CORESPACE
Dedicated Servers and Colocation

7505 John W. Carpenter Fwy.
Dallas, TX 75247

INCIDENT REPORT – DDoS Outage 7/14/12 – 7/16/12

SUMMARY

Incident:	Distributed Denial of Service (DDoS) - Advanced Persistent Threat
Date/Time:	Approximately Noon CST 7/14/12 to Approximately 11:45am CST 7/16/12
Impact:	High
Report Author:	CoreSpace Executive and Network Administration Teams
Date of Report:	7/30/12

INCIDENT DESCRIPTION

Approximately Noon CST Saturday, July 14, 2012, the CoreSpace Dallas network came under attack by a new type of DDoS (Distributed Denial of Service) known as an Advanced Persistent Threat. An Advanced Persistent Threat is a mixture of different UDP and TCP SYN flood attacks dynamically targeting multiple IP addresses.

CAUSE

A targeted attack of inbound DDoS saturated our Corero IPS Network Security systems with over two million sustained packets per second resulting in massive packet loss.

SCOPE OF THE INCIDENT

The DDoS affected the entire CoreSpace Dallas data center network. It knocked out network service to most clients as well as internal email, phones systems and the CoreSpace website. It affected all CoreSpace IP ranges.

COMMUNICATIONS DURING INCIDENT

The DDoS inhibited CoreSpace from communicating with customers via phone or email during much of the attack. CoreSpace utilized the WebHostingTalk forum, specifically designated for Providers, to be able to communicate with clients during this outage. During the outage, the CoreSpace website was moved outside the Dallas data center, and was put back online. We included a splash screen with some basic outage information so our clients could be informed of the outage.

STEPS TAKEN TO RESOLUTION

The attack was identified almost immediately. The CoreSpace networking team quickly began putting measures in place to mitigate the threat, however the attacks where sophisticated and simultaneously deploying counter-measures.

CoreSpace consulted Corero, our partner for security services, to assist in tuning the IPS systems to mitigate the attack. During this time, we were looking for alternative solutions to help us resolve this powerful attack. After working to mitigate the attack for nearly 24 hours and having only successfully dropped the inbound packets to around 1/3 million per second, with fluctuating packet loss from 5 to 20%, the CoreSpace network team then engaged Black Lotus, a vendor who specializes in DDoS mitigations.

At approximately 5pm CST Sunday, July 15th, 2012, CoreSpace offloaded all inbound traffic to Black Lotus who cleaned and funneled the routes via a GRE Tunnel restoring connectivity to the CoreSpace network. At approximately 11:45am CST Monday, July 16, 2012, Black Lotus reported that the attack had been successfully mitigated and that the CoreSpace routes were ready to be moved back to the CoreSpace network.

PROSECUTION

CoreSpace has contacted FBI's Cyber Crimes Division and is in the process of filing a detailed report. We will work closely with the FBI to assist in finding the source and perpetrator of the attack. If the alleged offenders are identified, CoreSpace will prosecute to the full extent of the law.

IMPROVEMENTS

Network Security: The CoreSpace networking team has been working with the Security Support Engineers and Executive Management Team at Corero to perform a full audit of our Corero IPS Devices to identify areas that can be better tuned for more effective DDoS mitigation. This process may require some scheduled network maintenance to be performed during the CoreSpace Maintenance Window of 2am - 4am CST daily. As standard operating procedure dictates, clients will be notified at least 48 hours in advance of any scheduled maintenance unless the maintenance is deemed an emergency, upon which clients will be notified as far in advance as possible.

CoreSpace will also keep an ongoing relationship with Black Lotus as an additional line of defense against advanced DDoS attacks. In the event our internal networking solutions are overcome in an advanced DDoS situation, we will utilize Black Lotus and their DDoS filters to assist in mitigating the attack.

Phone Support: The CoreSpace VoIP system was utilizing the same network that was affected by the DDoS. We have since changed phone vendors and are installing a back-up line on a separate network for redundancy. This will avoid any phone outage in the case of another DDoS as well as provide a "back door" line of communication for Corero.

CoreSpace Website: The CoreSpace website was hosted on the same network that was affected by the DDoS. We have moved the website to our data center in Los Angeles and are putting in measures for even additional website redundancy and load balancing. Also, the CoreSpace website did not have an area for Network Status postings. We have added the link to the CoreSpace website and Client Portal. Future issues involving the network will be immediately posted on the Network Status page.

Social Media: Some customers communicated that we should have utilized the advantages of social media to communicate with customers during and regarding the outage. This would have given customers quick status updates on the condition of the network and the steps we were taking to eliminate the attack. We will begin utilizing social media accounts using Twitter and Facebook. Going forward, we will be sure to immediately post communications to keep our customers up to date on any events affecting service.

CoreSpace Emergency Response Plan: CoreSpace recognizes that how we respond to an emergency is just as important as prevention. CoreSpace is currently evaluating the Emergency Response Plan to identify areas that need to be adjusted to ensure a more effective and efficient response by the CoreSpace team. Specifically, we will focus on areas that involve internal communications and communications with clients.