Protect Your IP from Diversionary Attacks

- A DDoS Primer by

Merit Network, Inc.

merit

The Issue

DDoS attacks have become a prevalent challenge for higher education institutions, impacting monetary resources and well-established reputations. Considering the sheer potency of these events, all organizations that utilize the internet should be aware of and prepared for DDoS attacks. However, many organizations are sorely unprepared when they are targeted by hackers. This lack of preparation can result in extended downtime, customer complaints, revenue loss, and extensive mitigation costs. With a thorough understanding of the catastrophic potential of these attacks, Merit Network discussed the state of DDoS and what Merit is doing to protect their own network.

Discussion Participants

Pierrette Widmeyer - Facilitator
Director of Marketing, Communications and Events

Michael Milliken
Vice President of Technology and Operations

Kevin Hayes
Chief Information Security Officer

David Dennis
Executive Director of Product Management

DDoS Defined

DDoS stands for Distributed Denial of Service. During a DDoS attack, anywhere from hundreds to hundreds of thousands of internet bots are deployed, inundating a specific server, network, or application with requests and traffic. This results in service being denied to legitimate users, like customers, employees or students. The fundamental architecture of the Internet has created inherent vulnerabilities within websites based on the way machines communicate online. "Hackers have ways of inflating and coordinating different hosts on the Internet to send concentrated amounts of traffic to a victim's site, like one of our members, which could take their web properties down," said Milliken. Not only are the target's web properties or websites at risk, their general internet access can be severely impacted. This lack of connection can restrict access to commonly utilized cloud-based services, like Gmail, Google Suite or Office 365. "No one can access any of these services during a DDoS attack, because their internet connection would be full of all of this bogus traffic," Milliken continued.

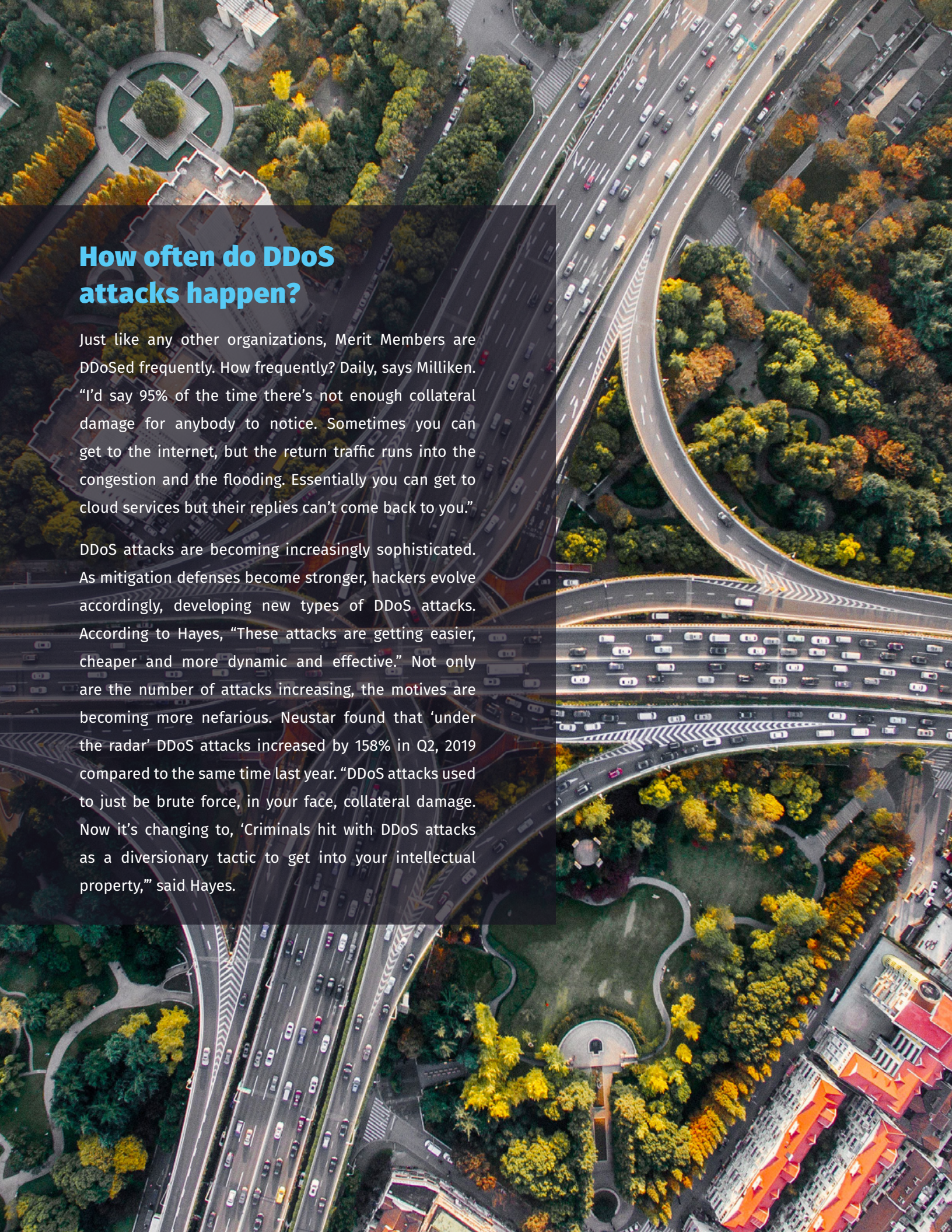
Hayes added that the perpetrator, "Doesn't have to be a sophisticated hacker to carry out these types of attacks." Anyone with a grudge and internet access can potentially inflict severe damage upon any organization of their choosing. "These attacks have been commercialized to the point where someone with almost no technical expertise whatsoever can go onto the dark web, pay some crypto currency, and say, 'I would like an attack launched on this organization, or server, or IP address.' And if that happens, it's game over."

Why would someone want to perpetrate this kind of attack?

Kevin Hayes has seen a few examples of motive. "We have seen students launching DDoS attacks on their schools to prevent the administration of tests or exams. We've seen DDoS attacks happen at universities where political activism or personal vendettas come into play in addition to online gaming feuds. One of the individuals being attacked could just be a student or employee on your network; because of a tiny little quarrel over a game, all of your business operations could be at risk."

"Someone with almost no technical expertise whatsoever can go onto the dark web, pay some crypto currency, and if that happens, it's game over."

- Kevin Hayes
CISO
Merit Network, Inc.



How often do DDoS attacks happen?

Just like any other organizations, Merit Members are DDoSed frequently. How frequently? Daily, says Milliken. “I’d say 95% of the time there’s not enough collateral damage for anybody to notice. Sometimes you can get to the internet, but the return traffic runs into the congestion and the flooding. Essentially you can get to cloud services but their replies can’t come back to you.”

DDoS attacks are becoming increasingly sophisticated. As mitigation defenses become stronger, hackers evolve accordingly, developing new types of DDoS attacks. According to Hayes, “These attacks are getting easier, cheaper and more dynamic and effective.” Not only are the number of attacks increasing, the motives are becoming more nefarious. Neustar found that ‘under the radar’ DDoS attacks increased by 158% in Q2, 2019 compared to the same time last year. “DDoS attacks used to just be brute force, in your face, collateral damage. Now it’s changing to, ‘Criminals hit with DDoS attacks as a diversionary tactic to get into your intellectual property,’” said Hayes.

How does Merit protect their members?

In response to these attacks, Merit enacts DDoS mitigation at least once a week. “If the traffic comes across our network, we enact mitigation that scrubs the traffic and returns clean traffic. It takes all of the threat vectors out,” said Milliken. Merit’s managed service is constantly developing a baseline from standard traffic patterns. “If you normally receive a few hundred DNS queries returned from the greater internet, and suddenly you get ten thousand, our managed service knows.” When the service identifies unusual traffic, it alerts Merit and mitigation protocol is applied.

Merit’s managed service is specifically targeted to relieve large, sustained events known as volumetric attacks. “The goal of this kind of attack is to either take you offline or cause collateral damage to your firewall or gateway,” said Miliken. “A student who doesn’t want to take an exam could use their phone and the organization’s internal wifi to figure out the IP address, load that into a network stresser, and next thing you know, they’ve rented a DDoS for the next half hour.”

“A student who doesn’t want to take an exam could use their phone and next thing you know, they’ve rented a DDoS for the next half hour.”

- Michael Milliken
Vice President
of Technology
and Operations
Merit Network, Inc.

> **"These attacks are getting easier, cheaper and more dynamic and effective."**
>
> **- Kevin Hayes**
> CISO
> **Merit Network, Inc.**

Can you afford good protection?

Effective security can be costly. One member transferred to Merit's service after spending more than $100,000 in one year with another mitigation service. Merit's approach is to pool resources within the community to create a low-cost alternative to other forms of DDoS protection. "We're trying to share the cost load with everyone in the community and so far that's been well-received," said Dennis. With this structure, the more members that buy in, the greater the level of protection that can be provided over time. "Sharing a resource and an insurance policy is one of the best values you can get and still have the protection." One factor ensuring that Merit's service is more cost-effective than other alternatives is the pricing model. "Many DDoS solution providers out there charge per incident. Organizations don't budget for that scenario because they can't predict how many times they're going to be attacked over the year. With Merit's pricing model, it's one set price for the entire year so members have consistency and their budgets aren't literally at the whims of attackers." Dennis continued.

Merit's evolution to continually provide the best DDoS protection

Merit continues to evolve in order to provide the best protection possible. Dennis believes that research and networking are key factors in this evolution. "Merit is continuing to track the industry. We're maintaining close contact with industry experts as well as the larger national research and education network community to pull in the best solutions for our members."

"As security professionals we need to stay on course and be as nimble as the attackers are. This is a constant cat and mouse game - we know these attacks are not going away, and we need to stay caught up," said Hayes. Merit is committed to staying abreast of industry events, adapting based on new information, and constantly refreshing protection mechanisms and service solutions to best serve our members.

"This is a constant cat and mouse game, we know these attacks are not going away, and we need to stay caught up."

- Kevin Hayes
CISO
Merit Network, Inc.

merit

Merit.edu | sales@merit.edu

For 50 years, Merit Network has been a trusted, Michigan-based nonprofit organization that provides shared IT resources, professional development courses and cybersecurity solutions for education, government, libraries and other nonprofits.

merit