A Risk Based Approach to DDoS Protection

For Credit Unions and Credit Union Service Organizations

Sponsored by CO-OP Financial Services

Ray Zadjmool
Tevora

Published: April 8th, 2013

Table of Contents

Table of Contents

DDoS, A New Emerging Threat 1

Background 1

- Operation Ababil 1
- Credit Unions Targeted 2
- How Susceptible are Credit Unions? 2
- Have Credit Unions had fewer or more attacks than banks? 3
- DDoS and Government Regulations 4
  - Federal 4
  - NCUA 4
- Types of DDoS 5
  - Volumetric DDoS 5
  - Layer 3 DDoS 6
  - Layer 7 DDoS 7

Formulating a Strategy, a Credit Union's Guide 8

- DDoS Strategic Thinking 8
- DDoS Strategy Recommendations 8
  - Recommendation 1: DDoS Risk Assessments 9
  - Recommendation 2: DDoS Incident Response Plan 10
  - Recommendation 3: Third Party Due Diligence 15
  - Recommendation 4: Evaluate DDoS Mitigation Services 16

Vendor Solutions 19

- DDoS Protection as a Feature 19
- Dedicated DDoS Protection Services 20
- ISP Clean Pipe 22
- DDoS Perimeter Protection Appliances 23

Conclusion 24

About The Author 25

Acknowledgements 25

Bibliography 26

Works Cited 26

DDoS, A New Emerging Threat

On February 21, 2013, the NCUA issued an alert to all federally insured credit unions as to the rise of Distributed Denial of Service Attacks (DDoS) targeted specifically at financial institutions. (1) In addition to raising awareness, the NCUA has issued several risk mitigation recommendations for implementing key strategies for mitigation of DDoS risk.

The purpose of this paper is to examine this emerging threat in detail, its effect on current and possible future regulations, and expand on the recommendations made by the NCUA.

Additionally, we will provide a broad overview of the DDoS prevention market, to include a review of solutions, price points, and other factors that should be considered by credit unions in establishing a risk mitigation strategy.

Background

Operation Ababil

Starting October 2012, HSBC Holdings, BB&T Corp and Capital One were amongst 10 U.S. banking institutions targeted by the activist group Izz ad-Din al Qassam in a series of DDoS attacks that spanned over five weeks. Siting the posting of anti-Islamic movie trailer on YouTube, the group outlined “Operation Ababil” as a multiple phase escalation of DDoS attacks until the movie was removed from the internet. (2)

On March 5th, 2013, Izz a-Din al Qassam announced that banks and credit unions should prepare for ongoing attacks beginning on March6. “During running Operation Ababil Phase 3, like previous phases, a number of American banks will be hit by denial of service attacks three days a week, on Tuesday, Wednesday and Thursday during working hours," hacktivists claim in their most recent post. (3)

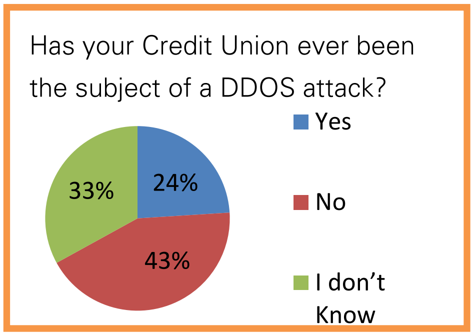
Credit Unions Targeted

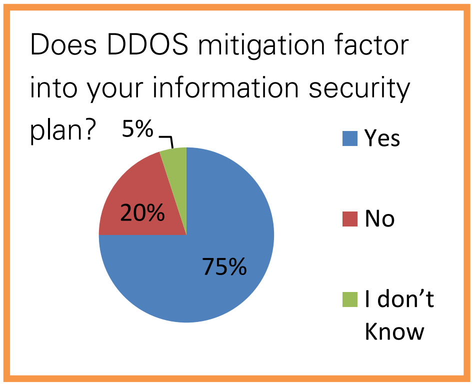
In January of 2013, University Federal Credit Union and Patelco Credit Union came under a DDoS attack believed to be originating from the same Iranian based hacktivist group behind Operation Ababil. The attacks were targeted at their main member-facing websites and resulted in outages lasting up to five hours. (4) (5)

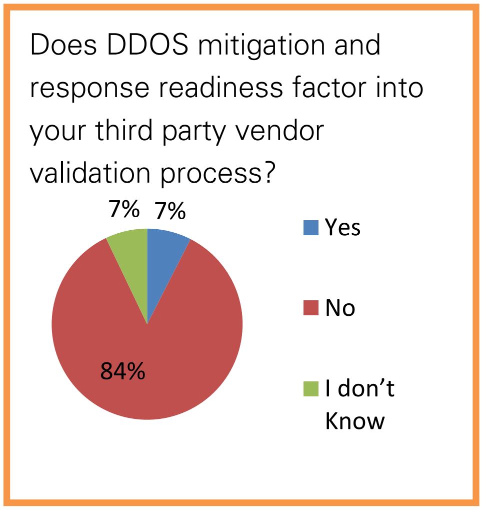
"The bad news, said experts, is that, right now, no credit union can any longer count itself as immune from large-scale DDoS attacks." (5)

How Susceptible are Credit Unions?

As part of the research that went into creating this whitepaper, we conducted a survey of 27 random, various sized Credit Unions and asked them about their exposure to large scale DDoS attacks and what, if any, mitigation strategies they had deployed.


Has your Credit Union ever been the subject of a DDOS attack?


Does DDOS mitigation factor into your information security plan?

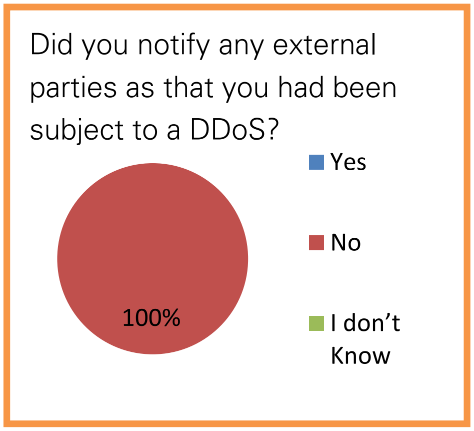

Does DDOS mitigation and response readiness factor into your third party vendor validation process?

Asked if they had ever been subject to a DDoS attack, a good third (33%) of respondent said yes, while almost half (43%) didn't know.

When asked about their level of readiness, a surprising number of Credit Unions said that it's a factor in their future information security planning (75%) while only a small percentage (7%) said that they had incorporated DDoS mitigation Response readiness into their third party validation process.

Lastly, Credit Unions that had experienced a DDoS attack did not report to any external parties, with all respondents stating that their only level of notification was internal.

Have Credit Unions had fewer or more attacks than banks?


Did you notify any external parties as that you had been subject to a DDoS?

"Well it's tough to tell," said Christina Whiting, Security Researcher with Tevora and former CSO of Kinecta Federal Credit Union, "currently the NCUA only requires a Suspicious Activity Report if an event has resulted in a potential compromise of member data and it is at the discretion of the credit union to alert the NCUA in any incidents that did not result in data compromise. DDoS attacks usually don't result in a direct loss."

"But that may soon change", said Bobby Dominguez, Chief Information Risk Officer of PNC Financial Services. "We are seeing a rise in potential ulterior motive for a DDoS attack: fraud. By disrupting the organization's alerting and monitoring defenses, the potential for committing fraud "undetected" has definitely increased." While not able to confirm any specific incident, "we are definitely aware of the risk," Dominguez concluded.

Acknowledging this, the NCUA notes in its alert that while the "attacks do not directly attempt to steal funds, they may be coupled with such attempts to distract attention and/or disable alerting systems". (1)

According to the NCUA, "Credit unions should voluntarily file a Suspicious Activity Report if an attack impacts Internet service delivery, enables fraud, or compromises member information. The NCUA also encourages credit unions to participate in information-sharing organizations, such as industry trade groups and the Financial Services Information Sharing and Analysis Center. (6)

DDoS and Government Regulations

Federal

There are few, if any requirements for DDoS mitigation or incident reporting by federal regulators. Although this has to do in part with the relative newness of the attack vector, the lack of guidelines can be attributed to the fact that DDoS attacks typically don't fall under established areas of regulation relating to data breach. Most requirements for security controls and incident reporting are targeted at customer data loss or fraud discovery. DDoS attacks do not typically result in either.

This could change as the federal government undertakes an ambitious program known as the Comprehensive National Cybersecurity Initiative (CNCI) aimed at defending the full spectrum of threats facing the nation's critical infrastructure. While sure to be far reaching, its effect on the enterprise is largely unknown at this time. However an examination of the plan goals outlines a key initiative to "ensure that government information security offices and strategic operations centers share data regarding malicious activities against federal systems". (7)

"The exchange of information and coordination of resources outlined in the CNCI is exactly the kind of framework that is sure to be adopted by the enterprise, especially in critical verticals like financial services" – Clayton Riness, security consultant with information security firm Tevora.

NCUA

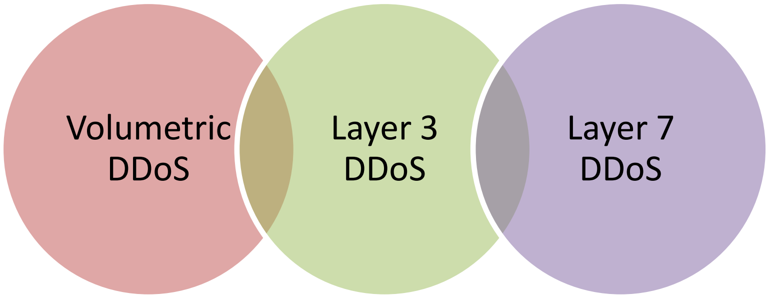
While the NCUA does not have any specific requirements for DDoS, the February alert coupled with specific recommendations that it published is a good indication of direction and intent. The recommendations are specific, actionable, and measurable such that it should be considered fair game in the future for internal audits.

In fact, that is most likely already occurring. Several credit unions we spoke to said that regulators are starting to ask questions about DDoS. Speaking on a condition of anonymity, one credit union CSO shared with us that they had in fact been hit with an NCUA audit finding relating to their lack of a DDoS mitigation plan.

Types of DDoS

In order to implement an effective strategy to mitigate the risk of a DDoS attack, it is beneficial to understand the various types of attacks that are being used today. Unlike traditional Denial of Service (DoS) attacks that can be deployed from a single computer, the term DDoS refers to coordination of several hundred and even thousands of computers participating in a distributed, concerted effort at a single target.

Currently, there are over 27 types of DDoS methods that attackers use. These methods of attack can be broadly grouped into three categories:



Volumetric DDoS

Volumetric attacks aim to saturate the bandwidth of the targeted host by sending a large amount of data to the target. These attacks usually come in the form of UDP floods or ICMP floods from attackers who have significant bandwidth and computing resources under their control. Attackers can amplify the amount of raw data they can send in a flood attack by leveraging a reflected/spoofed attack such as DNS amplification.

DNS Amplification was used in the recent Spamhaus DDoS attack that generated over **300 GB per second** of traffic at its target. (10)

With DNS amplification, "the basic attack technique consists of an attacker sending a DNS name lookup request to an open recursive DNS server with the source address spoofed to be the victim's address," US-CERT explains. "When the DNS server sends the DNS record response, it is sent instead to the victim. Because the size of the response is or not considerably larger than the request, the attacker is able to amplify the volume of traffic directed at the victim. " (8)

Volumetric attacks are the least sophisticated category of denial of service attacks as they do not rely on exploiting more esoteric protocol and application weaknesses.

Despite this, volumetric attacks are often very effective as large amounts of bandwidth are both difficult and expensive for targets to manage even if the traffic is easy to filter.

Layer 3 DDoS

Layer 3 attacks employ specially crafted packets designed to cause resource intensive processing, slow responses on target devices, or disruption of TCP state information.

These attacks usually come in the form of TCP SYN floods, TCP fragmentation attacks, Low-rate Denial-of-Service attacks, or Teardrop attacks. These attacks leverage issues in Layer 3 protocols and devices in order to cause significant disruption with much less attacker bandwidth than in a volumetric attack.

It is relatively easy, however, to filter most Layer 3 attacks as they can be filtered with simple signatures and usually consume much less bandwidth than a pure volumetric attack.

Layer 7 DDoS

Layer 7 attacks exploit application layer commands that cause slow processing or crashes in order to disrupt service to a targeted application. Layer 7 attacks usually target HTTP: either HTTP requests that cause the web application to perform resource intensive processing or vulnerabilities in unpatched versions of the web servers themselves.

These attacks are much more difficult to profile and filter at the network and often require changes to web applications themselves in order to mitigate. Common Layer 7 attacks include Slowlirs, R-U-Dead-Yet, and XDoS.

Formulating a Strategy, a Credit Union's Guide

DDoS Strategic Thinking

The development of a DDoS mitigation strategy for a Credit Union should follow its established processes for disaster recovery and incident response.

Christina Whiting says Credit Unions should first understand the impact of the threat. "If you think about the impact of a DDoS attack, it is much the same as a disaster that results in a disruption of a service. What would you do if your member center service was inaccessible? What would you do if you lost email? Your Call Center?"

"Rumors of DDoS against call centers have been circulating security circles as late. A flood of calls overloads the telephony of member services targeting fraud detection, and incident handling. The attackers then use the down time to conduct fraud that would normally be investigated." –Ray Zadjmool, Tevora

Credit Unions should therefore plan for a strategy that deals with DDoS much the same way as a natural disaster; an event that could disable critical services and impacts the ability to conduct business.

DDoS Strategy Recommendations

The NCUA outlines three key strategies for preparing for a DDoS disaster scenario (1):

- Perform risk assessments to identify risks associated with DDoS attacks.
- Ensure incident response programs include a DDoS attack scenario during testing and address activities before, during, and after an attack.
- Perform ongoing third-party due diligence, in particular on Internet and web-hosting service providers, to identify risks and implement appropriate traffic management policies and controls.

Recommendation 1: DDoS Risk Assessments

A risk assessment specific to the risk of a DDoS should follow established methodologies for identification, impact analysis, and treatment plan.

Scope

First understand the scope of your risk. What services are member facing? What services are internet facing? What is the criticality of these services relative to operations?

The full scope of a DDoS can only be understood if all internet facing services are reviewed. These include member services like online banking, transaction services like processing, and EFT (electronic funds transfer).

Impact

DDoS risk can be measured in terms of "mean time of detection" and "mean time to recover." With a DDoS attack, the impact of an extended outage can be measured in terms of revenue lost, resources required to recover, and cost to reduce risk.

Additionally, you must analyze the risk of how long it takes to identify that you are being attacked in the first place.

It is not enough to know the impact of downtime if you don't fully understand the risk with lack of monitoring. Ask yourself, how would you know if you had a DDoS? Do you have methods to report and escalate things like service disruption or slowdown? Do you have methods to rule out traditional IT outages like server crashes or circuit failure?

Treatment

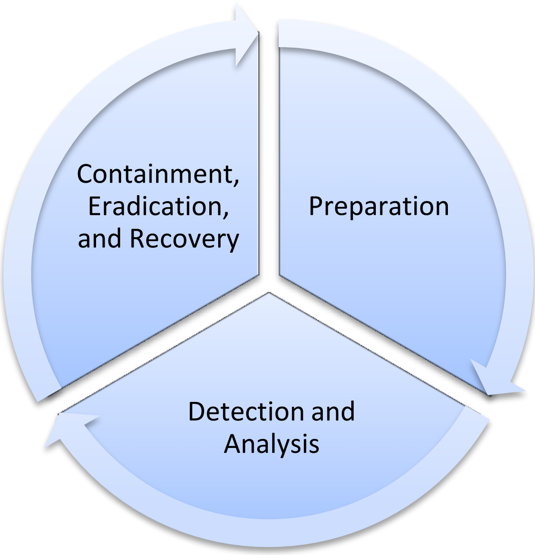
Identified risks should be quantified and classified in a manner that can be presented to management for treatment. Risk can typically be treated in one of four ways: acceptance, reduction, mitigation, or transference.

Credit Unions should make a concerted effort to understand the effects of a disruption of services, the expected time to recover, and the costs to remediate. Risk reduction options should also be presented to offer a balanced approach that can be periodically evaluated for feasibility and cost effectiveness.

Recommendation 2: DDoS Incident Response Plan

As with any disaster recovery or incident, a plan for coordinating the Credit Union's response should be documented prior to an attack. A good DDoS Incident Response Plan has to take in account the tools and personnel at the Credit Union's disposal that will be needed to help in the event of a DDoS attack.

A typical incident response plan has three main components:



Preparation

Identify your DDoS CIRT Team

If you haven't done so already, identify your CIRT (Computer Incident Response Team) team that is going to be responsible for dealing with the DDoS.
Recognize in advance that responding to a DDoS attack is going to be different than normal breach investigations. You will more than likely be dependent on third party service providers like your ISP or DDoS mitigation service.

Individuals designated as part of the CIRT should have specific training on what to expect, what tools are available to them, and how to best deploy containment and eradication strategies.

Create a DDoS Phone Tree

Once your CIRT team is identified, creating a phone tree of whom to contact during an attack is a good next step. Mapping to an existing DR plan is probably a good start but from there, additional resources might be necessary to deal with the unique circumstances of a DDoS.

ISPS usually have a separate, incident hotline that can be used in case of emergencies.

For example, consider your ISP: do they have a DDoS handling center that you can engage? Do you know how to reach them? What information will they need?

Most ISPs have some form of basic DDoS mitigation service that you can call on in case of an attack. In the very least, they can blacklist and shun traffic that is deemed to be creating an outage. This could be limited in effectiveness if the scale of the DDoS is large, but it's good to know what options are available to you and if there are any configurations that must be done ahead of time to take advantage of their services.

Lastly, don’t forget about third party service providers that may need to be contacted outside of your direct control. For example, if your online banking is being hosted by someone else, do you know who to call to report a DDoS? Do they have an escalation plan that requires you to authorize action?

Knowledge of who to call and how to report an incident is a key element of any incident response plan.

“Lite” Sites

Going “lite” on a service being impacted by a DDoS is an innovative technique that should be part of your incident response plan.

“Lite sites” are static versions of dynamic web content that can be put up in an emergency to give the appearance of being available. In addition to transforming server requests into static responses, they give the appearance of availability; reducing help desk calls.

This technique is useful against layer 7 DDoS attacks that attempt to overburden dynamic web services. Dynamic web content needs to query results each time requested so by simply requesting in rapid succession, the database backs up causing slowdown and resource bottlenecks. One common example that is relevant to credit unions is a web service ATM Locator.

“This is a type of service that can go lite with little or no customer impact,” explains Bobby Dominquez, Chief Information Risk Officer at PNC.

Media Relations

One area of incident response that is largely ignored is procedures for how to deal with media and notifications. Given the sensational nature of hactivism today, it’s probably a good idea to anticipate that a DDoS attack could carry with it some unwanted publicity.

As part of your planning, you should have an idea of whom and how you are going to respond to any media inquiries if the scale of the DDoS is large enough.

Conduct Table Top Exercises

A good plan should be tested and incident response plans are no exception.

To save time, consider adding DDoS mitigation to the annual DR table top review.

Table top exercises help flush out details and sticking points that would not otherwise come to light.
Make sure that you conduct a table top exercise at least annually and capture any lessons learned so that you can improve the plan continuously.

Detection and Analysis

One of the key problems with responding to a DDoS attack is the difficulty in simply knowing that you are under attack. DDoS attacks can be hard to diagnose especially if you don’t know what to look for.

Consider the data elements that you need to capture when planning for an incident. What services are affected? How do I know what normal is? Does the general staff know how to notify the team in case of an outage?

Capturing this data raising awareness to first responders can be time consuming, especially since a DDoS can look like a regular IT outage.

Engage the Help Desk

A good place to start is usually the help desk. Training and coordination efforts should be targeted at letting the help desk know what to look for and when to notify management. For example, if customer service gets inundated with service disruptions calls, an escalation process should alert the CIRT team members to a possible DDoS.

Including the CIRT team early is key so that they can start their analysis. Waiting to rule out server outages might take many hours and waste precious time that could have otherwise been used in initiating mitigation strategies

Performance Monitoring Tools

From there, other methods can be used to monitor uptime and responsiveness. Similar to IT monitoring, DDoS identification relies on a coordinated collection and analysis of performance data and alerts.

The incident response plan should take this into account. A list of data inputs and alerts should be identified as being critical in determining whether an attack is taking place.

Ensure that the DDoS CIRT team has been included so they can make a determination of if, and when to initiate mitigation strategies.

Don’t forget your call center! DDoS directed at call centers is a growing concern for financial services as it can be a threat vector to perpetrate fraud.

Make sure the CIRT team is being notified as to any call center outages.

Log collection

The incident response plan should also include information as to log sources that might be needed for further analysis.

Do you know where the attack is coming from? Can you track the IP addresses that offending traffic is coming from? This data is usually captured in logs at perimeter devices like firewalls and web servers.

Ensure that the plan has a list of logs that are deemed critical as well as how to access them. Procedures and processes to get access to logs should be included in table top testing.

Containment, Eradication, and Recovery

Once a DDoS attack has been confirmed, the CIRT needs to spring into action. This part of the plan should focus on escalation procedures, tools, vendors, and general things to do.

The tasks and procedures here should align with the vendors and solutions that you have identified. Escalation workflows should be documented with decision trees that give clear direction to the CIRT team as to how to proceed.

From there, document any procedures, processes, and tools that you need at every decision point.

With DDoS, it is very important to know when to escalate. Critical paths typically converge around trial and error. If solution "y" didn't work, go to "z".

For example, an attack identified as being volumetric might escalate directly to your ISP or DDoS mitigation service whereas a layer 7 DDoS might escalate first to your web application firewall (WAF).

Either way, plan your decision trees deliberately. The CIRT team should collaborate and try to think of all things that could go wrong. Contingency should be a factor in the incident response plan.

Lastly, make sure the plan accounts for recovery and improvement. "Don't forget to circle around and do a lessons learned", says Christina Whiting "complete the circle so you can improve for next time."

Recommendation 3: Third Party Due Diligence

The NCUA highlights the need for third party due diligence as one of the key strategies for mitigating DDoS risk. (1)

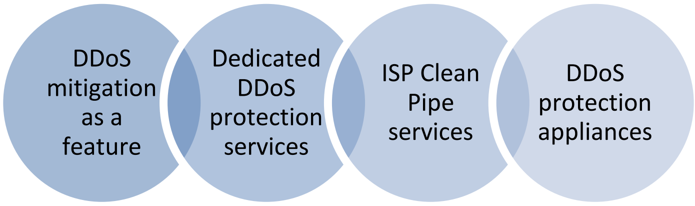
This should be looked at as an expansion of existing third party and vendor management activities to include a good understanding of criticality, risk, and readiness.

A good place to start is to classify third parties that may be susceptible to a DDoS. Consider critical infrastructure, but also web hosting and member facing services. The results of your risk assessment should give you an idea of your most critical vendors. From there, plan on engaging them in a process that captures their awareness, plan, and any mitigation services they have implemented.

Recognizing that not all third parties are created equal, plan on having a process by which to deal with any high risk vendors that are identified. Third party due diligence is a process that must take into account contractual and cost limitations. As with any risk, a proper risk treatment plan should be followed to give management the data they need to make informed decisions.

Recommendation 4: Evaluate DDoS Mitigation Services

The market for DDoS mitigation has grown to include both managed service providers and infrastructure solutions. Identifying what is right for your organization is a process that should start with understanding your options. Currently four types of DDoS mitigation solutions exist


DDoS mitigation as a feature
Dedicated DDoS protection services
ISP Clean Pipe services
DDoS protection appliances

:

DDoS Protection as a Feature

Content Delivery Networks (CDNs) and other services that offer content caching or distributed DNS often include DDoS protection as a feature of their service. Although preventing DDoS is often a secondary benefit, the primary being speed, these services tout the increased security they provide against DoS attacks. DoS protection is a natural fit for companies providing CDN service as they often have idle resources suited to combat denial of service and are already between the content being targeted and the attackers.

Since the DDoS protection provided by these services is usually an ‘extra’ rather than core functionality, they tend to buckle under more strenuous attacks. These services are also often much cheaper than dedicated DDoS services.

Moving to a CDN from a regular server can have integration challenges, though some newer CDNs such as CloudFlare use a caching reverse proxy architecture which allows for a much faster setup than the traditional distributed hosting architecture of most CDNs. CloudFlare can approximately match the response time of dedicated DDoS services for emergency deployment. (9)

Dedicated DDoS Protection Service

These services exist solely to protect against DDoS attacks. These services generally work like insurance: pay a monthly flat fee to protect yourself against a certain volume of attack.

They also usually offer much more expensive emergency implementation and mitigation service for damaging denial of service attacks already in progress. Traffic is tunneled or redirected to the services, usually via BGP, who then filter the traffic and deliver only clean data to the customer’s infrastructure. These services can usually handle extremely high volumes of attack traffic, but often at a correspondingly high cost. The emergency implementation these services offer, though expensive, provides the option for rapid response to an attack.

ISP Clean Pipe

These services are similar to, and often use the same technology as, dedicated DDoS protection services. Instead of redirecting the traffic via BGP or proxy, however, the ISP itself filters the data before delivering it to its customers. Clean pipes have the advantage of being totally in line and integrated with the internet service provider, but at the cost of added complexity and cost in environments where multiple ISPs are used and a separate service must be used for each provider.

If an ISP clean pipe is selected, options are limited and dependent on the ISP itself. ISP clean pipe services are also limited by the bandwidth of the ISPs backbone, where separate third party services can span multiple providers.

DDoS Perimeter Protection Appliances

DDoS Perimeter Protection Appliances are devices that are installed at the border of your network and are maintained by the vendor with signatures to filter Layer 3 and Layer 7 attack traffic. This form of protection will only provide a benefit if the DDoS attack is not saturating your internet connection, making them unsuitable on their own for volumetric attacks and high volume Layer 3 attacks. These boxes only function as a standalone DDoS solution for organizations with large multi-gigabit inbound pipes, such as hosting companies, ISPs, and managed security providers.

For smaller companies, these appliances should be deployed as a part of a multi-tier protection strategy with an upstream provider already filtering the majority of packets. The reason for this is that if the attack packets overwhelm the internet connection in front of the appliance, the filtering on the appliance is irrelevant as service is still denied.

The advantage of using a dedicated appliance in addition to upstream protection services is more capable Layer 7 filtering. These appliances have a reputation for performing much better at filtering application traffic than managed services protection and because they are on-site they can be quickly customized by administrators to defend against a particular threat.

Vendor Solutions

In each category of DDoS mitigation services, there is a group of leading vendors which offer the best protection and value for their customers.

The following will enumerate and detail the providers that have been found to be the best choices for DDoS protection.

DDoS Protection as a Feature

Name	Primary Service	Filtering	Price and Level of Protection
CloudFlare	Caching Reverse Proxy Content Delivery Network	Volumetric, Layer3, and Layer 7	Business: $200 per month per website | 100% uptime guarantee Enterprise: Starts at $3000 per month | 2500% SLA
Akamai	Distributed Hosting Content Delivery Network	Volumetric, Layer 3, and Layer 7	Based on clean bandwidth provided: approximately $0.05-$0.10 per gigabyte depending on size of deal

Akamai and CloudFlare provide great DDoS protection as a feature of their content delivery and web application acceleration services.

Akamai is the big name in traditional CDN Services and essentially provides distributed hosting to deliver content closer to its destination. The addition of DDoS protection is a compliment to their normal services and leverages the same support and management infrastructure.

CloudFlare is a relatively new, and somewhat disruptive company, who has shaken up the CDN model by providing reverse caching proxies instead of distributed hosting.

CloudFlare uses anycast to point users to the CloudFlare proxies while Akamai uses a tiered DNS server to point to their distributed hosts. Unlike Akamai the content is not hosted by CloudFlare, but rather proxied and cached. However if an attacker were to discover the real IP of the site behind CloudFlare, they could conceivably bypass CloudFlare's protection and services entirely.

Akamai and CloudFlare have both shown that they are capable at protection against DDoS attacks, with Akamai having filtered 124 Gbps of application traffic and CloudFlare having defended against the largest DDoS attack in the history of the internet.

Dedicated DDoS Protection Services

Name	Type	Filtering	Price and Level of Protection
Prolexic	BGP Redirect	Volumetric, Layer3, and Layer 7	Based on normal bandwidth usage. $7000 per month for 10Mbps clean pipe | SLA
VeriSign	BGP Redirect	Volumetric, Layer3, and Layer 7	$17,000 for 8gbps of protection per month | additional protection for 10,0000 per gbps per month during attacks greater than 8gbps up to 350gbps

Black Lotus	BGP Redirect DDoS Protected Hosted Servers	Volumetric, Layer3, and Layer 7	Pricing based on clean traffic: $1000 per month for 10mbps $2250 per month for 25mbps $2750 per month for 50mbps $3000 per month for 100mbps $4000 per month for 200mbps $6000 per month for 500mbps

There is a large number of dedicated DDoS protection services that provide very similar levels of service.

All of these services use the popular border gateway protocol (BGP) to redirect traffic to their filtering servers. By advertising a new BGP route for customers under a DDOS attack; the protection service can start receiving malicious traffic in minutes. The end result is "absorption" and "cleanse" of the offending traffic. These services rely on their immense network capacity to handle large traffic loads.

Black Lotus also provides a managed hosting service with native DDoS protection.

Prolexic and VeriSign have a reputation of being the more capable and reliable of the services in this field; largely due to their track record and history in the industry.

The advantage of these dedicated services are their simplicity, they only do one thing: prevent DDoS, and the relative ease of bringing them online and offline. By advertising a new route with BGP, the protection service can start receiving malicious traffic in minutes. These services also offer best of class Layer 7 protection, though a dedicated appliance is needed for the most effective Layer 7 filtering.

Choosing between one of these services is essentially a choice between expected uptime vs. price.

ISP Clean Pipe

Choosing an ISP Clean pipe vendor is simple, you must choose your ISP. The service available and level of protection varies greatly by ISP and location. Contact your ISP for pricing and service details to compare with other vendors. This option is usually best for Small to Medium Sized Businesses or other operations where all connections go through a single ISP.

DDoS Perimeter Protection Appliances

Name	Type	Filtering	Price and Level of Protection
Arbor	Dedicated DDoS Protection Appliance	Volumetric, Layer 3 and Layer 7	>$100,000 | 40Gbps of mitigation per appliance
FortiDDoS	Dedicated DDoS Protection Appliance	Layer 3 and Layer 7	$24,0000 for FortiDDoS-100A | 1Gbps of total traffic $50,000 for FortiDDoS-200a | 2Gbps of total traffic $70,000 for FortiDDoS-300a | 3Gbps of total traffic
Radware DefensePro	IPS with DDoS Protection	Layer 3 and Layer 7	Starts at $12,000 to $20,000 for DefenseProx02 Models | 100Mbps to 500mbps of total traffic. Starts at $45,000 for DefenseProx20 Models | 600Mbs to 3Gbps of total traffic

Arbor offers by far the most capable DDoS mitigation appliance and is a good choice for ISPs, or hosting companies and other managed service providers that want to include DDoS protection in their product suite. This is validated by Arbors commanding 3/5s control of the market and is used by many dedicated DDoS protection companies, such as VeriSign, to provide their protection. Arbor also provides an optional API to automatically request upstream DDoS protection from its partners when the internet pipe is saturated.

Radware provides a very good IPS which also provides good DDoS mitigation features, though the 3gbs appliance at the high end would be easily saturated by many attackers. This appliance provides a great value for SMBs and small enterprises that need both an IPS and want to provide enhanced Layer7 protection. Radware is second to Arbor in market penetration and has a very good reputation for performance and effectiveness.

FortiDDoS does not compete on throughput with Arbor and has no IPS features like Radware. This appliance is a good option for companies that just need a dedicated DDoS appliance and do not want to deal with the complexities of an IPS or need the high throughput of an Arbor device.

Conclusion

Distributed Denial of Service attacks have become a significant risk for financial services and their ability to continue providing uninterrupted services to their members. As such, regulators have started to engage members more directly and expect a concerted effort in developing a comprehensive DDoS risk mitigation strategy. As such, this should be considered a priority for all Credit Unions and Credit Union Service Organizations.

Implementing a DDoS mitigation strategy should take into account a formal assessment of risk, prior planning, third party due diligence, and capital investment. By implementing a variety of methods, Credit Unions and Credit Union Service Organizations can prepare for a security threat that is poised to grow over time.

About The Author

Ray Zadjmool is the President and Principal Consultant of Tevora. He is a CISSP, MCSE, PCI QSA, and PA-QSA with extensive experience across a number industries and client sizes. A PCI DSS expert, Ray has helped clients meet PCI DSS requirements under very challenging conditions without incurring significant cost.

Tevora is an information assurance consulting firm with a focus on compliance, risk management, and solutions integration. Tevora is an authorized PCI QSA firm and has among its financial customers one of the largest card brands, a major money transfer firm, and CO-OP Financial Services.

More information is available at www.tevora.com.

Acknowledgements

The author thanks the following individuals for their input, guidance, and peer review of this whitepaper:

1. CO-OP Financial Services Team
2. Bobby Dominguez, Chief Information Risk Officer, PNC Financial Services
3. Christina Whiting, Director, Enterprise Risk at Tevora
4. Kevin Dick, Information Security Analyst at Tevora

Bibliography

Works Cited

1. **NCUA.** Risk Alert No 13-Risk-01. *ncua.gov.* [Online] February 2013. [Cited: April 6, 2013.] http://www.ncua.gov/Resources/Documents/RSK2013-01.pdf.

2. **Kitten, Tracy.** Bank Attacks: 7 Steps to Respond. *Bank Info Security.* [Online] October 23, 2012. [Cited: April 6, 2013.] http://www.bankinfosecurity.com/bank-attacks-7-steps-to-respond-a-5221.

3. —. New Wave of DDoS Attacks Launched. *Bankinfosecurity.com.* [Online] march 6, 2013. [Cited: April 6, 2006.] http://www.bankinfosecurity.com/new-wave-ddos-attacks-launched-a-5584.

4. **Mcgarvey, Robert.** Patelco Confirms Five-Hour DDoS Takedown. *Credit Union Times.* [Online] January 29, 2013. [Cited: April 6, 2013.] http://www.cutimes.com/2013/01/29/patelco-confirms-five-hour-ddos-takedown.

5. —. Threat of the Week: DDoS Gets Real for Credit Unions. *Credit Union Times.* [Online] January 28, 2013. [Cited: April 6, 2013.] http://www.cutimes.com/2013/01/28/threat-of-the-week-ddos-gets-real-for-credit-union.

6. **ANDERSON, HEATHER.** DDoS Attacks Prompt NCUA Risk Alert. *Credit Union Times.* [Online] February 20, 2013. [Cited: April 8, 2013.]

7. **Obama, Barack.** *The Comprehensive National Cybersecurity Initiative.* s.l. : White House, 2009.

8. **Kerner, Sean Micheael.** US-CERT Warns about DNS Amplification Attacks. *eSecurity Planet.* [Online] April 1, 2013. [Cited: April 6, 2013.] http://www.esecurityplanet.com/network-security/us-cert-warns-about-dns-amplification-attacks.html.

9. **Prince, Matthew.** The DDoS That Almost Broke the Internet. *CloudFlare Blog.* [Online] March 27, 2013. [Cited: April 8, 2013.] http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet.

10. **Markoff, John.** Firm Is Accused of Sending Spam, and Fight Jams Internet. *New York Times.* [Online] March 26, 2013. [Cited: April 6th, 2013.] http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0.