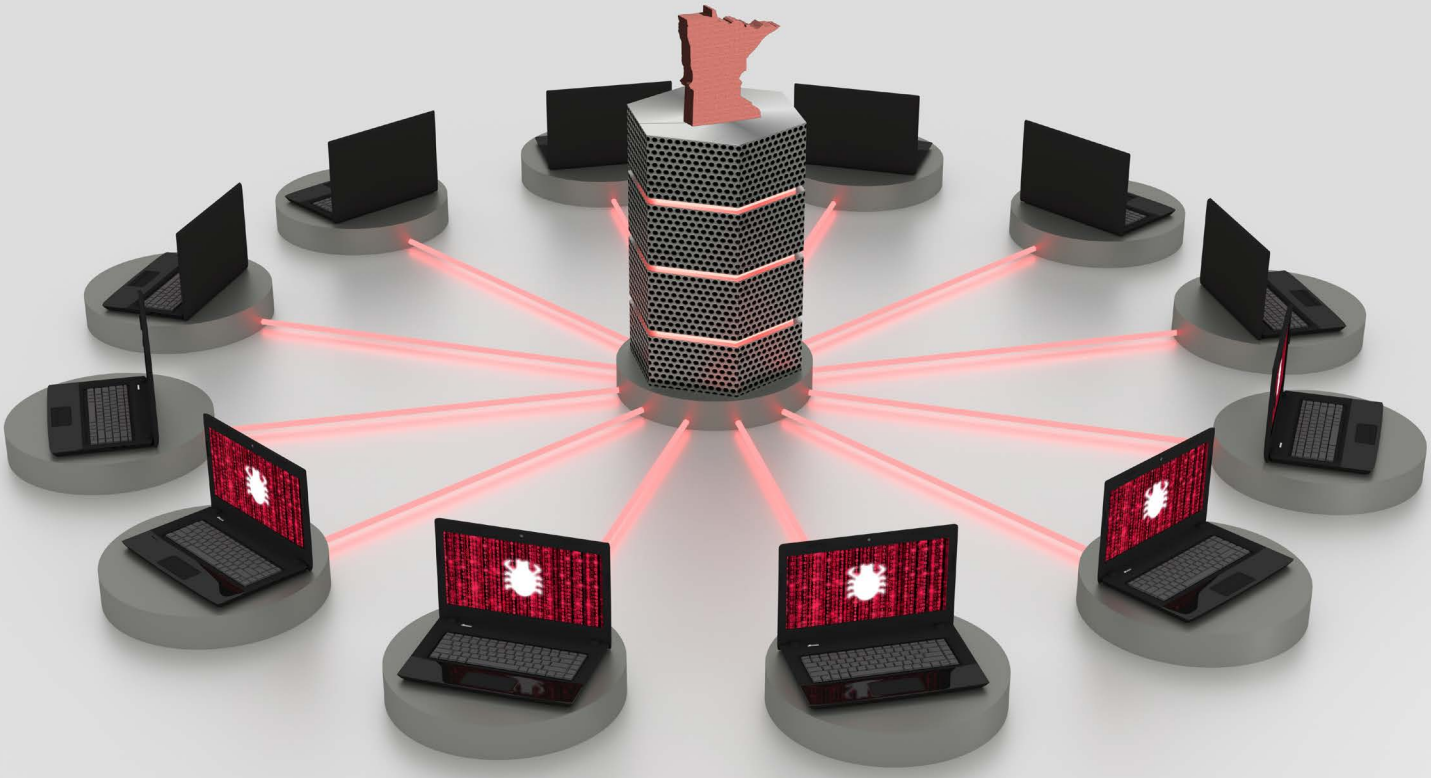


Detecting and Diminishing DDoS Attacks Across Minnesota

State of Minnesota — Minnesota IT Services

CATEGORY:
Cybersecurity

CONTACT:
Emily Dornfeld
Director of Communications
emily.dornfeld@state.mn.us
(O) 651-201-1011
(C) 651-485-1354

INITIATION DATE:
June 2020

END DATE:
December 2021

MINNESOTA IT SERVICES

Executive Summary

After the murder of George Floyd in Minneapolis in June 2020, MNIT's Security Operations Center (SOC) defended against distributed denial-of-service (DDoS) cyber-attacks aimed at overloading state information systems for 14 consecutive days. While the immediate incident response was complex and successful, the long-term implications of sustained and unprecedented volumes of DDoS attacks led to structural changes within the SOC.

The waves of these DDoS attacks over the two-week period had shifting tactics: targeting different resources or modifying attack patterns to skirt security defenses. The SOC ensured our DDoS mitigations continued to function for the immediate threats, and MNIT gathered intelligence from partners to quickly implement advanced defenses that would prepare critical resources from the evolving DDoS attacks. While defending from the attack and simultaneously advancing infrastructure capabilities on a compressed schedule, MNIT ensured that state websites remained available over 98.6% of the time during the DDoS attacks.

In the days and months following these attacks, MNIT implemented additional protections to enhance state defenses against ever-growing volumetric DDoS attacks and added additional defensive layers to protect web applications from advanced, scripted attacks from non-human actors (bots). These advanced bot defenses improve web service availability and allow MNIT to automatically allow known-good bots (like authorized web indexing crawlers) and block suspicious and malicious bots that attempt to compromise or overwhelm state web services. They also tell us when we are seeing spikes in bot traffic. For example, we know that in a typical month (February 2022), 9% of our web presence are bots, and a spike would deviate from that trend and indicate something to investigate. These services were so successful in defending state sites from attacks that MNIT expanded the use statewide and implemented a new web application firewall and bot management service that can be used on any state website.

Idea

What problem or opportunity does the project address?

DDoS attacks quickly evolve in both complexity and volume every year. In June 2020, in the midst of the COVID-19 pandemic and the devastating tragedy of the murder of George Floyd, the State of Minnesota and the City of Minneapolis were targeted by distributed denial-of-service (DDoS) cyber-attacks. The constant volumetric and application-level attacks concentrated on critical web applications in areas like public health and safety, as well as other vital services that the state uses serve Minnesotans. The attacks quickly overwhelmed in-place defenses and resulted in service disruption.

To put the attacks in scale, in 2019, the Security Operations Center saw 16 denial of service incidents across all our Minnesota government partner systems, out of over 3,000 detected incidents. During this DDoS event, the SOC saw 14 consecutive days of DDoS attacks.

Why does it matter?

Minnesota's mission is to improve the lives of Minnesotans by working collaboratively to implement policies that achieve results. Cyber-attacks that aim to overwhelm and take down state systems directly inhibit our ability to serve that mission.

Our adversaries include hostile nation-state actors. Because smaller partners in Minnesota government typically do not have the resources for protective tools, they are often victims of targeted attacks. New tools put in place after these DDoS attacks help protect crucial infrastructure for the state agencies, tribal nations, counties, cities, law enforcement, school districts, and boards that ensure a high quality of life for our residents.

What makes it different?

This effort was an expansion and enhancement of previous DDoS protections. A protective tool was placed at the border of the state's wide area network, Minnesota's Network for Enterprise Telecommunications (MNET). MNET by itself offers volumetric protection for all subscribers:

- All branches of Minnesota government
- County and local municipal governments
- Port cities
- Tribal nations
- K-12, and higher education

MNIT has had DDoS protections on the MNET border since the Minnesota Judicial Branch was targeted with recurring DDoS attacks in 2015, but the 2020 attacks exceeded the capacity of those protections.

Another unique aspect of this solution is that we created this through a partnership with the University of Minnesota and Minnesota State Universities. This triad of public sector network operators in Minnesota continuously coordinates resources to provide secure, reliable internet connections to all of our collective constituents. MNIT is the largest provider of the three.

A key part of this effort is that we approached this problem by trying to solve for all state entities – not just for the specific services being targeted, making this more unique than what other states have done.

What makes it universal?

The three letters in "CIA Triad" stand for **Confidentiality, Integrity, and Availability**. The CIA triad is a common model that forms the basis for security system development. It is used for finding vulnerabilities and methods for creating solutions. DDoS attacks undermine the Availability leg of the CIA triad. Every government organization must protect its ability to provide service to the people they serve by defending against DDoS attacks and upholding the availability of their services. This DDoS protection covers all MNET subscribers, and thus, all Minnesota government entities. The lessons we learned in implementing it are valuable to other states as they confront similar attacks, and as we prepare for more sophisticated future attacks.

Implementation

Who was involved?

The DDoS attack immediately gave us high-level support from all state and municipal leadership, from Minnesota's Governor Walz on down. MNIT teams from the Security Operations Center, Network, Threat and Vulnerability Management, Web Management, the University of Minnesota, and MNIT's security tool vendor.

When the attack happened, on-premise tools became overwhelmed. We first engaged an existing vendor who offered a more robust solution. The vendor and MNIT teams collaboratively added the solution. All the teams worked around the clock for 48 hours to fully mitigate the attacks so that the websites, services, and systems were functional and accessible.

What was the roadmap, and how did you do it?

MNIT has provided DDoS protections for MNET in partnership with our upstream network providers since 2015. These protections have been valuable but offered finite capacity in an era when we are seeing global DDoS events multiply and the average volume of traffic in each attack grow exponentially.

As the cyber-attacks during the 2020 civil unrest unfolded, MNIT, partners, and vendors analyzed the attacks and discussed possible solutions to maintain services and prepare to restore services in a short amount of time if attacks exceeded the capacity or capabilities of current protections. As attacks started to evade the current defenses, teams and partners quickly tuned the in-place defenses to bring partial restoration of services. The capacity and complexity of the attacks required an emergency implementation of cloud solutions to handle the current attacks, and any future high-intensity attacks in a very compressed timeframe.

We purchased, implemented, and tuned two cloud solutions – a cloud-hosted volumetric DDoS solution and Cloud Web Applications Firewall (Cloud WAF) with advanced bot management capabilities – in a very short amount of time to restore the targeted services. The tool also relieved the stress on our upstream connections to the internet.

The cloud-hosted DDoS solution quickly expanded the capacity of the existing on-premises DDoS protections by allowing MNIT to quickly divert traffic destined for impacted networks to the cloud DDoS provider via BGP route changes. This allowed for quick response to new attacks that could potentially exceed the capacity of the on-premise solutions and block the DDoS activity before it ever reached MNET. This solution quickly proved its worth within a week when ongoing attacks on the state eventually exceeded the prior capacities. Because these additional services were in place, MNIT was able to quickly protect the targeted sites with the new solution. Following the 2020 attacks, MNIT worked with its upstream providers and network partners to expand this new cloud DDoS solution to all MNET customers – ensuring that all state and local governments using MNIT's network services could take advantage of these same protections. Since this expansion, MNIT has automated the diversion

process to automatically redirect targeted networks for scrubbing using the Internet2 backbone for clean traffic return – ensuring even greater reliability than most alternative solutions available today.

MNIT implemented Cloud WAF because we needed a tool that would extend protection to a large number of applications without the staffing required by traditional on-premise Web Application Firewalls. The tool uses machine learning algorithms to understand legitimate use patterns of the protected web applications, which it then uses to detect illegitimate traffic. It also includes advanced volumetric DDoS protections and advanced bot management protections to identify and block malicious scripted attacks while allowing legitimate, beneficial scripts (aka bots) to crawl protected sites. The resulting accuracy and managed support offering drastically reduced how much staff time we needed to support the tool. Application security specialists were still required but could support more systems at once. The team onboarded 40 additional web applications within the first year of the program and have created a Cloud WAF and Bot Management service to expand these protections to all MNIT partners and services. We anticipate onboarding an additional 80 applications in the next six months.

As each application had different traffic patterns, they could not all be protected by one large application at the perimeter. MNIT's Threat and Vulnerability Management Unit (TVMU) formed relationships with the individual website owners to improve security across state agencies – taking a close look at application security issues. When new applications were onboarded to the new Cloud WAF, it improved their performance by filtering out unwanted internet traffic. That traffic was stopped by the cloud tool, so it never reached the application servers. Bot traffic was also reduced. The tool also found legitimate bot traffic in the millions of illegitimate web requests. This ensured that our external organizations, such as members of the press and health research institutions, that were legitimately using automated web scraping tools could continue using their "friendly" bots while the bot protection was in place.

We put in place other strategies to ensure that our defenses were prepared in advance of future attacks. These were approved by the MNIT Commissioner, the State of Minnesota Chief Information Security Officer, and other MNIT leadership. The additional efforts shored up our on-premise appliances to handle an increased capacity and increase collaboration between our partners, vendors, and internal teams.

Impact

What did the project make better?

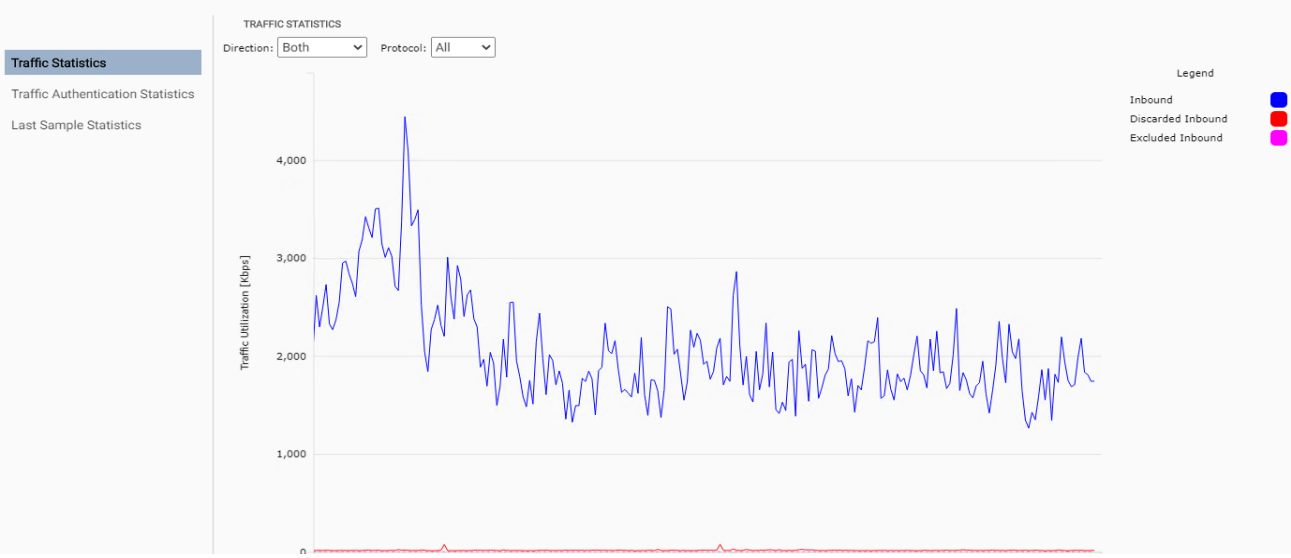
The network DDoS protection improved cooperation and collaboration across various branches of government. DDoS protections were immediately valuable to MNET subscribers and served to strengthen the trust these entities had in the state-level Security Operations Center. As DDoS attacks increased against Minneapolis and state-level law enforcement agencies, government leaders and stakeholders were reassured by the comprehensive DDoS protections – in place so swiftly and early in the emergency. This ensured that critical government functions across the state could continue. MNIT's security team proved that it could roll out a solution that worked in a very short period of time in a

manner that extended to far-flung government entities across the state. The new capabilities have continued to demonstrate value; over the last two years MNIT has been able to successfully defend additional government partners that have been targeted with recurring DDoS attacks.

How do you know?

During monitoring, the team noticed that DDoS infrastructure actively detected and mitigated traffic from blocked countries.

Figure 1: The graph shows the spikes of traffic during the attacks.



Results after the attacks

- The total traffic running through Cloud WAF tool is between 1Mbps to 15Mbps.
- Since June 2020, DDoS attacks have not taken down critical services.
- One county had persistent DDoS attacks for four months. Due to the protective tool, the county services remained functional with no degradation in speed or quality of services.

What now?

The long-term plan for the project is to continue protecting the government domains in Minnesota with the DDoS protection appliance at our border. Some Security Operations Center staff remain devoted to monitoring Cloud WAF. We also pay for a cloud service that is activated when Cloud WAF detects spikes in traffic above a certain volume. This helps ensure that the Cloud WAF itself does not become overwhelmed in an attack.

In addition to this DDoS protection at our statewide network border, we are building out protections for application-layer attacks that Cloud WAF cannot detect because the attack traffic is encrypted by the application's HTTPS encryption. To address this need, individual applications critical to Minnesotans

have been onboarded into a Cloud Web Application Firewall which is tuned to detect and stop application layer (Layer 7) DDoS attacks, unwanted bot traffic, and web application attacks. Some of our web applications have been attacked by bots that guess passwords and search for vulnerabilities, and the Cloud WAF has mitigated those attacks. Going forward, MNIT is implementing Cloud WAF protection for all critical state web applications.