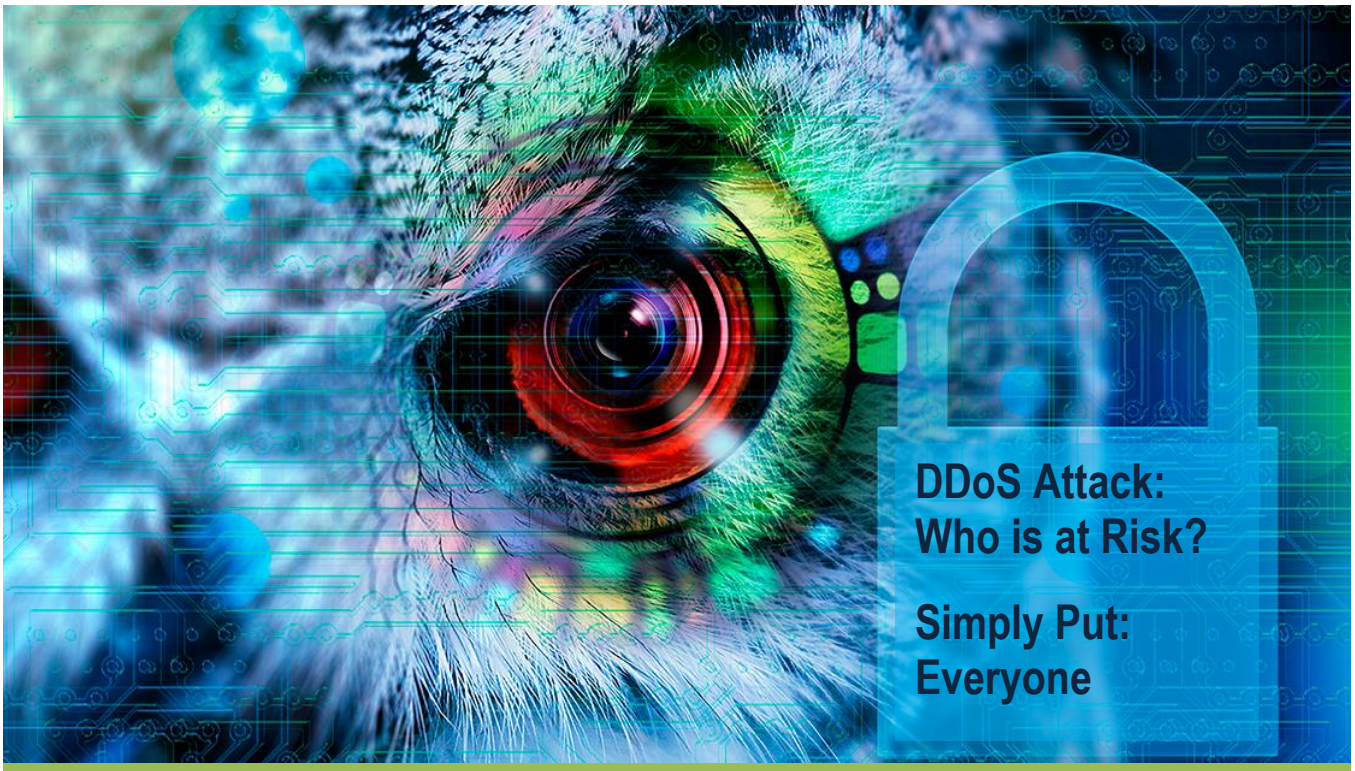
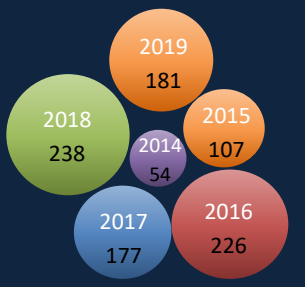


Smart Ways to Defend Against the Most Common Cybersecurity Threat

NASCIO Award Category
Cybersecurity

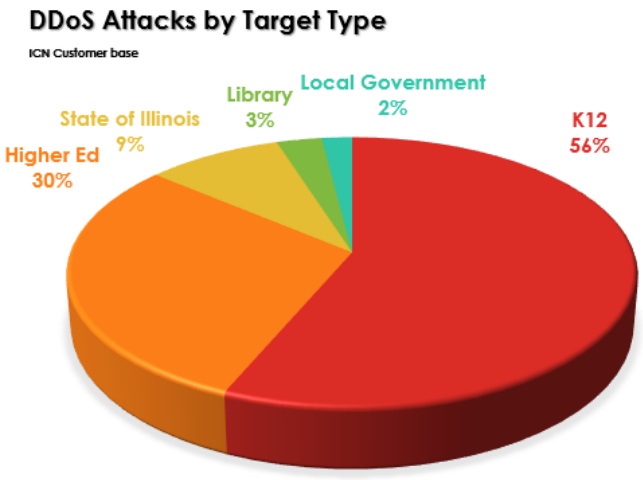
State of Illinois

Dale Walters, Chief Networking Officer
Department of Innovation & Technology
Network Operations and Telecom
Dale.Walters@illinois.gov



Initiation Date: December 2016
End Date: Ongoing

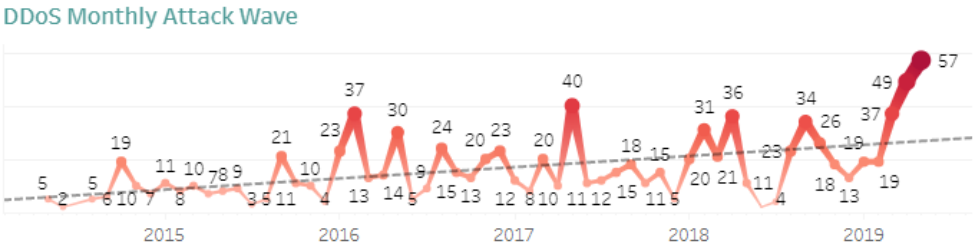
EXECUTIVE SUMMARY



With the proliferation of malware infected devices used to launch denial of service attacks and easy access to inexpensive DDoS booter platforms, DDoS4hire services have become one of the most common ways to settle online score. Denial of service attacks are all too common and they are here to stay because cybercrime rings turned this technology into a money-making platform contributing to an annual cybercrime profit of over $6T. No wonder that State and Education infrastructure experience such attacks almost daily, requiring Illinois to be poised and prepared to provide a proper response to attempts to deny our citizens the services upon which they rely and our children the education that they need and deserve to succeed in life. Since the State of Illinois is positioned to be at the forefront of such disruptive and frequent attacks it has taken steps to enhance its infrastructure and extend its cybersecurity protection to its constituents. The State infrastructure is highly redundant with the capacity and intelligence to provide strong protection against both old and emerging techniques. Nevertheless, it is a constant cat-and-mouse game where cybercriminals never sleep, so the State of Illinois must be ever vigilant.

While the State of Illinois has elevated its security posture over the last four years combatting ubiquitous phishing and ransomware campaigns, data exfiltration attempts and emerging threats like crypto mining and supply chain software attacks, one type of threat has remained near the top: Distributed Denial of Service (DDoS).

Worldwide DDoS statistics are alarming with over 500 attacks taking place every hour. The State of Illinois Department of Innovation and Technology (DoIT) manages the Illinois Century Network (ICN) and is charged with protecting various State of Illinois assets and constituents. On average staff manage 20 significant DDoS attacks monthly, with an upward trend. This allows the State to appreciate cost avoidance and an increased security posture.



In addition to an enhanced security posture, the State has integrated data analytics with a DDoS solution to more efficiently inform stakeholders of emerging trends and provide targets for action, whether it be augmenting the solution or reconfiguring to adjust posture. By merging Cyber Security and Data Analytics, a more comprehensive DDoS solution (always ready for emerging attack trends) is leveraged to protect the Statewide network.

Business Problem and Solution

PROBLEM

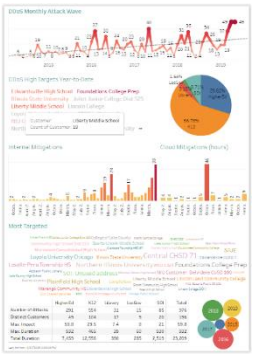
DDoS continues to be placed in the top five cyberthreats targeting organizations. DDoS occurs when cyber-criminals attempt to make an online service unavailable by sending large amounts (or in some cases confusing amounts) of traffic to the targeted service or resource, making it unavailable. For example, a successful attack could prevent Amber Alerts from triggering properly or make health care services unavailable for Illinois veterans. Following the lessons of the Ferguson, Missouri rioting in 2014 and the cyberattacks on resources of the State of Missouri, as well as the Vikingdom attacks targeting State of Illinois and other states, the Illinois leadership team

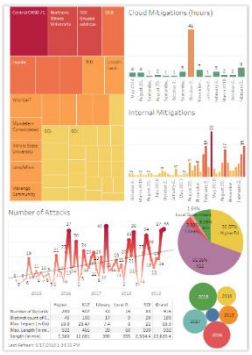
recognized the importance of ensuring that Illinois assets are protected against cybersecurity threats specifically related to DDoS. In 2018, Illinois moved forward with offering this protection to units of local governments and boards of election as it has become painfully clear they are also targeted by rogue groups and nations.

The ICN serves some 70 agencies and 2000 anchor institutions[1] consisting of Illinois K-12, higher education, museums, libraries, healthcare organizations, state and local governments serving the citizens of Illinois. The DDoS attacks targeting them are on the rise. In 2016, the ICN detected and mitigated 226 attacks against 58 customers, in 2017, 177 attacks against 56 customers were detected and mitigated and in 2018, the ICN detected and mitigated 238 DDoS attacks against 57 anchor institutions and agencies. In2019, has already seen more than half that in the first 5 months. One ICN customer has been attacked nearly 150 times. The longest attack lasted 16 hours and the largest attack mitigated was 60 Gbps.

Adding Data Analytics

One additional benefit to the DDoS solution, is that it has added an incredible amount of data. In many DDoS solutions the data is stored and used only for reporting using integrated tools. DoIT Staff have integrated data analytics into the DDoS solution by tapping this large data store and using it to provide staff with detailed, actionable statistics that provide direction, highlights and targets new attack trends and identifies significant threats before they can impact operations. The added analytics delivers customer reporting, providing State of Illinois stakeholders with comprehensive reports of DDoS attacks as well as important baselining and visibility into their own networks to aid in their individual network and security planning. It also allows us to correlate these attacks with other types of attacks as is often the case when DDoS attacks are used as a distraction from data exfiltration or other malicious activity. Staff are currently working on API integration which will allow the State to simultaneously enhance the DDoS service as well as the State's security posture.





SOLUTION

The ever-increasing cyber threats and DDoS attacks demanded a robust and reliable solution to protect the assets of the State of Illinois. DoIT's team of engineers developed a hybrid DDoS mitigation solution and turned it into a reliable service that significantly reduces and/or removes the impact of DDoS attacks against the State infrastructure. Moreover, the solution brought additional benefits by expanding this service to other entities throughout the state, including but not limited to local law enforcement, boards of elections and anchor institutions with an enhanced insight into traffic patterns for identifying and troubleshooting not only DDoS or DoS but other network issues and threats. In 2018, DDoS Protection service was offered to all customers and included a customer dashboard providing quick access to decision critical information.

In developing this solution, the DoIT team established the following criteria:

- Accurate and timely detection and mitigation.
- Must intelligently support an automated hybrid solution with "on-demand" and "always-on" options.

[1] *Anchor institutions are universities, hospitals and other enduring organizations that play a vital role in their local communities and economies. They tend to remain in their geographical settings, even as conditions change around them. They are vital assets to their communities providing services to the public.

- Use of state-of-the-art technology able to adapt to new trends in cyberwarfare.
- Up-to-date threat intelligence with new attack vectors and countermeasures.
- Secure/hack-proof implementation with built-in redundancy, geographic diversity and flexible mitigation capacity and growth, capable of handling smallest and largest attacks.
- Experienced security team trained in threat identification and effective threat mitigation.
- 24/7 automated and redundant alerting system and Network Operations Center (NOC) Response Team alert verification, ticketing and customer follow up.

With these criteria in mind, Staff developed the State of Illinois DDoS Solution. In addition to DDoS attack protection, with new features and capacity, this implementation provides customers with robust email or text capable alert features partnered with strong reporting capabilities available to customers via dashboards. It also provided access to and support from the Network Operations Center and DDoS Response Team, trained in threat verification and customer engagement following the DDoS Response Playbook and routine table top exercises.

The solution not only protects against DDoS attacks but includes ongoing attack monitoring, threat detection, auto-mitigation, dashboard access, incident reporting, cyber-attack consultation, malware and command and control detection, traffic pattern and baseline analysis, and reporting features. It has enough capacity to withstand large attacks and is tuned to detect the smallest of attacks. It has built-in flexibility to respond to various changing attack vectors. Since its implementation, the DDoS solution has withstood over 1000 DDoS attacks. The system has been enhanced, geographically diversified, and has been repeatedly tested. Daily stats and KPI are kept and made available to management using Tableau Dashboards.

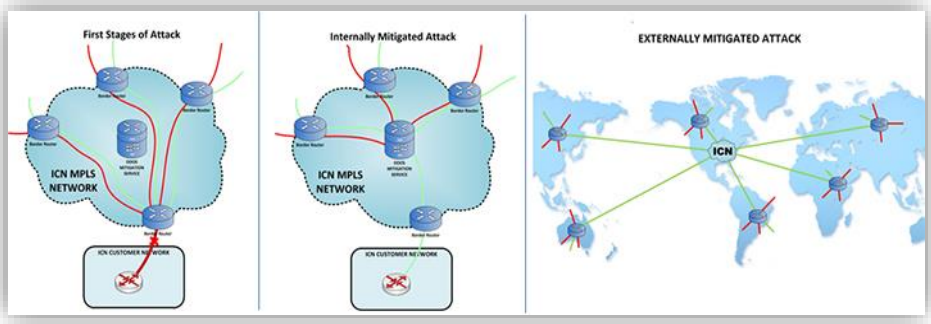
CONCEPT

The State of Illinois is entrusted with a wide variety of services critical to citizens, government agencies and businesses. These services include education, employment, health, financials and access to various Internet resources. High availability is of utmost importance for those services.

The solution must be instantaneous, all-encompassing, flexible, redundant, accurate in detection and mitigation, with sufficient capacity, expandable and cost effective (especially as it relates to staff time). It also requires comprehensive training, experienced integration into existing network, a dedicated team of subject matter experts for mitigation, traffic analysis and reporting, and cross-agency/cross-customer engagement. These requirements have been met and, in some cases, exceeded. Illinois has a sufficiently redundant, internal and external hybrid mitigation system operated by well trained staff and a 24/7 NOC and DDoS Response Team. Additionally, we have well documented processes involved in implementing this solution as well as produced training materials, playbooks, flowcharts, and presentations, thus reducing staff time needed to efficiently identify, verify and mitigate attacks. We rolled out DDoS Protection as a service to all of the ICN customers in 2018.

ICN DDoS Mitigation (how it works)

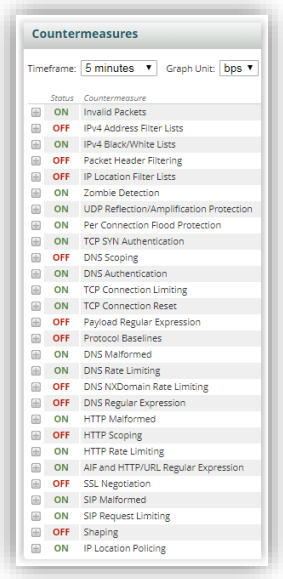
A DDoS attack requires a proactive approach, one that identifies the malicious activity and mitigates the attack immediately to protect business continuity and ensure resource availability. Once mitigation starts, all traffic for an attacked resource is



diverted to one of our Scrubbing Centers. Mitigation "cleans" the traffic, dropping bad packets and allowing good traffic through to the customer. Since Egress bandwidth is still affected by the attack, internal capacity will continue to be used until there is a need to take mitigation to the cloud implementing Generic Routing Encapsulation (GRE) tunnels.

DATA ANALYTICS

Coupling the State's Data Practice with the DDoS Solution was not an easy task. While new APIs are being made available, today the systems are disparate and must be linked together appropriately to provide analytics and visualizations that are helpful for planning purposes. Staff has linked our data analytics tools to the many databases as well as integrated DDoS system statistics into a Network Operations Dashboard.



The entire State of Illinois network infrastructure is protected by analyzing traffic:

- Using flow records, Simple Network Management Protocol (SNMP) and Border Gateway Protocol (BGP) data to build network-wide relational models of traffic:
  - Detecting, generating alerts and mitigating attacks
  - Using multiple customer specific countermeasures
  - Monitoring and reporting on network services including:
    - Hypertext Transfer Protocol (HTTP)
    - Voice Over Internet Protocol (VoIP)
    - Multi-Protocol Label Switching (MPLS)
    - Virtual Private Network (VPN)

Once an attack is detected, classified and mitigation started, the traffic for a host(s) is diverted to a Scrubbing Center and various countermeasures are used as defense mechanisms to target and surgically remove attack traffic.
Countermeasures are tailored to stop various types of attack traffic, for example Invalid Packets and Zombie Detection.

SIGNIFICANCE

The ICN provides proven, on-premise DDoS protection for the most critical enterprise and customer networks, enhanced by an integrated external DDoS detection and mitigation capabilities against both known and emerging threats to ensure State of Illinois agencies and customer organizations can maintain business continuity. Included in DDoS Mitigation system are a security platform for detection, analysis, and reporting integrated with redundant threat management systems for surgical mitigation of attack traffic.

The system allows us to utilize the following protection phases:

- Preparation - offers a means to gain pervasive network visibility and recognize normal traffic patterns
- Identification - models network behavior, creates a baseline, and alerts for network anomalies
- Classification - identifies DDoS and zero-day threats and determines type, severity, and size
- Trace Back - allows performance of real-time historical analysis of all network activity
- Reaction - allows initiation of the appropriate mitigation process to stop a threat
- Post Mortem - provides detailed mitigation reports with explanation and "lessons learned" discovery

Solution Features:

- ICN DDoS detection tools identify and drop malicious traffic before it reaches the customer.
- ICN provides immediate DDoS protection from various DDoS attacks that threaten service and application availability.

- ICN provides a full suite of protection tools with over 30 different countermeasures used to isolate attack vectors and provide the best customer protection.
- A hybrid solution is implemented which utilizes fast-flood detection and auto-mitigation as well as internal and cloud-based mitigation, which allowed the ICN to successfully mitigate large and small attacks.
- ICN engineers and the NOC Center are available 24/7 to provide DDoS protection and quickly block attacks to protect ICN services and customers.
- ICN provides custom DDoS Protection with immediate DDoS mitigation for existing and new customers which is easy to install, configure and use.
- ICN also analyzes attacks and provides custom DDoS mitigation consultations and recommendations
- ICN provides a proactive DDoS Detection and Mitigation with automated DDoS detection and mitigation BEFORE service performance is impacted. Little to no user interaction is required, lessening the burden on local security teams.

Additional features/benefits:

- Analysis of network traffic for lateral movement, data exfiltration, and network disruption.
- Augmentation of existing network monitoring and alerting.
- Implementation of mitigation responses to events using various security tools.
- Rapid response and prioritization of the criticality of events and mitigation options.
- Proactive and reactive response to mitigate security attacks against SOI assets.
- Analysis of network traffic for attack and malicious traffic patterns.
- Identification of non-attack and self-DoS occurrences and using available countermeasures to avoid or minimize outages.
- Proactive and real-time guidance for customers on network countermeasures, security protocols, and defensive security response and follow up.
- Engagement and support of cross-functional teams and collaboration with internal/external customers.
- Appropriate management of time and customer issues based on issue severity and business needs
- Collaboration with IT management and DoIT Security on requirements, product updates, configuration changes and suspicious activity reports.
- Identification, definition and implementation of process and procedure improvements.
- Documentation of current processes and procedures.

IMPACT

Since the implementation of the DDoS Solution, multiple agencies and anchor institutions have been relying on keeping their services running without interruption 24/7. We keep our five nines and consistently get positive customer feedback. Even though the State has experienced multiple attacks and has seen a 45% increase of attacks over the same time last year, none of them were able to effectively disrupt essential services and leave a lasting negative impact. Moreover, we are not complacent and look for ways to improve the service.

Since DDoS Protection implementation:

- 196 distinct customers were protected, some repeatedly attacked 20-40 times.
- 1,000+ attacks were detected and mitigated
- Average attack length is 22 minutes and average impact is 2.2 Gbps
- 21 Gbps is the largest attack mitigated internally (59.8 Gbps externally)

- 932 minutes (16 hours) was the longest uninterrupted attack mitigated and the longest attack on a customer lasted two months
- Most common attacks we see: IP Fragmentation, chargen, SSDP, NTP/DNS amplification, TCP SYN and CLDAP
- Alarming trends: memcached server amplification and carpet-bombing attacks and use of cloud hosting.
- Service has been extended to all of the ICN customers in 2018.

The State is now able to provide robust DDoS protection services to its constituents with a solution that supports Integrated On-Premise and Cloud-Based DDoS Protection, Real-Time DDoS Forensics, Built-in SSL Inspection to Block Encrypted Traffic, Inbound Reputation-based DDoS Protection, Inbound and Outbound Advanced Threat Protection, Cloud-based and on-premise DDoS Defense Service. While these are a lot of industry catch-phrases, the impact to operations has been substantial.

MEASURING SUCCESS

So how do we measure success? We measure by speed and accuracy of detection, by effectiveness of mitigation, by response time and follow up. When the ICN customers do not even notice that they have been undergoing a DDoS attack is a great metric. Another measurement is how fast the system and our staff are informed of an attack. We can now measure response in seconds as opposed to minutes or hours. Our overall goal is to maintain normal operations and ensure our customer does not experience any outages due to a targeted DDoS attack. As our CISO once said, "This is one area of cybersecurity I do not lose sleep over," – a highest praise for the team that implemented the solution and sustain operations.

DIFFERENTIATION FACTOR

What makes this so different from so many other DDoS protection services?

- Our DDoS Solution is tightly integrated into our network infrastructure and Egress which allows us to be flexible and accurate in detecting, verifying and mitigating attacks, thus keeping the rate of false positives/negatives negligible.
- We share and cooperate with other state groups so that we are stronger together and better prepared.
- ICN staff intricately understands the DDoS Solution systems and network itself which gives us an advantage over third party implementations.
- ICN staff is also very familiar with our customer base and knows what to expect from customer traffic patterns or any changes.
- ICN pursues customer feedback and builds experience and service improvements on it. We actively follow up with customers after every attack they experience.
- ICN gathers and analyzes statistical trends which allow us to prepare for changing network behavior and threats.
- ICN assists our customers not only in defending against DDoS attacks but helps them track the origins of these attacks based on our gained experience and point them to other available recourses.
- ICN provides presentations, webinars, training sessions, consulting, how-to manuals for customers to educate them regarding this common threat.
- ICN goes the extra mile by customizing the DDoS Solution to closely fit our customer needs in troubleshooting network issues that were not necessarily caused by a DDoS attack.

Internal Protection

The first line of defense for an effective DDoS protection plan includes existing firewall, intrusion prevention system (IPS), and load balancers. Additionally, dedicated DDoS protection devices can provide specialized mitigation against large-scale and advanced DDoS attacks. It's important that these DDoS protection devices provide enough headroom in terms of bandwidth, throughput, and connectivity to deal with DDoS attacks while maintaining service availability. But even with the best tool you are limited to the egress bandwidth you purchased.

A few things you need to know about DDoS attacks:

- Firewalls/gateways/load balancers cannot protect against complex DDoS attacks, and instead, act as DDoS entry points.
- Attacks pass right through open firewall ports which are intended to allow access to legitimate users.
- Over 60% of firewalls fail at first try.
- The average downtime due to a DDoS attack is 54 minutes with an average cost of $22,000 per minute.
- On average an unmitigated DDoS attack requires 20-30 minutes for the network to normalize after it stopped.
- You may experience DDoS even if you are not the intended target.
- Installing and implementing on-premises devices, relying on hardware, or on firewalls installed on premises is good but insufficient. This will require large upfront capital expenditures that will have their own life cycle. It will also require hiring experts with the right skill set to successfully use this hardware to mitigate risks. When used inline, protection is always on and is in use whenever an attack starts. However, on premises hardware attempts to stop a DDoS attack at the edge of the network or at a firewall/gateway.

For network layer attacks, ensure that enough network bandwidth is available to easily deal with massive amounts of traffic. If you are not able to purchase enough capacity on your own because it will go unused most of the time, cloud services or your ISP can get you access to the extra bandwidth you need to absorb the attack. It is important to have enough bandwidth on your "backup" connections for normal traffic baselines but keep in mind that if you are using multiple ISPs all your connections can be saturated as the destination of the attack is internal to your network.

The DDOS Solution has allowed the State to mitigate outages, in most cases with customers unaware of the issue until notified by our NOC of the mitigation.

FUTURE DIRECTION

Staff also continues to ensure success by fine-tuning the system to reduce false positives and false negatives to a negligible minimum. Additionally, our goal is not only to protect against current attacks but be ready for new types of threats by keeping our staff trained, our equipment up-to-date, and be on the look-out for new/better solutions to continue providing highest level of service.

USE CASES

As part of the cybersecurity defense effort that spans multiple IT groups, our DDoS Response Team is tasked with detecting and mitigating denial of service attacks. Statistics show an average of 20 monthly DDoS attack including at least one against a State agency. A typical attack is 30 minutes and 2.2Gbps strong. We continue seeing persistent multi-vector spanning five of seven OSI layers.

USE CASE 1 (Targeting Elections)

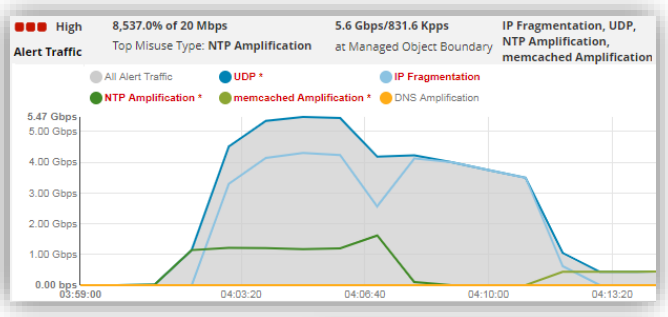
2016: Elections are underway and voting results are sent to the Illinois Vital Records for processing. Our cybersecurity team is on high alert in case of a cybercriminal breach. Within minutes, we receive an alert that a cybercriminal group originating from Hungary is attempting to take down the IVR servers with a DDoS attack. We mitigate the attack and engage other cyber teams working in tandem to make sure the voting results are processed properly, and no breach is taking place while we are distracted with a head-on 10Gbps+ DDoS attack.

USE CASE 2 (Targeting License Renewal)

2017: A cybercriminal is targeting the Secretary of State's cyberdriveillinois website that is used by the citizens of Illinois to renew their driver licenses, car plates and receive various other services. We detect and mitigate a series of attacks while ensuring that there is no disruption in service. We do not spread the good news, and no one knows (except the DDoS attacker) that another attempt has been thwarted and citizens can use the services at any time.

USE CASE 3 (Targeting Shared Services)

2018: Using memchached amplification a cybercriminal is targeting an extended set of government public facing resources thus disrupting various services Illinois citizens rely on every day. We detect and mitigate a series of attacks while ensuring that there is no disruption in service. The incident is discussed internally for lessons-learned. .



USE CASE 4 (Carped Bombing State resources)

2019: State network infrastructure receives a series of attacks over several days mimicking Mirai botnet behavior by using various source hosts on port 2323 and targeting various ports on the state side. Since each host is attempting to establish a limited number of embryonic connections, the firewalls process them as legitimate. Traffic patterns consistently do not exceed the thresholds which makes it very difficult to detect and mitigate the attack. Using our DDoS mitigation system in conjunction with the reports from our Security Information and Event Management (SIEM) system we successfully correlate events, identify and block all subnets that are involved in the cyberattack thus stopping attempts at disrupting normal operations and services provided by the State of Illinois. Again, we keep quiet the fact that another attempt has been thwarted and citizens can use the services they need.

PROTOCOL	FLAGS	IP SOURCE/ DESTINATION	PORT	INDEX	PACKET SIZE
tcp	S	45.195.133.17 100.100.116.88	28192 2323	27 49	48
tcp	S	45.195.133.213 100.0.100.41.181	16889 2323	27 49	48
tcp	S	45.195.133.189 100.100.127.200	49253 22	27 49	48
tcp	S	45.195.133.111 100.0.100.30.156	21022 2323	101 73	48
tcp	S	45.195.133.105 100.100.158.105	35390 22	101 73	48
tcp	S	45.195.133.165 100.0.100.11.38	26813 22	59 73	48
tcp	S	45.195.133.134 100.100.17.98	18795 2323	59 73	48
tcp	S	45.195.133.134 100.0.100.14.145	65112 2323	59 73	48
tcp	S	45.195.133.8 100.100.23.189	6332 2323	27 49	48
tcp	S	45.195.133.188 100.0.100.58.46	9883 2323	27 49	48
tcp	S	45.195.133.32 100.100.27.8	37641 2323	27 49	48

Note: IP addresses have been altered