CloudFlare is at the center of internet attacks.

John Graham-Cumming, Michael Daly & Ólafur Guðmundsson
CloudFlare Inc.

CloudFlare is a young company working hard to make websites faster and safer. Everyday, we serve between 6-9% of all web requests globally. We've gained this scale by making it as easy and inexpensive as possible for new sites to be added to our network. Because of our growing Internet presence, we've attracted a large number of "disagreeable" sites as customers, and since there are many people out there who would prefer that these sites be knocked off the web, number of attacks we see each day is ever increasing. As a fast-growing startup with limited resources, CloudFlare has focused on making our service fast and reliable; however, we are also seeing a huge potential for analyzing attack traffic.

CloudFlare sees every type of Internet attack imaginable. We see everything from from simple attempts to flood a site with high volume of traffic, to attacks directed at our DNS and web servers, to sophisticated Layer 7 attacks that target sign-in screens using incorrect login information over and over again in order to block a user from being able to access their accounts. Attackers are constantly scanning servers for vulnerabilities, and test runs of attacks, C&C for botnets, and other malicious activities are crossing our network non-stop. However, we aren't always looking for these new types of attacks and sometimes it takes outside information for us to notice. Our thought is that with better interpretation of our network traffic, we can gain the ability to to predict future attacks.

Abuse

As a network operator, CloudFlare relies on third party anti-abuse organisations and their notifications to give us a much broader view of our network and the activities on it. In its current state, our network automatically parses notifications received from these organisations into our systems for processing; however, and sadly, we find that while there seems to be an accepted standard of notifications, ARF (or RFC 5965), it's our experience that these standards are not used often enough which adds additional development time to create custom solutions and slows the implementation of otherwise good data that can be used to make the internet a better place.

DNS

Every minute CloudFlare experiences DNS DoS attacks either against us, our customers (or, in some cases, our own DNS servers, despite our efforts to make them less appealing to attackers by making our DNS answers as as small as possible, are being used as amplifier in attacks against other site). We've developed a number of tools and techniques to mitigate and absorb these attacks, but at the moment, the only people we communicate with about these attacks are the customers that are being affected by them. In many cases, we simply absorb the attacks without noticing.

Attacks are growing in volume every week, but so is our ability handle them. This arms race has serious implications for medium and small DNS providers that they simply can't handle the scale of newer attacks and need help coping, this is an obvious area of collaboration.

When DNS service moves around that can be done by renumbering the nameservers or by moving Anycast blocks between providers. Both approaches have certain delays. The time to renumber nameservers is affected by the TTL on the address records. Adding new Anycast blocks needs coordination with upstream providers. Renaming nameservers does not work, due to long TTL's in parent zones/TLD's.

Netops <needs more>
Network operators are more concerned with delivering traffic than scrubbing attacks from it. The whole Internet would benefit if there was a way to reliably push authenticated scrubbing rules upstream to bandwidth providers. Right now, we are forced to handle most of the attacks with our server farms, and this sometimes requires multiple data centers to handle the traffic flow from a small set of attackers. More widespread use of BGP-38 would help in particular at hosting providers as well as at Tier-1 network operators.

Security
CloudFlare is an active participant in the security community. As a company dedicated to improving the security of the Internet, we take security vulnerabilities and security intelligence very seriously. We use responsible disclosure when dealing with vulnerabilities discovered by our security researchers. We also reward and protect security researchers who find vulnerabilities in our software with our bug bounty program.

CloudFlare has contributed to the public discourse about several high profile security issues leading to improved public understanding of Internet security. For example, information obtained and published by CloudFlare during a large NTP reflection attack led to a large reduction in the number of vulnerable servers on the Internet, reducing efficacy of this attack vector. Also, the CloudFlare Heartbleed Challenge helped raise awareness about the severity of the Heartbleed vulnerability. Furthermore, work by CloudFlare researchers has been instrumental in understanding security issues such as ShellShock, SuperFish, and more. We will continue to share information and intelligence about new attacks that we see against our network and the security exploits we encounter.

Layer 7 attacks
Many of the modern attacks CloudFlare servers see are at the application layer, e.g., SQL injections, buffer overflow attempts, etc. We currently deflect most of these attacks using fast patching of systems, and application specific firewalls that can block these attempts. Learning about new attacks and blocking them is a high priority for us and our customers. When we discover or learn of new attacks we can block them and monitor attempts to exploit the vulnerability for all of our customers across our global network.