corero | JUNIPER NETWORKS

2023 DDOS THREAT INTELLIGENCE REPORT

CONTENTS

FOREWORD
FROM CORERO CTO

Welcome to the Corero 2023 Threat Intelligence Report, in which we share our insights on the evolving landscape of distributed denial of service (DDoS) attacks over the past year. Our Threat Intelligence team, comprising experienced security engineers and analysts working at the forefront of DDoS defense, has compiled the data and observations here from attacks against Corero customers between January and December of 2022 and compared them with our data from previous years.

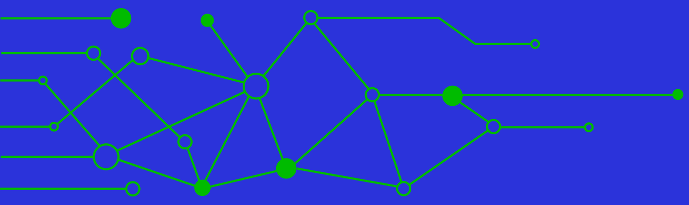
As we progress through 2023, we are witnessing continuing significant changes in the global DDoS attack landscape. Corero has once again detected an increase in the overall volume of attacks, as well as variations in their nature, with attackers employing increasingly potent and intricate tactics with increasing frequency.

DDoS attacks aim to incapacitate online services by inundating them with traffic from multiple sources, typically through botnets and reflection-amplification techniques, to consume available bandwidth and paralyze internet communication. DDoS attacks target both service and network availability, leading to downtime and internet disruption, and to the potential loss of revenue, business continuity, customer loyalty, and brand trust.

While traditional bandwidth-oriented DDoS attacks typically employ packets of larger sizes, our observations indicate that an increasing percentage of recent attacks are employing smaller-sized packets, aiming to overwhelm a victim's transactional processing rate. In general, attackers are deploying ever-increasing packets-per-second rates in their attacks, highlighting the critical need for robust packet rate DDoS protection for the service and hosting providers who maintain customer internet availability. At the same time, customer tolerance for internet service outages and response times has become much more demanding, with expectations now measured in seconds and not minutes.

One of the most concerning developments in DDoS attacks during 2022 has been the measurable rise of 'carpet bomb' attacks, posing a significant new threat. By launching multiple small attacks across a wide address space, carpet bomb attacks can evade, neutralize, or overload traditional victim-oriented detect-and-redirect DDoS protections. Our report offers a perspective of the triple threat posed by the rise of this new vector as well as several other emerging and evolving DDoS threats.

In conclusion, our key takeaway is that DDoS protection continues to be a multifaceted challenge. No single point of DDoS detection or mitigation appears resilient to today's complex vectors. Effective DDoS protection will increasingly require the coordination of multiple detection and mitigation locations including upstream, edge, core, inline, and out-of-band. Corero continues to lead the industry in automatic DDoS protection, and we hope this threat report will help companies better understand and respond to the myriad threats facing us in 2023 and beyond.



ASHLEY STEPHENSON
CTO, Corero Network Security

EXECUTIVE SUMMARY _

We recommend that companies employ advanced, holistic detection and protection to combat the rising risk of carpet bomb attacks. We also recommend flexible protection that can adapt to the ever-changing DDoS landscape to help organizations maintain their business continuity and protect against future threats.

DDoS threats continue to grow in both volume and sophistication. Over the past year, Corero's customers have seen a significant increase in certain kinds of attacks.

- Carpet bomb attacks have increased by 300%, creating a triple threat. These attacks can evade detection, neutralize security techniques, and overload system capacity.
- Mirai-like DDoS attacks have also increased significantly, with over seven times as many attacks in 2022 than 2021.
- Although the IPv6 landscape remains somewhat murky, it's clear that we're seeing a major rise in the share of malicious DDoS traffic carried by this protocol, to the tune of 600%.
- While the UDP protocol has long been the major DDoS attack vector, our team has observed a 70% increase in TCP-based vectors. This growth of malicious TCP traffic presents new problems in detecting and mitigating threats.
- Although directed DNS traffic represents a smaller percentage of overall attacks, it is growing at a faster rate, doubling from 2020 to 2022.

75%
DDOS ATTACKS LAST LESS THAN 10 MINUTES

25%
INCREASE IN HIGH PACKET RATE DDOS ATTACKS

300%
INCREASE IN CARPET BOMB DDOS ATTACKS

60%
INCREASE IN DDOS ATTACKS LASTING OVER 60 MINUTES

27%
LIKELIHOOD OF A REPEAT ATTACK IN SAME WEEK

98%
DDOS ATTACKS LESS THAN 10 GBPS

SECTION 1: KEY FINDINGS _

2023

Another year of DDoS evolution has delivered another batch of new or resurgent attack vectors that must be addressed with enhanced detection and protection solutions. In reviewing the key findings of our 2022 Threat Intelligence research, it is worth highlighting the following immediate threats to network and service uptime.

CARPET BOMB ATTACKS

Legacy DDoS protection solutions may fail to correctly detect and identify carpet bomb attacks, and they may lack protection techniques to effectively block malicious traffic without false positives. In addition, legacy solutions are likely to suffer operational or reporting overloads as a result of the large number of victim IP addresses involved.

NEW MIRAI-LIKE BOTNETS

Because they leverage derivative or enhanced Mirai-like attack libraries, these new generations of botnets do not exclusively rely on pwned or compromised IoT devices or vulnerable weak-security stack systems. It seems likely that many are now based upon paid-for higher performance hosting resources. The falling cost and widespread availability of pay-to-play distributed computing platforms appears to justify the cybercrime economics of buying weapons.

DNS SERVICE ABUSE

The prevalence of readily available DNS brute force tools, originally developed to explore the publicly visible DNS infrastructure for exploitable vulnerabilities, appears to have contributed to the increase in excessive query rate abuse that many authoritative DNS services are reporting. If these DNS services are not well configured or resourced, this can result in greatly degraded performance or outages – and ultimately a denial of service for legitimate DNS query resolution.

ONGOING TRENDS

Other important trends that we will continue to monitor in 2023 include the increase in malicious IPv6 traffic and the increase in TCP-based DDoS traffic.

While these vectors are not currently contributing to a significant number of downtime events or DDoS incidents, they are becoming more frequent. This growth indicates that we should anticipate a more challenging future environment for TCP and IPv6 communication over the internet.

SECTION 2:
THE GROWING DANGER OF ‘CARPET BOMB’ ATTACKS

So-called ‘carpet bomb’ attacks distribute traffic across a large number of targets rather than a more easily identifiable single target. Also known as spread-spectrum or spray attacks, their approach challenges standard victim-oriented detection, mitigation, and alert techniques.

While carpet bomb DDoS attacks were observed in 2020 and 2021, this vector was still relatively uncommon. However, the Corero Threat Intelligence team had observed a significant increase of up to 300% during 2022. Carpet bomb attacks are difficult to defend against, stymying many of the traditional detect-and-redirect DDoS mitigation techniques. Victims face a triple threat because of the attack’s ability to:

1. EVADE

Avoiding detection and isolation by flying under the radar of per-destination IP traffic analysis techniques or thresholds.

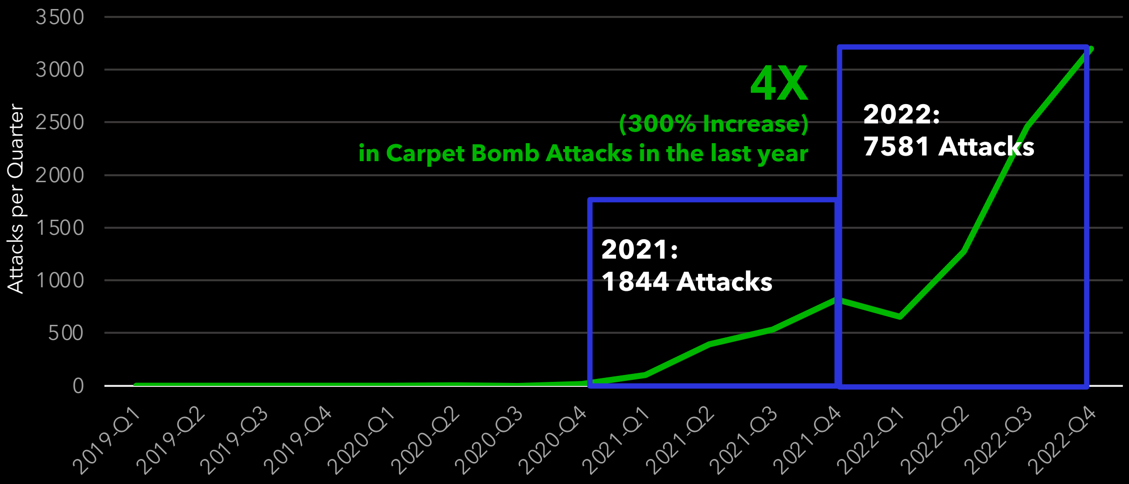
2. NEUTRALIZE

Invalidating the practical use of ‘black hole’ or null routes techniques for the avoidance of link saturation or collateral damage.

3. OVERLOAD

Exceeding scrubbing lane capacity, straining cloud redirection budgets, or confusing alerting and reporting systems, due to the way they present as many simultaneous attacks targeting large numbers of victims.

GROWTH IN CARPET BOMB ATTACKS TREND



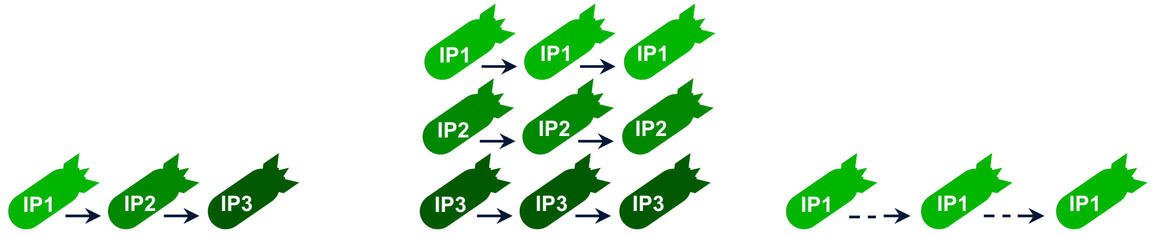
Carpet Bomb Attacks Explained

Carpet bombing, as the name suggests, is characterized by spreading indiscriminate attacks over a wide area rather than concentrated attacks on specific targets. The analogy in DDoS results in malicious attack traffic being distributed over a large destination IP address space. From a DDoS perspective, this results in simultaneous lower volume packet floods spread over multiple destination IP addresses.

In DDoS carpet bombing, the IP addresses are all chosen to target the network where the victim resides. Within this victim network, the small attacks will still add up to the level of a significant volumetric attack and can cause disruption.

As there are no absolute or definitive criteria for what qualifies as a carpet bomb attack, there is a potential overlap with rotating address pulse attacks and aggressive address space scans, which also exhibit a wide range of target addresses. These techniques are also becoming more common and may sometimes be confused or conflated with true carpet bomb vectors.

CARPET BOMBING TECHNIQUES INCLUDE SPRAYS, SPREAD-SPECTRUM, PULSED AND SCAN ATTACKS.
Includes Sprays, Spread-Spectrum, Pulsed, Scans, and more. Presents detection and mitigation challenges.



SPRAYS:
- Attack traffic volumes directed at sequential IP address (full rate to each IP – moving target)
- Can also be aggressive scans/reflections

SPREAD-SPECTRUM:
- Attack traffic volumes divided across many IP address at once (small rate to reach IP – rate dilution)

PULSED:
- Periodic or intermittent attack, repeating on some duty cycle

The Carpet Bomb Triple Threat, Part 1: EVADING DETECTION

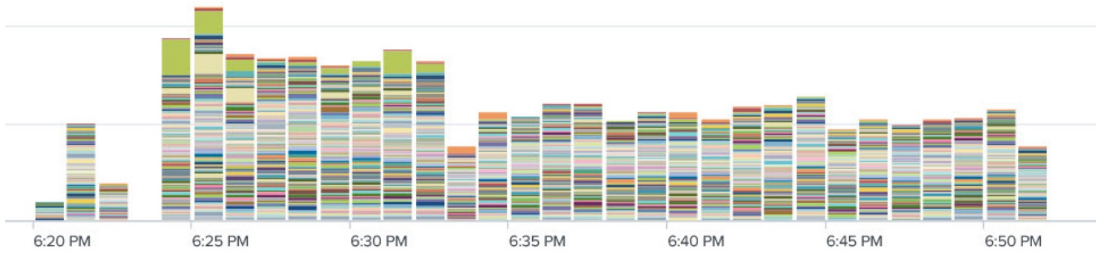
Many DDoS detection mechanisms incorporate either configured or learned thresholds. These thresholds define the amount of acceptable traffic to an individual destination IP address and are used to identify anomalies. Setting acceptable traffic thresholds too low can result in false positives, in which legitimate traffic may be unnecessarily mistaken for an attack and redirected to scrubbing systems or the cloud for mitigation.

Other DDoS detection mechanisms use alternate attributes of the traffic destined for a specific IP address to determine if it is malicious, often using known attributes of the protected target to minimize the threat surface or track behavior.

By spreading a DDoS attack over 100 or more destination IP addresses, the carpet bomb technique seeks to evade, avoid, or confuse the detection mechanisms associated with each of the individual IP addresses being targeted. Even if a few of the destination IP addresses trigger and register an anomaly, the vast majority of the malicious traffic flowing to all the other IP addresses will get through. We believe this provides a stealth advantage to carpet bomb attacks not only on the victim network but also on the intermediate provider networks that are transporting the DDoS traffic from the many remote attackers. Less intermediate detection and mitigation means that more DDoS traffic ultimately reaches its intended destination.

The figure below shows a carpet bomb DDoS attack targeting multiple victim IP addresses in a single minute. This indiscriminate attack contrasts with normal DDoS attacks, which generally attack a single IP address.

GRAPH DETAILING A 30-MINUTE CARPET BOMB ATTACK, SHOWING NUMBER OF VICTIM IPS (BY COLOR) PER MINUTE



Note: Multiple victims being attacked in a single minute with arrows pointing to the columns.

Carpet Bomb Attacks Explained (cont.)

The Carpet Bomb Triple Threat, Part 2: NEUTRALIZING MITIGATION

Since the early days of DDoS attacks, the most common mitigation tool of last resort has been the null route or black-hole. The black-hole technique is still widely used today by many providers or businesses when they have no other options at their disposal.

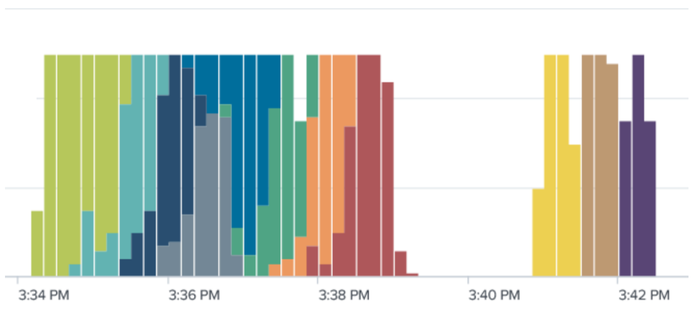
In scenarios where a DDoS victim is attracting large amounts of unwanted attack traffic to a network or service, the service provider or business has the option to sacrifice the DDoS victim for the greater good by requesting a null route or route-to-nowhere for the victim's traffic. All traffic sent to the null route is dropped and never seen again on the network, hence the term 'black-hole'. The decision to null route a victim IP address does prevent collateral damage to the rest of the network and customer base, but it effectively completes the denial of service of the victim by also sending all their legitimate traffic to the black hole.

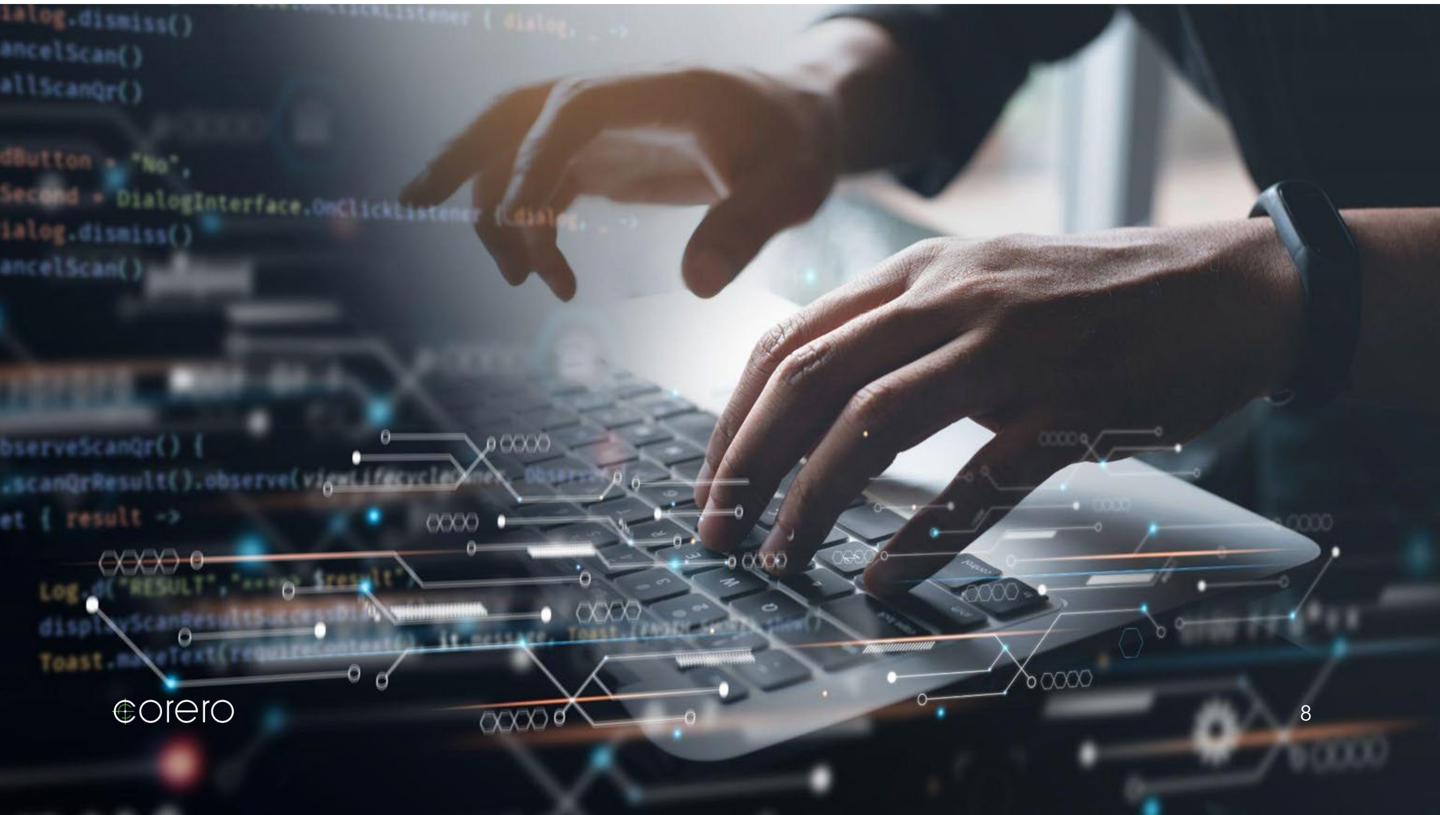
The carpet bomb attack neutralizes this last-resort technique by making it impossible to identify an individual DDoS victim IP address to sacrifice. With carpet bomb attacks, there are many proxy victims spread across the attacked IP space. In the simplest carpet bomb attacks, the attacker will visit every single IP address of the target subnet containing the true victim. In more complex carpet bomb vectors, the attacker may have researched all the IP addresses associated with the victim network and will expand the target range accordingly. If the service provider were to try and black-hole all the IP addresses being attacked, it would result in the sacrifice of legitimate traffic to all customers represented by the attacked IP space, effectively taking the service provider offline.

.

CARPET BOMB ATTACK SWEEPING ACROSS VICTIM SUBNETS (BY COLOR) EACH WITH 100S OF IP ADDRESSES]

The figure on right shows a carpet bomb attack sweeping across target subnets. Each colour represents 100s of victims. This attack occurs in overlapping waves, spreading across the entire network that is hosting the victim. It is indiscriminate.





Carpet Bomb Attacks Explained (cont.)

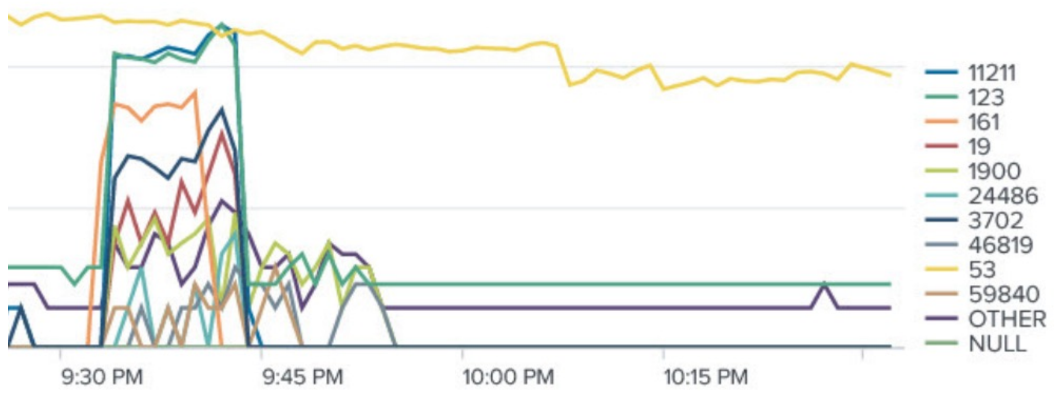
The Carpet Bomb Triple Threat, Part 3: OVERLOADING SYSTEMS

DDoS attacks inherently originate from many potential sources, hence the "distributed" in distributed denial of service. The primary motivation is to boost the size or effectiveness of the attack by combining the power of many distributed smaller attackers, focusing them on the IP address of a single victim.

In a clever twist, a carpet bomb attack seeks to expand the target beyond the single IP address of the victim to a range of IP addresses that share the same network provider or data center as the victim. This has the potential to trigger several diverse overload situations.

From our analysis, we believe that some DDoS reflection/amplification resources (aka DDoS attack weapons) are able to transmit more attack traffic when requested, to spray it across multiple destination IP addresses. There are a few possible explanations for this behavior. First, RSS technology enhances server performance in a way that may benefit carpet bombing. Second, IP-based request rate throttles will only work to limit the number of requests from a single IP address, meaning that they do not limit the effect of carpet bombing. We believe that both explanations may be contributing to the noticeably higher reflection/amplification bandwidths that we see in many carpet bomb attacks.

MULTIPLE UDP REFLECTION VECTORS BY SOURCE PORT IN A 15 MINUTE CARPET BOMB ATTACK



This diagram shows: a carpet bomb attack occurring over a 15-minute period. DDoS protection is designed to spot an attack, mitigate it, and stop it; however, a carpet bomb confuses and overloads the reporting & DDOS alerting system.

This shows the variety of different reflection vectors that occurred during a 15-minute attack.

Protecting large ranges of IP addresses exposes DDoS mitigation mechanisms to much greater levels of legitimate traffic. Instead of having to process the legitimate traffic of a single victim IP without false positives, DDoS systems dealing with a carpet bomb vector may have to simultaneously process and accurately protect the legitimate traffic of hundreds or even thousands of IP addresses that are under attack. This potential thousand-fold increase in the level of required context tracking can cause the overload or wash-out of traditional systems that treat each IP address as a discrete victim.

In addition, DDoS mitigation mechanisms that have been designed to redirect IP addresses under attack to on-network scrubbing centers or cloud mitigation solutions do not scale well for carpet bomb attacks. If the carpet bomb attack is hitting the entire address space of the provider, then these mitigation systems would attempt to redirect the entire incoming traffic load to the scrubbing center or cloud mitigation solution. These solutions cannot be economically scaled for this level of traffic redirect, resulting in overload.

The operational side of many DDoS protection solutions are similarly oriented to single-victim IP attacks, often with the ability to track only a few dozen attacks at once. The nature of carpet bomb attacks can make traditional systems interpret the incoming traffic as hundreds or thousands of attacks. This can result in an overload of attack reporting and analysis mechanisms, along with potential alert or email storms. Other side effects may include crowded dashboards, confused summaries, and a general drowning out of important information due to the volume of redundant reporting.

SECTION 3:
2023 AND BEYOND: ADDITIONAL THREATS

LANDSCAPE 2023

The online threat landscape continues to evolve quickly, with attackers launching more sophisticated and coordinated DDoS attacks every year.

We’ve observed four other noteworthy and ongoing DDoS trends from the past year:

- More Mirai-like, botnet-originated DDoS attacks
- An increasing share of IPv6 DDoS attacks
- A shift toward TCP DDoS attack vectors
- A rise in DNS attacks: DDoS attacks targeting DNS ports or services

640%
INCREASE IN MIRAI-LIKE BOTNET ATTACKS

500%
INCREASE IN THE SHARE OF IPV6 BASED DDOS ATTACKS

70%
INCREASE IN THE SHARE OF TCP-BASED DDOS ATTACKS

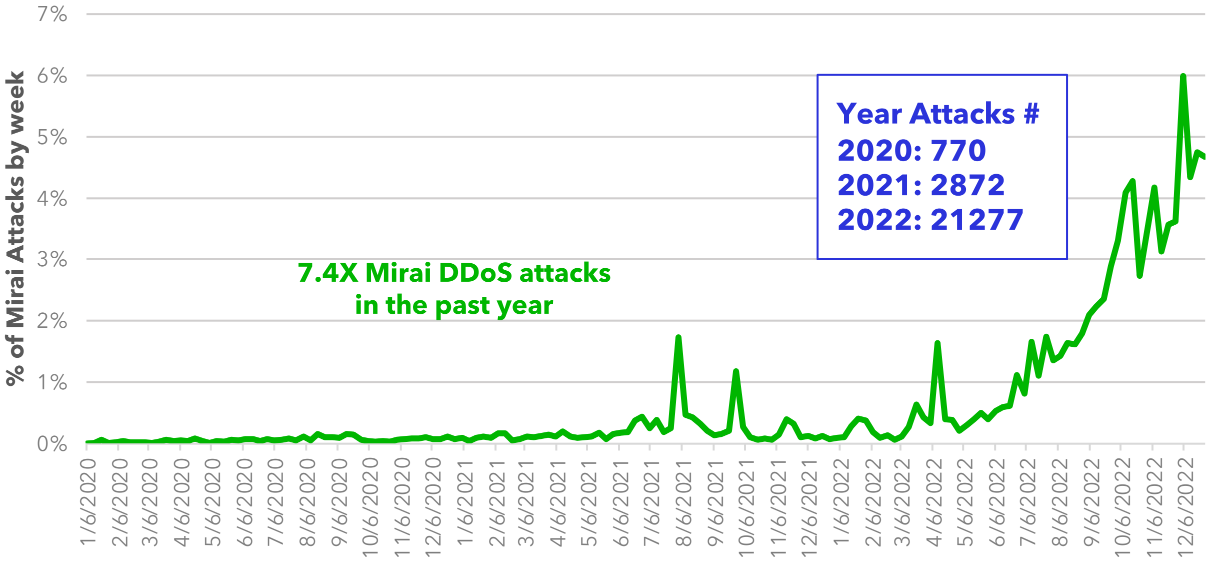
We’ll describe each of these trends in more detail below.

What Lies Ahead:
More Mirai-like Botnet Originated DDoS Attacks

In 2022, the Corero Threat Intelligence team had observed a significant resurgence of Mirai-like botnet attacks. These attacks had been characterized by patterns or profiles of malicious traffic that allowed us to identify with a high degree of confidence that their source was a botnet based upon Mirai or a variant that was leveraging the Mirai attack library.

It is now more than six years since Mirai DDoS attacks hit the headlines and details of the Mirai botnet were first widely disclosed. In the intervening period, the industry has tracked the emergence of many Mirai family variants with enhancements to command and control, viral propagation methods, and attack libraries. For these reasons, we expect to continue to see the extended Mirai-based family of botnets deployed as a potent DDoS weapon in the years ahead. With the threat landscape constantly evolving, solutions that deliver zero-day protection continue to be the best form of defense.

MIRAI ATTACK VECTOR GROWTH TREND



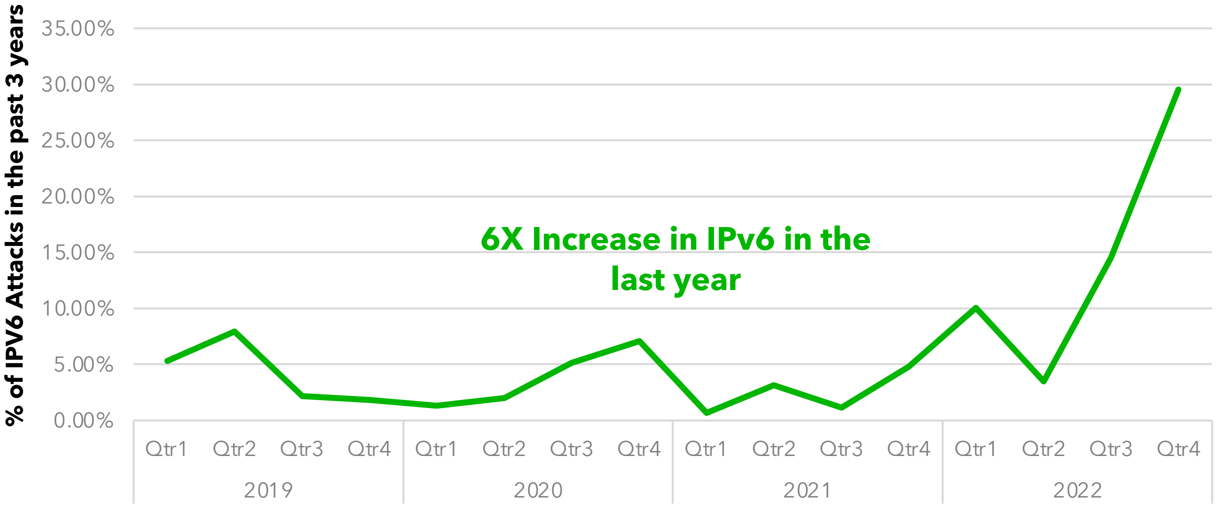
What Lies Ahead:
An Increasing Share of IPv6 DDoS Attacks

It is challenging to get a clear picture of current IPv6 protocol use on the Internet. A wide range of IPv6 growth statistics are commonly quoted, including the number of IPv6 capable users, the number of advertised IPv6 routes, the percentage of IPv6-accessible leading services, and the percentage of websites offering IPv6 access.

From the perspective of DDoS, it is very clear that IPv4 remains the dominant protocol. The majority of traffic traversing the internet is still IPv4, and the majority of victims present themselves to the Internet via IPv4. Perhaps most importantly, the vast majority of DDoS weapons and vulnerabilities are still based upon IPv4, with the most common examples being the widely used reflection and amplification vectors. For these reasons, the protocol of choice for DDoS attacks is still IPv4.

Despite the prevalence of IPv4, the Corero Threat Intelligence team has observed a notable 600% increase in the share of malicious DDoS traffic carried by the IPv6 protocol during 2022. This upward trend is expected to continue in the coming years as attackers focus more attention on leveraging exploitable IPv6 services and targeting IPv6 victims on the internet. In some cases, this approach will also multiply the number of discrete attack types used in multi-vector IPv4/IPv6 attacks and correspondingly impact the number of potential traffic redirections or mitigations associated with a specific DDoS incident or campaign.

IPV6 DDOS ATTACK TREND



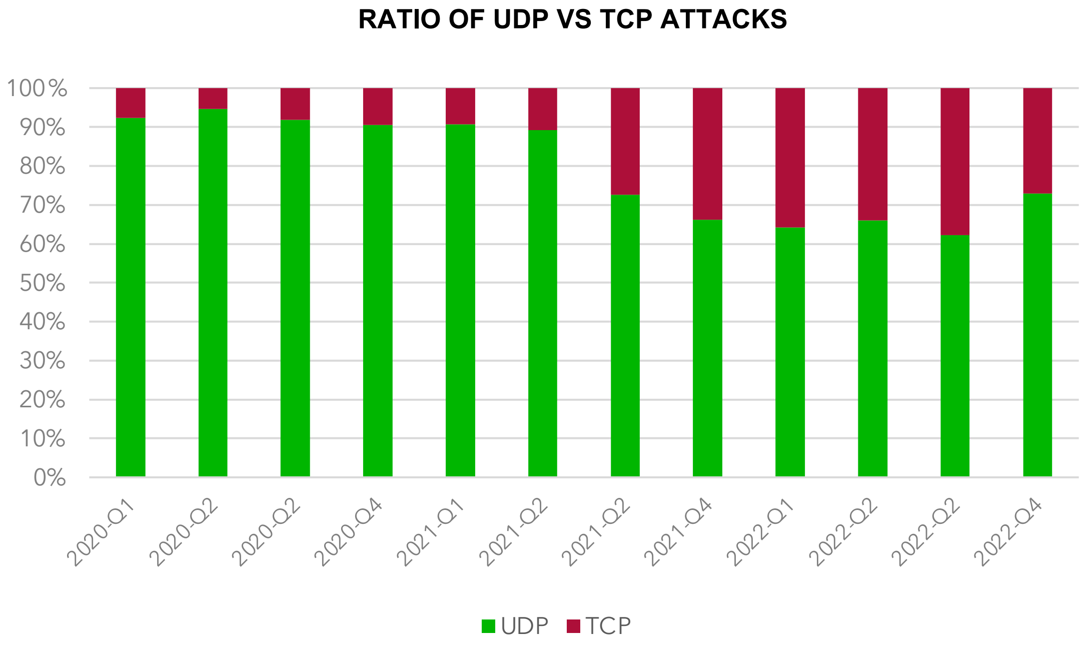
What Lies Ahead:
A shift toward TCP DDoS attack vectors

The Corero Threat Intelligence team had observed continued growth in the number of TCP attacks, both in overall numbers and as a share of all DDoS attacks. These were attacks carried out via the Transmission Control Protocol (TCP), the most common and reliable networking protocol online.

This was a change from the past, when the vast majority of DDoS attacks were dominated by malicious traffic carried by the User Datagram Protocol (UDP). The use of UDP has been historically attributed to both the prevalence of exploitable UDP-based reflection and amplification hosts and the ease of leveraging these vectors using source-spoofing attack initiation botnets. For these same reasons, UDP vectors also featured prominently in dark web DDoS-for-hire services, also known as booters and stressers.

Data compiled by the Corero Threat Intelligence team and shown in figure 8 confirms a significant 70% increase in the percentage of successfully detected and mitigated DDoS attacks using TCP-based vectors. Speaking generally, TCP-based DDoS vectors can be harder to detect and mitigate without false positives due to the connection-oriented nature of many TCP services. TCP DDoS vectors are also more likely to penetrate simplistic but prudent static ACL (access control list) or firewall protection policies, such as blocking all UDP traffic to TCP-based services.

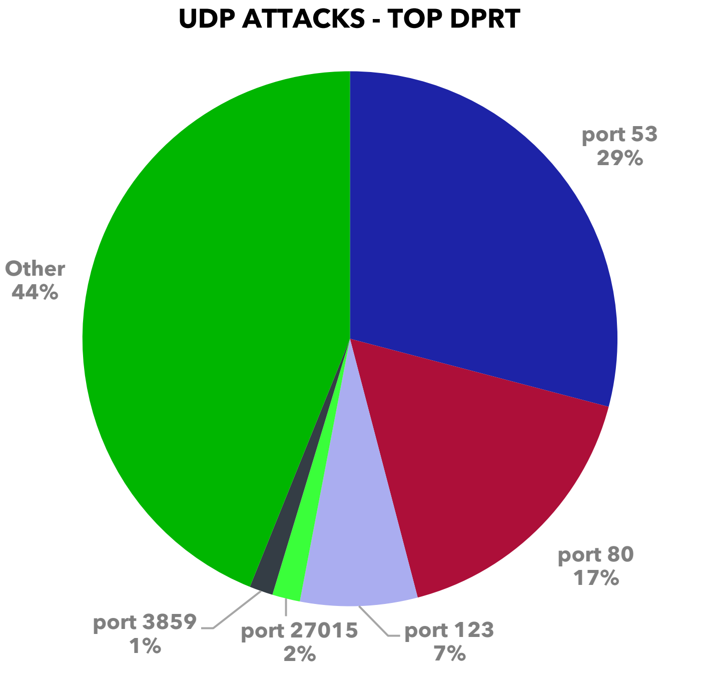
RATIO OF UDP-BASED TO TCP-BASED ATTACKS. THIS SHOWS THE GROWTH IN SHARE OF TCP BASED ATTACKS.



What Lies Ahead:
A shift toward TCP DDoS attack vectors (cont.)

A further analysis of the top destination ports used by UDP DDoS vectors illustrates some of the challenges of managing the UDP DDoS attack surface. More than 50% of the malicious DDoS traffic is arriving for destination ports 53 (DNS), port 80 (Web/QUIC), and port 123 (NTP). This is problematic, as many firewalls leave these exact ports open in order to support the correct operation of important internet services like DNS (Domain Name Service), web servers, and NTP (Network Time Protocol). So, while DDoS attackers are not attacking DNS, web, or NTP, they are still using these ports as entry points because they are left open for those legitimate services. (Note that we are not referencing the source port of reflection or amplification attacks, as that traffic is generated by exploiting these very same services.)

DISTRIBUTION OF DESTINATION PORTS (DPRT) OBSERVED IN UDP-BASED ATTACK VECTORS

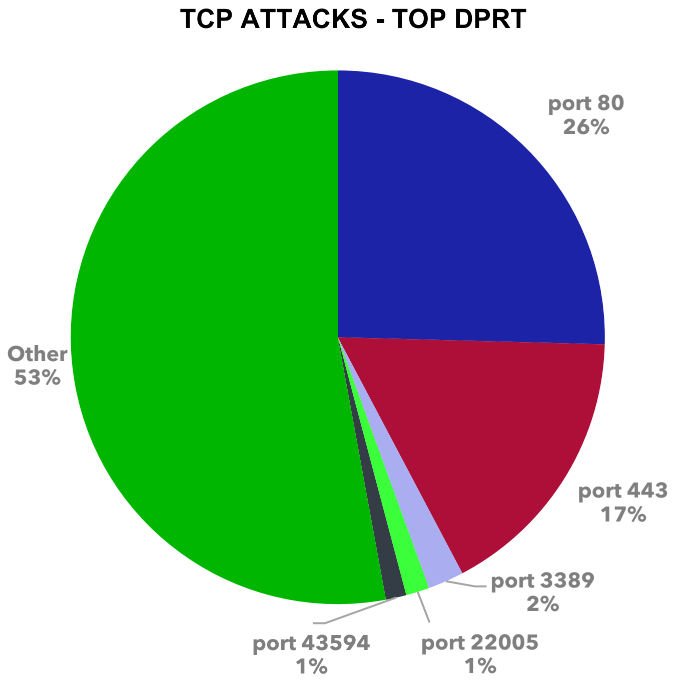


It is not possible to pinpoint the precise reason for the choice of these destination ports. But, based upon a mapping of the target ports on the intended victim IP/system, our analysis suggests that it is not primarily to attack these specific DNS, web, or NTP-based services. Instead, we believe that these ports are chosen for the access they provide for malicious traffic to enter the network via open ACL/firewall rules. Similarly, Another possible reason attackers choose these ports is because DDoS traffic riding along with legitimate traffic on the same protocol and destination ports requires more sophisticated protection to avoid false positives. Elsewhere in the distribution, there are ports that are more likely to be directed targets, such as port 27015 targeting the online gaming Steam client.

What Lies Ahead:
A shift toward TCP DDoS attack vectors (cont.)

In contrast, the top destination ports used in TCP DDoS vectors focus on ports often open for TCP-based services. The data in figure 10 suggests significant generalized targeting of ports 80 and 443 along with port 3389 (Microsoft RDP) and likely directed targeting of port 22005 (online gaming – RAGE).

DISTRIBUTION OF DESTINATION PORTS (DPRT) OBSERVED IN TCP-BASED ATTACK VECTORS



In analyzing both UDP and TCP attack vector traffic, it is notable that close to half of all malicious packets are distributed indiscriminately across a wide range of destination ports. In contrast to the specific top destination ports previously discussed, this malicious DDoS traffic would most likely overlap with legitimate inbound responses to ephemeral port ranges used by generic outgoing requests from the network or service under attack. Examples of legitimate ephemeral port traffic might include outbound DNS requests (UDP) or outbound SYN requests (TCP) from users on the victim network.

Because this kind of legitimate traffic overlaps with malicious DDoS traffic, organizations cannot respond by simply blocking all traffic. Better detection strategies are needed in order to block attacks more accurately.

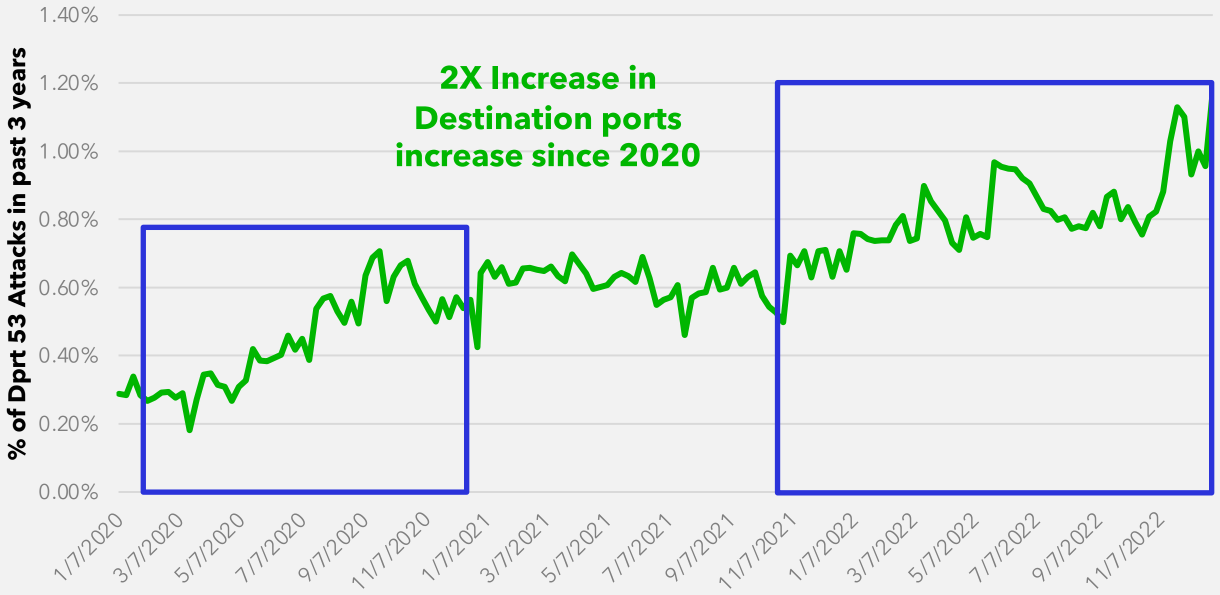
What Lies Ahead:
A rise in DNS attacks

Our general analysis of malicious UDP traffic indicated a significant but stable portion (29%) directed at UDP port 53. We can also analyze the same traffic for directed DNS attacks. While this directed DNS traffic represents a smaller percentage of overall attacks, it is growing at a more significant rate. According to our analysis, 2022 DNS attacks show a 100% increase over the previous two-year period.

IN 2023, WE ARE SEEING AN EVEN GREATER INCREASE OF DIRECTED DNS TRAFFIC IN THE FORM OF ATTACKS, ABUSE, AND VULNERABILITY SCANS. THE VARIOUS MALICIOUS DNS VECTORS BEING OBSERVED TYPICALLY FALL INTO ONE OF FOUR CATEGORIES:

- **DNS NX (non-existent subdomain lookups)**
- **DNS water torture (e.g. random subdomain)**
- **DNS query floods (direct or via resolvers)**
- **DNS vulnerability scans**

INCREASE IN DESTINATION PORT 53 DDOS ATTACKS TREND



SECTION 4: RECOMMENDATIONS

1

TO MITIGATE THE RISK FROM CARPET BOMB ATTACKS, ORGANIZATION SHOULD LOOK FOR ADVANCED, HOLISTIC DETECTION AND PROTECTION.

The double-sided distribution of source and destination of IP addresses of carpet bomb attacks makes them extremely difficult to detect and mitigate, as they were designed to circumvent legacy DDoS detection and mitigation capabilities by their very nature. Their signature characteristics of evading, neutralizing, and overloading legacy detect-and-redirect solutions to render them ineffective.

To counter carpet bomb attacks, we recommend a DDoS solution that is capable of viewing IP address space holistically to detect, mitigate and report on this malicious behavior and that also provides protection in seconds versus minutes. Advanced detection is imperative in preventing downtime from carpet bomb attacks, and many legacy approaches may never detect the attack, let alone provide immediate protection. Companies should therefore seek solutions that can shrink the detection-to-protection timeline to seconds.

2

EVALUATING DDOS PROTECTION VENDORS: HOW TO ENSURE COMPREHENSIVE, FLEXIBLE PROTECTION.

DDoS attacks remain a persistent threat, with cyber criminals continuing to utilize them due to their ease of deployment and effectiveness. Our research shows that attackers are continuing to evolve their techniques to evade legacy technologies. For internet service providers, hosting providers, and SaaS providers, ensuring service availability is critical to maintaining customer loyalty. As such, having a reliable and evolving DDoS protection solution is essential.

When evaluating potential DDoS protection vendors, organizations should consider the following:

- A modular platform with suitable protection for their specific requirements.
- A flexible deployment model with hardware, virtual, and integrated options to align with their architecture.
- Protection that extends beyond brute force mitigation to eliminate any impact on their business or their customers' businesses.
- Optional managed service offerings to supplement their existing staff or expertise.

Effective DDoS protection requires a solution that detects and adapts to new and emerging attack vectors as soon as they are discovered. This approach minimizes the risk of downtime and business disruption.

SUMMARY

2022 DDOS TRENDS

75%
DDOS ATTACKS LAST LESS THAN 10 MINUTES

25%
INCREASE IN HIGH PACKET RATE DDOS ATTACKS

300%
INCREASE IN CARPET BOMB DDOS ATTACKS

60%
INCREASE IN DDOS ATTACKS LASTING OVER 60 MINUTES

27%
LIKELIHOOD OF A REPEAT ATTACK IN SAME WEEK

98%
DDOS ATTACKS LESS THAN 10 GBPS

ABOUT CORERO NETWORK SECURITY

Corero Network Security is a leading provider of distributed denial of service (DDoS) protection solutions. We are specialists in automatic detection and protection solutions, that include network visibility, analytics, and reporting tools. Corero's technology provides scalable protection capabilities against both external DDoS attackers and internal DDoS threats, in even the most complex edge and subscriber environments, ensuring internet service availability and uptime. Corero's key operational centers are in Marlborough, Massachusetts, USA, and Edinburgh, UK, with the Company's headquarters in London, UK. The Company is listed on the London Stock Exchange's AIM market under the ticker CNS.

For more information, visit www.corero.com, and follow us on [LinkedIn]() and [Twitter]().