ERT Threat Alert
Memcached Under Attack
March 2, 2018

Abstract

On February 27, 2018 several organizations began publicly disclosing a trend in UDP amplified attacks utilizing exposed Memcached servers. The Memcached protocol was never intended to be exposed to the Internet and thus did not have sufficient security controls. Because of this exposure, attackers are able to abuse Memcached UDP port 11211 for reflective, volumetric attacks.

Background

On the last week of February, Radware's Threat Detection Network signaled an increase in activity on UDP port 11211. At the same time, several organizations began alerting to the trend of attackers abusing Memcached servers for amplified attacks. A Memcached amplified attack makes use of legitimate third party Memcached servers to send spoofed attack traffic to a targeted victim. Memcached, like other UDP based services (SSDP, DNS and NTP), are Internet servers that do not have native authentication and are therefore hijacked to launch amplified attacks against their victims.

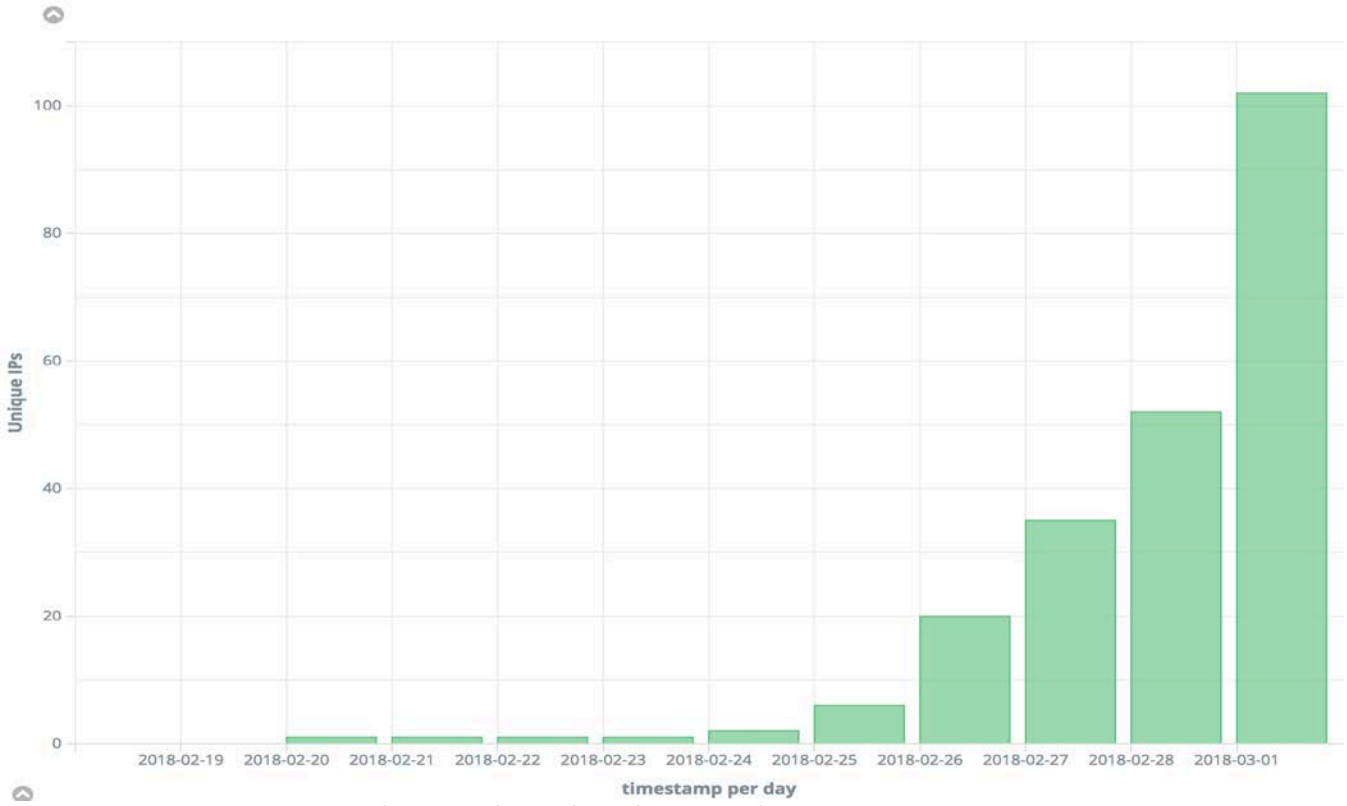

Figure 1: Threat detection network: UDP port 11211

A spoofed attack uses IP packets with illegitimate source IP addresses for the purpose of hiding the attackers true source IP. More ominously, by changing the source IP address of a packet, the targeted machine will send its reply packet to the false IP header address using the reply itself as a secondary attack. Those wishing to launch a DDoS attack without a large number of botnets can therefore send packets with random spoofed source IP addresses to both conceal their own origin IP address and launch volumetric attacks.

Due to the volume that can be reached with a single amplification list, attackers do not need a massive IoT botnet to launch 1Tbps+ assaults as with Mirai. At the core of the Memcached problem is the number of exposed servers on the Internet. With just under 100,000 exposed Memcached servers, it creates a prime reflector for an amplified attack. On February 27, Memcached version 1.5.6 was released which noted that UDP port 11211 was exposed and fixed the issue by disabling the UDP protocol by default. The following day, before the update could be applied, attackers leveraged this new attack vector to launch the world's largest attack.

Attack Methods

Memcached is a general purose, 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. Memcached APIs provide a large hash table (key-value) distributed across multiple systems. Most deployments of Memcached are within trusted networks where clients without authentication connect to any server. Memcached can be compiled with optional SASL authentication support but was deployed with TCP/UDP port 11211 exposed to the Internet. As a result, attackers can abuse this service to launch large-scale amplified attacks. The Bandwidth Amplification Factor (BAF) in the Memcached attack ranges between 10,000x and 52,000x, resulting in volumetric attacks that can easily reach well over 500Gbps. All the attacker has to do is scan the Internet for vulnerable Memcached servers to create an amplification list. Once the attacker has a Memcached amplification list they are able to craft a custom script to send spoofed requests to UDP port 11211 on the amplification list with the victim's spoofed IP address. The Memcached servers will respond to the request by sending an amplified request, vastly larger than the original request, to the victims IP address. The result is pipe saturation and service degradation.

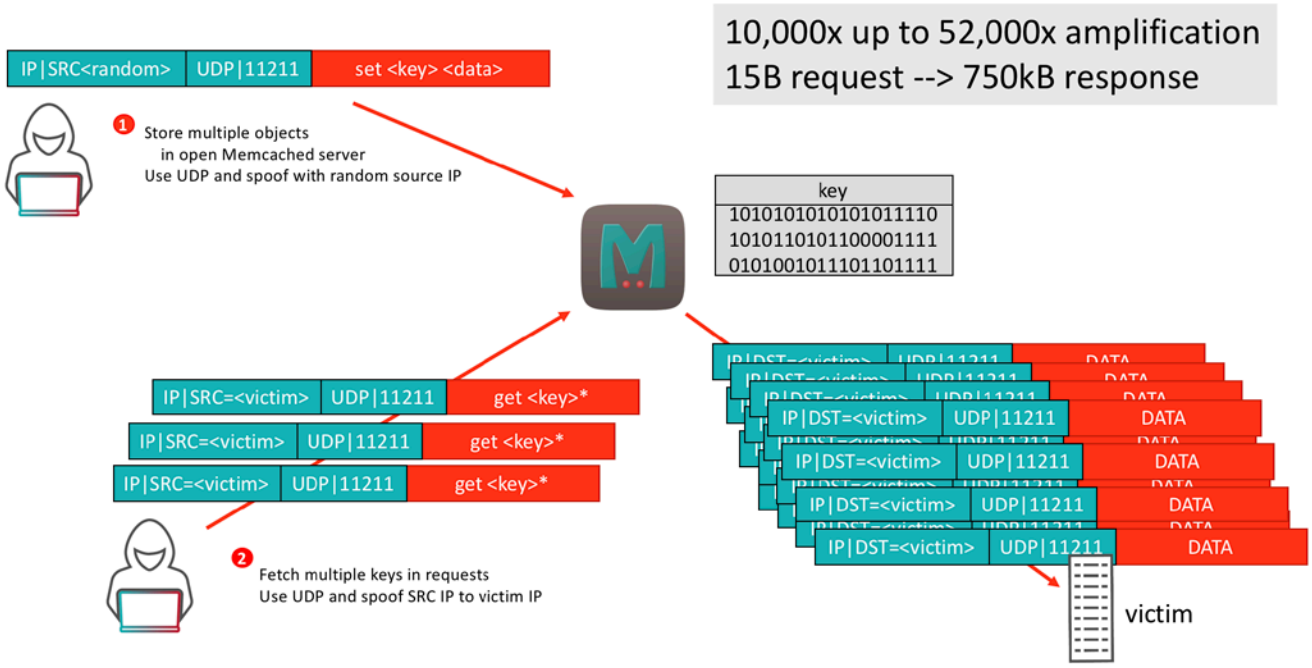

Figure 2: Memcached Attack

Targets

On March 1, 2018 Akamai and Github announced the world's largest DoS attack was recorded, targeting Github. The 1.3Tbps attack utilized thousands of vulnerable Memcached servers.

Reasons for Concern

There are two main concerns in regards to the Memcached vulnerability. The first issue is centered around the number of exposed Memcached servers. With just under 100,000 servers and only a few thousand required to launch a 1Tbps attack, the cause for concern is great. Most organizations at this point are likely unaware that they have exposed Memcached servers exposed to the Internet and it will take time to block or filter this service. Memcached servers will be vulnerable for some time, allowing attackers to generate volumetric attacks with few resources.

The second concern is the time it took attackers to begin exploiting this vulnerability. The spike in activity was known for several days prior to the patch and publication of the Memcached vulnerability. Within 24 hours of publication, an attacker was able to build an amplification list of vulnerable MMemcached servers and launch the world's largest DDoS attack, a title previously held by the Mirai botnet that had enslaved hundreds of thousands of IoT devices to launch a 1.2Tbps attack.

The days of amplification attacks are not behind us. Most attackers invest very little time in researching new vulnerabilities. Often times they just reuse the newest toolkit that produces the biggest results. Over the previous year, amplification attacks have taken a backseat to IoT botnets. Why? It is easy to scan the Internet for a specific device, allowing an attacker to automate a brute force attack against a list of devices, resulting in the ability to infect specific devices with a malicious payload. While amplification attacks are currently not the most popular attack vector, this doesn't mean amplification attacks are still not leveraged.

How to Prepare

On the Memcached server side, mitigation includes disabling UDP, updating to the latest code version (1.5.6 as of this writing) which disables UDP by default, or enabling the optional SAML authentication.

On the client side, Radware's Emergency Response Team confirms that Radware DefensePro owners are fully protected from Memcached reflection attacks who use the configuration settings recommended in the table below, which includes Radware's Behavioral Analysis (BDoS) technology:

Radware Memcached Attack Mitigation – Recommended Settings			
Attack	**DefensePro Mitigation**	**Details**	**Notes**
UDP Port 11211 Reflection	Blacklist: Protocol: UDP Source IP: ANY Source Port 11211 Destination IP: Customer_Network Destination Port: ANY	Add via Vision GUI or CLI	This is the standard Memcached reflected attack vector
UDP Frag	BDoS fragmented UDP engine or Dos-All/ DDOS-udp-frag-oddness	Mitigating fragmented UDP related attacks using BDoS or Dos-Shield Signatures	This additional vector has been seen in some attacks
All	BDoS	In most cases should be configured as on by default	BDoS can mitigate these attacks as well, and acts as an effective catch-all should other vectors be introduced

Radware also recommends ensuring all DefensePro devices are updated to the latest versions recommended by your support team.

See More

For more information about recent UDP amplification attacks see the United States-Cert Alert.

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

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.