Security software company Webroot came under fire recently when its antivirus program mistakenly flagged and removed legitimate files in Microsoft Windows, as well as Windows applications. How did these false positives occur, and what did Webroot do to resolve the issue?

Webroot Inc.'s issue happened on Apr. 24 between 1800 and 2100 Coordinated Universal Time, and it tagged particular Windows OS system files as part of the W32.Trojan.Gen. Once these files were tagged as malicious, they went into quarantine, and the systems were left inoperative.

An antivirus signature update was pushed down from the Webroot cloud service, updating the agents with the false positive and triggering a chain reaction for all the systems receiving the update to cause the Windows systems to quarantine the files. It was reported that the antivirus signature update was only active for 13 minutes, but that many managed service providers were utilizing the service and pushing updates to their clients that it propagated the issue to additional endpoints.

Shortly after the issue, Webroot started working on ways to remediate the problem, and social media started lighting up with comments and potential workarounds in an attempt to get the files back -- including removing Webroot, restoring the needed files from backup and rebooting.

The Webroot team released an application, which can be found on its forum, to remediate the false positives. This issue affected both the home and business users; Webroot asked users not to delete the quarantined files -- especially if the user didn't have a backup of the data -- in order to have things restored.

During this time, there were multiple calls into Webroot's support line, and many users took to Twitter to try to find a solution. It was also noted that the software was miscategorizing Facebook and Bloomberg, both nonmalicious websites, as potential phishing sites.

Webroot isn't the first endpoint security company to create issues by pushing down updates that create havoc for customers. This particular issue caused a lot of pain for customers because it removed files that were part of the actual operating system, not a random executable or instance of software, as is normally the case for other vendors causing false positives. It's hard to determine where the breakdown actually occurred; proper quality assurance of software updates before they were deployed should have picked this up before it was sent out to customers.

Also, as the industry evolves, it relies less and less on antivirus signature updates as it does on machine learning and behavior analytics. This can reduce the deployment of new antivirus signatures and updates that cause false positives when deployed and relies on an understanding of the file itself, big data and behavior. This is an area that Webroot is currently playing in, and the issue itself seems to have involved a heuristics rule that triggered on particular Microsoft Windows files.

Even with all the damage done, Webroot took full responsibility for the issue, set up a communications portal for updates and actively worked to resolve the issue as quickly as possible. It was a pain to deal with from the customer side, and one that Webroot has to manage going forward, but it seems that its remediation efforts to fix the false positive were smooth after it determined how to remediate the issue.