An Update on False Positive Remediation Thursday, April 22nd, 2010 at 11:04 pm by Barry McPherson

As you know, McAfee on Wednesday released a faulty signature update file (DAT file) that caused problems for a number of our customers.

First off, I want to apologize on behalf of McAfee and say that we're extremely sorry for any impact the faulty signature update file may have caused you and your organizations.

I want to give you a brief update on what has happened since we first became aware of the false detection. McAfee team members have been working around the clock to fix the problem and work with impacted customers. We estimate that the majority of the affected systems are back up and running at this time and more systems are coming back online quickly.

Early Thursday morning (at around 1 AM PT) we published a SuperDAT Remediation Tool to help customers fix affected systems. The tool suppresses the driver causing the false positive by applying an Extra.dat file in folder. It then restores the "svchost.exe" Windows file, the file quarantined as a result of the false detection.

The tool has been successful at remediating the problem caused by the faulty DAT update for multiple customers. The tool itself and more details on how it works are available in our knowledge base. Additionally, we have support team members onsite and on the phone to assist impacted customers.

Of course many of you are asking how the faulty DAT made it past our quality assurance checks. The problem arose during the testing process for this DAT file. We recently made a change to our QA environment that resulted in a faulty DAT making its way out of our test environment and onto customer systems.

To prevent this from happening again, we are implementing additional QA protocols for any releases that directly impact critical system files. In addition, we plan to add capabilities to our cloud-based Artemis system that will provide an additional level of protection against false positives by leveraging an expansive whitelist of critical system files. (More details are available in an FAQ that was published Thursday night.)

Again, on behalf of McAfee, I'm very sorry for how you may have been impacted by the faulty DAT file update and thank you for your continued support and cooperation as we work to remediate the situation.

Barry

Tags: mcafee, Support

- Posted in Support

Feeds & Podcasts
Meet the Bloggers
Archive
Categories

Blogroll

- CNET Security News
- eWeek Security Watch
- Krebs On Security
- StorefrontBacktalk
- UnsafeBits
- Zero Day – ZDNet.com

April 2010

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

« Mar

-  Security Insights Newsletter
-  Security Insights on the Web

- About this blog
- View all posts by Barry McPherson
- View all posts in Support

4 Comments to “An Update on False Positive Remediation”

-  Charles H April 22nd, 2010 at 11:30 pm

- Barry,
  First of all let me say I am glad we have switched nearly 75% of our clients away from your product prior to this happening. I can’t imagine the chaos if we hadn’t. It was chaos enough for us running all over town and billing our client’s for a software glitch on a program that we recommended to them… Many of them have told us to bill McAfee but we know that bill won’t get paid… Thanks for the boost in revenue, but next time give us a little warning so I can clear my Engineers schedules.

-  Tantyo April 22nd, 2010 at 11:34 pm

- I am glad that in my company with over than 3000 computer installed with Mcafee TOPS which spread out Indonesia’s five major island not affected by faulty Dat 5958.

I think we safe due to time different and time of our EPO pull repository.

Please make sure this faulty will not happened again in anyway.

Thank you.

- Vinod April 22nd, 2010 at 11:39 pm
- The turn around time for getting this arrested is commendable not to mention the accountability exhibited by your team barry
- Jerry Van Der Werff April 23rd, 2010 at 12:34 am
- Since so many are likely sending in comments, you probably won't read my input past the first sentence or two (if at all). But this was such a big impact, I believe it merits attention. A great deal of your feeback this point I don't feel comfortable about downloading anything from McAfee, so when I get the next popup about installing updates, I don't think I will. In which case what good is it to me as a consumer to even buy/renew my subscription.
  Hey I'm not a novice, I work in technologies so I know it's extremely difficult to catch every problem before it hits production but for heaven's sake your company's whole reputation is based on 'trust'. If you expect customers to buy your produtct you damn well better make sure what you release is as solid as a rock. You shouldn't be on the list of risky software downloads! ! ! !

Submit your comment

Name (required)

Mail (will not be published) (required)

Website

XHTML: You can use these tags: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

You must read and type the **5 chars** within **0..9** and **A..F**, and submit the form.

submit

Oh no, I cannot read this. Please, generate a new ID

The postings on this blog are the opinions of the individual posters and don't necessarily represent McAfee's position or opinion on this subject.