services. This allowed us to capture the list of most (if not all) DDoS-for-hire services offered from so-called “booter” and “stresser” websites. As a result, we identified the hosting providers used to supply these websites.

We also obtained packet captures and tracked down amplifiers, DNS payloads, NTP servers, ICMP and other relevant metrics relating to the attacks, taking a broad range of measurements. We shared some of our techniques and algorithms at NANOG82.

Using all this information, we created “fingerprints” for each DDoS attack to help us correlate their signatures with new DDoS attacks happening across the internet.

The knowledge we gained enabled us to identify the originating domains for DDoS attacks. Before our analysis, these domains had largely been hidden behind reflectors or amplifiers.

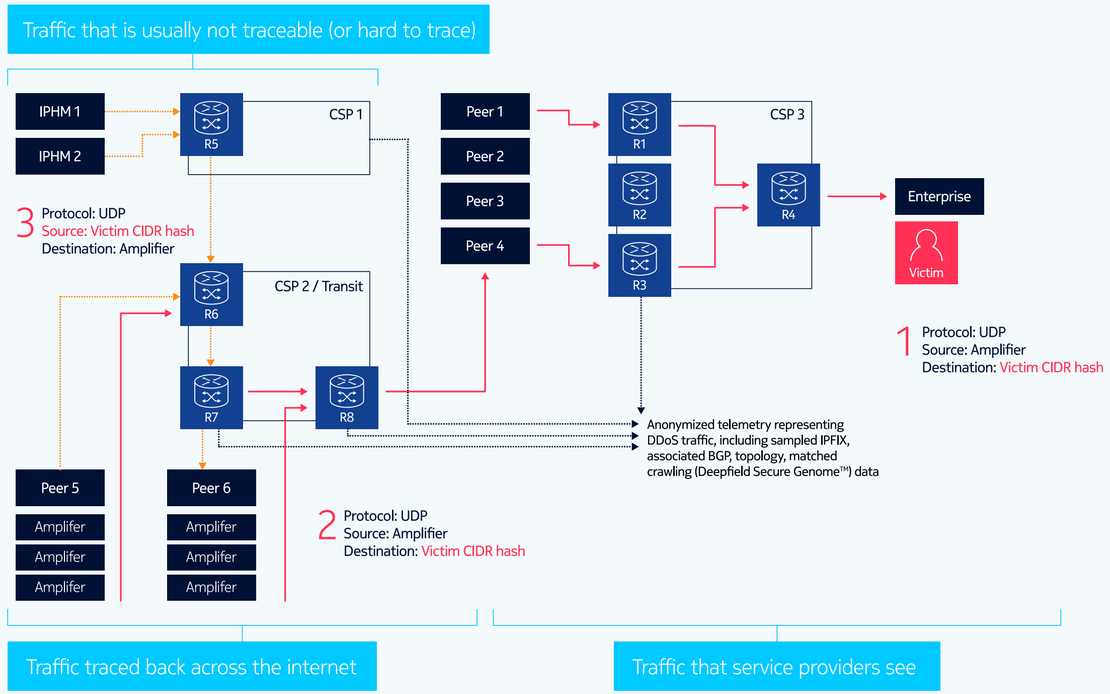


Figure 3. Tracing DDoS back to its origins

> In 2021, for the first time ever, Nokia Deepfield was able to identify the origins of spoofed DDoS traffic on the internet.

DDoS for hire: Booter and stresser websites

The conventional wisdom is that DDoS attacks come from everywhere or are unstoppable. Our analysis showed that most DDoS attacks come from a tiny number of hosting providers that offer a safe haven for DDoS-for-hire services.

By June 2021, there were approximately 100 booter websites on the internet. For a small fee, starting from about US$50 per month, they provide a menu of options to attack an enterprise, a gaming server or anyone in a service provider network – for example, a particular subscriber, a banking institution or an online gambling company. These websites advertise their services for penetration testing, keep no logs and accept payments in cryptocurrencies. They have thousands of customers and generate millions of dollars in revenue per month.

Interestingly, all these booter sites take a similar approach. They offer a range of plans between US$50 and US$1,000 per month depending on the attack's sophistication, frequency and intensity. They also offer a range of services such as IP address spoofing, which allows malicious parties to specify that attacks should appear to originate from legitimate sites such as Google, Microsoft or Cloudflare. Some of the sites are bold enough to advertise that they offer the ability to launch attacks over 2 Tb/s.

We found that most DDoS attacks do not come from individual hackers. Instead, the vast majority of DDoS attacks are orchestrated by around 100 websites hosted by fewer than 50 hosting providers.

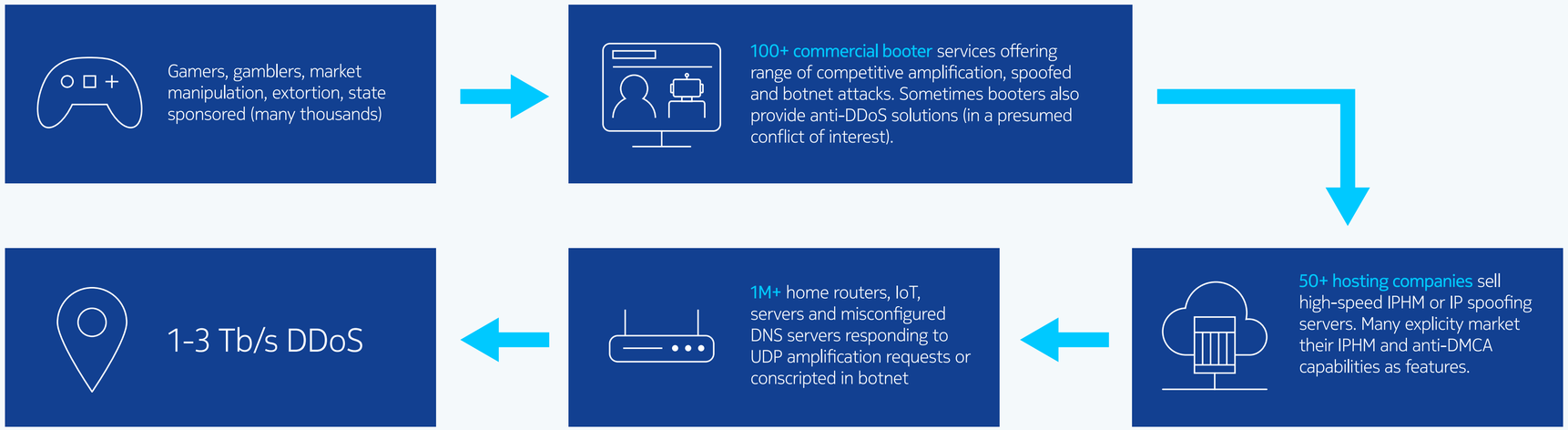


Figure 4. DDoS-for-hire ecosystem

DDoS hosting providers

We found around 50 globally distributed providers that allow DDoS attacks to originate from the web servers they are hosting: several of them in the US, a few in Asia and a large number in Eastern Europe. They allow hosting of DDoS booter services. The geographical choice largely reflects jurisdictions where DDoS attacks are not considered a criminal offense. These providers are not the familiar, large commercial web hosting providers. Most well-known and reputable hosting providers check and block spoofed IP traffic.

We looked deeper into providers allowing hosted websites to offer DDoS-for-hire services and found that they fall into three categories.

In the first category are companies operating as **typical content piracy servers**. These providers advertise offerings such as IP spoofing on dubious websites. Typically, they also offer to host "private content," which generally refers to copyrighted content, adult content or any other type of illegal content. About one-half of these providers are out in the open and are very explicit about their services. Typically, they operate in "gray area" jurisdictions, where they may be beyond the reach of law enforcement.

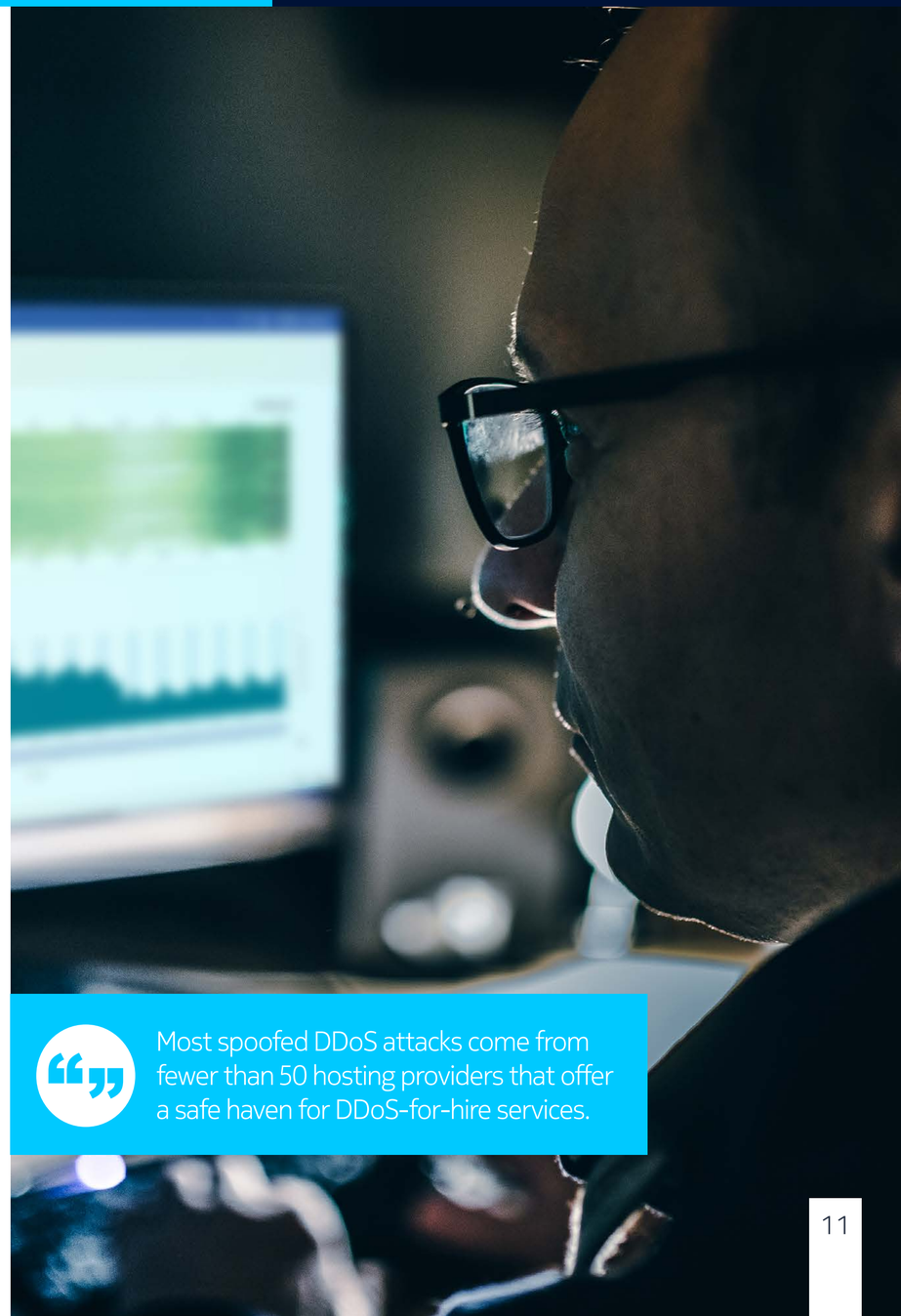
The second category is **hosting companies** that usually hide that they are offering these services. Typically, they hide in layers because most hosting on the internet is resold.

Often, the companies at the bottom layer operate reputable businesses. At the top are two or three layers of increasingly less reputable businesses that resell the same infrastructure and hardware.

This means that all these seemingly disparate businesses belong to the same company. They are simply different brands within the same ownership structure.

Websites hosted by these companies do not advertise DDoS or spoofing capabilities directly on their web pages. Instead, they may embed their offers and terms in the source code to allow internet search engines to point to them.

The third type of DDoS hosting provider was a major surprise. These are **DDoS mitigation companies**, or companies that advertise that they provide DDoS mitigation services. We discovered that three of the top DDoS mitigation services are also three of the top sources of DDoS attacks on the internet. We can only presume that this is a conflict of interest - similar to thieves offering home protection services.



> Most spoofed DDoS attacks come from fewer than 50 hosting providers that offer a safe haven for DDoS-for-hire services.

DDoS threat potential is over 10 Tb/s

The largest reported attacks before 2021 ranged between 2 Tb/s and 3 Tb/s. In late 2021, we recorded an attack exceeding 4 Tb/s. These attack levels are certainly more than enough to interrupt service to many corporate and residential customers.

Significant terabit-level attacks were rare until a couple of years ago. Today, we see aggregate DDoS traffic levels of that capacity every day, which means that volumetric DDoS attacks are happening on the internet almost constantly. In other words, DDoS has become a significant source of "traffic noise" in networks. In some networks, daily DDoS traffic levels have risen enough to be causing upstream congestion issues (e.g., with international connectivity.) These are troubling developments.

One of our study's major findings – based on open and vulnerable systems and hosts on the internet – is that there is a large DDoS threat potential for attacks yet to be launched. Potential for attacks yet to be launched. When we consider the global internet infrastructure that can be leveraged for DDoS attacks (including hijacked IoT devices and unsecured or misconfigured servers and hosts), we see potential attack volumes of more than 10 Tb/s.

> Considering all open and vulnerable systems in the internet that can be exploited (including IoT), there is threat potential for attacks larger than 10 Tb/s.

The clear and constant danger of DDoS

DDoS traffic has become a clear and constant source of danger in almost all service provider networks. Looking at the second half of 2021, we noticed that the average peaks of DDoS attacks ranged anywhere between several Mb/s and hundreds of Gb/s. Figure 5 shows average peaks across DDoS categories.

While the volume and intensity of amplification/reflection attacks are much higher, the growing frequency of IPHM/spoofing and botnet/application attacks makes them equally concerning.

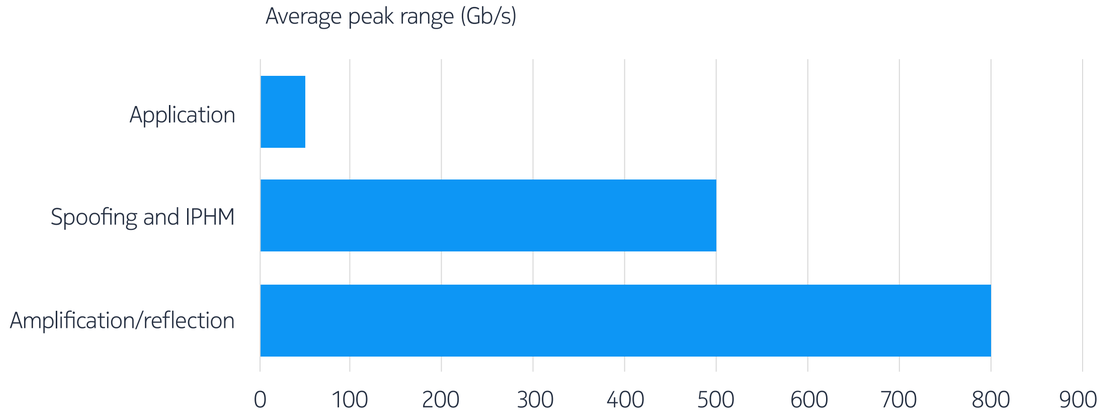


Figure 5. Average peak rates for DDoS attacks, per attack type (recorded in 2H 2021)

> In the second half of 2021, the average peaks of daily DDoS attacks ranged between several Mb/s and hundreds of Gb/s.

The rise of botnet DDoS

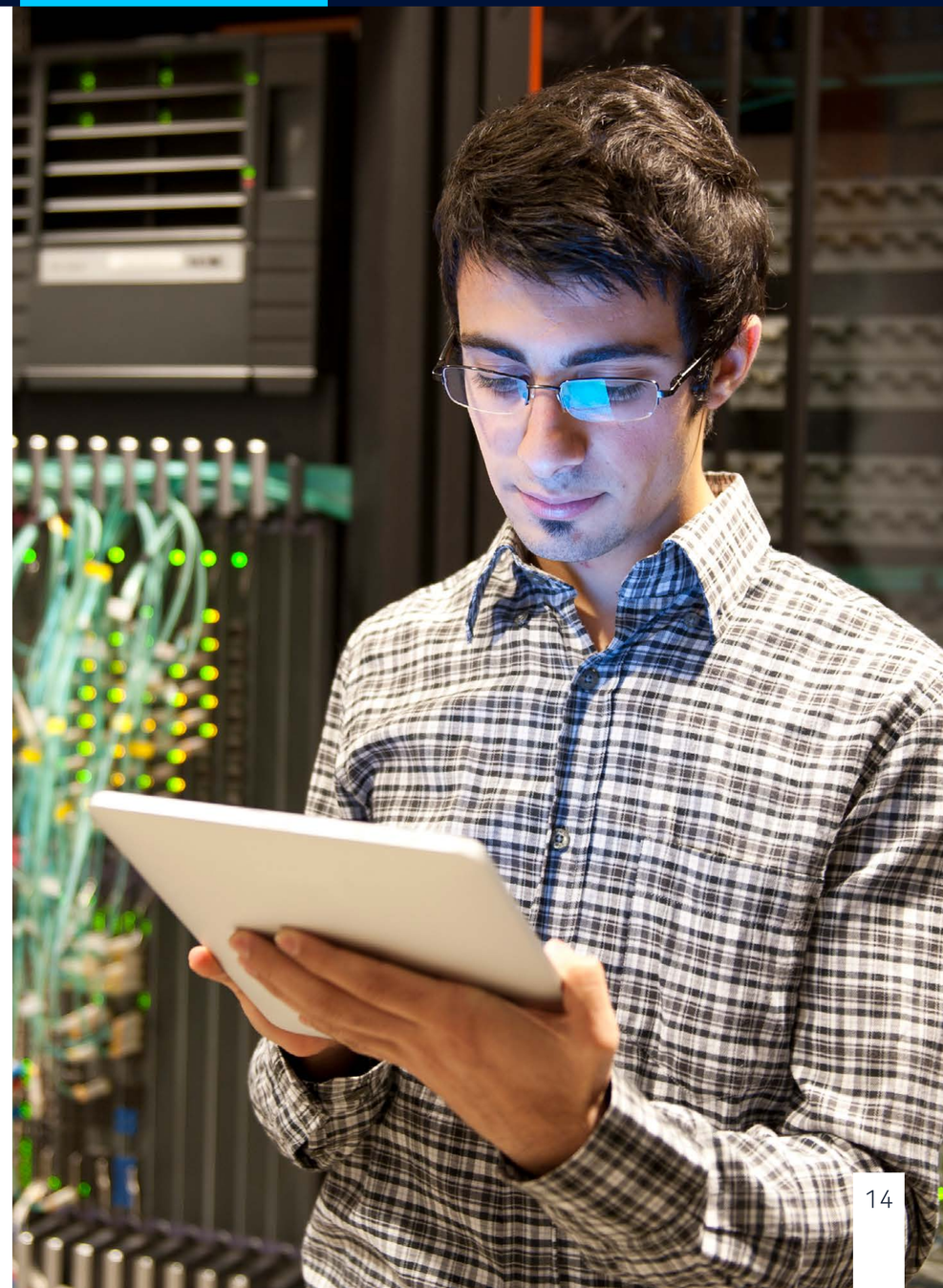
The second half of 2021 brought a significant shift in the DDoS threat landscape. We noticed a significantly higher incidence of botnet DDoS attacks that used a variety of IoT devices, from unsecured (and hijacked) VoIP terminal adapters to always-on high-bandwidth security cameras, CPE devices and even parking meters.

We also noticed a 33 percent decrease in the number of booter and stresser sites and hosting domains from June to December 2021. Whether this decrease was an outcome of the Biden–Putin cybersecurity meeting in June 2021 (or our study) is yet to be determined.

The combination of explosive growth in IoT technology and the distributed and global reach of cloud computing has created a new environment for launching DDoS attacks. It offers additional benefits to criminals in the form of an increasingly lucrative extortion market. Ransom DDoS has become a weapon for extortion, and is often used with other ransomware, as covered by our Nokia Threat Intelligence Lab.

Botnet DDoS attacks are becoming larger and significantly more challenging to detect and mitigate. Unlike their synthetic amplification and flooding counterparts created for DDoS purposes, botnet DDoS attacks use valid IP addresses, full TCP-IP stacks, legitimate operating system-generated protocol headers, correct checksums and payloads that match the statistical distributions seen in normal application traffic (e.g., web agent, form fields). Many botnets can reportedly also pass CAPTCHA challenges.

Unlike other types of DDoS attacks, botnet DDoS attacks do not exhibit distinguishable header or payload features such as poorly randomized headers and patterns in attack payload. As a result, they present a significant new challenge to DDoS detection and mitigation.



Anatomy of a botnet DDoS attack

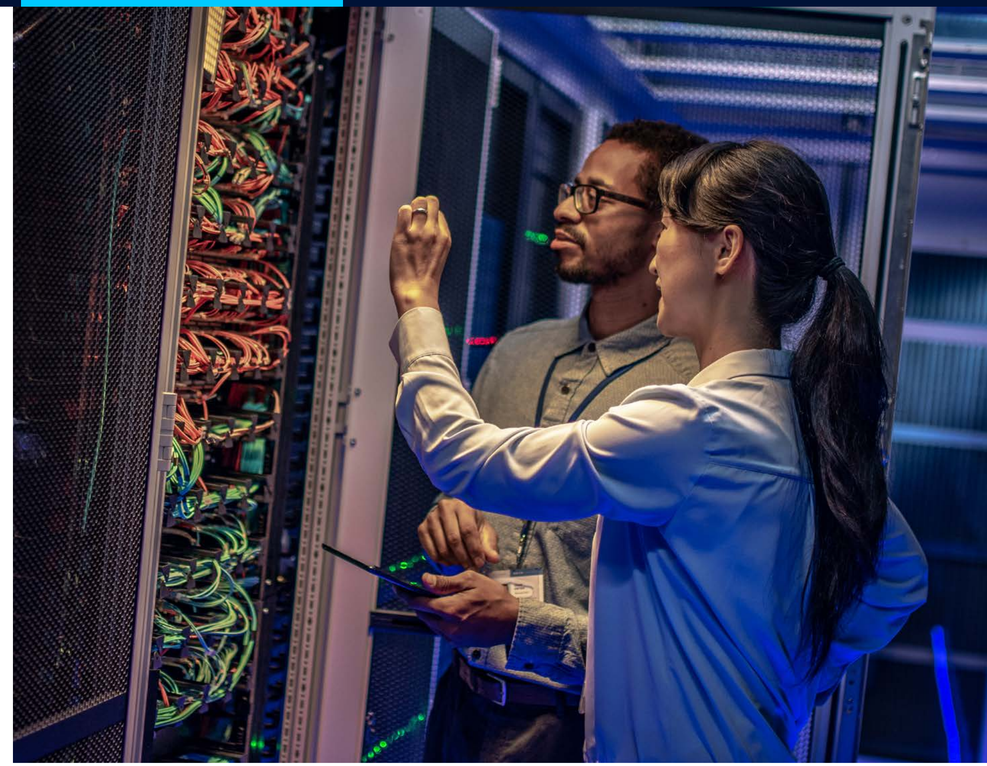


Figure 6 captures a botnet DDoS attack from December 2021.

Summary

15,457	3	860.2	86.53
Unique source IPs	Unique destination IPs	Peak Gb/s	Peak Mp/s

DDoS attack bandwidth over time

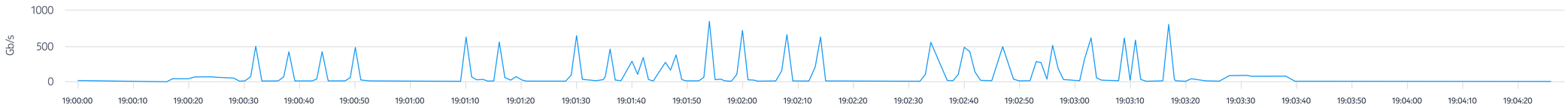


Figure 6. A snapshot of a botnet attack from December 2021 (Source: Nokia Deepfield DDoS Library)

This attack peaked at 860 Gb/s (86.53 million p/s) and involved over 15,000 unique source IP addresses.
The main challenge in detecting this attack was that all the IP addresses involved were legitimate (i.e., not spoofed).

Figure 7 shows the locations of the devices involved in the attack.

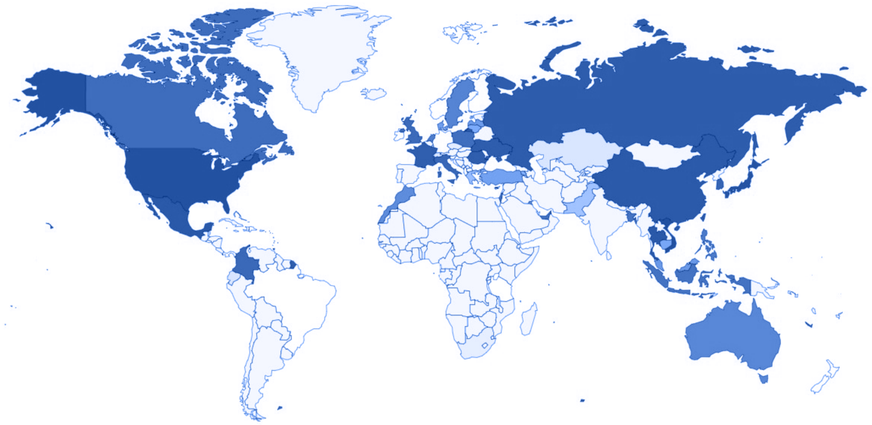


Figure 7. Geographic distribution of IP addresses involved in this DDoS attack

With so many IP addresses involved, it was important to understand how they contributed to the overall attack traffic. Figure 8 shows the cumulative distribution of DDoS traffic volume against the number of IP addresses involved in the attack.

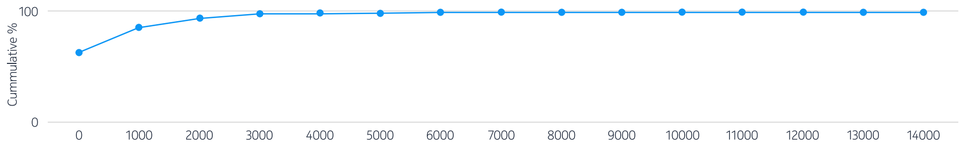


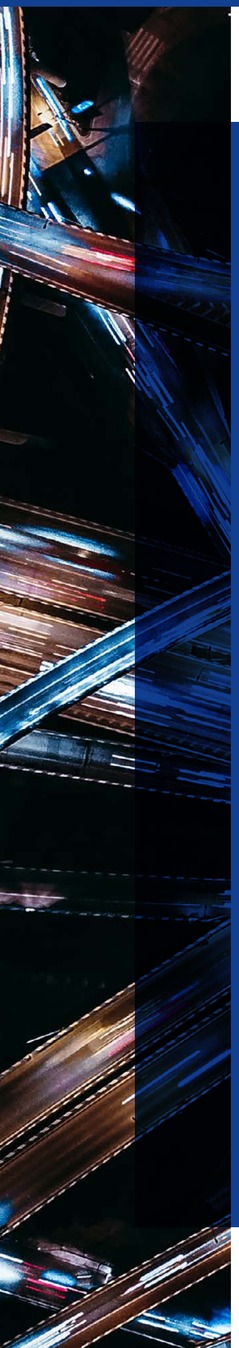
Figure 8. Cumulative distribution of DDoS traffic against the number of IP addresses used in this botnet DDoS attack

It turned out that about 2,000 IoT devices were contributing to about 98 percent of the total attack volume. The knowledge of which IP addresses contributed the most allowed for effective mitigation of the largest part of this attack.

The days of botnet DDoS attacks launched from compromised home computers with limited bandwidth using poorly written shell scripts are over. In addition to booter- or stresser-originated DDoS attacks, the torrent of poorly secured IoT devices throws more fuel on the DDoS fire. The number of exploitable devices is doubling or tripling each year. Many of these devices have high-speed internet connectivity and run full-stack Linux.

However, while the number of malicious IoTs is growing, many botnet DDoS attacks repeatedly employ the same subsets of IoT devices. Prior knowledge of "repeat offenders," as well as better internet security context, can offer an excellent foundation for detecting and mitigating botnet DDoS attacks.

> Botnet DDoS attacks are becoming larger and significantly more challenging to detect and mitigate.



Conclusion

DDoS attacks are a major threat to networks, services and users. Fortunately, the techniques and solutions available to detect and mitigate DDoS attacks have significantly evolved from legacy approaches created to fight them decades ago.

Today, a combination of advanced big data network security analytics and programmable routers can cost-effectively and efficiently block most of the DDoS attacks we see on the internet.

With a much-improved internet security context and tools that enable tracking of DDoS attacks and sharing of the most important findings, we can achieve better, more accurate and more agile detection.

The time has come to leave costly, reactive DDoS protection behind and embrace smarter and more proactive approaches. More scalable and cost-effective mitigation can be achieved using the concept of a self-defending network. This means embedding security in the IP network and combining advanced detection capabilities with sophisticated features of the latest generations of router silicon, which allow security enforcement at line speed. Next-generation, mitigation-optimized DDoS solutions can deliver higher accuracy at much lower cost.

The automation of DDoS protection has also evolved. Automation can enable the self-defending network with zero-touch or minimal operator supervision, and deliver high performance, scale, efficacy and economic efficiency. DDoS automation can quickly block DDoS attacks and ensure that valid traffic passes through with minimal impact on the network, services and users.

As the DDoS threat evolves and better tools emerge to combat it, the internet community needs to take a firmer stance. The battle against DDoS must be fought with technology, as well as with more involvement and better cooperation from service providers, hyperscale cloud builders, end users, regulators and governments.

With the right tools and commitment, we can block DDoS attacks and minimize their effects on internet services and applications.

> A combination of advanced big data network security analytics and the latest generation of commercial routers can cost-effectively and efficiently block most of the DDoS attacks we see on the internet.

Nokia Deepfield DDoS solution

Nokia Deepfield is a suite of software-based network analytics and DDoS security applications for large-scale IP networks. It enables network operators to optimize their networks and services, enhance the customer experience, improve network security and increase operational agility. Deepfield applications are deployed globally in diverse networks by fixed and mobile service providers, cable companies, cloud companies and digital enterprises.

The Deepfield approach uses big data IP analytics, combining network data (including telemetry, DNS and BGP) with the patented **Nokia Deepfield Genome**, a live data feed that tracks internet content, applications and services and provides DDoS security context.

As a result, the Deepfield portfolio provides a cost-effective way of obtaining multidimensional, real-time insights about IP-based services and applications running across the entire IP network – from content-originating domains and CDNs, peering and backbone networks, and all the way to the customer edge.

Within this portfolio, **Deepfield Defender** provides a foundation for next-generation DDoS detection and mitigation, leveraging big data analytics, rich telemetry and programmability of the IP network itself.

With the added internet security context – including knowledge about known amplifiers/reflectors, IPHM domains and active bots – obtained through the **Deepfield Secure Genome™** data feed, the Deepfield portfolio facilitates much better and more accurate DDoS detection.

DDoS mitigation is as important as detection.

Major innovations such the **Nokia FP5 chipset technology** equip the latest generations of production routers to be super-scalable, cost-effective and used as network-wide enforcement points to implement agile and granular countermeasures. The capabilities of new, advanced routers for **IP network security** can radically change the economics of DDoS protection.[1]

The Nokia Deepfield DDoS solution offers significant benefits over legacy appliance-based or DPI-based approaches, including better scalability, more accurate detection, higher cost efficiency and full traffic visibility as end-to-end encryption becomes the norm. It delivers the holistic, 360-degree DDoS security required for the 5G, cloud and IoT era.

[1] A Nokia Bell Labs **study** shows cost savings of over 65 percent compared to legacy approaches.

Nokia Oyj
Karakaari 7
02610 Espoo
Finland

CID: 211059 (February)

nokia.com

About Nokia

We create the critical networks and technologies to bring together the world's intelligence, across businesses, cities, supply chains and societies. With our commitment to innovation and technology leadership, driven by the award-winning Nokia Bell Labs, we deliver networks at the limits of science across mobile, infrastructure, cloud, and enabling technologies.

Adhering to the highest standards of integrity and security, we help build the capabilities we need for a more productive, sustainable and inclusive world. For our latest updates, please visit us online www.nokia.com and follow us on Twitter @nokia.