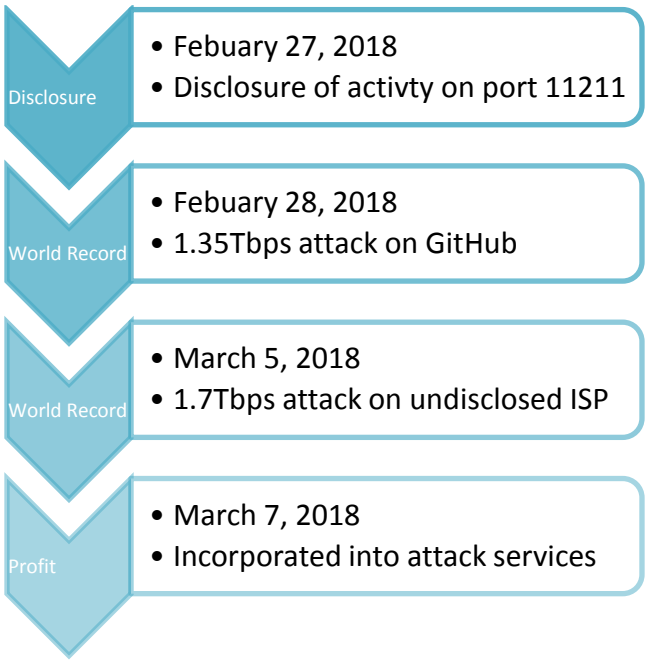
ERT Threat Alert
Memcache: DDoS-as-a-Service
March 12, 2018

Abstract

The record-breaking denial-of-service attacks launched against GitHub and other organizations quickly caught the attention of both the security community and the public. Along with this attention comes opportunity for cyber-criminals looking to profit. This can include ransom-based cyber-attacks, but for the purpose of this alert we will be discussing the evolution of the attack service industry and how quick they have included Memcache into their latest attack vector offerings.



Background

On February 27, several organizations began publicly disclosing a trend in UDP amplification attacks utilizing exposed Memcached servers. Attackers quickly mobilized and launched thousands of DDoS attacks, including two world records, as the attack scripts and amplification lists became public.

In 2016, the infamous Mirai botnet stunned the security community with the first 1Tbps attack on record. That year, the Mirai botnet was responsible for the three largest DDoS attacks in history. These attacks targeted Brain Krebs, OVH and DynDNS. When the source code to the Mirai botnet was released on HackForums, cyber-criminals modified their own variant with additional attack vectors. It wasn't long until the vendors and websites began selling spots for their Mirai botnet on both the clear and darknet.

Defcon.pro, a notorious stresser service, has already incorporated Memcache into their premium offerings. Stresser services are quick to utilize the newest attack vector for many reasons. The first reason, publicity. Attackers looking to purchase a DDoS service will search for a platform offering the latest vectors. Including them in a service shows demand for the latest vectors. In addition, an operator might include the Memcache attack service so they can provide their users with more power. A stresser service offering a Memcache attack service will likely attract more customers who are looking for volume and once again plays into marketing and availability.

Defcon.pro is a stresser service that also offers API access so others can run their own stresser services. It gained media attention last year when researcher Derrick Farmer discovered the leaked content of TrueStresser. BleepingComputer reported that TrueStresser had created a business out of Defcon.pro's API service. TrueStresser had 331 customers who all made upstream calls to Defcon.pro servers. At the time Defcon.pro had 7,700 customers and had launched 117,000 DDoS attacks as of September 1, 2017.

As of March 11, Defcon.pro reports that they have 11,260 customers and have launched a total of 2,107,817 attacks. The DDoS-as-a-Service industry can be profitable for select services and when you are first to market offering a new attack vector you can expect an increase in subscriptions. Defcon.pro states it's capable of launching a total of 42 concurrent attacks from 17 servers and offers 8-12Gbps worth of volume from their DNS attack vector if the network load is below 50%.

DDoS-as-a-Service operators are running a business and are currently evolving at rapid rates to keep up with demand. Often times these operators are using the public attention created by news coverage similar to extortionists. Ransom denial-of-service (RDoS) operators are quick to threaten the use of new tools as well due to the threat they pose. DDoS-as-a-Service will do the same, but once the threat is mitigated by security experts, cyber-criminals will look for new vectors to incorporate it into their latest toolkit or offerings.

Due to their effectiveness, amplification-based attacks are the default attack technique offered by most stresser services. These attacks are easy to conduct and rely on misconfigured services. The attacker sends a spoofed packet with the victim's IP to the service resulting in a response from the server sent to the victim's IP. Attackers will also use reflection-based attacks by misusing popular content management systems like WordPress to generate HTTP requests to target web servers. They will also abuse gaming consoles and routers in an attempt to generate larger attacks. By using reflection and amplification, attackers are able to mask their origin and turn a small amount of bandwidth into larger assaults.

Attack Methods

Attack methods are broken down into three categories on Defcon.pro. The first category is normal attack vectors. This includes amplification attacks such as DNS, DNS-SEC, NTP, SNMP, and CLDAP. UDP attacks such as VSE, STORM, SOURCE and REK. It also includes three TCP attack vectors. XSYN, XACK and XMAS. Premium attack vectors include a similar mix of vectors such as WOLF, TS3-DROPER, TS3-FUCK, GRENADE, ABUSE, TCP-AMP, TCP-SACK, UBNT and the now notorious vector MEMCACHE. The last group are Game Killers. Game Killers are attack scripts designed to target game services based on game protocol. These scripts include STEAM, STAMP, MTA, MINECRAFT, COD, BF, CSm QUAKE, VINESITY, TF and MoH.

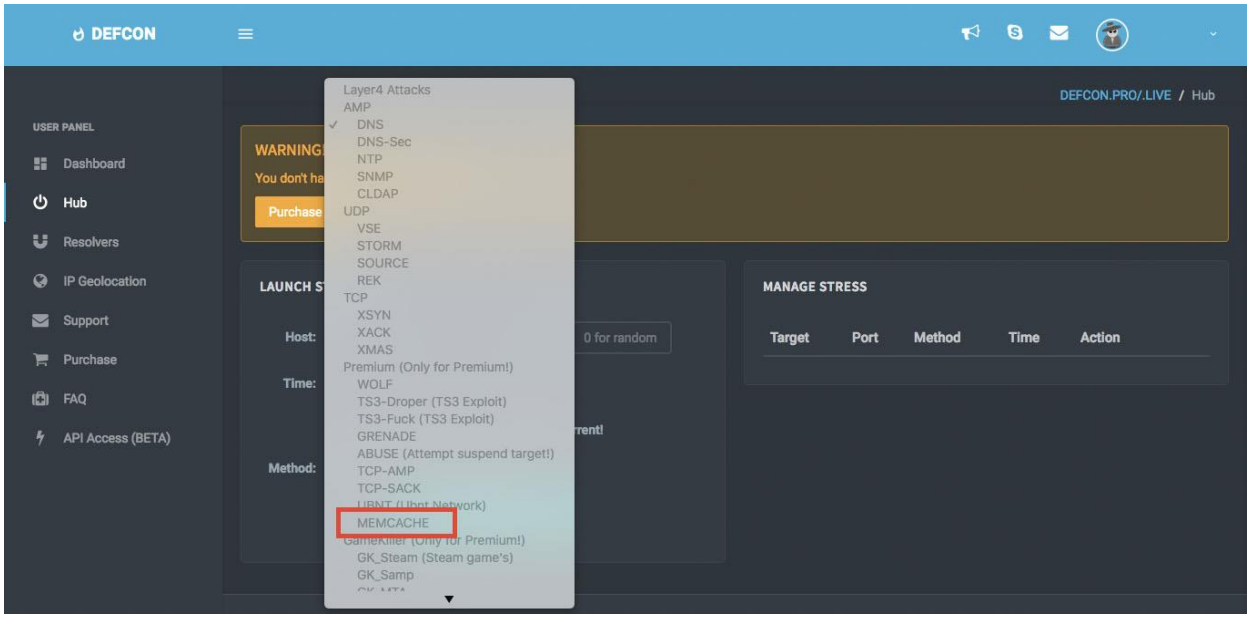


Figure 1: Memcache attack vector on Defcon.pro

Memcache – A Memcache amplification attack is a UDP volumetric denial-of-service attack where the attacker performs two malicious task similar to that of a DNS attack. The attacker builds an amplification list of vulnerable Memcache servers with UDP port 11211 exposed. The attacker will then send a spoofed GET request to the vulnerable Memcache servers on the amplification list. As a result, the Memcache servers will reply to the GET

request and forwards an amplified response to the spoofed IP address, the victim. Memcache bandwidth amplification factor can range between 10,000x and 51,000x.

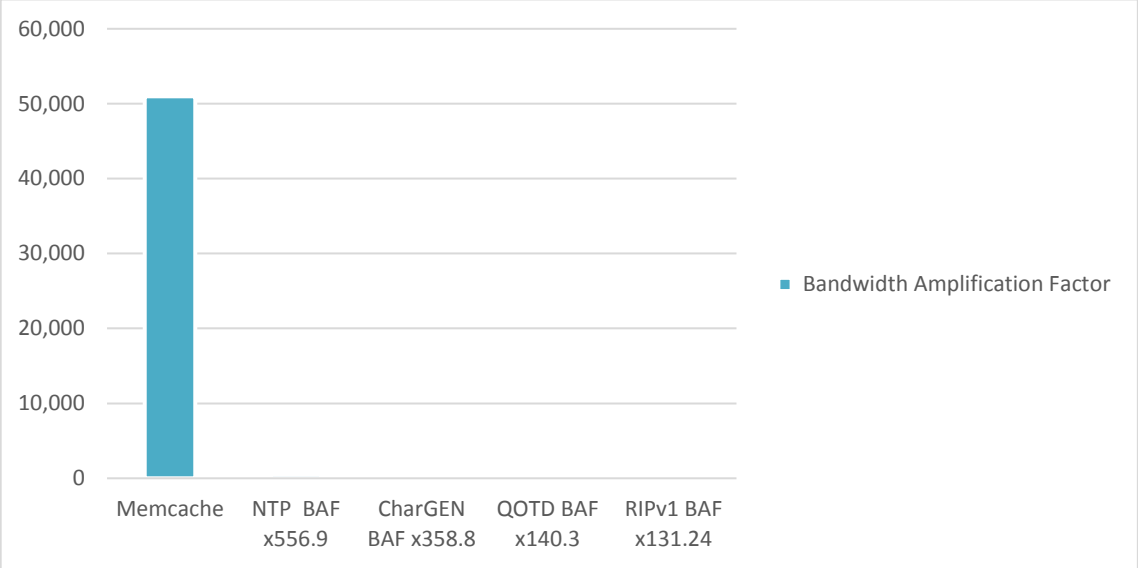


Figure 2: Top 5 bandwidth amplification factors

Defcon.pro offers trail packages that last three days and allow the user to launch one attack at a time for 200 seconds. The Captain Premium package is $20 per month and allows the user to launch one attack at a time for 1800 seconds. The biggest package a user can purchase is the Overlord package. This package includes the ability to launch five attacks at a time for 7200 seconds over 30 days.

PURCHASE

Choose a plan and have fun!

Plan	Max Boot Time	Concurrents	Length	Premium/API access	Price (USD)	Payment Gateway
TRIAL - Premium	200 Seconds	1	3 Days	✔	$3	Cryptocurrency (BTC/LTC/ETH/more)
Captain - Premium	1800 Seconds	1	30 Days	✔	$20	Cryptocurrency (BTC/LTC/ETH/more)
Chief - Premium	800 Seconds	2	30 Days	✔	$25	Cryptocurrency (BTC/LTC/ETH/more)
Admiral - Premium	3600 Seconds	1	30 Days	✔	$28	Cryptocurrency (BTC/LTC/ETH/more)
Knight - Premium	3600 Seconds	2	30 Days	✔	$45	Cryptocurrency (BTC/LTC/ETH/more)
Lord - Premium	3600 Seconds	3	30 Days	✔	$68	Cryptocurrency (BTC/LTC/ETH/more)
Champion - Premium	3600 Seconds	4	30 Days	✔	$125	Cryptocurrency (BTC/LTC/ETH/more)
Overlord - Premium	7200 Seconds	5	30 Days	✔	$250	Cryptocurrency (BTC/LTC/ETH/more)
Captain - Premium (Quarterly 10% OFF)	1800 Seconds	1	3 Months	✔	$54	Cryptocurrency (BTC/LTC/ETH/more)
Chief - Premium (Quarterly 10% OFF)	800 Seconds	2	3 Months	✔	$67	Cryptocurrency (BTC/LTC/ETH/more)
Admiral - Premium (Quarterly 10% OFF)	3600 Seconds	1	3 Months	✔	$75	Cryptocurrency (BTC/LTC/ETH/more)
Knight - Premium (Quarterly 10% OFF)	3600 Seconds	2	3 Months	✔	$121	Cryptocurrency (BTC/LTC/ETH/more)
Lord - Premium (Quarterly 10% OFF)	3600 Seconds	3	3 Months	✔	$183	Cryptocurrency (BTC/LTC/ETH/more)
Champion - Premium (Quarterly 10% OFF)	3600 Seconds	4	3 Months	✔	$337	Cryptocurrency (BTC/LTC/ETH/more)
Overlord - Premium (Quarterly 10% OFF)	7200 Seconds	5	3 Months	✔	$675	Cryptocurrency (BTC/LTC/ETH/more)
Captain - Premium (Semiannually 18% OFF)	1800 Seconds	1	6 Months	✔	$98	Cryptocurrency (BTC/LTC/ETH/more)

Figure 3: Package pricing on Defcon.pro

Reasons for Concern

Stresser services are not necessarily illegal and there are many legitimate uses for such tools. Most legitimate services will require you to provide proof that you own the website and have agreed to the network test. Unfortunately, most of the stresser services that Radware has observed do not require you to submit proof, let

alone verify the email address used to register an account. Instead they try to hide behind their terms-of-service by putting the legal responsibility back onto those carrying out the attacks. These off-the-shelf attack services are commoditizing the art of hacking, making it possible for novice hackers with little knowledge to launch attacks via affordable tools that are available on the clear and darknet.

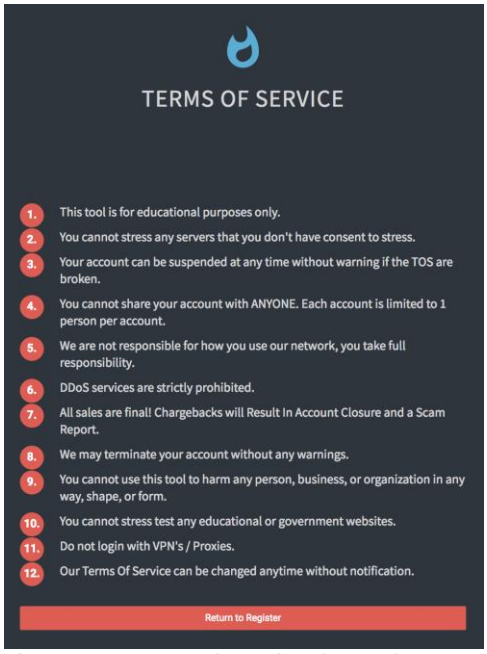


Figure 4: Terms of service for Defcon.pro

These services can be very profitable for the operators. Today you can find hundreds of these services publicly available via a simple search on Google. This is why they are targeted by both hackers and law enforcement. To make matters worse for the operators, most of these services are utilizing similar templates and are deployed with misconfigurations, making them a prime target for hackers like in the case of TrueStresser and PirateStress.

A main concern behind the Memcache attack vectors is the speed in which attackers evolved. Within a day of seeing a spike of activity against UDP port 11211 attackers launched the world's largest DDoS attacks. Five days later a 1.7Tbps attack was reported targeting an ISP as multiple scripts and amplification lists started to become public. Seven days after the first record-breaking attack was launched, the DDoS-as-a-Service industry began offering the Memcache attack vector.

To impound the concern, ransom groups will likely start sending out letters threatening the use of Memcache attacks as we saw directly after the release of Mirai's source code.

The last concern is one of a perpetual state. What's next? Memcached is a general purposed, distributed memory caching system typically used to speed up dynamic web applications by caching data and objects in RAM and reducing backend database or API round trips and should have never been exposed to the Internet. The exposure of the Memcached protocol to the Internet allowed attackers the ability to exploit the protocol to perform UDP-based amplification attacks. Now that attackers are contemplating amplification attacks again and are looking for exposed servers with vulnerable port caching large amounts of data, the question is, what will they target next?

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.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** 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-premise, out-of-path, virtual or cloud-based

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.