WHITE PAPER

The new cyber arms race

A changing attack landscape requires a modernized strategy

Rapid changes in DDoS attack landscape require companies to re-evaluate their existing approach to DDoS security.

LUMEN®

DDoS attacks are changing. Is your strategy keeping pace?

Attack frequency on the rise and severity of impact greater than ever

In early 2020 Lumen began tracking a trend of increasing distributed denial of service (DDoS) attacks. DDoS attacks have seen average annual growth over 15% over the last five years. Not surprisingly, there is often an upward arc of DDoS attacks and cyber-extortion campaigns during the holiday shopping season. Historically they have focused primarily on retail, gaming and other organizations that rely on their websites and web applications for a significant portion of their revenue during the holidays. What is unique in this case is that the new wave of attacks is taking place outside of the traditional holiday season, and the targeted companies are not just the typical industries. Several recent attacks were sustained for weeks in some cases in industries that were as varied as healthcare, manufacturing, insurance and logistics. What were once intermittent ransomware incidents are evolving into full-blown extortion campaigns. Clearly new patterns are emerging.

2.3 Tbps

Largest attack recorded in 1H20[1]

24%

In 2019, DDoS attacks accounted for external attacks on enterprises globally[2]

14%

Annual growth rate of number of DDoS attacks (2018-2023)[3]

Importantly, these disruptions are occurring at the same time companies are dealing with an increasingly remote work force that needs to access corporate assets and populations who, because of Covid-19, are more reliant than ever on conducting everything from grocery shopping to attending school online. While our collective dependency on internet-accessed services is increasing, threat actors are seeing this as their perfect opportunity to pursue cybercrime and extortion, continuing their hockey-stick-like growth in attacks.

All told, DDoS attacks in April-May set historic precedents with 929,000 attacks according to Netscout: these were "the single largest number of attacks we've ever seen over any 31-day period. Moreover, attack frequency jumped 25 percent during key pandemic lockdown months."[4]

LUMEN®

Attacks becoming more sophisticated

From July to October 2020 attacks continue, and Lumen has seen as much as a 1200% monthly increase in emergency DDoS mitigation activations. It is clear that the tactics and targets of DDoS attacks are changing yet again and cyber-extortion against multiple industries is underway, with attackers both demonstrating their capability to directly extort companies, and the monetary asks increasing more than ten-fold, ranging from $20,000 historically to $340,000 to call off the attack according to the FBI.[5]

From July to October 2020, Lumen has seen as much as a 1200% monthly increase in emergency DDoS Mitigation activations

In other words, the criminals are adapting to the changing landscape and seeing opportunity. These attacks are large and extensive enough to raise the ire of the FBI, which issued a Flash Alert on the trend urging businesses to prepare and report attacks regardless of whether they paid ransom or not. The FBI has indicated that thousands have already reported attacks. Lumen sees this trend continuing as businesses become ever more dependent on the public internet.

Historically, attacks can range from generic script-kiddie varieties that can be easily ordered anonymously for as little as ten dollars over the internet to attacks backed by nation states. Increasingly, many attack vectors are mixed – this is a change from the early days when attacks were easily mitigated with simple filters, one that Lumen and others including Netscout have noted: attacks using multiple vectors (the most complex types of attacks to mitigate) "grew 2,851 percent from 2017 [a time] when such attacks were considered outliers."[4]

Lumen mitigates ~140 DDoS attacks daily

~89% of the top 100 DDoS attacks were multi-vector

~19% of the top 100 DDoS attacks targeted the application layer

These new tactics reflect a very business-like approach to targeting companies with complex layered approaches in the multi-gigabit range. The FBI Flash reported "observed DDoS attacks were primarily reflective attacks with ranges in peak volume from approximately 28.8 gigabits per second (Gbps) to 200 Gbps. UDP and UDP-Frag floods, some leveraging WS-Discovery amplification, combined with TCP SYN, TCP out-of-state, and ICMP Floods" to name a few of the vectors.[5]

These new tactics, techniques and procedures (TTPs) are more traditionally associated with nation-state actors like the Iranian team that remains on the FBI's Most Wanted list and exhibits TTPs: the FBI reports they are "consistent with two previous cybercriminal RDoS campaigns in 2017 and 2019 in which a group identifying itself as 'Fancy Bear' sent RDDoS extortion emails."[5]

RDDoS goes big, becomes a mature criminal enterprise

Whether these attacks are truly nation-state sponsored, it is clear that Ransom DDoS (RDDoS) has gone fully commercial from an extortion standpoint: extortionists are methodically layering attacks pursuing a structured list of varied verticals and businesses, including e-commerce, financial services, retail, healthcare, state and local government, education, gaming, media and entertainment – and more. Regardless of where these attacks are coming from, every business needs to be prepared to match defense capabilities against the new attack landscape which is increasingly becoming a cyber arms race. In the second half of this brief, Lumen outlines questions you can use to help ensure your business is prepared.

How can your business address this emerging landscape?

While many companies have adjusted their cyber-hygiene strategy to deal with traditional ransomware attacks, DDoS has often remained on the periphery, tasked to the network operations team and often an after-thought to security and incident response teams. We suggest the following topics and questions to evaluate your company's current posture and preparedness.

Don't panic. Don't pay. Do prepare.

Common sense questions arise. Does it really make sense to pay off an unknown adversary with blackmail capability? Will my adversary reinvest that into increasingly sophisticated or damaging attack vectors in the future? If you are not prepared to pay, you need to understand the impact you face and review the level of preparedness you have. If you have no protection today, many companies such as Lumen offer emergency turn up services, but as fast as these can be invoked, they may not be fast enough to completely ward off the damage. The best approach is to prepare ahead of time.

Lumen customers reduced meantime-to-detect (MTTD) and meantime-to-respond (MTTR) for DDoS attacks by over 75%.[6]

Understand the blast radius, understand the impact

Clearly DDoS attacks disrupt the services companies provide to customers online. But the blast radius extends even further than that with so many workers relying on company resources accessed from their homes. A business can quickly come to a complete standstill if its remote workers cannot reach resources under DDoS attack. What's more, the rise of SD-WAN and public IP telephony services has also increased our dependence on the internet. Companies under a DDoS attack increasingly face the possibility of more extensive disruption.

It is important to understand the financial impact of an attack down to the minutes level. Which services will be disrupted? Which partners and projects rely on those services and what are the financial impacts of even the slightest disruption, let alone a sustained attack? Small businesses are not immune: ITIC reports those with 200-500 employees estimate just one hour of disruption could result in $100,000 or more. For large enterprises, the damages easily top $5 million for verticals including: banking/finance; food; energy; government; healthcare; manufacturing; media and communications; retail; transportation and utilities.

Want to see what a DDoS attack could cost your business? Use the Lumen DDoS Calculator.

LUMEN®

Revisit your Edge security, DDoS and RDDoS strategy

Are you prepared for new and evolving attack vectors? Do you have adequate protection? What new attacks can you expect, and how will they potentially impact your business? How can you address this as part of your cybersecurity strategy? At Lumen, we provide a roadmap of focus areas and questions to consider that will begin to bolster your environment to meet the challenge of the next generation of DDoS attacks:

Review your DDoS governance

Resist the temptation to focus on the tool. Focus instead on the basics first, identifying the gaps in your existing programs and opportunities for reducing risk. Lumen recommends establishing governance and compliance programs that consider DDoS an essential part of a cybersecurity program. Start with these questions:

1. Is your Risk Management program factoring in DDoS attacks and the potential for disruption to determine gaps and additional investments required? Is the business impact of DDoS fully quantified?
2. Have your Incident Response plans kept pace in identifying who has authority to mitigate, which teams are notified and where you can escalate support? Are debriefings of attacks included or regularly reviewed?
3. Is your SOC properly prepared to contact and activate the necessary scrubbing services, actively troubleshoot, and invoke containment measures?
4. Are you proactively, periodically reviewing mitigated attacks and identifying possible trends and improvements?
5. Are current and predicted changes to the IT environment likely to require new protective measures around DDoS, and have they been factored into IT planning?

LUMEN®

Identify the right approaches: volumetric, premises, Edge and beyond

Many teams are still surprised to discover that DDoS protection options cover several solutions that can work in concert to stop attacks. Lumen provides a variety of coverage options and tailored approaches based on modern edge architecture needs of evolving businesses.

Volumetric (aka) carrier-based solutions

Network providers are best suited to deal with the largest attacks because of their capability to absorb the pervasive armies of bots and uniquely support controls such as BGP FlowSpec to provide highly scalable attack mitigation. This is often the first place to start addressing what are the most historically prevalent types of attacks. Below we cover some of the questions for each service area.

1. Does your current subscription match the increased flow of your network?
2. Is your time to mitigation important enough to consider Always-On mitigation?
3. Have your routing and IP space been tailored to the appropriate response for mitigation? Some assets are attacked more frequently or present greater risk: are they protected appropriately?

Why Lumen for DDoS?

Global peering/carrrier agnostic

120+ Tbps of global network capacity, localized privated peering with private interconnects maximizes performance - more than 9,000 unique AS interconnects[8]

Tiered scrubbing architecture

Escalated to super or regional centers when thresholds exceeded, reduces collateral damage

First line of defense

Internet backbone as a layer of defense: 85+ Tbps of FlowSpec defense capacity, provides additional layers of mitigation against volumetric layers 3 & 4 attacks

Botnet takedowns

Black Lotus Labs removes ~63 C2s monthly from the Lumen network, less malicious traffic hitting customer firewalls

Lumen: Deep expertise backed by a global network, a broad portfolio and Black Lotus Labs

- Lumen® Professional Security Services offer hands-on support from a deep bench of certified in-house consultants and engineers so organizations battling limited or overtaxed resources can refocus their specialized security staff on what's most important to their business.
- Our team of experts is backed by a broad portfolio of security and networking solutions that can be tailored to meet our customers' specific transformation needs, including:
  - One of the largest and most deeply peered global IP networks with 9,000+ unique Autonomous System (AS) interconnects so we see more and can protect our customers at a scale that our competitors cannot easily replicate.
  - End-to-end layer 3/4 and layer 7 protection from one of the largest DDoS mitigation deployments in the world, with 15 global scrubbing centers hosting 85+ Tbps of FlowSpec mitigation capacity.
  - A DevOps-friendly edge compute platform that accelerates application performance to enhance digital interactions globally, with a modular marketplace of next-gen WAF, bot management and API protection solutions delivered through Lumen® CDN Edge Compute platform containers
  - Our threat research team, Black Lotus Labs, which helps protect the internet by leveraging Lumen's extensive global threat visibility to share threat intelligence and proactively take down known threats.
  - Automated threat detection and response built into security services to automatically block threats at the network before they cause harm to our customers.

Premises solutions

Following the layered attack vectors, many DDoS attacks attempt vectors that are not picked up by volumetric monitoring, flying under the radar and surgically striking services. They attempt to exhaust firewalls stealthily or take down select services distracting the IT teams while they exfiltrate data and execute other non-DDoS attacks. While firewalls have come a long way, they are not purpose-built to detect or mitigate these stealth attacks. However, appliances can be configured to work in concert with volumetric services. Lumen uses the fine-tuning of appliances in concert with our volumetric services to foil some of the most complex attacks. Here are some additional questions to ask:

1. Is your industry concerned by the disruption a stealth attack can have? Do you have a target-rich environment such as financial services where attackers may deploy DDoS as a smoke screen for a layered attack?
2. Does it make sense to invest in a premises-based solution? Prem-based DDoS can immediately and appropriately signal volumetric services when they are truly needed. Will the quick activation of DDoS prevent significant revenue loss?
3. Are you being attacked frequently with low and slow activations that force frequent cloud switch-over? Are you concerned about customer experience during peak periods if you have to use the sledgehammer of volumetric services where the finesse of a premises appliance will do?

Customers using the Lumen® DDoS Mitigation solution realized a 222% ROI over three years.[6]

Edge and beyond

With demand on content to be more feature-rich, there is a need to bring the interaction closer to the end user – which is why organizations are looking to the edge to serve content. DevOps teams must be empowered to easily configure, stage and push changes into production quickly without taking environments offline, diminishing user experience or making web applications vulnerable to threats. The traditional days of monolithic, centralized applications with large-scale infrastructure and IP addresses being protected has been increasingly blended with a variety of content, edge and cloud environments – each with unique requirements supporting a variety of workloads. Lumen, with its deep knowledge of content delivery experience, edge platform and rich heritage of managed services, has orchestrated solutions to accelerate and protect applications wherever they reside and to bring the application closer to the user. Teams concerned about denial of service across new environments can start with the following questions:

1. To what extent do I need to tailor my security experience based on the applications I need to protect?
2. Do I have regulatory or geographical restraints on where my data can reside?
3. How is security impacting my user experience and how do I optimize it to enhance my DX?
4. Is my existing environment foolproof? Can it be attacked and what would be the denial of service vectors that could be used?
5. How do I ensure my web security seamlessly forms part of my DevOps process? Are our existing cloud and edge protections adequate, able to be orchestrated and easy to manage and report on?
6. Does my team have the architectural and operational experience to provide security governance across the emerging edge landscape to identify risks and provide compliance assurance?
7. Are these new environments presenting opportunities to optimize and redefine my security posture and solution sets to provide more agility in dealing with emerging threats?

According to Forrester, nearly 60 percent of mobility decision makers are looking at implementing edge computing in the next year.[9]

Final thoughts

Covid-19 has shown us that even – or especially – in our darkest hours, predators will seek to exploit environments and will evolve their tactics to do so. The 4th Industrial Revolution presents us with enormous opportunities and challenges us to up our cybersecurity game at the same time. Lumen is prepared to help.

1. Ars Technica, AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever, June 17, 2020.
2. Forrester, The Total Economic Impact™ Of Lumen DDoS Mitigation Service, June 2020.
3. Cisco, Cisco Annual Internet Report (2018–2023) White Paper, March 2020.
4. Netscout, Threat Intelligence Report: Cybercrime: Exploiting a Pandemic,1H 2020.
5. FBI, Flash Alert FLASH-MU-000132-DD, Aug. 28, 2020.
6. Forrester, The Total Economic Impact Study of Lumen DDoS Mitigation Service, April 2020.
7. ITIC, Hourly Cost of Downtime Survey, June 2019.
8. Telegeography, Global Internet Geography Executive Summary, 2020
9. Forrester, Predictions 2020: Edge Computing Makes The Leap, 2019.

877-453-8353 | lumen.com | info@lumen.com