ERT Threat Alert
Putinstresser
March 19, 2018

Abstract

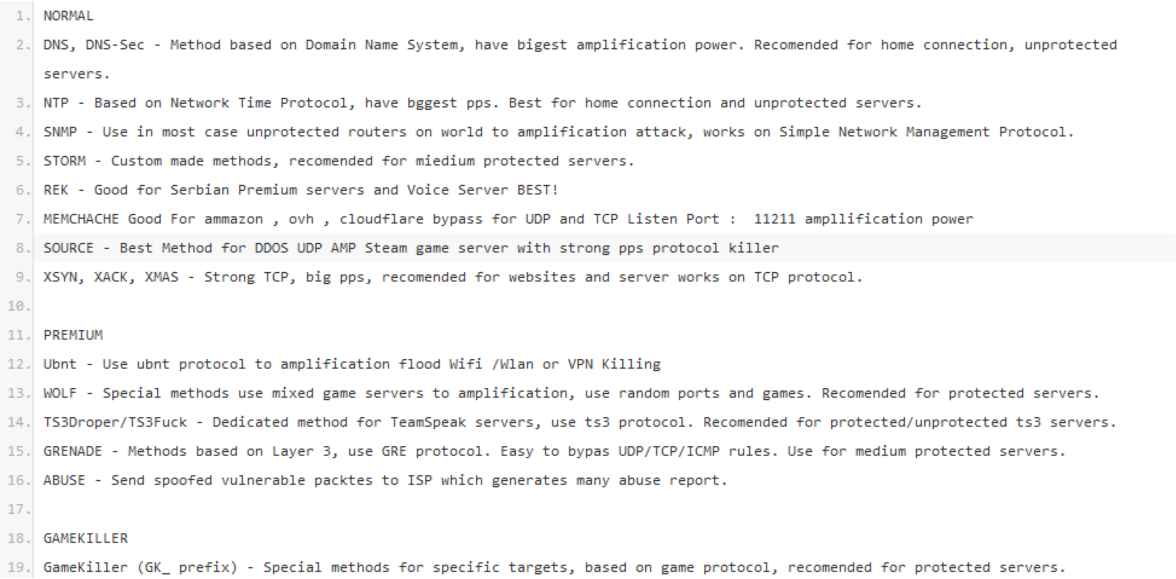
Putinstresser.eu is a recent DDoS-as-a-Service tool and is one of the newest additions to the growing array of low-priced services commonly known as ‘booter’ or ‘stresser’ services. The site illustrates the ease of access these services have reached. It provides different payment options, discovery tools, customer support and a variety of attack vectors for a wide range of customers. According to its FAQ, the booter performs up to 350Gbps per stress using DNS amplification attacks. TCP stress provides 600,000pps per stress.

Background

There are hundreds, maybe thousands, of these services on the dark and clear nets to make money from customers looking to perform illegal DDoS attacks. Their target audience varies and includes hacktivists, ransom engineers and even businesses.

Attack Methods

The attack methods or vectors available to choose from include the ‘golden standards’ such as DNS, NTP, SNMP amplification attacks as well as the latest Memcached attack. It also includes traditional TCP XSYN, XACK and XMAS floods, GRE-based assaults, attacks dedicated to TeamSpeak servers using the TS3 protocol and attack vectors that target different multi-player gaming platforms such as Valve Source Engine (VSE), Minecraft, Counter Strike (GK_CS), Steam and San Andreas Multi-Player (GK_Samp). The owners of the site advertised their attack vectors on Pastebin with a short description and some help for unseasoned attackers.

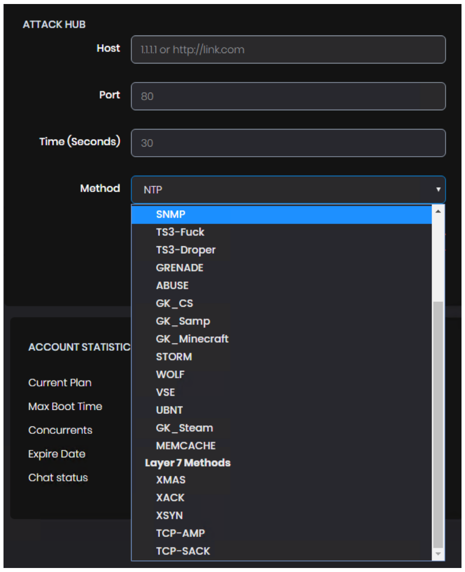


```
NORMAL
DNS, DNS-Sec - Method based on Domain Name System, have bigest amplification power. Recomended for home connection, unprotected servers.
NTP - Based on Network Time Protocol, have bggest pps. Best for home connection and unprotected servers.
SNMP - Use in most case unprotected routers on world to amplification attack, works on Simple Network Management Protocol.
STORM - Custom made methods, recomended for miedium protected servers.
REK - Good for Serbian Premium servers and Voice Server BEST!
MEMCHACHE Good For ammazon , ovh , cloudflare bypass for UDP and TCP Listen Port :  11211 ampllification power
SOURCE - Best Method for DDOS UDP AMP Steam game server with strong pps protocol killer
XSYN, XACK, XMAS - Strong TCP, big pps, recomended for websites and server works on TCP protocol.

PREMIUM
Ubnt - Use ubnt protocol to amplification flood Wifi /Wlan or VPN Killing
WOLF - Special methods use mixed game servers to amplification, use random ports and games. Recomended for protected servers.
TS3Droper/TS3Fuck - Dedicated method for TeamSpeak servers, use ts3 protocol. Recomended for protected/unprotected ts3 servers.
GRENADE - Methods based on Layer 3, use GRE protocol. Easy to bypas UDP/TCP/ICMP rules. Use for medium protected servers.
ABUSE - Send spoofed vulnerable packtes to ISP which generates many abuse report.

GAMEKILLER
GameKiller (GK_ prefix) - Special methods for specific targets, based on game protocol, recomended for protected servers.
```

Figure 1: Attack vector library on Pastebin



ATTACK HUB

Host: 1.1.1.1 or http://link.com

Port: 80

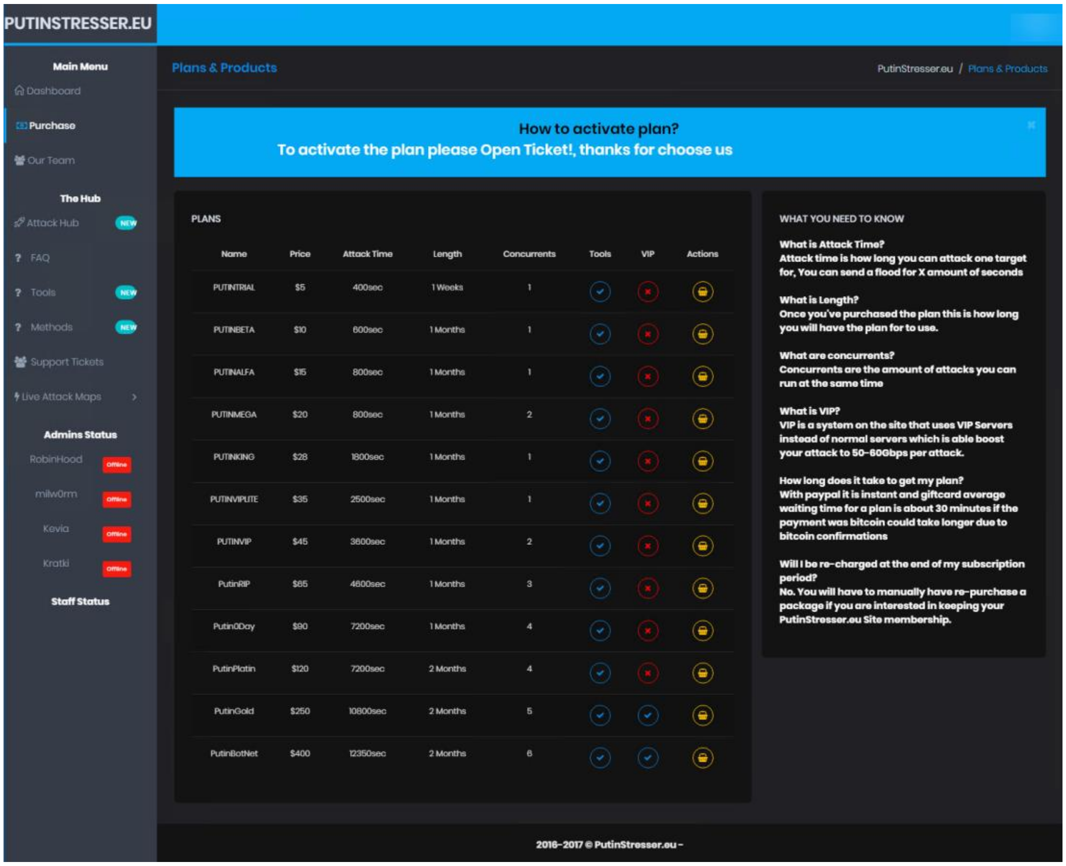
Time (Seconds): 30

Method: NTP

Figure 2: Attack vectors dropdown menu from the attack hub

Plans and Products

Plans start with a trial plan at $5 for a 400-second attack time that remains valid for one week. The first full plan starts at $10 per month for a 600-second attack time with one concurrent attack. The highest plan provides nearly 3.5 hours of attack time for $400 and includes the ability to run six concurrent attacks.



How to activate plan?
To activate the plan please Open Ticket!, thanks for choose us

PLANS

Name	Price	Attack Time	Length	Concurrents	Tools	VIP	Actions
PUTINTRIAL	$5	400sec	1 Weeks	1	✓	✗	🛒
PUTINBETA	$10	600sec	1 Months	1	✓	✗	🛒
PUTINALFA	$15	800sec	1 Months	1	✓	✗	🛒
PUTINMEGA	$20	800sec	1 Months	2	✓	✗	🛒
PUTINKING	$28	1800sec	1 Months	1	✓	✗	🛒
PUTINVIPLITE	$35	2500sec	1 Months	1	✓	✗	🛒
PUTINVIP	$45	3600sec	1 Months	2	✓	✗	🛒
PutinRIP	$65	4600sec	1 Months	3	✓	✗	🛒
Putin0Day	$90	7200sec	1 Months	4	✓	✗	🛒
PutinPlatin	$120	7200sec	2 Months	4	✓	✗	🛒
PutinGold	$250	10800sec	2 Months	5	✓	✓	🛒
PutinBotNet	$400	12350sec	2 Months	6	✓	✓	🛒

WHAT YOU NEED TO KNOW

What is Attack Time?
Attack time is how long you can attack one target for, You can send a flood for X amount of seconds

What is Length?
Once you've purchased the plan this is how long you will have the plan for to use.

What are concurrents?
Concurrents are the amount of attacks you can run at the same time

What is VIP?
VIP is a system on the site that uses VIP Servers instead of normal servers which is able boost your attack to 50-60Gbps per attack.

How long does it take to get my plan?
With paypal it is instant and giftcard average waiting time for a plan is about 30 minutes if the payment was bitcoin could take longer due to bitcoin confirmations

Will I be re-charged at the end of my subscription period?
No. You will have to manually have re-purchase a package if you are interested in keeping your PutinStresser.eu Site membership.

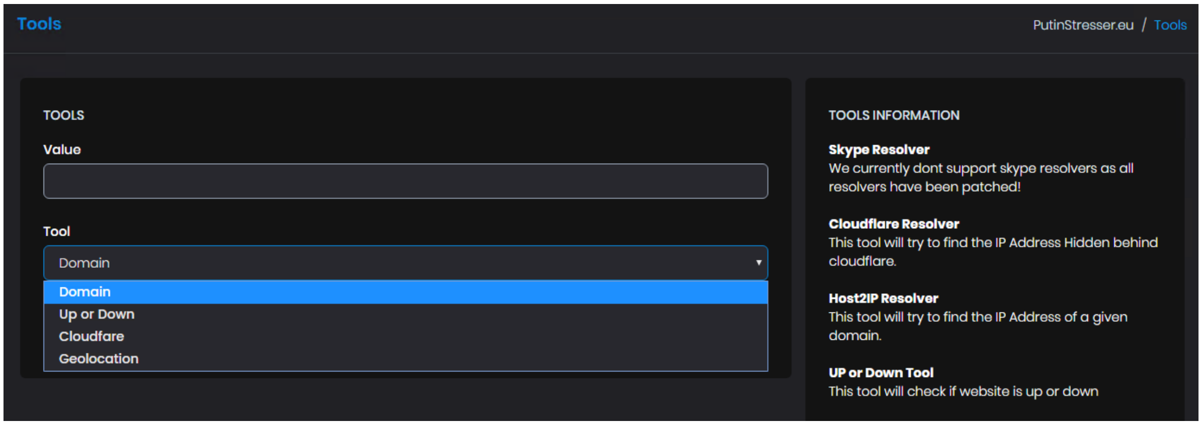
2016-2017 © PutinStresser.eu -

Figure 3: Subscription pricing

The site provides several payment options including PayPal, Bitcoin, paysafecard, Skrill and CSGO Skins (CSGO skins have turned into a currency between gamers and can be traded online via sites such as csgo-skins.com and skins.cash).

The service operators offer live chat and support for users requiring assistance and features a support feature to submit and track support tickets as well as live chat options via Discord.

The site features convenient tools for resolving IP addresses and checking if a targeted website is “up” or “down.” It also includes an option to find the IP address of services protected (hidden) behind Cloudflare.



Skype Resolver
We currently dont support skype resolvers as all resolvers have been patched!

Cloudflare Resolver
This tool will try to find the IP Address Hidden behind cloudflare.

Host2IP Resolver
This tool will try to find the IP Address of a given domain.

UP or Down Tool
This tool will check if website is up or down

Figure 4: Monitoring tools

Effective DDoS Protection 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 Cyber-Security 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, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of 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.