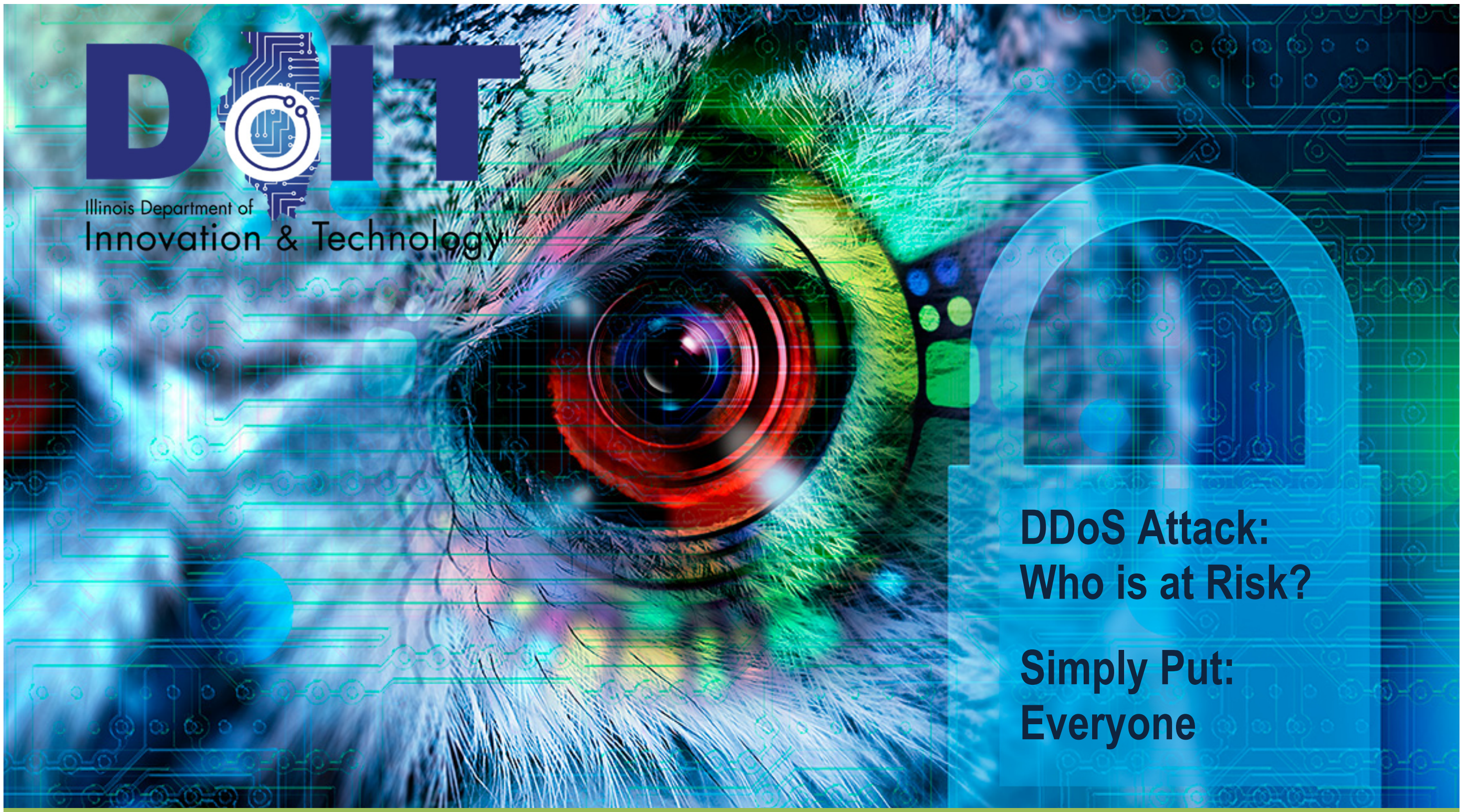


DoIT Illinois Department of Innovation & Technology

DDoS Attack: Who is at Risk?

Simply Put: Everyone

Smart Ways to Defend Against the Most Common Cybersecurity Threat

NASCIO Award Category
Enterprise IT Management Initiatives
State of Illinois

Lori Sorenson, Chief Networking Officer
Department of Innovation & Technology
Customer Account Management
Lori.Sorenson@illinois.gov

Initiation Date: July 2016
End Date: August 2017

EXECUTIVE SUMMARY

DDoS Attack: Who is at risk?
Simply Put: Everyone

In 1988, Robert Morris tested the limits of network security by launching a worm. Disputes still remain on what Morris intended, but the worm showed us how a networked system can fail. This led to widespread efforts to keep systems up to date with security patches and the fundamental pattern of adding security still exists. Today, a worm that infects a few thousand machines would barely make the local news. But in 1988, the Internet and Networks were far different than they are today.

As part of Governor Bruce Rauner's digital transformation strategy, the Department of Innovation & Technology (DoIT) led by Acting Secretary Kirk Lonbom, has undertaken many enterprise management initiatives to create a cyber-secure Illinois by protecting state data and systems against attacks, utilizing best-in-class capabilities.

The challenges we face in protecting the privacy of our citizens, the confidentiality of our information and the ability to provide critical state services are vast. In addition, the State of Illinois must lead efforts toward a more cyber-secure state by helping protect the state's critical infrastructure, prepare the state for potential cyber disruption, and promote cyber-security best-practices across the private and public sector.

The most common cyber-attack today known as a Distributed Denial of Service (DDoS), occurs when a cyber-criminal attempts to make an online service, website or network unavailable by disrupting normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic, stopping even legitimate traffic. Following the lessons of the Ferguson, Missouri rioting in 2014 and the cyberattacks on resources of the State of Missouri, the Illinois leadership team recognized the importance of ensuring that Illinois assets are protected against cybersecurity threats including DDoS. DoIT's Illinois Century Network (ICN) handles approximately 190 DDoS attacks annually.

The ICN serves 70+ agencies and 2000+ anchor institutions consisting of Illinois K-12 schools, higher education, museums, libraries, healthcare organizations, state and local governments serving the citizens of Illinois. 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 state infrastructure.

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

- Accurate and timely detection and mitigation
- An intelligent hybrid solution with both on and off-net detection and mitigation
- State of the art technology
- Up to date threat intelligence
- Availability of automation
- Secure implementation
- Experienced security team
- 24/7 alerting and Network Operations Center (NOC) Response Team

The underlying foundation of this service has built-in scalability, robust alerting features and strong reporting capabilities that are available to our customers. 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. Implemented in 2016, the DDoS solution has withstood over 500+ DDoS attacks since its implementation.

CONCEPT

The State of Illinois is entrusted with a wide variety of services critical to citizens, government agencies and businesses. Reducing the risks to our citizens, ensuring delivery of state services and protecting the state's critical infrastructure is our mission. We provide countless services to improve the quality of life for our citizens. From state troopers to healthcare program personnel to child care case workers, there is strong reliance on the state's information system to serve and protect the public. We are entrusted with the personal information of millions of its citizens and other constituents. Unfortunately, the likelihood of being the victim of a cyber-attack has never been higher. The ICN is strategically placed at the forefront of cybersecurity protecting the assets of the citizens of the State of Illinois. We must be vigilant and always on the lookout for yet another ingenious and nefarious way cyber criminals are using to break down our cyber-walls and inflict as much damage as possible.

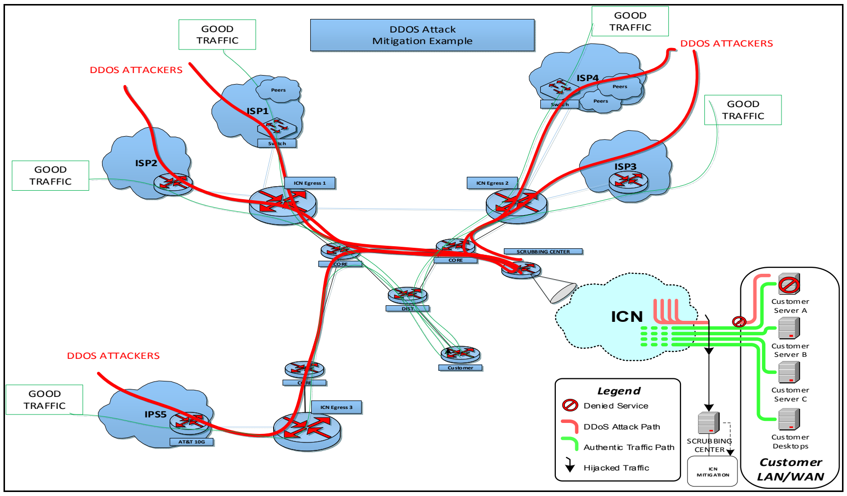
DDoS is the most common cyber-attack today since they are so easy and inexpensive to launch. There are over 2000 DDoS attacks per day; 1/3 of downtime is linked to DDoS; attack size grows 10-30% per year; an average peak hourly revenue loss is calculated to be approximately $100,000; 35% of attacks will be repeated; 30% of attacks are over 1Gbps; 88% of attacks are multi-vector; and many attacks are used as a distraction for other cybercrime activities. Understanding the criticality of the situation, our enterprise IT required a permanent and forward-thinking solution that would allow us to protect the assets not only today but in the future.

The team was tasked with the following requirements for DDoS Protection:
It must be instantaneous, all-encompassing, flexible, redundant, accurate in detection and mitigation, with sufficient capacity, and expandable. We also required comprehensive training, experienced integration into existing system, 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 highly redundant, internal and external hybrid mitigation system operated by highly trained staff and a 24/7 NOC trained in DDoS Protection. Additionally, we have documented the processes involved in implementing this solution as well as produced training materials, playbooks, flowcharts, and presentations. Furthermore, we have added automation and are currently working on API integration which will allow us to enhance the service.

ICN DDoS Mitigation

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 address is diverted to one of our Scrubbing Centers. Mitigation "cleans" the traffic, dropping bad packets and allowing good traffic through to the customer. Bad traffic still flows across our backbone destined to the Scrubbing Center. 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.

See image below.



SIGNIFICANCE

From the beginning, the DDoS Protection solution was envisioned to be a fundamental improvement over any other existing solutions without negative impact to existing infrastructure. After experiencing a large and what could have been costly attack, our DDoS Protect Team worked with management to develop the right solution that could be quickly implemented. We designed our network and trained staff so that our protection was always "on" with active detection and mitigation at a moment's notice.

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

Some of ICN DDoS Protect solution features are listed below:

- 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.

With the implementation of the DDoS Protect solution, we have also benefited in the following areas:

- 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.
- 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

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 availability threats to ensure State of Illinois (SOI) agencies and customer organizations can maintain business continuity.

Included in DDoS Mitigation system are a security platform for analysis and reporting and coupled with threat management system for surgical mitigation of attack traffic.

Our entire network infrastructure is protected by analyzing traffic:

- Using flow records
- Using Border Gateway Protocol (BGP) data to build network-wide relational models of traffic
    - Detecting, generating alerts and mitigating attacks (manually or automatically)
    - Using multiple finely tuned 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)

We have two threat management systems located in both Springfield and Chicago. Additionally, we have an augmented cloud based system that can be utilized as needed.

Once an attack is detected and mitigation started, the traffic for a host(s) is diverted to our 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.

ICN DDoS Service includes:

Monitoring	**Detection**
▪ Advanced heuristics to profile normal versus anomalous traffic patterns	▪ Signature Analysis & Misuse Detection
▪ 24x7 customer traffic monitoring by ICN Network Operations Center	▪ Predefined deviations recognition
▪ Customer-specific alerts enabling trained security experts to immediately identify nascent potential attacks	▪ Dynamic Profiling
▪ Detailed and unified event reporting for multiple environments through a secure portal	▪ Normal traffic baselining
Mitigation	**Analysis & Reporting**
▪ On-demand mitigation	▪ Application & Protocol Reports
▪ On-ramping traffic	▪ Event & Fingerprint Reports
▪ State-of-the-art filtering technology	▪ QoS Reports
▪ Off-ramping of clean traffic	▪ Top Talker Reports

The ICN incorporates advanced anti DDoS protections, or countermeasures, that have proven effective in the world's largest and most complex network environments. These countermeasures include a set of packet-based and event-driven protections developed by experts in the field of network security that neutralize the vast majority of global botnet threats.

Integrated On-Premise and Cloud-Based DDoS Protection
A leading cause of network downtime is the time it takes a cloud-based provider of DDoS protection to respond and initiate DDoS mitigation when the attacks are too big for on-premise solutions to handle on their own. The ICN provides a hybrid solution, both on-premise and in the cloud, which significantly reduces time to mitigation. This tight integration is the best way to deliver DDoS protection and ensure the availability of critical network resources.

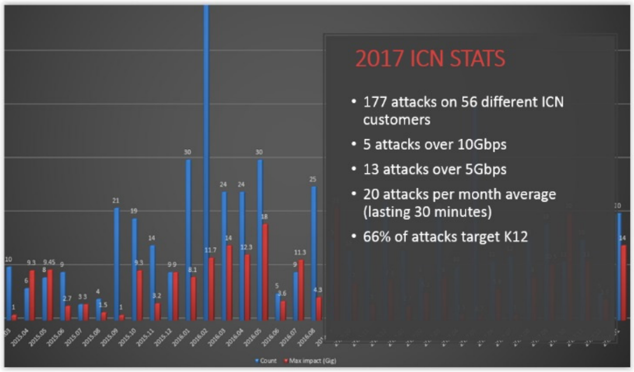
Real-Time DDoS Forensics
The ICN produces in-depth, real-time attack reports that are easy to understand along with DDoS mitigation forensics detailing blocked hosts, origin countries of attacks and historic trends.

Built-in SSL Inspection to Block Encrypted Traffic
As the Internet evolves to increasingly rely on SSL encryption, DDoS attacks have also evolved to encrypt the malicious traffic and evade DDoS protection solutions. The ICN uses tools that inspect encrypted traffic for DDoS threats. These tools experience DDoS mitigation in real-time as normal traffic passes uninterrupted – all without forcing changes to existing network and application infrastructure.

Inbound Reputation-based DDoS Protection
The ICN uses tools which include expanded DDoS mitigation capabilities backed by the global threat intelligence and reputation-based research. In-depth analysis expands the breadth of DDoS detection and DDoS mitigation of various types of availability attacks based on the source of the traffic participating in known DDoS attacks.

Inbound and Outbound Advanced Threat Protection
Organizations need a way to stop threat communications to protect internal systems from being compromised. ICN applies global threat intelligence and reputation-based research to block both inbound and outbound threats via domain and IP reputation and identifies malware and botnet communications to the Command & Control servers.

2017 ICN STATISTICS
The ICN protects 70+ agencies and 2000+ anchor institutions. In 2018, the ICN detected and mitigated 110 DDoS attacks against multiple anchor institutions and agencies. In 2017, 177 attacks against 56 customers and in 2016, 226 attacks against 58 customers were detected and mitigated. One ICN customer was attacked 148 times. The longest continuous attack lasted 16 hours and the largest attack mitigated 50Gbps in the cloud.



2017 ICN STATS

- 177 attacks on 56 different ICN customers
- 5 attacks over 10Gbps
- 13 attacks over 5Gbps
- 20 attacks per month average (lasting 30 minutes)
- 66% of attacks target K12

- We have protected 120 different customers, many of those repeatedly attacked
- Detected and mitigated 700+ attacks on customers
- Detect and mitigate 20+ attacks monthly on average
- Average length of an attack is 22 minutes
- Average Impact is 2.2G
- Largest attack mitigated 21Gb internally
- Longest uninterrupted attack mitigated lasted 932 minutes (16 hours)
- Longest attack on a customer lasted 2 months
- Most common attacks perpetrated on customers are IP Fragmentation, Chargen, SSDP, NTP amplification, TCP SYN and CLDAP

USE CASES
The world of cybercrime never sleeps. If they are not trying to hack you, they are trying to steal your identity. If they are not trying to infect you with Ransomware or other malware, they are trying to deny you access to the Internet.

We have many stories to tell but obvious constraints allow us to present just a few examples here.
As part of the cybersecurity defense effort that spans multiple IT groups, our DDoS Protect Team is tasked with detecting and mitigating any denial of service attacks coming our way. Current statistics reflect that in an average month we protect assets of our customers 22 times and deflect at least 1 DDoS attack targeting agencies with an average length of 30 minutes and 2.2GbpS impact. The attacks are likely to be multi-vector and range from Layer 4-5 to Layer 7, and they will be persistent. For instance, one asset was targeted 148 times in the last year.

A few real-life examples of how we protect SOI assets and customers are below:

USE CASE 1 - 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 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 - 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 various services. We detect and mitigate a series of attacks while ensuring that there is no disruption in service. No one knows (except the DDoS attacker) that another attempt has been thwarted and citizens can use the services at any time.

Regrettably, such DDoS for hire services are all too common these days with the proliferation of malware infected devices and annual profit of over $6T. Thus, we are facing such attacks daily. Illinois is poised and prepared to provide a proper response to attempts to deny our citizens the services upon which they rely. SOI systems are highly redundant with the capacity and intelligence to provide strong protection against both old and emerging techniques. It’s always a cat and mouse game where cybercriminals never sleep, so Illinois is ever vigilant. Our constant monitoring and our advanced tools ensure that many of our customers don’t even know that they have been hit with another DDoS attack.

From a risk mitigation perspective, DDoS protection is an important control that protects Illinois citizens and state assets to ensure services are delivered securely, without interruption. DDoS attacks have been used in some of the most successful attacks on state government, local businesses, education entities and more. With the added controls and procedures that DDoS protection provides, the risks from these types of attacks are significantly reduced. With further expansion of the use of DDoS, we will see ongoing savings, cost avoidance, and increased security. DDoS protection is an important tool for the customers we service and is a key component of Governor Rauner’s goal to create a cyber-secure Illinois.