**WHEN ANTIVIRUS SOFTWARE CRIPPLES YOUR COMPUTERS**

McAfee is a prominent antivirus software and computer security company based in Santa Clara, California. Its popular VirusScan product (now named AntiVirus Plus) is used by companies and

individual consumers across the world, driving its revenues of $1.93 billion in 2009. A truly global company, McAfee has over 6,000 employees across North America, Europe, and Asia. VirusScan and other McAfee security products address endpoint security, network security, and risk and compliance. The company has worked to compile a long track record of good customer service and strong quality assurance.

At 6 a.m. PUT April 21, 2010, McAfee made a blunder that threatened to destroy that track record and prompted the possible departure of hundreds of valued customers. McAfee released what should have been a routine update for its flagship VirusScan product that was intended to deal with a powerful new virus known as 'W32/wecorl.a". Instead, McAfee's update caused potentially hundreds of

thousands of McAfee-equipped machines running Windows XP to crash and fail to reboot. How could

McAfee, a company whose focus is saving and preserving computers, commit a gaffe that accomplished the opposite for a significant portion of its client base?

That was the question McAfee's angry clients were asking on the morning of April 21, when their

computers were crippled or totally non-functional. The updates mistakenly targeted a critical Windows

file, svchost.exe, which hosts other services used by various programs on PCs. Usually, more than one

instance of the process is running at any given time, and eliminating them all would cripple any

system. Though many viruses, including W32/wecorl.a, disguise themselves using the name svchost.exe to avoid detection, McAfee had never had problems with viruses using that technique before.

To make matters worse, without svchost.exe, Windows computers can't boot properly. VirusScan users applied the update, tried rebooting their systems, and were powerless to act as their systems

went haywire, repeatedly rebooting, losing their network capabilities and, worst of all, their ability to

detect USB drives, which is the only way of fixing affected computers. Companies using McAfee and

that relied heavily on Windows XP computers struggled to cope with the majority of their machines

suddenly failing. Angry network administrators turned to McAfee for answers, and the company was initially just as confused as its clients regarding how such a monumental slipup could occur. Soon, McAfee determined that the majority of affected machines were using Windows XP Service Pack 3 combined with McAfee VirusScan version 8.7. They also noted that the "Scan Processes on enable" option of VirusScan, off by default in most VirusScan installations, was turned on in the majority of affected computers.

McAfee conducted a more thorough investigation into its mistake and published a FAQ sheet that

explained more completely why they had made such a big mistake and which customers were affected. The two most prominent points of failure were as follows: first, users should have received a warning that svchost.exe was going to be quarantined or deleted, instead of automatically disposing of the file. Next, McAfee's automated quality assurance testing failed to detect such a critical error because of what the company called "inadequate coverage of product and operating systems in the

test systems used."

The only way tech support staffs working in organizations could fix the problem was to go from computer to computer manually. McAfee released a utility called "SuperDAT Remediation Tool," which had to be downloaded to an unaffected machine, placed on a flash drive, and run in Windows Safe Mode on affected machines. Because affected computers lacked network access, this had to be done one computer at a time until all affected machines were repaired. The total number of machines impacted is

not known but it doubtless involved tens of thousands of corporate computers. Needless to say,

network administrators and corporate tech support divisions were incensed.

Regarding the flaws in McAfee's quality assurance processes, the company explained in the FAQ that they had not included Windows XP Service Pack 3 with VirusScan version 8.7 in the test configuration of operating systems and McAfee product versions. This explanation flabbergasted many of McAfee's clients and other industry analysts, since XP SP3 is the most widely used desktop PC configuration. Vista and Windows 7 generally ship with new computers and are rarely installed on functioning XP computers.

Another reason that the problem spread so quickly without detection was the increasing demand for faster antivirus updates. Most companies aggressively deploy their updates to ensure that machines spend as little time exposed to new viruses as possible. McAfee's update reached a large number of machines so quickly without detection because most companies trust their antivirus provider to get it right. Unfortunately for McAfee, it only takes a single slipup or oversight to cause significant damage to

an antivirus company's reputation. McAfee was criticized for its slow response to the crisis and for

its initial attempts to downplay the issue's impact on its customers. The company released a