the Availability Digest

www.availabilitydigest.com

Twitter Taken Down by DDoS Attack

August 2009

On Thursday, August 6, 2009, the Twitter social networking site went down. It suffered repeated outages, timeouts, and serious slowdowns for at least two days. What caused this failure?

To add to the mystery, Facebook and LiveJournal simultaneously had similar problems. Were these outages somehow related? They occurred at about the same time as the 2009 Defcon 17 hackers conference held from July 30th to August 2nd. Could this have been some misguided mischief?

But first, what is Twitter? For those who haven't yet become addicted, Twitter is a microblogging social networking site that allows users to communicate what they are doing to their "followers" at any time via 140-character text messages, or "tweets." Twitter was born in 2006 and has exploded in use. It currently has about five-million registered users, and an estimated 45 million people follow these users via their tweets.

Twitter sprung into the mainstream when Republican presidential candidate John McCain joined the 21st century technology by embracing tweeting following the 2008 U.S. presidential election. Even more recently, and perhaps more importantly, Twitter was the primary communication mechanism to the rest of the world from those Iranians participating in the major rallies decrying the recent Iranian presidential election process. The untimely death of Michael Jackson also saw a massive increase in tweet volume.

The Twitter Outage

Access to Twitter Lost

Twitter has not been known for its availability record. Pingdom, a web-site monitoring service,[1] reports that Twitter was down for 84 hours in 2008, achieving only a 99% uptime.[2] It should be noted, however, that Twitter is working hard to improve this record; and its uptime improved significantly in the second half of 2008.

All that progress was threatened at 9 AM EDT on Thursday, August 6, when Twitter suddenly became unavailable to those trying to use it. During that day and much of the next, Twitter was down for a few hours, would seem to recover but would be sluggish or subject to timeouts, and then would go down again. Continuous periods of outages and timeouts continued well into the next day. Was this just another Twitter outage?

[1] You can track your web site's uptime and performance by signing up with Pingdom at www.pingdom.com.
[2] Study: Twitter's Uptime Horrible in 2008 but Improving, *PC World*; February 19, 2009.

It didn't take long for Twitter to conclude that no, this was not just another outage. Rather, it seemed to be a target of a distributed denial of service attack (DDoS) in which its servers were being swamped by spam messages. At 9:43 AM, EDT, on its service-status blog, Twitter staff said that "We are determining the cause and will provide an update shortly." It did not take them long to verify the cause. At 10:49, they added "We are defending against a denial-of-service attack, and will update status again shortly."

Is This Really a Big Deal?

The outcry over the Twitter outage showed just how far Twitter has come as a source of information for millions of people. But did this outage have any serious consequences? After all, isn't Twitter just a social network used for communicating between friends and following the antics of the well-known? Isn't it a waste of employees' time in a corporate environment? The Marines have banned all social networking among its troops for the next year. The NFL has banned Twitter.

However, the answer to the above questions is "not any more." In just a short time, the importance of Twitter has grown far beyond that of simply social networking. It has established itself as a crucial platform for information exchange in the face of global events where more traditional means of broadcasting have been inaccessible or blocked, as shown by the recent events in Iran. Furthermore, many companies are discovering the value of Twitter in their public relations, marketing and sales efforts. They find that Twitter allows them to engage with customers in real time.

Companies are now experimenting with Twitter in two ways:

- Outbound messaging – Companies are posting tweets about corporate accomplishments, new product announcements, and other information to their followers. AT&T uses Twitter to communicate network outages to their ISPs. Many power companies are using tweets to inform their customers about the status of power outages. Airlines are advertising cheap fares good for just a few hours on undersold flights. Even the SEC, the U.S. Securities and Exchange Commission, has three Twitter accounts – one for news, one for investor relations, and one for employment opportunities.

- Inbound messaging – Companies are using the Twitter search feature to track tweets concerning them. Many tweeters have been quite surprised when complaint tweets that they have just sent to their friends suddenly get a response from the company offering help. Companies taking advantage of this source of real-time customer satisfaction information include Comcast, Dell, GM, H&R Block, Kodak, Whole Foods Market, Jet Blue, Southwest Airlines, and United Airlines.

Though social networking certainly is not yet mission-critical, Gartner Group's July 2008 report added microblogging to its list of technologies that will transform business over the next two to five years.

Yes! The Twitter outage due to a DDoS attack is certainly significant.

Facebook and LiveJournal Outages

But Twitter seemed not to be alone. The Facebook and LiveJournal social-networking web sites were also struggling with slowdowns and outages at the same time. LiveJournal was totally down for several hours, but came back up that afternoon. Facebook stayed up, but was facing slowdowns. It managed to minimize any impact to its sites.

24 hours later, Facebook and LiveJournal were back to normal operation; but Twitter was still in trouble. Working together, the staff of these social networks discovered that they were all the subject of the same DDoS attack. But why?

The Detective Work

What is a Denial of Service Attack?

A DDoS attack occurs when a web site is overloaded by a massive volume of unwanted traffic. In trying to respond to this traffic, it cannot respond to its normal traffic; and its web servers may even crash.

DDoS attacks are launched by a zombie army controlled by a single master. Prior to the attack, using security flaws in unprotected machines, the master installs malware on tens of thousands of PCs worldwide. This army of zombies is called a "botnet." The botnet is simply waiting for instructions from its master.

At some point, the master gives instructions to its zombie army to carry out some coordinated task. In the case of a DDoS attack, this task is to send messages carrying some particular content to one or more web sites. These web sites are now under attack and, unless protected, will suffer severe performance problems or crashes. Because of the distributed nature of the attack, it is extremely difficult to trace the attack back to the master.

DDoS attacks have been carried out for years. However, they did not garner much attention until one week in the year 2000, Yahoo!, CNN, Amazon, and eBay were all taken down by a DDoS attack launched by a Canadian teenager who wanted to make a hacker name for himself. DDoS attacks suddenly became part of the web mainstream.

The Clue

It didn't take but a few hours for the social networks, working in concert, to determine the reason for the assault. The spam messages were all queries against the blog of a single user who went by the user name Cyxymu. Clearly, someone was out to silence Cyxymu. But why?

Cyxymu

It turns out that Cyxymu is a pro-Georgian blogger, a 34-year old economics lecturer from Tbilisi, Georgia, who had been criticizing Russia's conduct in its war a year ago over the disputed South Ossetia region. Cyxymu is the name of a town in the former Soviet Union.

Cyxymu had accounts with Twitter, Facebook, LiveJournal, Google's Blogger, and YouTube. Upon further investigation, Google and YouTube were also targeted but were substantially unaffected. LiveJournal blocked access to Cyxymu's account in order to recover from the attack. Facebook, though experiencing slowdowns, managed to keep Cyxymu's account available.

In later posts, Cyxymu blamed Russia for the attack. He suggested that the timing of the attack was meant to silence him on the eve of the one-year anniversary of the Russian attack on Georgia.

Max Kelly, chief security officer at Facebook, is quoted as saying that "It was a simultaneous attack across a number of properties targeting him [Cyxymu] to keep his voice from being heard." However, Mr. Kelly declined to speculate on whether Russian nationalists were behind the attack.[3]

[3] Twitter, Facebook attack targeted one user, *CNet News*; August 6, 2009.

Protecting Against DDoS Attacks

How can you protect your web site from such attacks? It seems that there are two strategies:

- Have enough capacity to withstand such an attack. This can be accomplished by hosting your web site on the cloud. Many hosting services have tremendous data centers and through virtualization can provide additional capacity on demand to meet peek needs – even those dictated by a DDoS attack. You might pay more for the temporary additional capacity needed, but you won't go down.

- Detect the difference between legitimate traffic and spam, and direct the spam to a virtual garbage bin – a black hole. Like a pathogen, a disease-producing agent in the animal body, nefarious traffic is known as "pathological network traffic." This traffic can often be detected by its repetitiveness.

Products are available to protect against pathological network traffic. Cisco markets its Distributed Denial of Service Protection Solution[4] to ISPs. This product allows the ISPs to deliver "clean pipes" to their customers. The product distinguishes between legitimate traffic and pathological traffic and filters out the latter.

For the end user, Prolexic Technologies (www.prolexic.com) offers a service that will provide essentially the same function. Its DDoS mitigation service will filter out pathological traffic destined for a subscribing web site.

Lessons Learned

Launching a DDoS attack today is almost trivial for a qualified hacker. Such attacks occur frequently. Sites have been shut down for ransom, especially offshore gambling sites that are not high on the priority list of law enforcement agencies. Financial institutions and online stores have been shut down by such attacks and their traffic redirected through a DNS (Domain Name Server) security flaw[5] to fraudulent web sites in order to harvest credit card numbers.

A botnet can be rented for about 10 cents to 40 cents per PC. For $4,000, a nefarious antagonist can launch a sustained attack against your web site from 10,000 PCs; and you'll probably never be able to track down the perpetrator.

No matter how big you are, you should worry about the possibility that someday you may be the target of a DDoS attack. Take precautions today to protect yourself. Twitter has probably learned that lesson the hard way. Two years ago, it had a miserable availability record and has put a major effort into solving that problem. This was such an extensive effort that protection against a DDoS attack may well have fallen off of its priority list. I'll bet it's back on now.

Acknowledgements

In addition to the references already given, material for this article was taken from the following sources:

Twitter Downed By Denial Of Service Attack, *Information Week*; August 6, 2009.
Serious Twitter, LiveJournal Outage Ongoing, *The Washington Post*; August 6, 2009.
Twitter, Facebook, and LiveJournal Down at the Same Time, *ReadWriteWeb*; August 6, 2009.

[4] Cisco Distributed Denial of Service Protection Solution: Leading DDoS Protection for Service Providers and Their Customers, *Cisco white paper*, www.cisco.com.
[5] A correction is available for this flaw, but many DNS servers have yet to be upgraded.

Twitter Tanks on Thursday Morning, *CBS News*; August 6, 2009.
Why This Twitter Outage Matters, *PC World*; August 6, 2009.
Facebook Confirms Problems, But Is It an Attack?, *PC Magazine*; August 6, 2009.
How Did Hackers Cripple Twitter?, *Time*; August 6, 2009.
Twitter Outage Moves Into Day 2, *The Washington Post*; August 7, 2009.
Georgian blogger Cyxymu blames Russia for cyber attack, *Guardian*; August 7, 2009.
Russian Hackers Besieges Social Sites to Silence Pro-Georgia Blogger, *TechNewsWorld*; August 7, 2009.
How Companies Use Twitter to Bolster Their Brands, *Business Week*; September 6, 2008.
4 Ways Companies Use Twitter for Business, *ReadWriteWeb*; March 29, 2009.
Twitter, Facebook Attacks No Surprise to Security Experts, *Wired*; August 6, 2009.
Twitter, the New Investor Relations Communication Tool, *Email Wire*; July 16, 2009
A Survey on Solutions to Distributed Denial of Service Attacks, www.ecsl.cs.sunysb.edu/tr/TR201.pdf.