A CU*ANSWERS WHITEPAPER
APRIL 2013

ASSESSING THE RISK DISTRIBUTED DENIAL OF SERVICE (DDoS)

April 29, 2013

Distributed Denial of Service (DDoS) attacks are in the news and on the mind of examiners. The following is a guideline for assessing your DDoS vulnerability and practical tips for addressing those concerns.

Note: The use of this article should not be taken as an endorsement of the use of torrent sites. Use of a torrent site could potentially result in criminal and/or civil penalties.

LEGAL DISCLAIMER

*The information contained in this whitepaper does not constitute legal advice. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this whitepaper. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.*

CU*ANSWERS A CREDIT UNION SERVICE ORGANIZATION

AuditLink CU*ANSWERS Management Services

DDoS TAKES OUT THE FBI

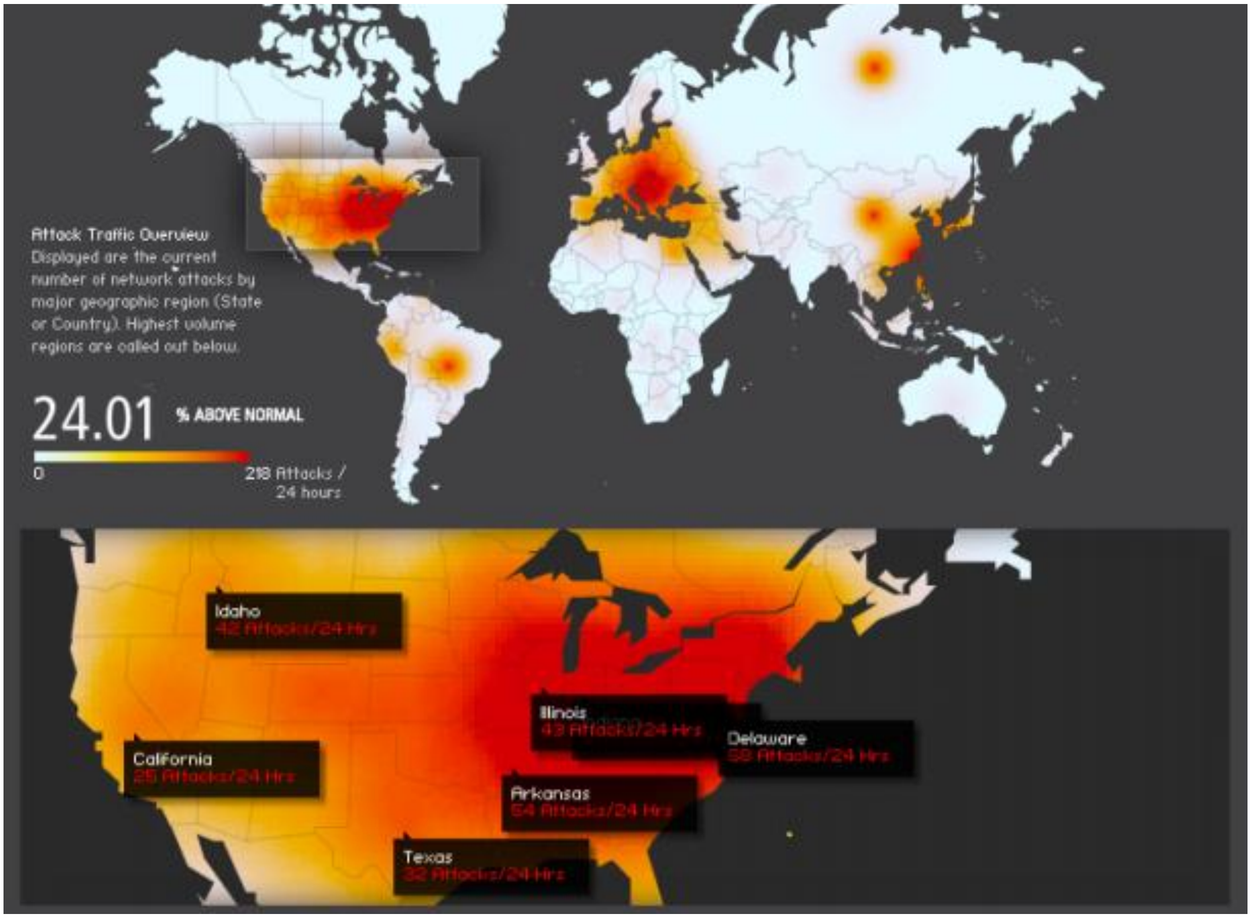
In early 2012, the torrent site Megaupload was both the fifteenth most popular site on the internet and a major target of international law enforcement. Claiming users of the site easily and freely distributed pirated material, U.S. and Interpol agencies estimated the site cost copyright holders upwards of $500 million in lost revenues. On January 19, 2012 a sting operation was launched, resulting in the arrest of four people in New Zealand and Megaupload going offline.

The timing of the Megaupload takedown was probably incidental, but the sting operation came at the same time large numbers of internet users were protesting the Stop Online Piracy Act, or SOPA, which would increase the authority of American law enforcement to look into file sharing sites and to increase the penalties for illegally sharing files. Upon learning of the Megaupload sting, some of these users struck back at the U.S. government.

Credit: Abode of Chaos

A mere few hours after the Megaupload news broke, DDoS attacks were launched against the website for the US Department of Justice. Next was the site for Universal Music Group, a SOPA supporter and the largest record label in America. Eventually, the web presence for the Recording Industry Association of America (RIAA), Motion Picture Association of America (MPAA), and Broadcast Music, Inc., or BMI, were all taken down. Most embarrassingly for the government, even the FBI website was compromised and shut down. The hacktivist group *Anonymous* took credit for orchestrating the attacks using software called *Low Orbit Ion Cannon*, or LOIC. The page below from akamai.com showed the spread of the attacks within a 24 hour period.

The attack was coordinated by sending links to users that purported to provide users with additional information about the FBI attack, but in reality automatically launched a Web-based version of LOIC. Innocent people just looking for information on the attack instead had their computers take part in the attack without the user's knowledge. No arrests have yet been made as a result of this attack. The Megaupload response, while not intentionally coordinated with the anti-SOPA protests, may have had an effect on Congressional support for SOPA, which never came to the floor for a vote. *Anonymous* took a hit as well, with increased scrutiny resulting in arrests for members who targeted PayPal, and the exposure of the names of some key *Anonymous* members. ◆



Credit: Akamai

UNDERSTANDING DDoS

Distributed Denial of Service (DDoS) attacks against internet targets have been around for a long time. As can be seen by the following page, a DDoS attack has relatively simple architecture. The sole purpose is to overload a network or service with so much traffic that it shuts down, similar to hundreds of letters being jammed through a mail slot at the same time. As illustrated in the attack on the FBI website, even persons who are not willing participants in a DDoS attack can have their machines compromised. Oil companies have been a frequent target of DDoS attacks, and in the last year or so the banking industry has been targeted more frequently.

The primary causes for the increase and severity of DDoS attacks is two-fold. First, the technical skill needed to launch these attacks is not very sophisticated. There are YouTube video tutorials that explain how to attack, and tools that can be downloaded to launch the attacks are readily available. Second, the technology needed to launch attacks requires only consumer-grade equipment, not commercial grade. Most individuals have the money to obtain the necessary hardware and software to launch attacks.

A common attack method is the use of botnets. Botnet is a jargon term for a collection of PC's that have been compromised by viruses, or bots, which autonomously follow the instructions given to it by an external controller. If a PC is infected with a botnet, it can be used surreptitiously to send traffic to the target of the attack. With hundreds of thousands of these compromised PC's, enough traffic can be generated to oversaturate network links or overrun the processing power of routers and servers. With the distributed nature of the attack, there are a huge amount of sources of the attack, making it difficult to block, and should anyone trace any particular attack back to its source, they will find a compromised PC rather than the true attacker. ◆

MOTIVES BEHIND DDoS

Although there may be other reasons for why an organization is singled out for a DDoS attack, most are the result of the following:

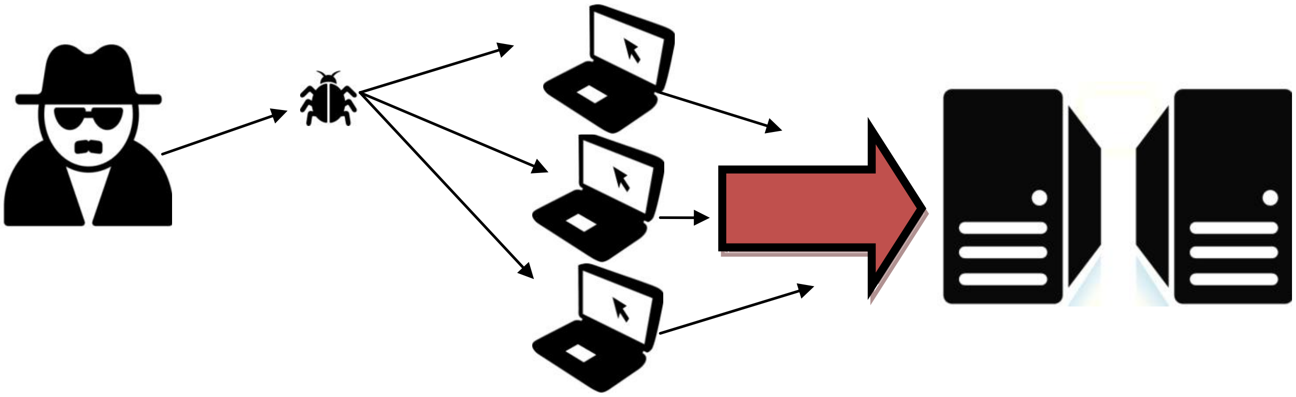
Hacktivism: *"Hacktivism" is using DDoS or other cyber attack against a company or an organization as a protest, usually in retaliation for an action taken by that organization. The takedown of the FBI site is an example of this type of DDoS assault. Hacktivism is not without its risk. Although attacks can be launched anonymously, if the identity of the attacker is compromised the criminal penalties for convicted offenders is generally much more serious than for physically occupying a business or government building as part of protests or civil disobedience.*

Blackmail: *There are gangs of Internet criminals who will use the threat of DDoS to force a business or organization to pay an extortion fee. Of course, there is no guarantee that the victim of DDoS blackmail won't be attacked anyway, or that other criminals will learn of the blackmail and make their own threats. This type of extortion does occur and should always be treated seriously.*

Revenge: *Although occasionally couched in hacktivist language, many attacks are motivated by revenge or retaliation. Disgruntled consumers or employees may target an organization.* Spamhaus, *a site dedicated to keeping ads for counterfeit Viagra and bogus weight-loss pills out of email inboxes, was the victim of a lengthy denial-of-service attack in March 2013, apparently from groups angry at being blacklisted.*

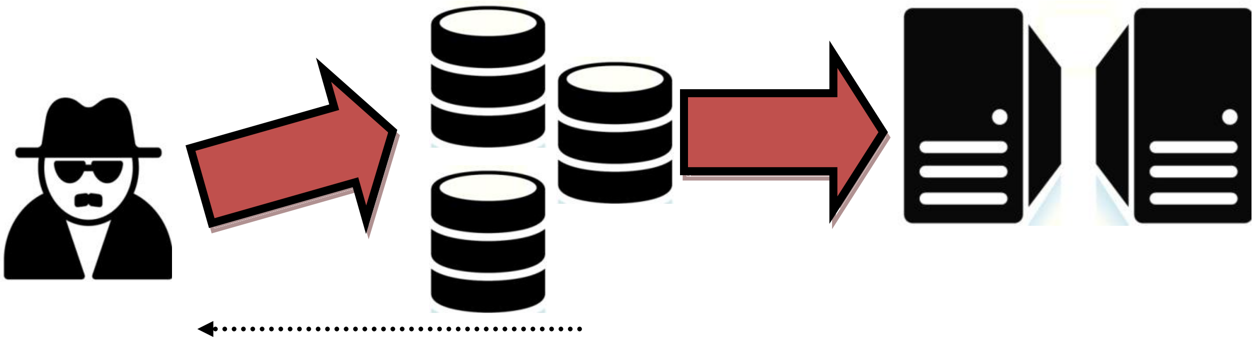
Whatever the motive, a successful DDoS attack will stop the organization from using internet based services to some degree. DDoS has even been used to cheat during online video games by knocking the victim offline. ◆

BOTNET ATTACK ILLUSTRATION



In a botnet attack, the criminal installs malware on unsuspecting PCs, often masquerading as legitimate software. At the command of the criminal, these infected machines all send traffic at once to the victim, overwhelming the machines to the point of failure. The attack on the FBI was a variant, where unwitting users went to web page, rather than having software directly installed on their machines.

DNS ATTACK ILLUSTRATION



In a DNS attack, the criminal sends a large number of requests to DNS servers and asks for a response. But instead of sending the response back to the criminal, the criminal fools the servers into responding to the victim. If enough responses are sent to the victim, those machines will be overloaded and shut down. This was the type of attack used against Spamhaus.

There is a way for DNS servers to be protected against this type of attack. A protocol called *Best Control Practices 38* (BCP38) provides methods to stop this from happening. While the vast majority of DNS servers are actually protected this way, there are enough unprotected DNS servers on the internet that allow this type of attack to take place.

There are many other methods to disrupt a network using DDoS. The illustrations above are only illustrating a couple methods of DDoS attacks.

SELF-PROTECTION

Always keep in mind that DDoS attacks can be mitigated but never fully prevented. Be wary of extravagant claims of expensive solutions. Because the varieties of DDoS attacks vary greatly and can exploit a network in many ways, there is no one solution that will address every possible method of attack. Even so, there are some best practices every institution should consider implementing. These can help prevent or mitigate attacks and are useful for examinations.

Firewalls: Firewalls should deny most protocols, ports and IP addresses. If the network detects a number of unusual IP addresses reaching the firewall, rules can be put into place to drop all incoming traffic. Some firewalls have other capabilities to detect and thwart certain types of DDoS attacks. *Warning: sometimes very small attacks are actually reconnaissance for a subsequent massive attack. Staff should always maintain a state of high alert after a small attack is thwarted.*

Routers and Switches: Most routers and switches have ways to detect bogus IP addresses and other forms of attack.

Traffic Identification Appliances: This option analyzes network traffic as it enters the system, and then identifies them as priority, regular, or dangerous. Dangerous traffic can be stopped before it reaches the intended destination.

Intrusion Prevention Systems (IPS): IPS can be used to detect network traffic anomalies and prevent that traffic from reaching critical services.

None of these options are fool-proof, but utilization of these options can help the security posture of the business. ◆

NCUA REQUIREMENTS

In the *13-Risk-01 Letter to Credit Unions, Mitigating Distributed Denial-of-Service Attacks*, the NCUA offered preferred strategies for mitigating DDoS risk. The NCUA correctly noted that DDoS does not present the risk of stealing funds or data, but could potentially be used as a distraction while an actual security breach is taking place elsewhere.

The NCUA wants federally-insured credit unions to take the following actions:

1. Complete a risk assessment focusing on DDoS.

2. Ensure DDoS is part of the incident response program of the credit union.

3. Have third parties perform tests on DDoS-vulnerable web-facing applications and services, and follow the recommendations provided by the third parties can be supported by the business.

4. Voluntarily file a Suspicious Activity Report (SAR) " … if an attack impacts Internet service delivery, enables fraud, or compromises member information."

This response need not be especially difficult or time-consuming. This is a legitimate concern and should be taken seriously by all financial institutions and businesses.

Outside of the NCUA requirements, credit unions should also consider pressuring their internet service providers to offer DDoS mitigation strategies. Large numbers of consumers placing pressure on providers is likely to effect change in the providers' security posture. ◆

ASSESSING DDoS RISK

The following elements should comprise a DDoS risk assessment:

1. *Business Impact*: What Internet-facing services are vulnerable? Is it a major issue if members cannot get to your website? What about the connection between the credit union and CU*BASE?

2. *Controls*: For vulnerable systems, what controls are in place to prevent DDoS? Have the anti-DDoS capabilities of firewalls and other network equipment been evaluated and put into place?

3. *Testing*: Have these controls been tested by a third party firm? Have recommendations come out of testing? Is the board of directors aware of the recommendations? Has the board had an opportunity to approve the implementation of stronger controls or accept the risk due to the costs of implementation?

4. *Disaster Recovery*: Does the disaster recovery plan address DDoS? How would communications go out to members? Is the need for a SAR addressed? How would law enforcement be involved?

5. *Training*: Do staff involved in IT have adequate training to recognize and respond to a DDoS attack? Does management know how to respond to DDoS blackmail threats? Is staff on alert if a consumer or former employee begins making threats?

These evolutions do not need to be especially complicated. DDoS response is very similar to any response the institution might have if a system were unavailable for other reasons, such as a natural disaster. Having these answers readily available can be very useful during a real DDoS emergency. ◆

SAMPLE ASSESSMENT

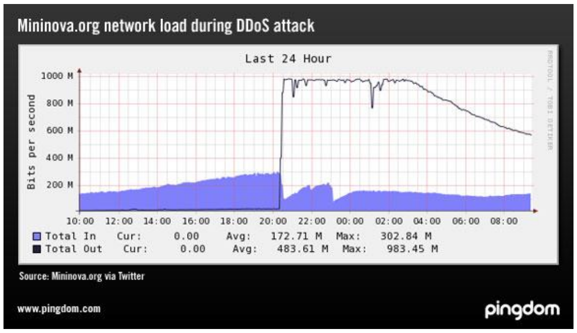
System	Critical?	Related Systems	DDoS Controls in Place?	Penetration Tested?	BoD Reviewed Results?	Recommendations?	Implemented?	Part of Disaster Recovery?	Comments
Web Page	N	Online Banking	Y	Y	Y	Y	N	Y	The web page has intrusion detection and firewall controls, and its covered in the disaster recovery plan. Recommendation for a newer IDS system was brought to attention of the board of directors, but cost was too prohibitive at this time for a non-critical system.

ANALYSIS OF A DDoS ATTACK

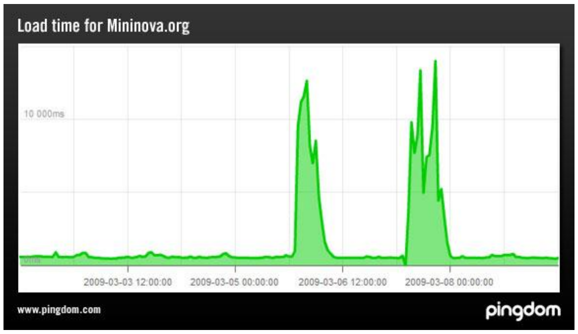
In 2009, the torrent site MiniNova was the victim of a DDoS attack. MiniNova shared information on the attack with pingdom.com. Much of that information was published on March 10, 2009 by pingdom, entitled "The Anatomy of a DDoS Attack." Some of the discussion will be technical.

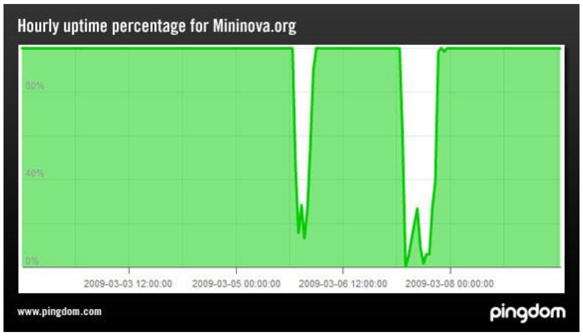
MiniNova's site was attacked by a botnet using UDP connections and employing hundreds of unwitting computers. The attack was successful almost immediately.

There were two separate and successful attacks on MiniNova. The load time of the sites (not including things such as images) was significantly impacted. Many times the attempt to load the page timed out, in addition to slowing network traffic to the web page. Based on the graphs shared, both attacks resulted in approximately 14 hours of downtime for the MiniNova site.



Source: Mininova.org via Twitter


Load time for Mininova.org
10 000ms
0ms
2009-03-03 12:00:00
2009-03-05 00:00:00
2009-03-06 12:00:00
2009-03-08 00:00:00
www.pingdom.com
pingdom


Hourly uptime percentage for Mininova.org
2009-03-03 12:00:00
2009-03-05 00:00:00
2009-03-06 12:00:00
2009-03-08 00:00:00
www.pingdom.com
pingdom