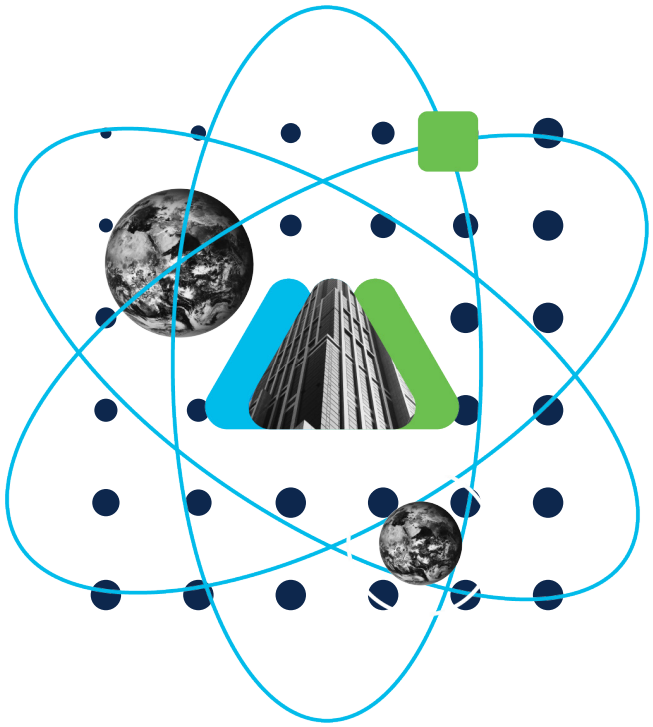
CISCO
SECURE

White paper
Cisco public

Cybersecurity Alert

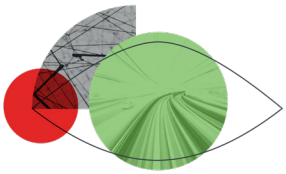
The Continued Evolution of DDoS Attack Vectors



January 2021

Developed in conjunction with our partners at Radware

Contents



DDoS-for-Hire threat landscape continues to grow

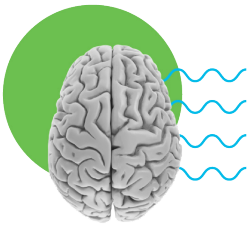
OVER THE LAST TWO YEARS, CORPORATIONS, INDEPENDENT RESEARCHERS, AND LAW ENFORCEMENT AGENCIES AROUND THE WORLD HAVE ATTEMPTED TO CURB THE GROWTH OF THE DDOS-FOR-HIRE INDUSTRY THROUGH A SERIES OF TAKEDOWNS AND ARRESTS. DESPITE GLOBAL EFFORTS, THE ILLICIT INDUSTRY CONTINUES TO GROW, UTILIZING NEW ATTACK VECTORS AND PRODUCING LARGE-SCALE, RECORD-BREAKING DDOS ATTACKS.

Arrests and takedowns have little impact

Traditionally, takedowns and arrests are effective forms of control over criminal activity. They serve as an applicable way to remove known threats and send a clear message to criminal operators. The problem is that the booter and stresser industry is complicated, dynamic, and a profitable venture for cybercriminals. If you remove one threat, dozens of other criminals will seize the opportunity to fill the void.

For example, over the last two years we have seen several notable takedowns related to botnet activity. At the end of 2018, the **FBI seized the domains of 15 booter services** that were known to represent some of the world's leading DDoS-for-hire services. In October 2019, Dutch police **seized servers from bulletproof hosting provider K.V. Solutions.** These servers where known to be malicious, hosting several command-and-control servers for IoT botnets. In April 2020, Dutch police working with hosting services, registrars, the international police force, Europol, Interpol, and the FBI **took down another 15 unnamed booters.**

One would assume this would have put a noticeable dent in the overall booter and stresser industry. And while some have reported minor decreases in DDoS-related activity after the arrests and takedowns, overall, these actions were ineffective. In fact, in 2019, a white paper titled **DDoS Hide & Seek: On the Effectiveness of a Booter Service Takedown** reviewed the 2018 takedown by the FBI and determined that these activities led to a temporary reduction in attack traffic. Criminals were quick to replace those that have been removed.



The advertisement problem

Just like any other industry, legal or illegal, criminal booters must find a way to distinguish themselves and advertise their services. In the past, groups like Lizard Squad would engage in "stunt hacking." This involved launching large-scale DDoS attacks and using Twitter to post about the outage as a form of advertising.

Today, things are different. We no longer have notorious DDoS groups roaming social media or launching attacks. The landscape seems quiet, but that is not the case. Raging underground is a scene overpopulated with script amateurs looking to impress their friends, cause outages, and turn a profit.

One of the reasons for this growth is due to the accessibility of open source code used to build IoT botnets. The booter and stresser industry have grown so much that it has left law enforcement agencies around the world wondering how they can get a grip on a problem that is spiraling out of control. In the United Kingdom, Britain's National Crime Agency **(NCA) decided to advertise the legal consequences** of launching DDoS attacks through Google Ads.

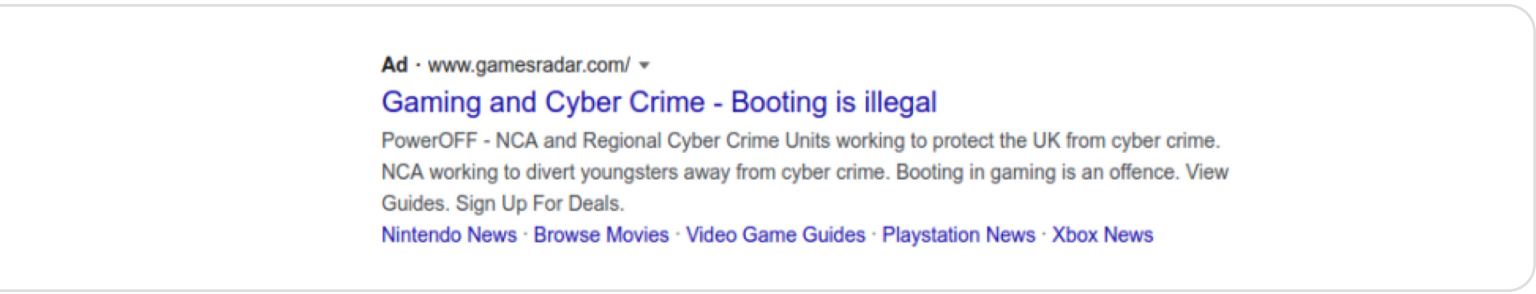


Figure 1. Google ad warning against DDoS services

Unfortunately, Google has become a common location for booter and stresser services. While DDoS is illegal, the law has not prevented search engine algorithms from indexing criminal websites. Even worse, there is nothing preventing cybercriminals from paying and using Google advertising to advertise their services. While the NCA tactic to create awareness was a noble one, the impact is minimal when the same service is used to advertise the illicit service that the NCA is trying to stop.

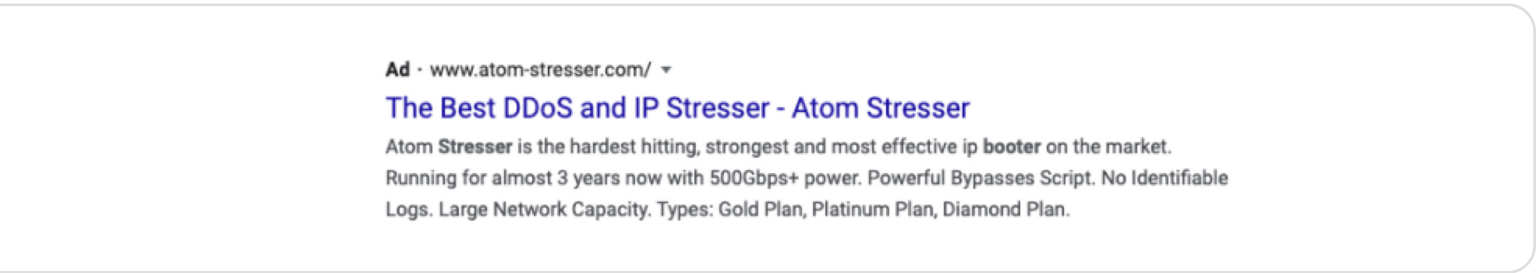


Figure 2. Google ad offering DDoS services

Front-Page problems

This is not just a problem for Google. All major search engines appear to index illegal booter and stresser services. Just a simple search will produce dozens of results that take you directly to the criminal services used to launch denial-of-service attacks for a fee. They also index videos about how the services work, demo attacks, or how to build your own.

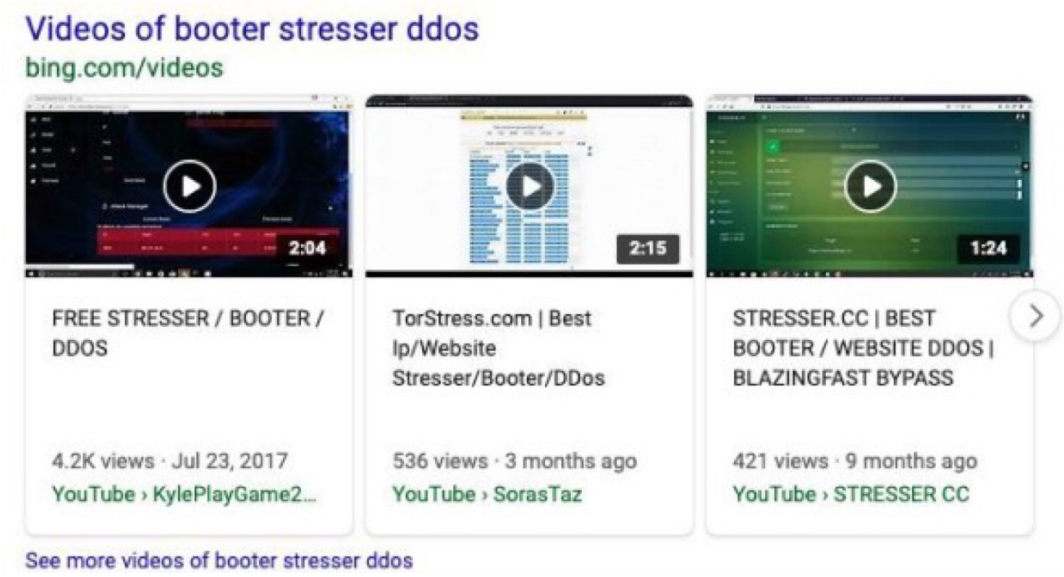


Figure 3. Booter videos on first search result page

One of the biggest problems about indexing illegal services is the perceived notion that the activity is in a legal gray zone. While most teenagers understand that DDoS is illegal, there is still a trove of resources and services readily available for them to abuse.

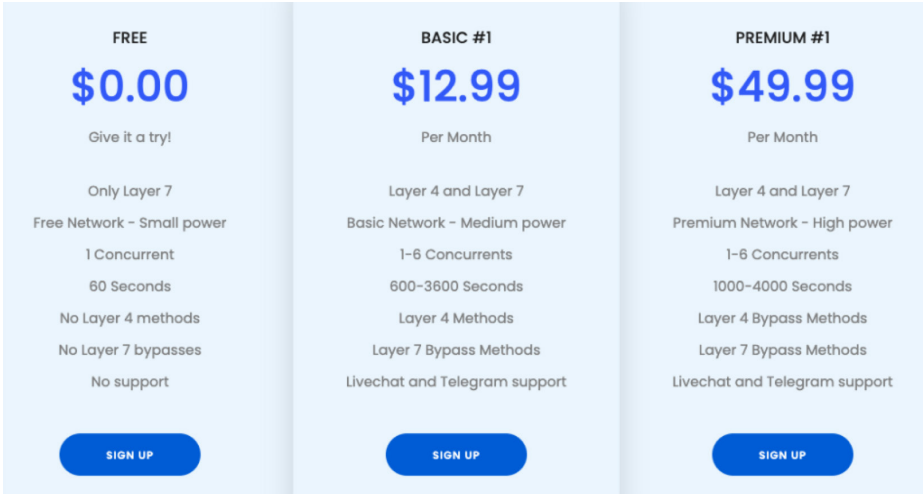


Figure 4. Stresser service offering

Potential pay-to-play criminals, after a quick scroll through any search engine, will typically find a stresser service with a similar offering. Nowhere on the websites can you find a warning that the service is illegal. Only on a few services will you find a Terms of Service (TOS) that attempts to shift legal responsibility to the user, ignoring the fact that the service likely leverages compromised devices.

To add to the confusion, these services also offer live chat and Telegram support for users that require assistance. Basic packages for DDoS-for-hire on the clearnet have remained relatively unchanged over the last 5 years. Basic packages still range between $9.99 and $19.99 a month. Paying for the service normally grants you access to the attack panel for 30 days, allowing you to launch limited timed attacks that range between 300 and 3600 seconds.

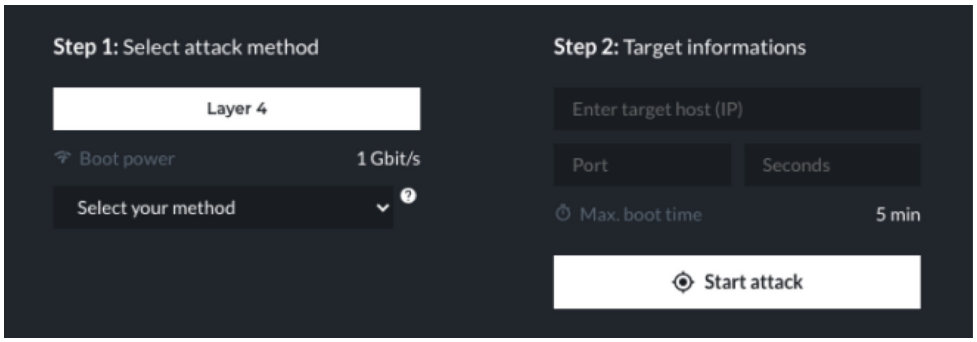


Figure 5. Stresser service attack panel

A **recent leak has** shown that some of these booter and stresser services offer custom monthly packages outside of API services for anywhere between $150 and $5000 a month, depending on the service level and target. The leaks also underscore how lucrative some of these services can be, allowing some criminals to generate around $1000 a week. In 2016, after arresting the operators of vDOS, it was reported that the **service generated an excess of $600,000** over two years.

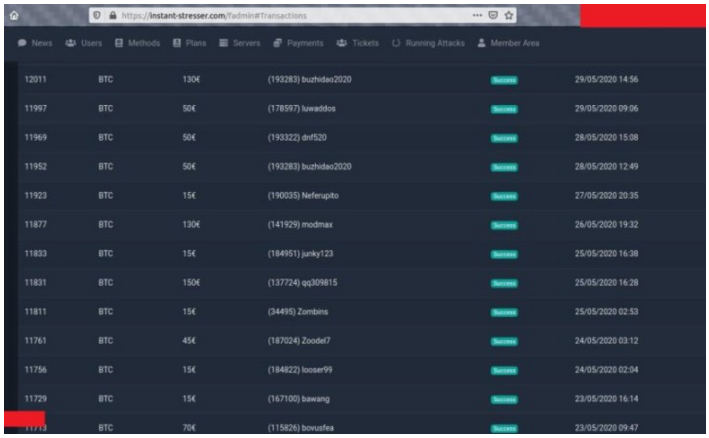


Figure 6. Leaked transaction information

Another growing concern are the new features that are being found inside the services. Not only do they have chat support to ensure you are launching the right attack, they also offer multi-factor authentication for their users and referral links so the user can make money as a reseller.

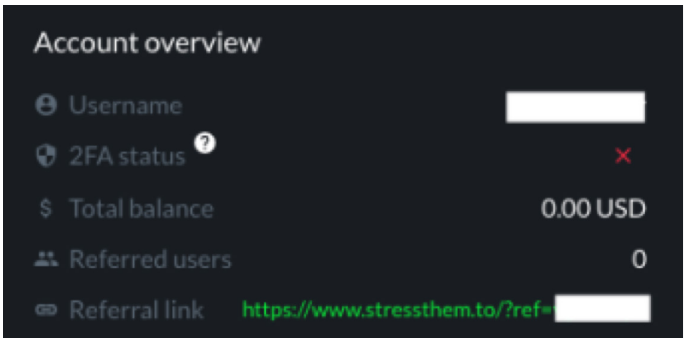


Figure 7. 2FA and referral link

Darknet marketplace and forum services

The past few years for darknet marketplaces have been rough. Between the takedowns by both law enforcement and vigilante hackers, there has not been a lot of stability on the network. While some sites on the Onion network have attempted to implement their own DDoS mitigation features, they have largely failed to protect their domains. As a result, there has been a noticeable impact on the darknet. Once a place to purchase source code and attack services, it is now largely dead with illegitimate or unverified offerings.

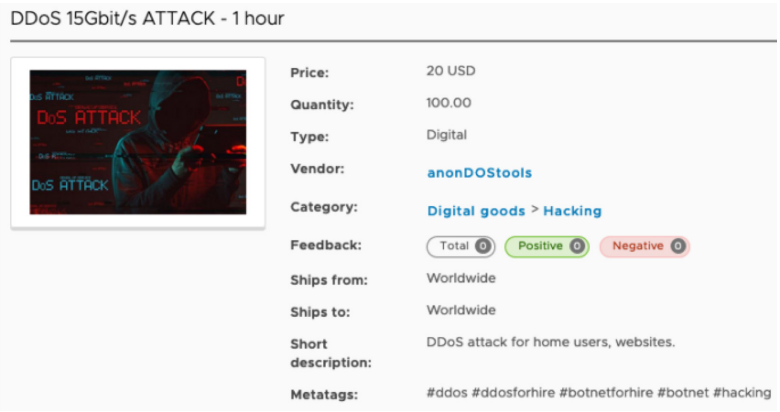


Figure 8. Darknet marketplace

The darknet forums, if they are up or if you can solve their impossible CAPTCHAs, have largely been abandoned. Most of the noticeable activity comes from websites that provide both a clearnet and a ‘Onion’ domain. Offerings found in the forums for DDoS attacks are generally sold by the hour, day, week, or month. A one-hour attack can cost up to $5 and is generally reserved for a sample attack. A 24-hour attack will

range between $25 and $35 a day, while a one-week attack can cost anywhere between $150 and $250. A persistent campaign that lasts 30 days could cost anywhere between $600 and $900 a month.

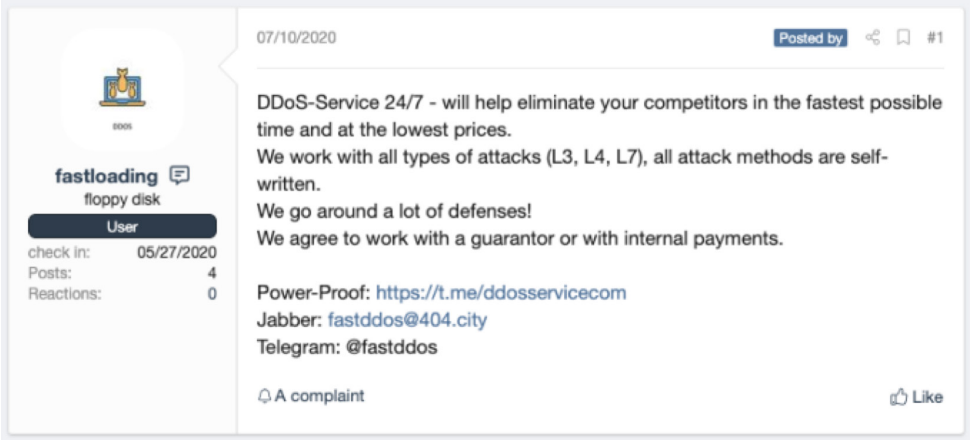


Figure 9. Criminal forum post offering DDoS services

One of the more interesting aspects of buying from a forum is the intended target. Some bot herders will charge a different rate depending on the tier of the target. There can be a significant price difference if your target is a popular stream versus an unprotected site. Packages for top-tier attacks sell for up to $1000 a day.

Instagram

Instagram is the new platform for the booter and stresser industry. The platform allows bot herders to advertise their illegal services by posting images of their botnets. In general, bot herders enjoy showing off their printed text and bot count as a form of advertisement. Regardless if they disclose sensitive information, they will still post images on Instagram for advertisement.

Figure 10. Virum botnet advertisement on Instagram

Prices for renting a botnet on Instagram are very low compared to underground forums. This is likely due to their low bot count and limited capabilities. Typically, you will find bot herders selling access for one-hour, one-day, and one-month periods. Most of those selling on Instagram will also sell lifetime packages, capping out at around $50. This is likely due to low bot counts and thus low attack power and no guarantee for future updates.

Some bot herders have gone as far as to add their Instagram or other handles into their bot malware binaries. Below is an example of a malware binary caught by Radware®'s deception network. Inside the binary data you can read "Botnet Made By @Ryanlpz9." Further review of the actor's account leads us to Greek.Helios' account and his reseller, @Thar3seller.

Figure 11. Instagram handle in malware binary

One of the more interesting aspects of the Instagram market is the ability to see the actions and platforms used by criminal actors. On Greek.Helios' page, you can find several videos of the actor demonstrating and launching denial-of-service attacks from a discord channel. Discord is the **modern incarnation** of a command-and-control platform, replacing the aging IRC platform as a service for a bot herder to control their bots from a central console.

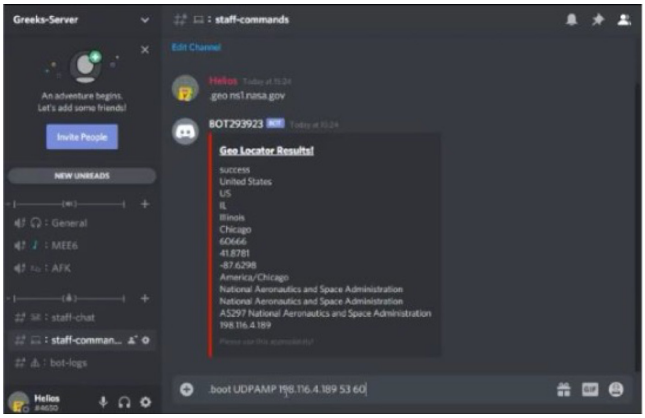


Figure 12. Discord as command-and-control server and console

New attack methods

Despite the takedowns and arrests, the industry is flooded with bot herders, and the reality is that it is very unlikely they will be arrested. Time and again, only top services are occasionally culled to send a message to other operators. The problem is that this message has no barring as the likelihood of getting arrested is slim.

Over the last two years of takedowns and arrests, the DDoS mitigation industry has seen six new attack vectors—so much for curbing the growth. Specifically, Memcached and TCP reflection attacks have been notable. In March 2019, a record-breaking 1.3-Tbps attack **abusing exposed Memcached servers** by exposing a protocol that was never intended to be exposed to the public was launched against GitHub. Just seven days later and **the attack vectors were seen quickly being added to booters and stressers.**

Even more recently, a malicious actor was able to abuse the TCP protocol to cause a **TCP Reflection attack.** In August 2019, researchers at Radware discovered this trend during a campaign targeting the financial services industry. These attacks were unique and evolved into a level of sophistication not previously seen from TCP reflection campaigns. This was due to a wrong assumption that TCP reflection attacks could not generate enough amplification in comparison to UDP-based reflection attacks. Attackers still explore the possibilities of a TCP reflection attack. Below is a short review of the most recent attack methods disclosed in the last few months.

Memcached

Memcached is a database caching system for speeding up websites and networks. A Memcached denial-of-service (DoS) attack leverages an exposed UDP service that provides massive amplification to overload a targeted victim with internet traffic, a volumetric attack. The attacker spoofs requests to an exposed UDP service on a Memcached server with the IP address of its victim. The UDP service accepts any requests and responds to the victim with a very large response without verifying the origin of the request, potentially overwhelming a victim's resources. While the target's internet infrastructure is overloaded, new requests cannot be processed and regular traffic is unable to access the resource, resulting in denial of service.

Web Service Dynamic Discovery (WSD)

WSD is a technical specification that defines a multicast protocol to locate services on a local network. It operates over TCP and UDP port 3702 and provides connected devices with a convenient way to discover services automagically on a (home) network. UDP can be spoofed, just as in the Memcached attack, and a WSD service that was exposed to the internet will respond with large replies to small requests, sending large streams of traffic to a victim following a limited stream of requests generated by an attacker. The problem is not the protocol itself, but the careless implementation of the service on consumer and connected devices that enable the protocol on all interfaces by default, including public-facing interfaces.

Apple Remote Management Service (ARMS)

This attack vector gives attackers the ability to abuse Apple's Remote Management Service (ARMS) to launch an amplified denial-of-service attack. By sending malicious datagrams to exposed ARMS services on UDP port 3283, attackers can perform an amplification attack. Attacks leverage the ARMS of macOS on systems connected to the internet without firewall or local network protection.

NXNSAttack

Unlike DDoS floods or application-level DDoS attacks that directly target and impact a host or a service, the **NXNSAttack** targets the domain name resolution capability of its victims. Like the NXDOMAIN or DNS Water Torture attack, this DDoS attack is aimed at disrupting the authoritative servers of the domain by overloading them with invalid requests using random domain request floods through recursive DNS resolvers. This attack is hard to detect and mitigate at the authoritative server because the requests originate from legitimate recursive DNS servers. By disrupting

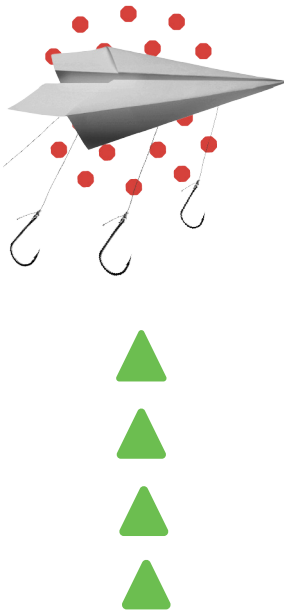
name resolution for the domain, attackers effectively block access to all services provided under the domain. New clients will not be able to resolve the hostname of the service while under attack because they have no way of locating the IP address to connect to the service.

TCP Reflection

In a TCP SYN-ACK **reflection attack,** an attacker sends a spoofed SYN packet, with the original source IP replaced by the victim's IP address, to a wide range of random or preselected reflection IP addresses. The services at the reflection addresses reply with a SYN-ACK packet to the victim of the spoofed attack. While your typical three-way handshake might assume for a single SYN-ACK packet to be delivered to the victim, when the victim does not respond with the last ACK packet, the reflection service will continue to retransmit the SYN-ACK packet, resulting in amplification.

Jenkins

Jenkins, by default, supports two network discovery services: UDP multicast/broadcast and DNS multicast. A vulnerability in Jenkins allowed attackers to abuse the servers by reflecting UDP requests off UDP port 33848, resulting in an amplified response containing Jenkins metadata. This is possible because the Jenkins Hudson service does not properly monitor network traffic and is left open to discover other Jenkins instances.



New techniques

Motivated attackers, over the last year, discovered not only new DDoS attack vectors, but also a new technique to evade or slow down detection, known as carpet bombing. This attack technique has become very common and a mild level of sophistication from the threat actor. The technique is typically used in combination with reflection and amplification attack vectors, such as TCP reflection. At the end of 2019, Radware research observed several attacks using carpet bombing to target South African ISPs.

Carpet bombing

Carpet bombing is used by attackers to evade or slow DDoS detection by not targeting a single IP but the full CIDR of the victim. By spreading the attack across many targets, threshold and statistical detection will have a harder time to detect the small ripple versus a large peak that would hit a single target.

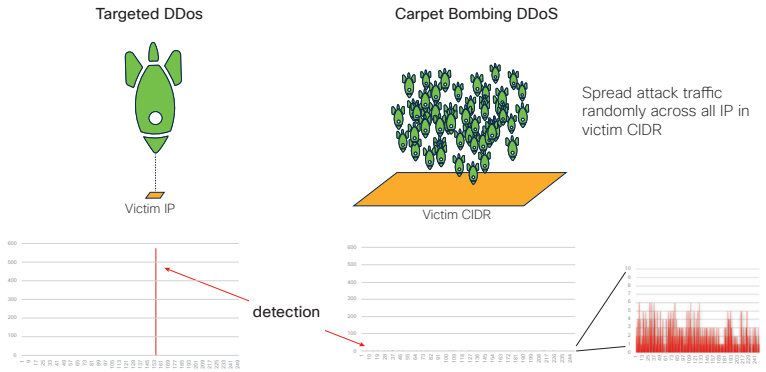


Figure 13. Carpet bombing technique

Prevention

Takedowns are not the long-term solution. Denial of service should be mitigated in different ways. To curb the growing booter and stresser industry means addressing the core problem: the devices and servers used to create large-scale botnets and world-record volumes. Address the growth of the IoT market and the lack of regulation and security standards for devices that get connected to the internet. In addition, address the issues surrounding open resolvers and reflectors on the internet. While disclosures of new attack vectors are hard to keep pace with, we need to put steady pressure on those who are not patching in a reasonable amount of time and develop ways to cope with open resolvers such as DNS and NTP.

While the solution sounds obvious, the distributed nature, the multiple levels of ownership of the problems, the lack of financial incentive, and the lack of knowledge and a sense of urgency for security creates significant challenges.

However, if devices can be infected within seconds and open services and resolvers remain, the problem will continue. Removing that vast attack surface from the bot herders plus proper mitigation which that increases the resistance against successful DDoS attacks is the only way to demotivate criminals. The ultimate solution is to make launching these assaults too difficult and too expensive. Doing so will put an end to smaller cybercriminals and wannabee hackers.

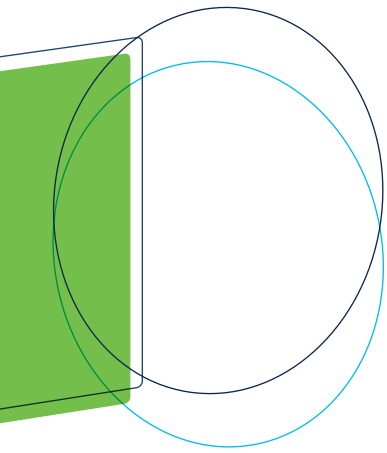
Effective DDOS protection essentials

- **Hybrid DDoS Protection** - On-premises and cloud DDoS protection for real-time DDoS attack prevention that also addresses high-volume attacks and protects against pipe saturation.
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through.
- **Real-Time Signature Creation** - Protection from unknown threats and zero-day attacks.
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks.
- **Intelligence on Active Threat Actors** – High-fidelity, correlated, and analyzed date for preemptive protection against currently active known attackers.

For further network and application protection measures, Cisco and Radware urge companies to inspect and patch their network in order to defend against risks and threats.

Effective web application security essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – use negative and positive security models for maximum accuracy
- **Auto policy generation** – use capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premises, out of path, virtual, or cloud based



Learn more

Cisco partners with Radware to provide best-of-breed DDoS, WAF, SSL, and bot management solutions that enhance network resilience, ensure application availability, and protect digital enterprises worldwide.

To learn more, please visit:

Cisco.com cisco.com/go/secure

- Cisco.com "What Is a DDoS Attack?" cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html
- Live DDoS Threat Map: livethreatmap.radware.com
- Cisco Security Blog: blogs.cisco.com/security
- Radware DDoS Blog: blog.radware.com/
- Radware DDoS Warriors: https://security.radware.com

For questions about our solutions or for sales support, please contact Cisco at www.cisco/com/c/en/us/buy.