Hacker’s Corner

Reboot: The Return of Stressers

Oct 24, 2019

Professional Door Service

At the beginning of 2018, things looked as if they were about to snowball out of control. It seemed every week there was a new critical vulnerability affecting an IoT device or enterprise solution, which was quickly followed by a newly discovered botnet variant leveraging the same recently disclosed vulnerability. Bot herders were moving quickly: by February 2018 the Memcached vulnerability was leveraged within 24 hours of its disclosure, launching a record-breaking DDoS attack. Eight days later, it was incorporated into one of the more notorious DDoS-for-hire services at the time, Defcon[.]pro.

Soon after, federal agents around the world began working to dismantle the DDoS-for-hire industry. They arrested operators and users of these illegal services.

On April 24, 2018, Dutch Police, the United Kingdom’s National Crime Agency, and Europol[1], in addition to other law enforcement agencies around the world, launched Operation Power Off, aimed at arresting the administrators of the DDoS-for-hire service, Webstresser[.]org. Agents seized the domain and arrested the administrators in the United Kingdom, Croatia, Canada, and Serbia. In addition, law enforcement agencies globally also targeted the users of the service. In total, Webstressers had 136,000 registered users who launched a total of 4 million cyerattacks.

On December 20, 2018, the United States Department of Justice announced that they seized 15 domains associated with DDoS-for-hire services and arrested the administrators behind the attack platforms[2].

- Anonsecurityteam[.]com
- Critical-boot[.]com
- defianceprotocol[.]com
- ragebooter[.]com
- str3ssed[.]me
- bullstresser[.]net
- Quantumstress[.]net
- Booter[.]ninja
- downthem[.]org
- netstress[.]org
- Torsecurityteam[.]org
- Vbooter[.]org
- defcon[.]pro
- request[.]rip
- Layer7-stresser[.]xyz

These 15 stresser services represent some of the more notable attack platform advertised both on the clear and darknet. For example, Downthem had over 2,000 users who launched over 200,000 DDoS attacks. Quantum Stress had over 80,000 users who launched launched over 50,000 attempted DDoS attacks in 2018.

Amid the crackdown, the Department of Justice announced in February 2019 that a former administrator for eight DDoS-for-hire websites had pleaded guilty for conspiracy to commit computer damage and abuse[3].

- Exostress[.]in
- QuezStresser[.]com
- Betabooter[.]com
- Databooter[.]com
- Instabooter[.]com
- Polystress[.]com
- Decafestresser[.]com
- Stress[.]net

[1] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down

[2] https://www.justice.gov/opa/pr/criminal-charges-filed-los-angeles-and-alaska-conjunction-seizures-15-websites-offering-ddos

[3] https://www.justice.gov/opa/pr/former-operator-illegal-booter-services-pleads-guilty-conspiracy-commit-computer-damage-and

Exostresser advertised that its service launched over one million DDoS attacks and caused over 100,000 hours of network downtime. It is estimated, in the Department of Justice announcement, that the two operators behind these services made over $500,000 USD during their time in business.

Following these operations, law enforcement targeted KV Solutions. In October 2019, Dutch Police[4] raided the notorious bulletproof hosting provider, KV Solutions, that was known to host C2 servers for several botnet variants. To give perspective, KV Solutions network was so active it registered 945,436 events from only 98 unique IP addresses against Radware’s TRC network in its last month of operation.

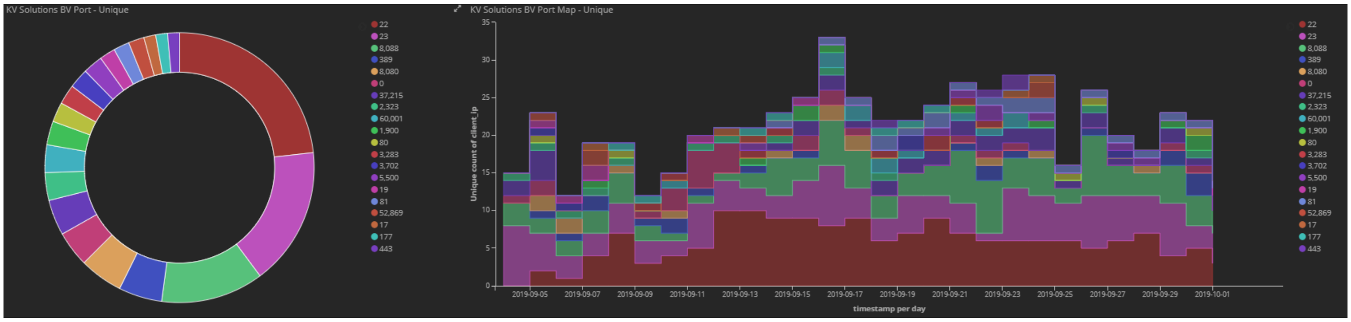
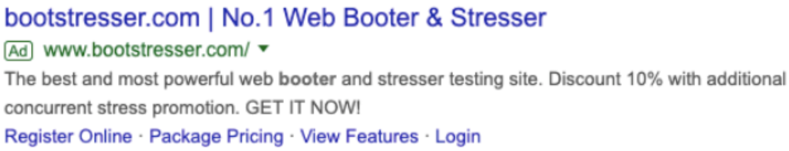


Figure 1: Ports targeted by KV Solutions

After two years of raids, arrests, and takedowns, the problem that is DoS is solved, right? Think again.

Hail Hydra!

Cut one head off, and two more grow in its place. With a quick search of Google, Bing, Yahoo or AOL you’ll quickly discover the problem is far from solved; it’s still openly advertised.



bootstresser.com | No.1 Web Booter & Stresser

Ad www.bootstresser.com/ ▾

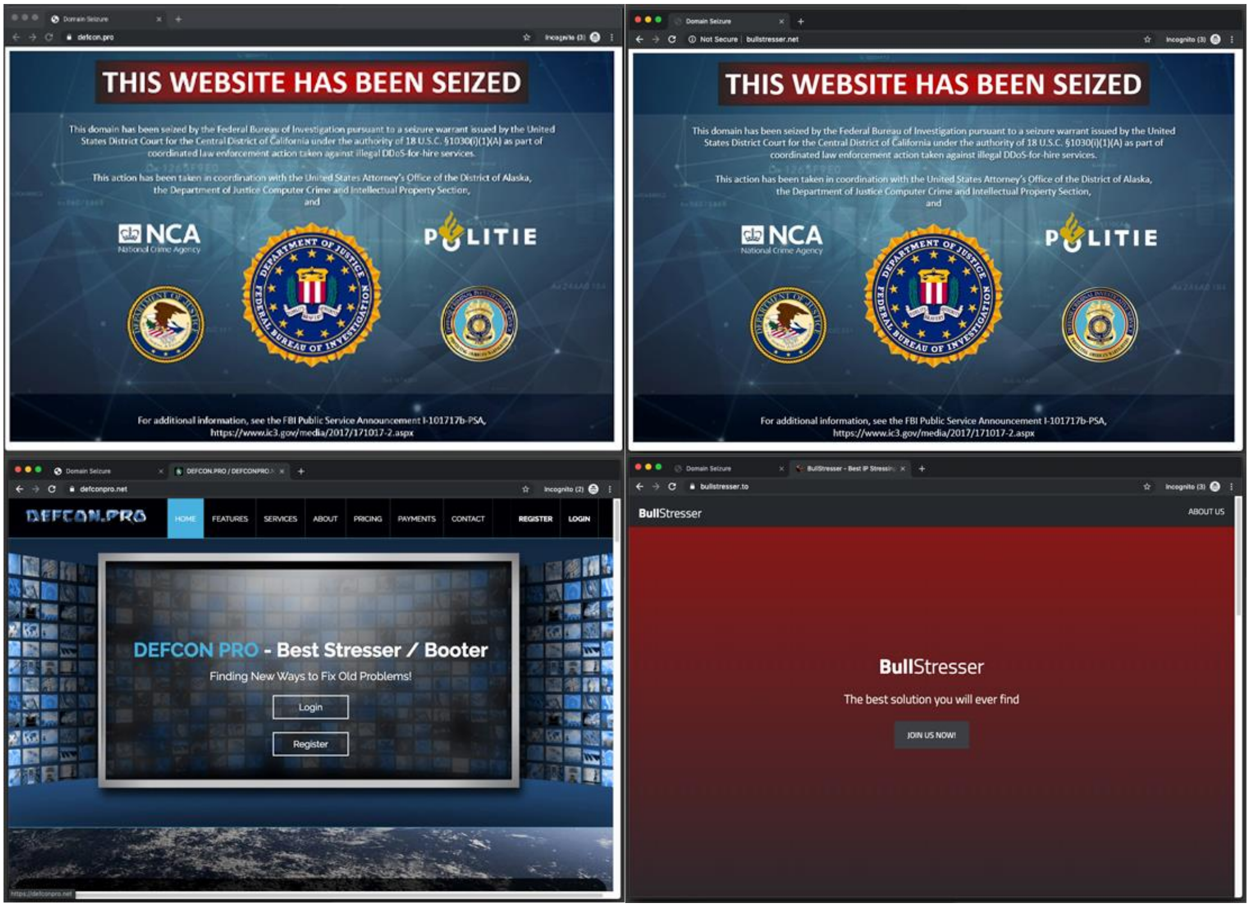
The best and most powerful web **booter** and stresser testing site. Discount 10% with additional concurrent stress promotion. GET IT NOW!

Register Online · Package Pricing · View Features · Login

Figure 2: Stresser service advertisement on Google

While I have not had the chance to examine every service found on Google, there appears to be a resurgence in similar domains of those taken down over the past two years. Below are two examples of this. Both domain’s Defcon[.]pro and bullstresser[.]net were seized, but clones have now appeared on defconpro[.]net and bullstresser[.]to. At any rate, it’s clear that hosting providers and search engines are not removing abusive services such as DDoS-for-hire.

[4] https://www.politie.nl/nieuws/2019/oktober/2/11-servers-botnet-offline.html



THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Central District of California under the authority of 18 U.S.C. §1030(i)(1)(A) as part of coordinated law enforcement action taken against illegal DDoS-for-hire services.

This action has been taken in coordination with the United States Attorney's Office of the District of Alaska, the Department of Justice Computer Crime and Intellectual Property Section, and

For additional information, see the FBI Public Service Announcement I-101717b-PSA, https://www.ic3.gov/media/2017/171017-2.aspx

THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Central District of California under the authority of 18 U.S.C. §1030(i)(1)(A) as part of coordinated law enforcement action taken against illegal DDoS-for-hire services.

This action has been taken in coordination with the United States Attorney's Office of the District of Alaska, the Department of Justice Computer Crime and Intellectual Property Section, and

For additional information, see the FBI Public Service Announcement I-101717b-PSA, https://www.ic3.gov/media/2017/171017-2.aspx

DEFCON PRO - Best Stresser / Booter

Finding New Ways to Fix Old Problems!

BullStresser

The best solution you will ever find

Figure 3: Seized and current stresser with similar domains and identical layouts.

List of Stresser Services

- booter[.]vip
- booter[.]xyz
- bootstresser[.]com
- bootyou[.]net
- defconpro[.]net
- directnodes[.]net
- freeboot[.]to
- instant-stresser[.]to
- iraven[.]cc
- meteor-security[.]to
- str3ssed[.]co
- stressed[.]host
- stresser[.]cc
- stresser[.]me
- ts3booter[.]net
- undisclosed[.]to
- vdos-s[.]co
- webstresser[.]biz
- bullstresser[.]to
- stresshub[.]io
- stressthem[.]to
- xyzbooter[.]online
- xzstresser[.]co
- zodiac-stresser[.]com

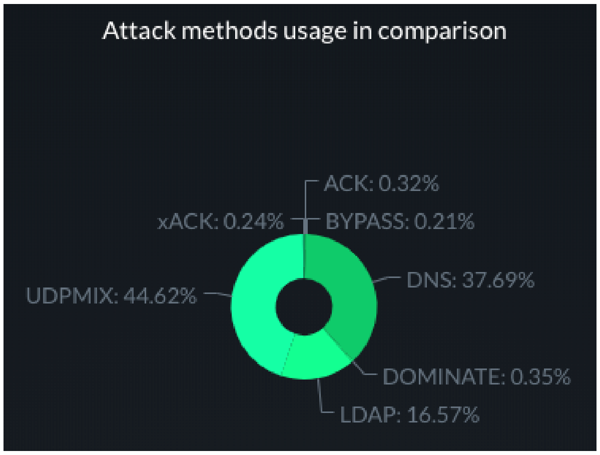


Figure 4: Advertised attack method popularity

Re:boot

In general, it’s fair to say that while raids are disrupting criminals, they have hardly put a dent in the overall activity or economy of the DDoS-as-a-service industry. Takedowns represent a temporary solution.

DoS is still a very profitable industry for cybercriminals. For example, within 24 hours of the Dutch Police raiding KV Solutions, criminals began moving their C2 infrastructure to new hosting providers. Downtime is costly, even to bot herders.

It’s no surprise that DDoS operators that haven’t been arrested are still operating and are still easily found via Google and Instagram. DDoS operators and bot herders are patiently awaiting to take over the business lost by those that have been arrested over the last two years.

Amplification

User Datagram Protocol (UDP) is a connectionless protocol that uses datagrams embed in IP packets for communication without needing to create a session between two devices. In the world of DoS attacks, a UDP Flood does not exploit a specific vulnerability. Instead, it simply abuses normal behavior at a high enough level to cause congestion for a targeted network. A UDP Flood sends a large number of UDP datagrams from potentially spoofed IP addresses to random ports on a target server.

The problem is, some application layer protocols rely on UDP and are unnecessarily exposed to the internet. They also can be easily abused by botherders looking to launch denial-of-service attacks. In this attack method, attackers forge a packet datagram to include a spoofed source IP address — that of the victims. When the packet is sent, the destination server responds to the victim’s IP address and not the attacker. The trick is, certain application layer protocols produce a response much larger than the initial request. This is called amplification, and it's measured by the Bandwidth Amplification Factor (BAF). For example, a DNS amplification attack can see an amplification factor between 28 and 54, but a Memcached amplification factor ranges between 10,000 and 52,000.

Amplification attacks are mainly intended to saturate your internet pipe while impacting your firewall's resources. Amplification attacks are also "asymmetric," meaning that a relatively small number of servers or resources are required for an attacker to have a significant impact on the victim’s resources. Because of this, we still see amplification attacks and causing significate outages due to their inclusion in multi-vector attacks.

More to Come

Botherders looking to carry out denial-of-service attacks continue to leverage residential and enterprise devices to build massive botnets, but at the same time, they are also searching for new attack vectors to employ within their botnets so they can effectively carry out crippling network attacks.

One of the more notable attack vectors to come out this year was the announcement regarding the abuse of the Web Services Dynamic Discovery (WSD) protocol, UDP/ 3702, to launch amplified DDoS attacks. While this attack vector was known since the beginning of the year, no one publicly spoke about it until the third quarter when details slowly emerged that botherders employed a new attack vector into their amplification toolkit.

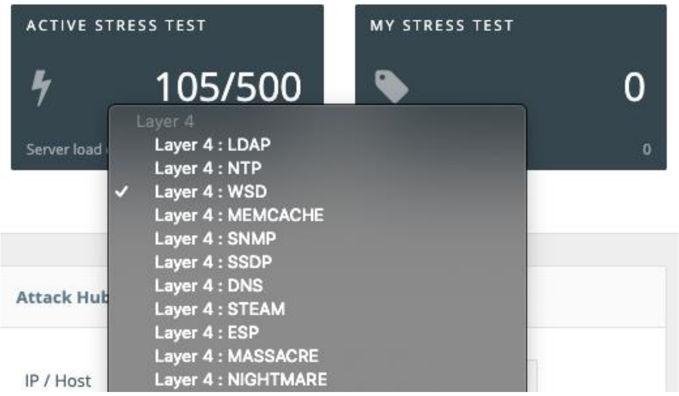


Figure 5: WSD attack vector offered via DDoS-for-Hire

Researcher's from Netscout announced a newly discovered vector of attack that allowed attackers the ability to abuse Apple's Remote Management Service (ARMS) to launch amplified denial of service attack. By sending malicious datagrams to exposed ARMS services on UDP/3283, attackers could gain an amplification factor of 35.5 to 1.

While UDP amplification attacks are fairly easy to mitigate with the right solution, bot herders will look to leverage new largescale volumetric attack vectors against those that are not prepared.

Corporate Insight

The escalation in the attack vector landscape will continue to evolve into 2020. One of the biggest attack trends outside of IoT botnets in 2018 was the focus by threat actors on amplification attack vectors after the disclosure of the Memcached vulnerability. This trend into amplification attack vectors continued into 2019 with announcements of WSD and ARMS. It's also expected that researchers and criminals alike will continue to discover vulnerabilities in application layer protocols in 2020 that can be leveraged to launch amplified denial-of-service attacks. It comes down to how fast can the public patch these vulnerabilities when they are announced and can companies properly mitigate multi-vector volumetric attacks that include undisclosed attack vectors in real-time?

DDoS Essentials

- Hybrid DDoS Protection - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- Behavioral-Based Detection - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- Real-Time Signature Creation - Promptly protect 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

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.