the Availability Digest

www.availabilitydigest.com

Anti-Virus – A Single Point of Failure?

May 2010

What do active/active systems, clusters, fault-tolerant systems, and standby systems have in common? They all avoid a single point of failure. True, fault-tolerant systems and clusters will not survive a site failure; and standby systems have been known not to come up when needed. But active/active systems are immune, right?

On April 21st, McAfee, one of the leading antivirus vendors, proved this conjecture to be wrong. It sent out an antivirus update that immediately took down hundreds of thousands – maybe millions – of computers worldwide. This one bad update could have stopped every node in an active/active system, and our "indestructible system" would have been destroyed – a single point of failure.

Worse still, the bad update required manual intervention on every individual computer to restore it to service, taking those data centers with thousands of Windows servers offline for hours and, in some cases, for days.

What Went Wrong?

svchost.exe

On every PC is a very critical executable – svchost.exe. svchost.exe is a generic process that runs dynamic link libraries (DLLs) assigned to it.

Some time ago, Microsoft moved functionality for Windows services out of dedicated executables to DLLs to improve reusability. But a DLL cannot be directly executed. It must be linked to a process that will execute it. Hence, svchost.exe. DLLs are packaged into groups associated with a certain service, such as network management, the firewall, and the user interface. Each group is assigned to an instance of svchost.exe responsible for executing those DLLs. Look on your Windows computer, and you will see many instances of svchost.exe running.

Clearly, svchost.exe is fundamental to the operation of a PC system. A Windows system cannot even boot up if svchost.exe is absent.

The Botched Update

Antivirus vendors, such as McAfee, Symantic (Norton), and AVG, are under increasing pressure due to the rate of creation of new virus attacks. It is reported that Symantic issues its Pulse updates every five to fifteen minutes to try to beat a virus to systems in the field. To avoid infection, time is so critical that updates are propagated automatically and usually take effect in a system without user action or knowledge.

© 2010 Sombers Associates, Inc., and W. H. Highleyman

But any update must be thoroughly tested to ensure that it is proper and will do no damage itself. In Microsoft systems, there are a multitude of versions of Windows that must be tested before an update can be released. However, the longer that testing takes place, the more likely it is that systems will be infected. Thus, there is a real trade-off between testing and effectiveness of an upgrade. McAfee has 7,000 employees, most working under this stress.

On April 21st, the McAfee team was racing to propagate an update to its users to defeat a variant of the W32/Wecorl virus. This virus attempts to attach itself to the svchost.exe file to gain control of a system whenever the svchost.exe file is executed as a process. It is one of many viruses that attack the svchost.exe file. McAfee propagates its updates as DAT files. DAT file 5958 contained the fix and was sent to all McAfee customers on April 21st. On most systems, the update was installed automatically and immediately.

The problem was that this update erroneously identified every running instance of the svchost.exe process as being infected. It therefore either quarantined the svchost.exe file or deleted it from disk. It then automatically rebooted the computer to effectuate the update.

The Consequences

The consequences were disastrous. Without svchost.exe, PCs could not boot up. They went into a continuous reboot cycle.

If a user acted fast enough, he could trap the reboot and bring the PC up in safe mode. But then what? He could discover that he had no access to the network and that even his USB port was probably not working. The PC was effectively isolated from the rest of the world.

McAfee quickly came up with a fix that it distributed in an emergency DAT – the EXTRA.DAT update. All users had to do was to download EXTRA.DAT and send it over their networks to fix the compromised PCs. The only problem was that there was no network access. Even if an unaffected computer could download EXTRA.DAT, it could not distribute it over a company's internal network to the failed computers.

To compound the matter even further, McAfee's support web site went down under extraordinary load; and many couldn't even get to the update fix. McAfee sent out a notice that said, "The McAfee Community is experiencing unusually large traffic which may cause slow page loads."

McAfee then published (again on their overloaded support site) other fix suggestions. All a user had to do was to unquarantine the quarantined svc.host file to return it to service (this could be done in safe mode). If the file had instead been deleted, the user could copy it from a good system to the failed system. The problem with the deleted-file method was that it required copying the file from a good system onto a USB flash drive and then loading the file from the flash drive onto the bad system. But the USB port on the bad system was likely not to be operational, so the copy could not be performed.

Early the next day, McAfee made available a semi-automated repair tool dubbed SuperDAT Remediation Tool. It was available from the network, but it was of no use to customers who had no network access.

Other workarounds were soon published by McAfee and by a number of other sites and bloggers. However, each one required individual hands-on work with each affected PC. In some data centers, this involved thousands of PCs and hours or days of work by onsite technicians.

© 2010 Sombers Associates, Inc., and W. H. Highleyman

The Scope of the Disaster

As it turned out, the bad update affected only Windows XP Service Pack 3. In an apology, McAfee said that only one-half of one percent of all corporate users were affected; and almost no consumers were affected. However, the blogs and comments on McAfee's web site told a different story. A Gartner Group analyst stated that Windows XP SP3 has over 50% of the corporate market. One comment on the McAfee web site said:

> "How the hell am I supposed to sign up for Support Notification Service if I can't even access my Internet? This is HORRIBLE. Where do I sign up for the HUGE class action lawsuit? I was on the phone over 3 hours yesterday with this issue. The first time I called, you wanted to charge me $89.50 to fix your problem! Also, I had two different techies say they would call me back. Guess what? They never did!"

McAfee's apology also stated that "the problem could result in moderate to significant performance issues." Continual rebooting is a moderate to significant performance issue?

From a crisis management and public relations viewpoint, McAfee's response was disastrous. McAfee downplayed the seriousness of the problem in their "apology." As of April 23rd, two days later, there was still no statement, apology, or clearly labeled link to support resources related to this issue on McAfee's home page.

Other stories in the press showed the breadth of the outages:

- Kentucky state police had to shut down their computer systems, including terminals in police cars.
- The computer glitch affected school districts across Kentucky.
- Rhode Island's Lifespan hospitals diverted all non-emergency care to other facilities after its computers were disabled.
- Court operations in many parts of Chile were shut down.
- The entire IT infrastructure of the University of New Hampshire was affected.

How Did This Happen?

McAfee has yet to explain in any detail how this update got released to its customers. However, Ed Bott of ZDNet claims to have been given a confidential copy of a McAfee release that was never published. In this release, the author said:

> "Some specific steps of the existing Quality Assurance processes were not followed. Standard peer review of the driver was not done. … There was inadequate coverage … in the test systems used. Specifically, XP SP3 … was not included in the test configuration …"

In its haste to get the update out, McAfee purportedly bypassed testing it on Windows XP SP3 – a fatal decision. The cure was worse than the disease.

As for the future, McAfee would only say that it is implementing additional QA procedures.

© 2010 Sombers Associates, Inc., and W. H. Highleyman

Lessons Learned

This was a nightmare scenario - an automatic update that wiped out a crucial system file on hundreds of thousands of computers and which could only be repaired manually. However, this is not the first time that this has happened:

- In the previous month, a BitDefender update took down 64-bit Windows systems.

- In May of 2007, a Symantic definition file crippled thousands of Chinese computers when it mistook two critical Windows DLL files as malware.

This is bound to happen again. What should we do to protect ourselves from the problem? One blogger put it succinctly:

> "All this negativity. Even if this slipped past McAfee, shouldn't everybody be testing their DAT files in their own lab environment? I test every one of mine in a VM lab environment to make sure nothing bad can come out of issuing a new DAT globally."

For critical enterprise systems, don't rush to automatically apply updates of any kind (antivirus, operating system, utilities, application fixes). Test them first in a safe environment, roll them out slowly one system at a time, or wait to see if problems are reported by others. For those with individual PCs, do the latter – wait a day or so to see if problems are reported.

By doing so, you may be opening yourself up to a higher probability of infection. But with proper firewalls, opening only trusted emails, and visiting only proper web sites, this probability is pretty small. Besides, an infection is probably more easily corrected than is a computer that is totally wiped out.

Acknowledgements

Material for this article was taken from the following sources:

McAfee KnowledgeBase KB68780; April 21, 2010.
McAfee Corporate KnowledgeBase; April 23, 2010.
A long day at McAfee, Barry McPherson, *siblog.mcafee.com/support/;* April 21, 2010.
McAfee Update Glitch Takes down Windows XP Computers, *PC Magazine*; April 21, 2010.
Flawed McAfee update paralyzes corporate PCs, *Computerworld*; April 21, 2010.
McAfee flub sets off Twitter backlash storm, *Business Week*; April 21, 2010.
McAfee update derails Kentucky police and a lot of XP machines, *ZDNet*; April 21, 2010.
Computer Glitch wreaks havoc statewide, *wkyt*; April 21, 2010.
McAfee shoots itself in the enterprise foot, *Download Squad*; April 21, 2010.
Faulty McAfee update fells hospital computers, *newsblog.projo.com*; April 21, 2010.
Chilean courts say computer virus shutting down many operations, *blog.taragana*; April 21, 2010.
McAfee admits "inadequate" quality control caused PC meltdown, *Ed Bott - ZDNet Blog*; April 22, 2010.
McAfee AV Update Issue Should Make Businesses Consider Controlled Approach, *eWeek*; April 22, 2010.
The McAfee update mess explained, *Computerworld*; April 22, 2010.
McAfee apologizes for crippling PCs with bad update, *Computerworld*; April 23, 2010.
Lessons of the McAfee False Positive Fiasco, *PC Magazine*; April 23, 2010.
What is svchost.exe and Why Is It Running?, *How-To Geek.*

© 2010 Sombers Associates, Inc., and W. H. Highleyman