AWS Shield threat landscape review: 2020 year-in-review

by Mário Pinho | on 20 MAY 2021 | in AWS Shield, Foundational (100), Security, Identity, & Compliance |

AWS Shield is a managed service that protects applications that are running on Amazon Web Services (AWS) against external threats, such as bots and distributed denial of service (DDoS) attacks. Shield detects network and web application-layer volumetric events that may indicate a DDoS attack, web content scraping, or other unauthorized non-human traffic that is interacting with AWS resources.

In this blog post, I'll show you some of the volumetric event trends from network traffic and web request patterns that we observed in 2020 as more workloads moved to the cloud. It includes insights that are broadly applicable to cloud applications and insights that are specific to gaming applications. I will also share tips and best practices that you can follow to protect the availability of the applications that you run on AWS.

DDoS trends as more developers rely on the cloud

In 2020, we saw an increase in developers building applications on AWS and protecting their availability with AWS Shield Advanced, which includes AWS WAF at no additional cost. The DDoS threat vectors we observed were similar to the ones that were observed in 2019, but they occurred with greater frequency. Between February 2020 and April 2020, we observed a 72% increase in the monthly number of events that were detected by Shield.

TCP SYN floods and UDP reflection attacks, which attempt to reflect and amplify packets off legitimate services running on the internet, were among the most common infrastructure-layer events detected by AWS Shield in 2020. (In this blog post, we'll use the term *infrastructure layer* to refer to Layers 3 and 4 of the OSI model.) These tactics attempt to affect the availability of an application by overwhelming its ability to process packets or establish new connections on behalf of legitimate users. One of the oldest UDP reflection vectors, DNS reflection, remains the most common, at 15.5% of all infrastructure-layer events detected by Shield. TCP SYN floods were the second most common at 13.8%. This is unsurprising, because web applications commonly rely upon both DNS and TCP traffic. Bad actors can find a consistent supply of systems on the internet that can be used as reflectors, due to the properties of these protocols, or system misconfiguration.

Bad actors may use application-layer requests, in isolation or together with infrastructure-layer attacks, in their attempt to affect the availability of an application. The most common application-layer attack observed by Shield in 2020 was the web request flood, an observation that is consistent with prior years. This vector gives a bad actor more leverage, meaning that they can have a greater effect with less traffic and effort. Instead of having to exhaust the capacity of a network path, device, or other lower-level component, they only need to send more web requests than the application is able to handle. This attack vector was a significant cause of increased volumetric events detected by Shield in the first half of 2020. For more information about events detected by Shield during 2020, see Figure 1.

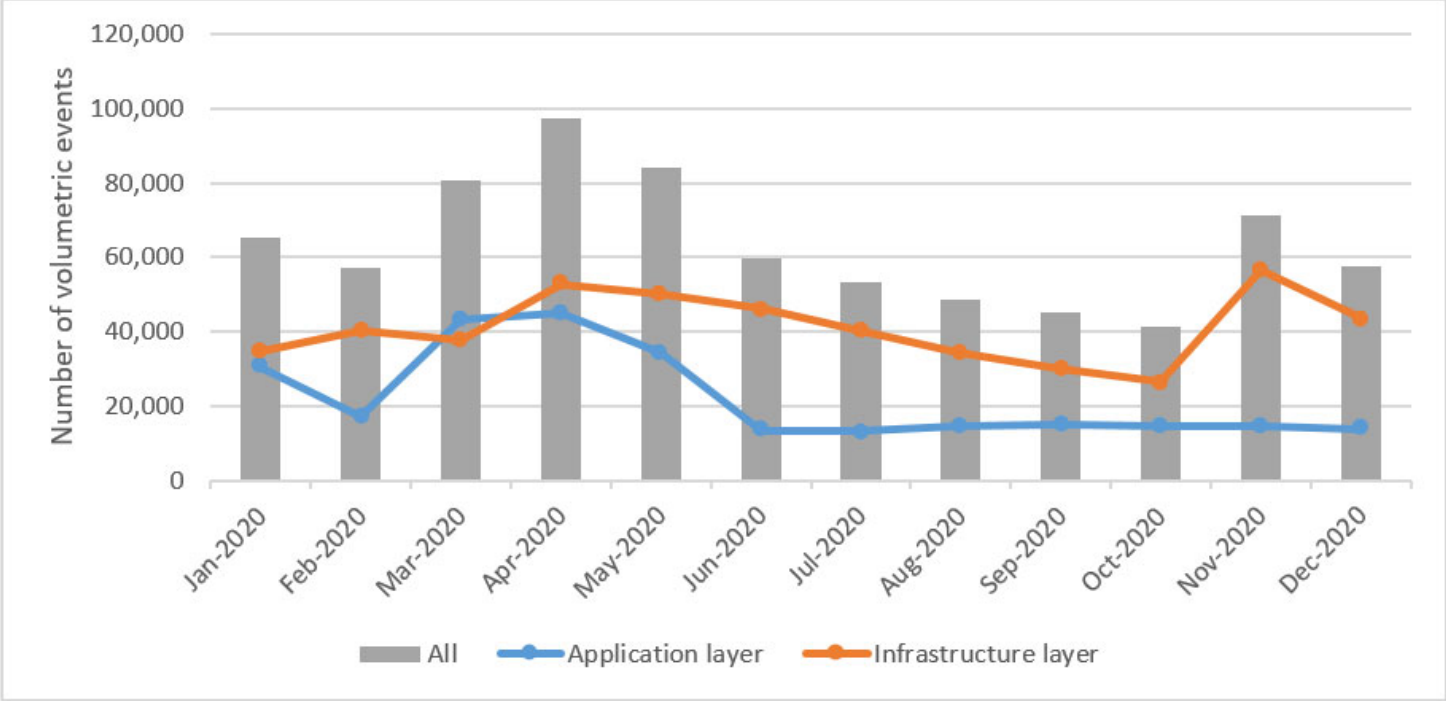

Figure 1: Monthly number of volumetric events detected by AWS Shield in 2020

A closer look at web application-layer attacks

The request volume of web application-layer events that are detected by AWS Shield has increased, an indication that bad actors are making greater investments in tactics that are more challenging to detect and mitigate than infrastructure-layer events. Shield continuously monitors DDoS activity and alerts customers if there is an elevated threat at any point in time. In 2020, Shield reported elevated threats on 53 days, 33 of which were caused by high-volume web request floods. There were 55 events with a volume of greater than 500,000 requests per second (RPS), some of which reached millions of RPS. The RPS of the 99th percentile (P99) of the volume of web request floods detected by Shield nearly doubled between the first and second halves of the year. (The 99th percentile is the request volume in RPS, below which 99% of request floods were observed.). For more information about the volume of web request floods detected by Shield in 2020, see Figure 2.

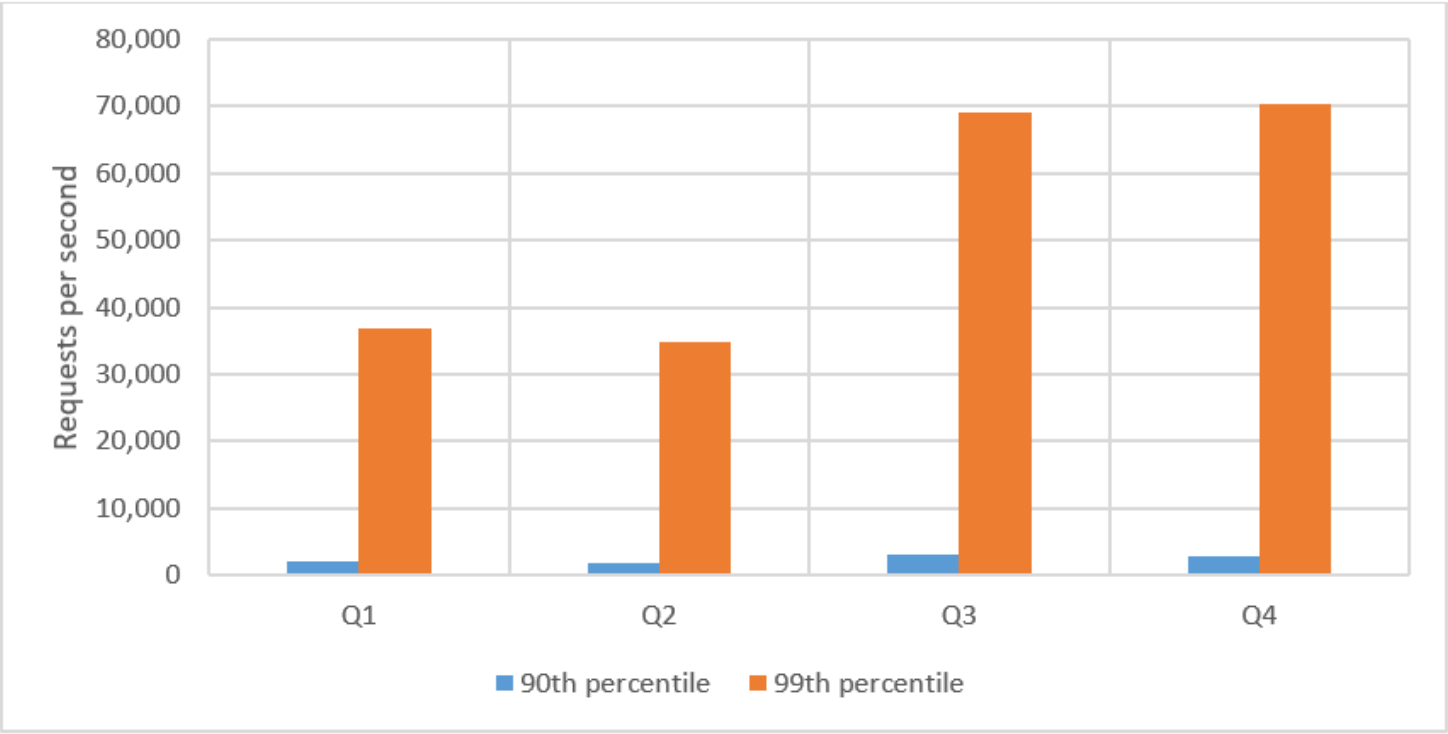

Figure 2: Quarterly P90 and P99 volume of web request floods detected by AWS Shield in 2020

It's important to protect web applications against DDoS attacks of any size. The more common request floods are relatively small, but smaller attacks can affect an application if it isn't architected for DDoS resiliency. You can follow these best practices to help protect your web application against request floods and other DDoS attacks:

- **Protect internet-facing resources with AWS Shield Advanced**. You can use AWS Shield Advanced to protect your applications that are running on AWS against most common, frequently occurring network and transport layer DDoS attacks. When you add protected resources in AWS Shield Advanced, network volumetric attacks against those resources are detected and mitigated more quickly. You also receive visibility into security events by using the AWS Shield console, API, or Amazon CloudWatch metrics. If you need assistance during an active event, you can quickly engage with AWS Shield experts or escalate to the AWS Shield Response Team (SRT).
- **Access greater network and request capacity with Amazon CloudFront and Amazon Route 53.** You can use these services to serve static and dynamic web content, as well as DNS answers, by using the global network of AWS edge locations. This provides you with greater capacity to help mitigate large volumetric attacks. Applications that are fronted by Amazon CloudFront and Amazon Route 53 also benefit from inline mitigation that continually inspects all traffic and mitigates most infrastructure-layer DDoS attempts in less than one second. CloudFront and the AWS Shield DDoS mitigation systems use *SYN cookies* to verify new connections, which protects against SYN floods and other traffic floods that aren't valid for the application. (A SYN cookie is a technique by which the Shield infrastructure encodes connection setup information into the SYN response (SYN-ACK packet) in such a way that the TCP connection resources are only consumed for legitimate clients who complete the TCP handshake.)
- **Use AWS WAF and rate-based rules to mitigate application-layer attacks.** AWS Shield Advanced provides you with protection against infrastructure-layer attacks that can be mitigated with network-based DDoS mitigation systems. When you add Shield Advanced protection to CloudFront or Application Load Balancer (ALB) for serving web content, you receive AWS WAF at no additional cost. AWS Managed Rules for AWS WAF makes it easy to

select and apply pre-configured rules, depending on your specific requirements. You also receive web request flood detection and can mitigate security events by configuring rate-based rules to match and temporarily block IP addresses that are sending traffic above a rate that you define. For larger applications, or applications that span multiple AWS accounts, you can use AWS Firewall Manager to deploy and manage rules across all of your resources.

Considerations unique to gaming use cases

On AWS, you can build and protect any kind of application. Internet-facing applications are more likely to receive DDoS attacks, particularly if a bad actor is motivated to disrupt the normal function of the application. We looked across AWS Shield data and found that one type of application stood out as the most likely to be targeted by DDoS attacks: gaming servers. Gaming servers host matches between players on their personal computers or gaming consoles. 16% of infrastructure-layer events detected by Shield in 2020 targeted gaming applications. The application might be targeted simply out of malice, or to gain an advantage in the game. Between Q1 2020 and Q2 2020, we observed a 46% increase in the frequency of events that were detected on behalf of gaming applications. This increase aligns with the increased use of residential internet networks during the same time.

There are unique considerations for protecting a gaming application against DDoS attacks. Many gaming applications rely upon UDP traffic, which makes it infeasible to block UDP as a countermeasure against the most common DDoS attacks, like UDP reflection attacks or UDP floods. You can nevertheless protect your gaming application and the experience of your players by using Elastic IP addresses and protecting these resources with AWS Shield Advanced. Shield Advanced has the ability to perform deep packet inspection of all traffic, even at extremely high PPS rates. Using that powerful tool, the AWS Shield Response Team (SRT) can work with you to understand your application and build a custom mitigation that allows only valid player traffic.

Reacting to extortion attempts

From August 2020 through November 2020, we saw a revival of DDoS extortion attempts, a tactic that is now more than six years old. Each extortion attempt reported by customers to the AWS SRT had familiar characteristics. A malicious actor would target an application that wasn't running on AWS as a proof of concept and then threaten a larger, follow-on attack if a ransom wasn't paid. Although it's very uncommon for the follow-on attack to actually occur, application owners take these threats seriously and use the opportunity to assess their own protection and operational readiness. In approximately 90% of AWS support cases related to these attempts, the SRT assisted the application owners directly with their preparation. We also assisted Shield Advanced customers who weren't directly targeted by extortion attempts but were aware of other extortion campaigns.

One question that we frequently hear is how AWS can help developers monitor their applications and take quick action if a possible DDoS attack is detected. When you protect your resources with AWS Shield Advanced, you have the option to associate an Amazon Route 53 health check. The status of the health check is used to improve the decisions that are made by the Shield detection system. If you have Shield Advanced proactive engagement enabled, the SRT is automatically engaged any time a Shield event corresponds to an unhealthy Route 53 health check that is associated to your protected resource. Based on the contact information provided in the Shield console, an SRT engineer will contact you to coordinate a response to the detected event. If you're running a web application, you

can choose to delegate access to your Shield Advanced and AWS WAF APIs to the SRT and provide the team with copies of your AWS WAF logs. During an escalation, an SRT engineer will evaluate your logs for DDoS signatures and robotic patterns and assist in building effective mitigations.

Summary

In this blog post, I shared some of the trends that were observed by AWS Shield in 2020, as well as steps that you can take to protect the availability of your applications against DDoS attacks. If you'd like to learn more about DDoS protection on AWS and configuring AWS Shield Advanced, check out the following resources:

- Getting Started with AWS Shield
- AWS Best Practices for DDoS Resiliency
- Guidelines for Implementing AWS WAF
- Shield Advanced proactive engagement
- How to Help Protect Dynamic Web Applications Against DDoS Attacks by Using Amazon CloudFront and Amazon Route 53
- Set up centralized monitoring for DDoS events and auto-remediate noncompliant resources

Want more AWS Security how-to content, news, and feature announcements? Follow us on Twitter.

TAGS: AWS Shield, AWS Threat Research Team, AWS WAF, DDoS, Gaming, Security Blog, threats, Web application