Verizon communications and sql slammer sapphire

Sociology, Communication

Verizon Communications, an America-wide broadband and telecommunications company, has several case studies. One in particular is the SQL Slammer, an infamous computer worm, which forced Verizon to pay a fine imposing an action to protect their network. In thiscase study, the researcher will elaborate if it is ethical to force companies—Verizon Communications, in particular—to payback large sums ofmoneyfor issues outside their control.

If the SQL Slammer event was not outside their control, the researcher will assess the case study and prepare a risk assessment in which he will make a survey to see recommendations and approval. Verizon Communications Verizon Communications was formerly named RBOC Bell Atlantic Corporation, founded in 1983 by the American Telephone and Telegraph (AT&T) and an element of the Dow Jones Industrial Average. Bell Atlantic Corporation formed a merger with independent telephone company GTE Corporation (General Telephone & Electronics Corporation), which, in 1997, acquired BBN Planet, one of the earliest Internet service providers.

The name BBN Planet was changed into GTE Internetworking; later, however, it detached itself from GTE as an independent named “ Genuity” to become a component of the GTE-Bell Atlantic merger that gave birth to Verizon Communications. The GTE-Bell Atlantic merger, effective on the 30th of June, 2000 as a result of a definitive merger agreement recorded on July 27, 1998, is considered one of the largest mergers in the history of US business, with the initial exchange rate of 1. 22 shares of Verizon Communications Common Stock to GTE Common Stock at $55 per share. Presently, it is considered America’s largest Telecommunications industry.

SQL Slammer Worm This worm, otherwise known as “ Sapphire”, is created definitively for the purpose of creating Internet traffic; thus exhibiting a denial of service (DoS) attack on different servers across the globe. The worm was released on the 25th of January, 2003, infecting thousands of computers in just ten minutes and causing several servers to shut down. Figure 1: Geographic spread of the Slammer/Sapphire worm 30 minutes after it was released into mainstream Internet. The blue dots in the second picture represent the number of affected computers within a specified area.

Retrieved May 9, 2009 from http://www. caida. org/publications/papers/2003/sapphire/sapphire. html The Worm propagated at a deadly pace: doubling rate at 8. 5 seconds at the beginnings of the attack, which focused on computers installed with Microsoft SQL Server Desktop Engine (MSDE), a relational database management system. The pathways of the worm, namely: the router, which controls traffic flow in the internet, are characterized in this paragraph from Spam Laws (2009): “ A router is designed to delay or temporarily halt traffic when it becomes too much to handle.

The Slammer worm caused these routers to crash instead, forcing neighboring routers to remove them from their routing table. This process was spread from router to router, causing the flooding of multiple routing tables, which eventually caused other routers fail. The routers were soon restarted, announcing their status and sparking another wave of updates in various routing tables. Shortly thereafter, large portions of internet bandwidth were consumed as the routers were in constantcommunicationwith one another trying to update their tables.

Because the Slammer worm was small in size, it was able to get through the network, putting the internet as standstill. ” In contrast to other forms of malicious software, the Slammer worm doesn’t contain any payload that could destroy software or hardware, for that matter; it only overloads networks and puts servers out of service. What makes it destructive is its random-scanning spreading strategy, wherein the worm randomly chooses IP addresses through a rather deficient Pseudo-Random Number Generation (PNRG) and attacks weak hosts.

This strategy acts fast on the first minutes of the attack; ironically, the worm’s downfall can also be attributed to its strategy. The spread of the worm soon slowed down because of the internet traffic and the bandwidth could no longer accommodate the generation in IP packet growth. Moreover, since the worm chooses randomly, the IP addresses from where it can choose becomes limited. It exerts more effort infecting addresses that are either already infected or is immune. This is referred to as the Random Constant Spread (RCS) Model (Moore, et al, 2003).

Verizon and Sapphire: The Connection One of the industries that were heavily devastated by the Slammer invasion is Verizon Communications. The corporation’s computer system was in a “ slam,” and the only way to control the spread of the worm is to eventually shut down their interfaces with all Competitive Local Exchange Carriers (CLECs)—AT&T and WorldCom—leaving these CLECs without Internet access from Verizon until in the afternoon of the 26th. The action has lead to Verizon being demanded to pay fines to the third party, which is the Maine Public Utilities Commission.

Verizon justified that their action is for the good of everyone: the worm was beyond their control; but since it has hampered the continuity of businesses with what they did, they are held responsible. Ethical and Moral Issues The primary defense argument of the Verizon Communications, Inc. is that the worm’s destructive capability was “ beyond their control. ” In a petition of waiver made by the Verizon’s attorney Jennifer McClellan (2003), she claims that although worms and viruses are already common, the intensity of Slammer worm’s attack was extraordinary.

The underlying point that the CLECs tried to ignore, still according to McClellan, is that “ while viruses and worm attacks may occur continuously… the Slammer Worm represented a new, much more dangerous breed. ” Moreover, she also states that “ Verizon cannot possibly be expected to know in advance—always and without fail—which of those multitudes of viruses are about to attack and should be given the highest priority,” since these events occur almost simultaneously. The CLECs had apparently tried to see the loopholes in Verizon’s situation.

It was known to them that Verizon is using Microsoft’s SQL Server 2000, which is vulnerable to this kind of malicious software. Mike Nash, Vice-President for the Security Business Unit under Microsoft Corporation, says that they have shipped a security patch for the SQL Server four days before the Slammer worm’s attack (in Lemos, 2003) and that it would have been enough protection against the onslaught of the infamous worm. AT&T was clear in demanding that these patches are easily installed and that there was ample time to have them installed by Verizon.

Ironically, however, is that Microsoft Systems per se is directly affected by the worm despite their claim that their patches are enough. It just goes on to prove that indeed, there are lapses and Microsoft or Verizon Communications, for that matter, is also vulnerable to these kinds of threats. McClellan (2003) stated that penalizing Verizon for this action can be regarded as " patently unreasonable," considering the fact that the patch wasn't even fully installed by its very makers anyway.

In connection, Verizon couldn't have possibly known that the Slammer worm would attack on that specified date for them to realize that it definitely is high-time for them to install the security patches. Despite all of these arguments, however, the petition for waiver by McClellan for her client, Verizon Communications in Maine, was denied. The company paid $62, 000 to CLECs as a rebate. Had the waiver been approved, the rebate would have gone down to only $18, 000 (Keschl, 2003). The Administrative Director of the Maine Public Utilities Commission stated that:

1) Although Internet worms and viruses do not appear frequently, they have been used regularly as an instrument of numerous attacks, an evidence of which is the frequent release and distribution Microsoft have of their security patches. The frequency is related to the need for constant vigilance; 2) They have found out that Verizon has not applied actions to minimize the attack, or any attack for that matter, beforehand; and 3) Verizon failed to take action in a levelheaded and judicious behavior, thus holding Verizon accountable for itsfailurein the SQL Slammer/ Sapphire worm attack.

People's Perspective The reactions of the people of the United States differ in varying degrees. Some say that it is Verizon's fault; others say that it is

Microsoft’s fault; a few says that it was no one’s fault but the author of the worm. Some hold Verizon at fault, seeing as they could have installed the patches with or without the knowledge of the attack. They compared the situation with drinking vitamins to protect children from any possible diseases (emphasis on possible); the kid doesn’t have to get sick before his parents would have to give him meds against it.

For those who look at Microsoft as the bad guy, they ask why Microsoft can’t protect itself when all the resources are made readily available to their access. If they could not protect their selves, how could they protect those they are serving? On another side ofthe fence, a few have said that there is no one to blame but the author of the worm. There are lapses in every company, every business ever established, and Microsoft and Verizon are just two of those companies. They assert that their can never be anyone who is already prepared for a disaster that cannot be foreseen.

First Person Point of View I actually consider the event to be solely the fault of the worm’s author. If it were not for him, then there wouldn’t have been a disaster of an event as this. Ironically though, is that we can appreciate what he has done because it brought out the flaws and lapses that the people don’t hink to be very evident in high-rise companies such as Microsoft and Verizon.

References:

Keschl, D. L. (30 April 2003). [director]. Request Denied for Verizon Maine’s Request for a Waiver of Certain Service Quality Results under the PAP for January 2003.

Retrieved May 9, 2009 from http://www. steptoe. com/assets/attachments/1670. pdf Lemos, R. (4 March 2003). Newsmaker: Decoding the Lessons of Slammer. CNet News. Retrieved May 10, 2009 from http://news. cnet. com/Decoding-the-lessons-of-Slammer/2008-1082_3-990757. html McClellan, J. (2003). [attorney]. Reply Comments of Verizon Virginia, Inc. on its Petition for a Waiver of Cretain Service Quality Results Measured under the Performance Assurance Plan for January 2003. Retrieved May 10, 2009 from http://www. scc. virginia.

gov/puc/comp/ccimom/ccimomfiles/vrespslam. pdf Moore, D. , Paxson, V. , Savage, S. , Shannon, C. , Staniford, S. , and Weaver, N. (2003). The Spread of the Sapphire/Slammer Worm. Caida: The Cooperative Association for Internet Data Analysis. CAIDA; ICSI; Silicon Defense; UC Berkeley EECS; and UC San Diego CSE. Retrieved May 9, 2009 from http://www. caida. org/publications/papers/2003/sapphire/sapphire. html Spam Laws (2009). The Slammer Worm. Retrieved May 10, 2009 from http://www. spamlaws. com/slammer-worm. html