REPORT REPRINT

Beam me up, Avi: Kentik CEO thinks we might need the Federation to block DDoS

PETER CHRISTY

23 NOV 2016

Longtime networking and industry expert Avi Freedman thinks that blocking the anticipatable monster DDoS attacks to come probably requires innovative business and commercial structures, not just technology.

451 Research®

Responding to questions from 451 Research about the current DDoS attacks, Avi Freedman, Kentik CEO (and longtime Internet infrastructure expert) described an innovative federated model for DDoS solutions, bearing some resemblance to some advanced CDN models that he has suggested in the past (Freedman led Akamai's early networking strategy).

The proposed solution architecture is based on both centralized (detection and control) and distributed (mitigation) elements, typically owned by many different parties – hence the need for federation. The most innovative (or challenging) aspect of what Freedman suggests is the economic model: make the mitigation technology is cheap as possible; include a 'settlement' system in the architecture that compensates those performing the mitigation when protection is invoked (incoming traffic would be redirected only when an attack is detected).

Freeman has been around the block many times, and understands that what he is proposing would be unlikely to happen under 'normal' circumstances. His hope is that the seriousness of recent threats, and the clear potential for much worse attacks, will be enough to motivate the Internet ecosystem to consider something new for the collective good.

THE 451 TAKE

Growing DDoS attacks unquestionably pose a risk to Internet use, a scary proposition given the increasing degree to which we depend on Internet services and connectivity for all aspects of our day-to-day life. So far, the magnitude of the largest attacks hasn't visibly triggered significant collective action (we're sure there is much discussion behind closed doors.) What Kentik's Freedman proposes is tantalizing because it seems like it could be deployed relatively quickly (a fraction of a year, not years), is based on existing technology and proven system designs, and provides a means for those protected to pay the costs when the protection is needed. The open question is how much worse things have to get before solutions like this receive serious and broad consideration.

CONTEXT

Distributed denial of service (DDoS) attacks are a very visible threat to the operational reliability of the Internet. DDoS attacks are mounted for a broad spectrum of reasons ranging from simple blackmail to political activism or disruption. The basic idea is simple: find a way to create large volumes of false traffic to a given website, service or (more recently) Internet infrastructure service (e.g., DNS services) such that the combined good and malicious traffic overwhelms the service capacity and, as a result most of the legitimate requests are 'denied.' In the past, many DDoS attacks were mounted using virus-infected PCs ('zombies') under control of a 'bot network.' In the most recent twist, consumer devices like security cameras – designed to generate high traffic volumes – have been added to the set of zombie devices, raising the total attack traffic to breathtaking new heights (in excess of 1Tbps – a million Mbps).

DDoS control, like spam control, is a network application where the solution is often best done distantly from where the problem is (in this case, near the source of the DDoS traffic). In the case of monster DDoS attacks to come, the mitigation has to be done as close to the source as possible to keep the attack traffic from overwhelming big chunks of infrastructure.

PRODUCTS

Freedman is proposing a way for the Internet ecosystem to prepare for the anticipatable, much larger (10 and 100Tb) DDoS attacks to come. The DDoS solution would be provided by using new 'scrubbing' appliances placed in the access networks near the sources of DDoS traffic. The edge network providers would deploy these new scrubbers as part of a community effort, but with each network's scrubbers under their ownership and control. The use of these scrubbers would be invoked by one or more DDoS detection systems, purchased and operated by the web sites, services or infrastructure providers desiring protection. When a DDoS attack was detected, attack traffic would be redirected through the scrubber(s) nearest to the source. After the attack, those protected would compensate the scrubber owners for the additional traffic, using an automated settlement system, at rates agreed to by the parties beforehand.

Freedman believes that a suitably programmed scrubber, running on an inexpensive, commodity server or white box switch, can scrub in excess of 10Gbps of volumetric attack traffic (Kentik builds similar monitoring appliances as part of its traffic analysis system, so the opinion is an informed one). These appliances could be built into larger scrubbing systems, adding additional servers as needed. An inexpensive 'white box' switch could handle the traffic distribution among the appliances.

It takes 100 10Gbps scrubbers to provide 1Tbps of protection. Building out to handle 100Tbps would require 10,000 scrubbers. If the server or switch costs $2,000, that represents $20m of capital investment, a significant sum but quite affordable if spread across the various access network providers. If there are two billion Internet access customers globally, the capex required is about $.01 per subscriber (order of magnitude).

Freedman is hoping that the scrubbing software can be provided at minimal cost through some community-driven open source or open core initiative. The minimal ongoing testing and distribution costs to maintain and evolve the software could be paid by product vendors of the detection and mitigation systems.

The other parts of the solution are DDoS detection and mitigation control systems. Kentik builds one of them. When a DDoS attack is sensed, it is characterized (the nature or signature of the attack traffic discovered) and using this information, mitigation services invoked (such as today's large A10 or Radware scrubbing appliances).

An appropriately sophisticated, new orchestration system could function as a 'phase-modulating shield' – sensing the changing nature of an attack, and dialing in the simple to sophisticated resources needed, in as distributed and sophisticated-response a fashion as required to react to the modern attackers, who change tactic and volume as defenders respond. Freedman says the current Kentik offering could be evolved to serve this function.

MARKETING

The market for this solution has two very distinct (but interconnected) elements: the specific web site services and infrastructure services with the most to gain by having a more robust DDoS protection mechanism in place, and the set of network service providers whose participation is required to make such a solution work. The on-demand mitigation devices don't have to be deployed universally, but do have to be deployed into enough networks with adequate global distribution and network capacity to intercept the anticipated huge attacks to come. The market issue is how best to create adequate distributed protection in anticipation of attacks.

Freedman doesn't think any existing mitigation system has enough capacity. CloudFlare was built from the beginning to add massive processing capacity at the edge, but has specialized in protecting Web systems, not arbitrary traffic. The largest general systems to date (e.g., Prolexic, now Akamai, as well as network provider internal systems similar to what AT&T has built and used) operate by flowing the attack traffic through a relatively small number of large mitigation systems. Freedman thinks this approach is unlikely to scale adequately in the face of attacks that he believes may be coming, and is intrinsically more expensive compared with a single-mitigator distributed edge approach.

In the case of the internet, the market includes the government because the internet is critical infrastructure and increasingly leveraged for government services and operations. Freedman believes that if the industry does not quickly deploy the assets to quench attacks close to the source, we could see well-intentioned regulation with unintended and potentially wide-reaching consequences; for example, government-imposed technical requirements for all consumer devices.

COMPETITION

The leading DDoS mitigation services today are provided by Akamai, Verisign and Neustar. These are relatively concentrated solutions with unknown capacity (they don't publish capacity for good reasons; industry experts speculate none could survive a 10Tbps attack). Radware, A10 and F5 sell a variety of enterprise and service provider DDoS protection systems. With current commercial models, you buy the protection potentially offered by these products up front, so the cost of these products is much more expensive (on a volumetric basis) than the cost of the server hardware needed to provide mitigation. This a perfect example of the economic elegance of the federation model, where the up-front cost is minimized and spread among many network providers, and the compensation dynamic based on use. A federated solution doesn't replace the need for such appliances, however, because they are still needed as part of a comprehensive site protection solution to detect and block sophisticated application-layer attacks. It would be up to those vendors to decide if they wanted to join a larger, federated approach (and provide local protection and control and settlement of distributed protection).

CloudFlare provides an attractive DDoS protection service for websites (as do other CDN vendors, including L3 Networks and Highwinds as well as Akamai's Kona). Each could be a mitigation service provider (all have distributed communications processing capability) if they chose to add the additional protocol capabilities and build out significant additional capacity.

SWOT ANALYSIS

STRENGTHS

What Freedman proposes is an innovative way of plausibly assembling available technology in an affordable way to build DDoS mitigation capabilities capable of scaling to the threat of modern attacks.

WEAKNESSES

This approach requires creative forms of business alliances assembled for the communal welfare, never easy to do, and Internet-scale detection and orchestration, which has not yet been released by Kentik or other vendors as a commercial offering.

OPPORTUNITIES

There is no reason to believe that the threat of crippling DDoS attacks is going to diminish; the only real question is how much worse they need to get – and how much collateral damage they will need to cause – before it serves as a call to collective action.

THREATS

Unless the Internet ecology drives a solution to DDoS attacks, it is likely that the government will take action or has to take action. In general, the government driving technology doesn't work out well.