NETSCOUT

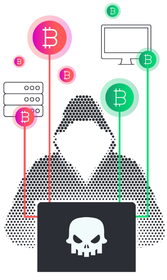
The Dark Side of DDoS-for-Hire

The dark web is a dangerous place where adversaries own and operate DDoS-for-hire platforms and botnets to launch everything from free tests to high-powered multivector attacks. ASERT explored this underground space to evaluate the kinds of attacks being launched. Likewise, we wanted to better understand the kinds of platforms used and their capabilities, to illustrate the low barrier to entry and why DDoS attacks are so prevalent.

From adding new weapons to their ransomware-as-a-service (RaaS) portfolio to offering payment portals and support centers for victims, ransomware gangs are laser-focused on parting unsecured organizations from their money.

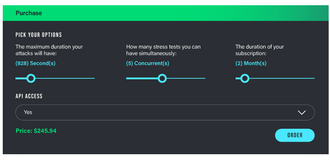
DDoS-for-Hire Services Investigated by ASERT

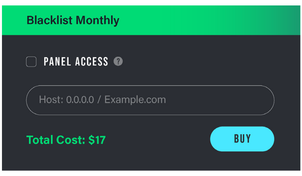
1. AnonBot
2. Booter
3. Booter SX
4. CryptoStressor
5. CyberVM
6. DDoS Service
7. Downed
8. FlyStress
9. Instant Stresser
10. IPStresser
11. NetworkStress
12. Project Delta
13. Str3ssed
14. Stresser GG
15. Stresser US
16. SunStresser
17. Toxicity
18. WebStresser
19. ZDStresser

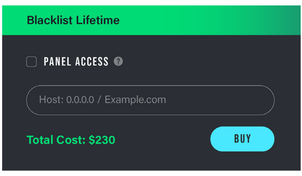


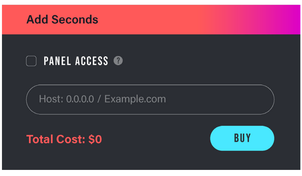
Although some of these services have static pricing models, many of them allow for custom configurations based on duration, concurrent tests, and power, which is how adversaries measure bandwidth and throughput.

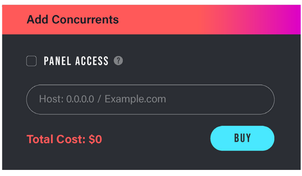
Prices for these services vary wildly. We found free tests, tests for $5 over a five-day trial, and full attacks for as much as $6,500, which included 100 concurrent attacks, no daily limits, and a committed 1 million packets per second (Mpps). NetworkStress service boasts a 1 Tbps attack size using 150,000 bots for $2,499. Although these services boast massive capacity, we have yet to observe any DDoS attacks sourced from them in the terabit range.











In the 2H 2021 Threat Intelligence report, we described how some of these underground services offer "blacklists" or delisting services to prevent attacks. One example of this can be found on Booter SX, where adversaries offer a temporary or permanent option for delisting IPs. At least three of the services noted above include this feature, which is anything but a guarantee the purchaser will not be attacked.

Nearly every service offers some form of free DDoS attack capability via Network Time Protocol (NTP), DNS, CLDAP, or a random UDP reflection/amplification attack vector. In addition to the free options, these 19 platforms combined boast a total of more than 200 different attack types, many of which are shared across platforms. UDP and TCP reflection/amplification are the most prevalent, followed by UDP and TCP floods. The services also offer varying degrees of UDP and TCP bypasses for CAPTCHAs or other anti-DDoS defenses.

Despite the incredible diversity of these platforms, the majority of attack types are recognized and predominantly mitigated via standard defensive practices. Our primary motivation in exploring these services was to determine the capabilities available to adversaries. Based on our research, none of the listed services was a surprise or provided something we haven't witnessed in the wild. Given a solid understanding of these attack methods and a properly tuned mitigation platform, network security professionals can create defensive measures and templates to counter attacks from booter/stresser services.

ATTACK TYPES OFFERED ON DDOS-FOR-HIRE PLATFORMS

- COAP amplification
- OVHGameTCP
- NTP amplification
- SNMP amplification
- SynAck
- DNS amplification
- CF-Bypass
- LDAP amplification
- WSD amplification
- DVR amplification
- HTTP
- CLDAP amplification
- ESP Flood
- SSDP amplification
- TCP
- FIVEM
- MixUDPAMP
- UDP
- SOURCE
- VSE amplification
- ARM amplification
- MINECRAFT
- IPSec
- HEAD
- GoogleCloud

Threat Intelligence Report Issue 8, Findings from 2H 2021

EXPLORE INTERACTIVE REPORT

NETSCOUT

©2022 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor, ATLAS, Cyber Threat Horizon, InfiniStream, nGenius, nGeniusONE, and Omnis are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

SECIG_018_EN-2201 03/2022