Abstract

Seasoned hackers have typically relied on a variety of sophisticated tools that allow them to orchestrate attacks globally. However, a series of new, off-the-shelf tools are commoditizing the art of hacking, making it possible for novices with little know-how to launch attacks via affordable tools that are available on the Clearnet. These new pay-as-you go solutions include Booters, Stressers, and IP Stressers,

Attack Methods

This situation has resulted in a wide array of powerful and affordable tools available in the dark marketplace. Since the beginning of 2016, Radware has witnessed these tools being used against ISPs, media, financial service companies, online gaming, and other industries. Organizations are being forced to improve defenses as these tools combine high traffic volumes with multi-vector attacks.

Booters

For a small fee, botnet owners provide access to leverage their network for the purpose of launching DDoS attacks. Called booters, they offer a web-based attack service that provides users with a user-friendly interface.

Various payment plans are available, and depend of the attack duration, volume, frequency of use, and number of concurrent attacks. Most booters also offer a range of additional cyber-attack tools and services such as Skype resolvers, IP trackers, credit cards and other resolving services. Subscriptions start at $19.99 a month and can go up to as much as $500 a month. Most vendors only accept Bitcoin, however some do accept PayPal.

Booters are popular among hackers because they make tracking harder and therefore considered by hackers as a low-risk tool. When the service does not track the user's IP address or server information, and does not block anonymizing services like VPN and Tor, the perpetrator will mostly likely not be caught.

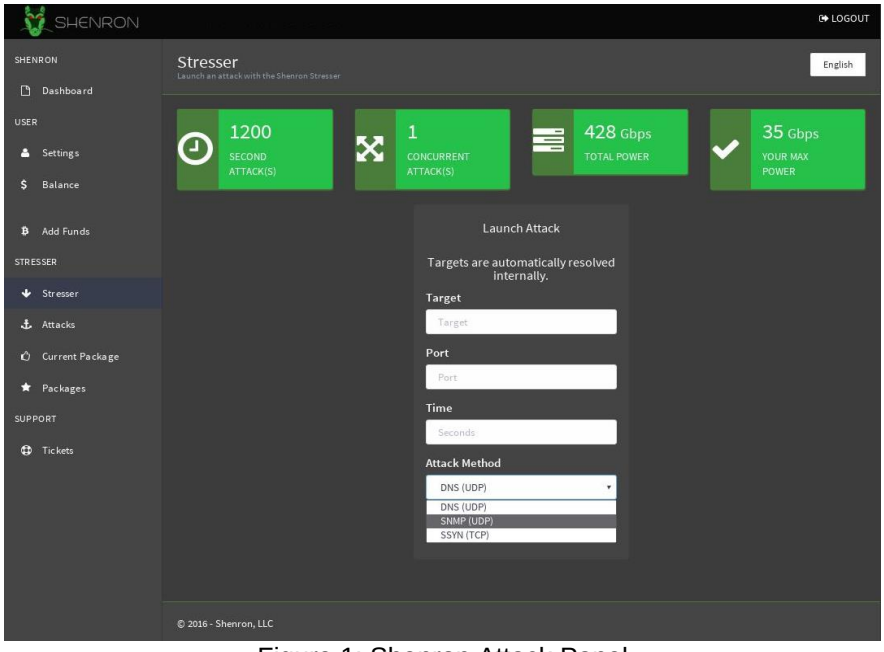

Figure 1: Shenron Attack Panel

Stressers

Many notorious DDoS groups like Lizard Squad, New World Hackers and others have entered the DDoS-As-A-Service business (DDoSaaS), monetizing their capabilities in peace-time by renting their powerful stresser services. The high demand for DDoSaaS makes it a very profitable business and can generate operators thousands of dollars a week. These groups have used their tools against high profile targets to showcase and promote their attack service. The entry level continues to decrease, allowing novice attackers the ability to carry out larger and more sophisticated attacks. For $19.99 a month, an attacker can run 20-minute bursts for 30 days, utilizing a number of attack vectors like DNS, SNMP and SSYN, and slow GET/POST application layer DoS attacks.

Popular stresser services:

- **LizardStresser –** up to 500 Gbps, prices range between $20 and $1000
- **Bang Stresser** – costs $12 to $100 for up to 1.5 hours' attack duration
- **uStress –** can generate a 20-minute 300 Gbps attack. Prices vary between $15 and $150
- **NetStresser** – Prices range from $10 to $150 for up to 1.5 hours' attack duration
- **vDoS –** over 200 Gbps of multi-vector attacks. Prices vary between $20 and $150

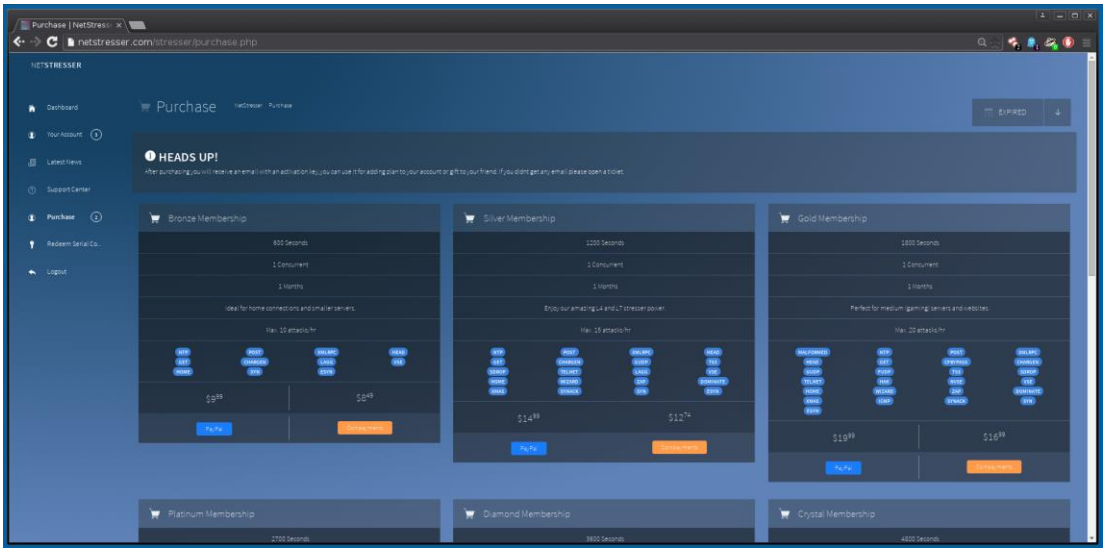

Figure 2: NetStresser DDoS as a Service portal

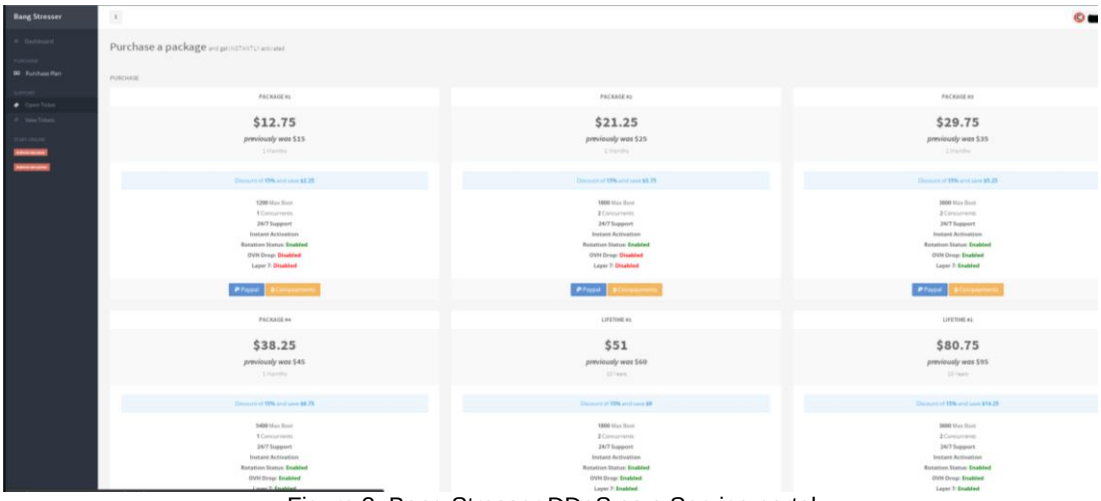

Figure 3: Bang Stresser DDoS as a Service portal

Attack Vector

DNS – A DNS amplification attack is a sophisticated denial of service attack where the attacker performs two malicious tasks. First, the attacker spoofs the IP address of the DNS resolver and replaces it with the victim's IP address, so all DNS replies will be sent to the victim's servers. Second, the attacker finds an Internet domain that is registered with many DNS records. During the attack, the attacker sends DNS queries that request the entire list of DNS records for that domain. This results in replies from the DNS servers, usually so big that they need to be split over several packets.

SNMP – A SNMP amplification attack is a sophisticated denial of service attack that takes advantage of the Simple Network Management Protocol, SNMP, an everyday protocol found in a number devices including routers, printers and switches, in order to amplify an attack. Like other reflective attacks, the attacker spoofs the IP address of the SNMP query and send the malformed packets to a number of devices, resulting in a very large response being sent to the victim's device.

NTP Monlist Flood - The NTP Amplification attack is an emerging form of DDoS that relies on the use of publically accessible NTP servers to overwhelm a victim's system with UDP traffic. The NTP service supports a monitoring service that allows administrators to query the server for traffic counts of connected clients. This information is provided via the 'monlist' command. The basic attack technique consists of an attacker sending a "get monlist" request to a vulnerable NTP server, with the source address spoofed to be the victim's address.

HTTP Flood - A method used by hackers to attack web servers and applications. It consists of seemingly legitimate session-based sets of HTTP GET or POST requests that are designed to consume a significant amount of server's resources, and can result in a denial-of-service condition - without necessarily requiring a high rate of network traffic.

SSYN – A SSYN attack is a spoofed SYN attack. In a SYN attack, the attacker floods their victim's computer with a large amount of SYN packets. This attack is intended to exhaust the victim's device. Once all of the connections are filled, the server will not be able to respond to legitimate users, thus causing a denial of service. In a spoofed SYN attack the attacker runs a similar script that spoofs the attacking IP addresses to prevent the attacker from being traced.

TCP flood – This is one of the oldest types of attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and store this state in tables that have limited size. As big as this table may be, it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall which also has to process and invest in each SYN packet. Unlike other TCP or application level attacks, the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.

UDP Flood – In a UDP flood, the attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is "connectionless" and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. Usually, the attackers spoof the SRC IP.

Key Considerations for Effective DDoS Protection

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application-based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe
- A hybrid solution that includes on-premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A solution that provides protection against sophisticated web-based attacks and web site intrusions to prevent defacement and information theft.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.

Radware recommends IT crews to monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats when they occur.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks 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.