Executive Suite Series

A Prolexic White Paper

Plan vs. Panic: Making a DDoS Mitigation "Play Book" Part of Your Incident Response Plan

PROLEXIC
DDoS Attacks End Here.

Introduction

When a huge Distributed Denial of Service (DDoS) attack took down the web site of a global web hosting provider, even the expensive DDoS mitigation hardware specifically purchased for such a scenario could not stop the attack. The e-mail customer support group and online forum were flooded with complaints from customers whose web sites were completely inaccessible. To make matters worse, the hosting provider's ISP refused to bring their servers back online until a reliable DDoS mitigation solution was put into place. The company's IT staff was at a loss at what to do or who to call next and dealing with the DDoS attack was the sole focus of the entire company for the next three days. Daily business was disrupted and all projects were put on hold as confusion and panic spread throughout the organization. Eventually, the hosting provider found a DDoS mitigation service provider with the expertise and capacity to mitigate the attack quickly and completely – but the damage was already done to the company's reputation, revenue stream, customer confidence, and productivity.

DDoS attacks are deliberate, targeted events – happening on a daily basis – that demand a preparedness plan much like homeowners preparing for hurricane season

A DDoS attack is an attempt to make a computer resource (i.e. web site, e-mail, VoIP, or a whole network) unavailable to its intended users. By overwhelming it with data and/or requests, the target system either responds so slowly as to be unusable or crashes completely. The data volumes required to do this are typically achieved by a network of remotely controlled computers known as Zombies or bots. These have fallen under the control of an attacker, generally through the use of Trojans.

When a DDoS attack cripples or brings down a web site, knowing who to call first and how to marshal the required resources for mitigation can make the difference between organization-wide panic and a calm, orderly response. Most importantly, planning ahead makes the difference between fast and effective DDoS mitigation and letting the attackers have the upper hand with a campaign of attacks that can drain thousands of dollars of revenue per hour. According to Forrester Consulting, the average revenue per hour loss during a Layer 7 DDoS attack is US$220,000 per hour, not to mention the frustration and eroding confidence of customers and business partners who cannot access web-based services and/or information.

Prolexic continues to see an increase in the number, size, and complexity of DDoS attacks, including multi-day campaigns characterized by rapid changes in attack vectors. DDoS attacks are also increasing in packet-per-second (pps) volume, which can be particularly devastating. Unfortunately, it's not a matter of "if" but "when" a web site will be hit with a DDoS attack. All industries are targets. Consequently, Prolexic believes that being prepared is the best defense, and that clear, organized communication with all stakeholders in the DDoS mitigation process is the key to fast, successful attack mitigation.

Why DDoS belongs in an incident response plan

Some companies have incorporated DDoS mitigation as part of their disaster recovery plan. However, disaster implies that something unexpected or accidental threatens business continuity. DDoS attacks are

deliberate, targeted events – happening on a daily basis – that demand a preparedness plan much like homeowners preparing for hurricane season. When the hurricane inevitably hits, they don't panic and the damage to the home is minimal because they knew what to expect and what steps to take to protect their investment. This type of incident response plan enables companies to be prepared to quickly and calmly respond to a DDoS attack and that can minimize both operational and financial damage to an online business.

A "play book" can be essential to a controlled, streamlined response to a DDoS attack

As noted earlier, Forrester has found that an online company loses an average of US$220,000 of revenue per hour during an unmitigated DDoS attack. If the communication structure for DDoS events is not spelled out in an incident response plan, IT may spend 45 minutes or more finding and engaging an on-call resource and bringing that engineer up to speed on what's happening. It takes even longer to resolve issues if IT management or another department manager panics and starts calling engineers randomly – and none of them know what to do. However, when a DDoS event has begun and a well-rehearsed plan is in place, IT management knows who to call first and that person knows exactly what to do and carries out the next steps in the incident response plan. There should be a single point of contact for communications about the event and everyone's roles should be clearly defined. As a result, DDoS mitigation services can be activated more quickly and the attack can be mitigated faster, resulting in far less financial and operational damage.

Developing a DDoS mitigation "play book"

Winning sports teams don't ad lib or panic on the field when the opposing team launches a surprise offensive play. They have a well-rehearsed "play book" with defensive moves that have been developed with their coach's expertise and built upon experience in multiple games with various opponents. When it comes to DDoS mitigation, a similar type of "play book" can be essential to a controlled, streamlined response to a DDoS attack.

In simple terms, companies work with their DDoS mitigation service provider to create a simulated DDoS attack or "dry run" that makes no actual changes to the network, but will help management see the best way to manage both internal and external communications when confronted with a DDoS attack. The incident response team works through a real-world DDoS attack without doing an actual live test, much like a military training drill in which no live ammunition is used. Depending on the size and complexity of the organization, this type of dress rehearsal exercise can be completed in a little over an hour, or slightly longer if the company's incident response plan has additional requirements. Executive management will understand how long it takes to put the mitigation plan in action. Following this exercise, optimizations may be developed to ensure a rapid, repeatable and predictable action plan.

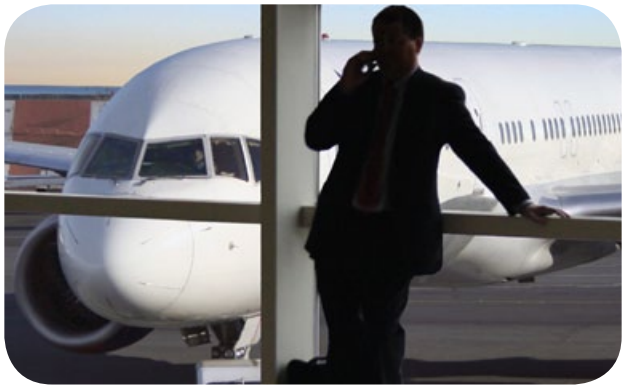
A DDoS mitigation "play book" must be a streamlined response plan which includes:

- **Managing communications** – DDoS attacks have an impact not just on IT, but on all users of the company's services, including non-technical departments. They also need to know who to call and what to do when issues arise during a DDoS attack without disrupting daily business. Prolexic advises incident response teams to have a single point of contact for relaying information and short "Twitter-style" updates internally across the organization. These short internal blasts should be confidential and help people understand what is going on during the attack so that they don't panic and create an additional internal crisis.

- **Identifying the key contact persons** – The main goal of the "play book" is to eliminate organization-wide panic that can delay the mitigation response when a DDoS attack occurs, so it is vitally important that the right people be notified of the attack immediately. In doing this simulation exercise, everyone in the triage team will understand what their role is in the DDoS mitigation process, what changes they need to make to the network, and how they can continue to maintain business as usual even when some resources are unavailable.

- **Organizing information for easy, fast accessibility** – Something as simple as keeping all names and phone numbers of key contacts in a single place can save valuable time. Overall, this facet of the DDoS mitigation process is all about containment and order – how to turn a DDoS attack from a major disaster into an incident that is routine when handled according to the well-rehearsed "play book."

A real-world example of DDoS attack readiness



A leading travel/hospitality provider and Prolexic client came under a very large and sophisticated DDoS attack one weekend. Although the company had high quality on-site mitigation appliances, these appliances could not scale to combat the escalating size and complexity of the attack. IT management also started working with the company's Internet provider to mitigate the attack, which continued for another 20 hours. After the Internet provider failed to halt the attack, the firm's next step was to contact Prolexic.

Fortunately, Prolexic and the travel/hospitality firm had planned ahead and worked together to develop a "play book" – a process in which both companies explored different attack scenarios and how to best communicate with different stakeholders for an effective, controlled mitigation plan, eliminating panic and confusion. This "play book" became a part of the company's incident response plan and fine-tuned the process. Most importantly, this plan identified the key communications channels within the organization and Prolexic, so that everyone was on the same page when Prolexic activated the mitigation service.

After receiving a call from the company at 8 a.m. on Monday morning, technicians at Prolexic's Security Operations Center (SOC) joined conference calls that the travel/hospitality customer was having with its Internet provider and telco equipment provider.

Prolexic technicians also began coordinating with their contacts at the company. At 10:00 a.m., according to the "play book" and Prolexic protocols, three teleconference bridges were opened up.

- **A Mitigation Bridge** – primarily for engineers to coordinate and monitor mitigation efforts
- **A Troubleshooting Bridge** – primarily for engineers and application owners to investigate any problems arising during the on-ramping
- **A Security Emergency Response Team (SERT) Bridge** – primarily for security and forensics participants.

These bridges were "always on," enabling participants to periodically check in and monitor the latest developments and communicate news and changes through the "play book" channels.

At 11:30 AM it was decided that that attack was too big for the Internet provider and traffic would be routed to Prolexic. Because of all the upfront planning and testing, this was a relatively simple and almost instant process.

By developing and testing a "play book", the company was able to deflect the usual panic that can grip an organization during a DDoS attack.

Thanks to the clear communication plans developed earlier as part of the "play book," Prolexic was able to more quickly route traffic from three of the firm's main data centers to its attack mitigation network or "scrubbing centers." As soon as traffic began flowing through Prolexic's scrubbing centers, it was possible to begin forensics and analysis. Later that afternoon, Prolexic's Security Emergency Response Team (PLXsert) reported a detailed analysis of the attacking botnets and IP addresses. This information was later provided to law enforcement authorities and was instrumental in degrading the attack.

Because both the travel/hospitality company and Prolexic had developed a controlled and streamlined communications plan or "play book" upfront – before a DDoS ever occurred – the company was able to deflect the usual panic that can grip an organization during a DDoS attack, and Prolexic was able to deploy its industry leading DDoS mitigation services even faster and more efficiently.

Conclusion

"Be prepared" is a classic motto with modern, serious implications for online businesses today that are in constant danger of DDoS attacks. Prolexic advises IT management to talk to their DDoS mitigation services provider before an attack happens. Ask questions and discuss all of the possible DDoS scenarios that the company could experience. The best defense against malicious cyber threats is preparedness and understanding how to use the vendor's DDoS mitigation services to the best advantage.

Any good mitigation service provider should have the expertise and capacity to serve many clients simultaneously – an important factor to consider as the daily occurrences of DDoS attacks escalate. Prolexic has been immersed in this cyber war for nine years and our SOC technicians are routinely mitigating a dozen or more attacks at the same time. In addition, all of our protocols are designed for rapid response to attacks and we use the same principles demonstrated in the simulations we complete with our customers. Our protocols and procedures are well defined and are tested on an hourly basis during real DDoS events.

In the end, when everyone in an organization – not just IT staff– understands what it is really like to be under a DDoS attack before one actually occurs, they will be able to face the actual event with more confidence, control and calm. As a result, the DDoS mitigation process will go more smoothly for a faster return to business as usual. That is why Prolexic advises all of our customers to prepare themselves for the real thing with a simulated DDoS incident and incorporating DDoS into an incident response plan.

About Prolexic

Prolexic is the world's largest, most trusted distributed denial of service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit **www.prolexic.com**, email **sales@prolexic.com** or call **+1 (954) 620 6002**.

© 2012 Prolexic Technologies, Inc. All rights reserved.
v.032012

PROLEXIC
DDoS Attacks End Here.