the Availability Digest

www.availabilitydigest.com

More Never Agains IX

July 2013

Our last several issues of the Availability Digest included many notable failures and cyber attacks that took down corporate systems. Spamhaus, a spam-site blacklisting firm, was taken down for days by a massive DDoS attack launched by one of their blacklisted sites. Two Middle Eastern banks were robbed of USD $45 million by hackers who compromised their gift cards. A phony AP tweet claiming the President had been wounded in a White House attack crashed the stock market. New York City's new 911 system crashed four times in the first two days of operations.

During this time, several other outages worth covering occurred. Some of these are summarized in this article.

International Space Station Incommunicado for Three Hours

NASA communicates with the International Space Station (ISS) from Houston via three geosynchronous communication satellites that transmit voice, data, and video. But on Wednesday morning (EST), February 20, 2013, something went wrong. The ISS suddenly lost all communication with NASA's controllers at its ground stations.

The outage occurred when NASA was making a routine update to the space station's flight computers. In order that normal functions would continue during the upgrade, the computer that controls these operations failed over to its backup computer. For some reason, the backup system could no longer communicate with NASA's Tracking and Data Relay Satellite System.

Communication was restored about three hours later. During the communication outage, station commander Colonel Kevin Ford was able to radio the ground as the space station orbited over ground stations in Russia. He verified that the station and its six astronauts were all safe and that the space station was otherwise performing properly.

Though NASA has not disclosed the reason for the communication outage, it recently launched the new Tracking and Data Relay Satellite K (TDRS-K) this past January. This was the first upgrade to the Tracking and Data Relay Satellite System since 2002.

Heat Spike Takes Down Hotmail and Outlook.com for Sixteen Hours

Microsoft has been a leader in operating data centers at warmer temperatures. This strategy can save significant energy by requiring less use of power-consuming chillers and cooling equipment. The downside of this strategy is that it leaves little room to recover from cooling failures.

Microsoft experienced this a little after noontime on Tuesday, March 12, 2013, in one of its datacenters. Microsoft was updating firmware for a part of its physical plant, a procedure it had done several times in the past. But this time, things went awry. The update failed in an unexpected way and resulted in a rapid and substantial temperature spike in the datacenter. The spike was significant enough to cause several servers in the datacenter to shut down as a safeguard. Microsoft is in the middle of transitioning its Hotmail user base over to its new Outlook.com service. It was the servers that predominantly hosted Hotmail and Outlook.com services that suffered the outages.

The heat spike was so rapid that it prevented any of the datacenter's infrastructure from executing automatic failover to an alternate datacenter to continue services. Based on the nature of the failure, a mix of infrastructure software and human intervention was required to bring the core infrastructure and the downed servers back online. This extended the time needed to recover the lost Hotmail and Outlook.com services.

Services were finally restored early in the morning on March 13, sixteen hours later.

Microsoft has suffered several cloud outages this year. In January, both Hotmail and Outlook.com suffered interruptions. Early in February, its Office 365 online software suite and its Outlook.com email-access cloud went down in North America because of network problems. Then in late February, Windows Azure suffered a worldwide outage on its HPPTS connections when an SSL certificate expired.

UPS Failures Knock DreamHost's Customers Offline for Two Days

DreamHost is a major hosting company with more than 350,000 customers and hosts 1.2 million web sites, blogs and apps.

On Tuesday, March 19, 2013, an uninterruptable power supply (UPS) failed suddenly at its Irvine, California, datacenter operated by Alchemy Communications. When the UPS system died, the emergency backup generators failed to kick in.

The power failure lasted for only a few minutes, but it created a number of major issues with DreamHost's servers and networks that took several hours for the operations team to correct. One serious problem was the loss of several critical pieces of networking hardware that did not survive the power outage.

It was reported that Alchemy may have been conducting unannounced UPS maintenance at the time of the outage. In any event, the UPS system failed again early Wednesday morning. This resulted in another power outage and an intense period of reboots, restores, and system tests. However, this time there were no hardware failures; and systems were brought online much more quickly.

DreamHost decided to run the datacenter on generators until the UPS problems were fully identified and resolved.

DreamHost has been involved in a number of high-profile outages over the years. In 2005 and 2006, it experienced several outages due to power problems. DreamHost is now building a new datacenter on the East Coast as part of an effort to improve its reliability and performance.

North Korea Loses Its Internet for Over a Day

On Wednesday, March 13, 2013, North Korea's Internet went down. North Korea. of course, blamed it on an international attack.

The Star is North Korea's sole Internet service provider. Its websites became inaccessible from outside the country during the outage. Service was restored about 36 hours later the next day.

North Korea does not have much of an Internet capability. Its main connection runs through China, and it has a backup Intelsat satellite connection. The country has just 1,024 IP addresses, making its network more like that of a medium-sized company. It has only a handful of Internet web sites, most of which post propaganda from the state-run media.

Only a few thousand people – mostly high-ranking government officials and scientists, have access to the worldwide Internet. The vast majority of North Koreans have access to a country-wide Intranet that has no access to the outside world.

Seacom Underwater Cables Cut Once Again

Seacom is a privately owned pan-African communication technology company that is driving the development of the African Internet. It financed and developed the first broadband submarine cable system along the eastern and southern African coastline. The cable went live in 2009.

In late March, 2013, multiple undersea cable cuts occurred in Seacom cables off the northern coast of Egypt in the Mediterranean Sea. This impacted a number of cable systems in Africa, the Middle East, and Asia that connect to Europe.

Seacom worked initially to reestablish communications using alternate capacity provided by other Internet providers across the Mediterranean Sea. Many customers had Internet service restored within a day. However, it was not until early April that the Seacom cables were repaired and back in service.

This is not the first time that Seacom has experienced an undersea cable cut. It suffered a similar outage in September of last year when both South African fibre networks were severed.

To improve its service, Seacom has selected Ciena Corporation's 6500 Packet Optical Platform and OneControl Unified Management System to upgrade its submarine network across the southern and eastern African coastlines.

A Rat Causes Massive Fukushima Power Outage

The Japanese Fukushima nuclear power plant was hit by an earthquake and tsunami in March, 2011, causing meltdowns which spewed radiation into the surrounding soil and water. 160,000 residents had to be evacuated from the area.

The big problem was that the nuclear reactor cooling facilities were shut down by the disaster, causing the meltdowns. Tokyo Electric Power Company (TEPCO) has since relied on makeshift equipment to maintain its fresh-water cooling pools to keep the reactor temperatures safe until all nuclear material can be removed, which might take up to forty years.

In late March, 2013, a switchboard short-circuited and disabled four cooling systems. It took technicians 30 hours to repair the system. According to TEPCO, the facility would be safe for at least four days without cooling water.

What caused the short circuit that took out the switchboard and the cooling pools? A ten-inch rodent was found fried and somewhat exploded in the switchboard. TEPCO is taking steps to ensure that animals cannot enter the switchboards in the future.

Hackers Attack WordPress

WordPress currently powers 64 million websites read monthly by 371 million people. In mid-April, 2013, WordPress was attacked by a botnet of tens of thousands of individual computers over the period of a week. The botnet targeted users with the username "admin," the default username, which unfortunately many users never change.

The botnet used over 90,000 IP addresses to avoid being shut down by firewalls and other attack-mitigation devices.

WordPress urged users to change their usernames and passwords and to use the two-step authentication procedure that it had just introduced the prior week. With two-step authentication, a one-time password is sent to a user's mobile phone when he attempts to log in.

One concern is that attacks on major web sites by PC botnets are an attempt to build stronger botnets. PC botnets have limited capacity to launch a Distributed Denial of Service (DDoS) attack. By gaining access to large servers with orders of magnitude more bandwidth, extremely dangerous DDoS botnets can be built.[1]

American Airlines Cancels or Delays 2,000 Flights

American airlines and its sister airline, American Eagle, operate about 3,300 flights a day. During the mid-morning of Tuesday, April 16, 2013, the airlines lost access to their computer systems that do everything from issuing boarding passes to determining how much fuel a plane needs. The result was the cancelation of 970 flights and the delay of 1,086 more flights – two-thirds of their total capacity.

American, which is merging with US Airways to become the world's largest carrier, could only apologize to the tens of thousands of stranded passengers as the airline worked through the problem. Passengers waited in long lines, shouted at the overstressed agents, and exploded their frustrations on social media. Without its computers, American could not even reschedule passengers on other flights.

Eventually, the FAA issued a ground-stop order for American flights around the country. Planes already in the air were allowed to continue, but planes on the ground from coast to coast could not take off.

American blamed the outage on a loss of access to its computer networks used for flight reservations and many other functions. These systems are used to track baggage, to monitor who boards planes, to update flight schedules and gate assignments, to file flight plans, and to arrange seating to properly balance the plane. When these systems are lost, an airline is paralyzed.

Unfortunately, this is not an infrequent occurrence. A possum ate through a cable in Tulsa, Oklahoma, bringing down an entire system. A worker used a metal tool instead of an insulated one, causing a short circuit that crashed a system. United Airlines suffered several similar outages last year as it consolidated its systems after its merger with Continental. In one case, 580 flights were delayed. In another, 636 flights were delayed.

Power Outage Costs Sears $2.2 Million

In June of 2013, Sears Holdings Corp. filed a lawsuit against its power-equipment vendors for two power failures in January that Sears says cost it USD $2.2 million in profits and another USD $2.8 million to fix.

The problems began on January 3, 2013, during the busy season just after the holidays. One of its four uninterruptable power supplies (UPS) failed. This was followed by the failure of the other three UPS systems. This was followed by the failure of its backup power facility, totally shutting down power to its main datacenter and disabling its retail web site.

It took five hours for Sears to start its backup generators and to bring its datacenter back online. According to Sears, this cost it USD $1.58 million in profit. It then had to run the datacenter on backup generators for eight days, costing it another USD $189,000 in diesel fuel.

Unfortunately, one of Sears' power-equipment maintenance vendors reset a circuit breaker for testing purposes after the first failure and did not return it to its proper setting. This caused a second outage on January 24th. Three of the four UPS units failed, shutting down the datacenter until Sears could fire up its

[1] History's Largest DDoS Attack? *Availability Digest*; April 2013.
http://www.availabilitydigest.com/public_articles/0804/spamhaus.pdf

backup generators. During this multi-hour outage, Sears claims that it lost another USD $630,000 in profit. In addition, a generator ultimately failed; and Sears had to rent another one for USD $ 13,500 per week.

Internet Outage Caused by Train Mishap

Service Electric provides cable, Internet, and phone service to much of the Lehigh Valley in Eastern Pennsylvania and Western New Jersey. On June 3, 2013, a tree fell onto a major fiber cable that crosses the Lehigh River, stretching and lowering the cable over a train track. Shortly thereafter, an oncoming train snapped the cable and dropped it into the river.

More than 8,000 customers lost all Internet, cable, and phone service for almost two days as workers repaired the cable.

This follows a major Service Electric outage following Hurricane Sandy last October. Tens of thousands of customers were without cable, Internet, and phone service for over two weeks.

Summary

During these last few months, outages were caused by a wide range of problems. Interestingly, over half of them were environmental. Some were power and cooling problems, but others were unimaginable – a rat shorting out a circuit-breaker panel and a train severing a fiber cable.

These incidents emphasize the need for a thorough, well-documented, and well-practiced business continuity plan that is independent of the causes of outages. You may think that you have all of your bases covered, but you never know what oddballs fate has in store for you.