Question

Applies to Virus and Malware | Microsoft Security Essentials | Scanning, Detecting, and Removing Threats
1704 views

Microsoft Antimalware has removed history of malware and other potentially unwanted software 1013

TO TommyKerans asked on October 2, 2011

I'm using Security Essetials as my resident AV. I am also running WinPatro Pro resident.
1. Why did "Microsoft Antimalware remove history of malware and other potentially unwanted software" and why is there no record of it in Security Essentials? (This is a message in the Event Viewer under System.)

2. Why does it have two different times listed? Please see the entire Event Property Description below:

Event Type: Information
Event Source: Microsoft Antimalware
Event Category: None
Event ID: **1013**
Date: **10/2/2011**
Time: 1:22:37 PM
User: N/A
Computer: TOSHIBA-USER
Description:
Microsoft Antimalware has removed history of malware and other potentially unwanted software.
 Time: **9/2/2011** 1:22:36 PM
 User: NT AUTHORITY\SYSTEM

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

3. Is Microsoft Antimalware part of Security Essentials?

3 people had this question

Me Too Reply Subscribe

✓ Answer

Kosh Vorlon replied on October 2, 2011
Insider ★, , , , Wiki Contributor

Still have questions?

Ask the community

Related Content

Show more content like this

Hi Tommy,

1. If you open MSE and go to the History tab and check detected items, you'll see the history of what [illegible] system for only 30 days and then it is automatically deleted). There's no way to save the information longer or extend the retention period or download it to keep a record. It's there for 30 days and then it's gone (though Event Viewer and some logs may provide some level of information for a longer period). You can check event viewer for every event that showed up in history for as far back as you have Event Viewer configured to retain information. For the other logs (which are drastically harder to read and interpret), see: http://social.answers.microsoft.com/Forums/en-US/msescan/thread/b9feaa4d-7300-4a76-97cb-fda4393ac50f and http://social.answers.microsoft.com/Forums/en-US/msescan/thread/e7ed7b1a-9015-4851-b550-3c013f8d1d44.

2. The first time represents when MSE cleared the history from 30 days ago. The second time represents the time of the information that was removed automatically. This is perfectly normal and no reason to be concerned about. It will occur from time-to-time as the history file is automatically maintained current. It may not occur every day if there isn't anything to clear from 30 days prior in the history report.

3. Yes, Microsoft Antimalware is a significant and major part of Microsoft Security Essentials. If you check Services, you'll notice that there's no service for MSE but there is one for Microsoft Antimalware and that's what makes MSE work. If you check C:\Program Data\ Microsoft, you'll find folders for Microsoft Antimalware, Microsoft Security Client, and Microsoft Security Essentials. All are part of MSE and work together to make it operate properly. If you open Task Manager (for all users if applicable), you'll find a process called MsMpENG.exe with a description of "Antimalware Service Executable." This is the process that manages your real-time scanning protection and also does most of the work during scans. You'll also find a process called msseces.exe with a description of "Microsoft Security Client User Interface". My point is that there are many different parts of MSE that are called different things that work together to make MSE function. Unfortunately, it's hard to find detailed reference materials on such things as I'm not aware of anything formally published to this level of detail though some of the threads in this forum do sometimes go that far.

I hope that helps. And BTW, I too use WinPatrol (but found the free version perfectly adequate) and if you were wondering, it has absolutely nothing to do with any of this. It does advise you of programs and services related to MSE that are checked to begin at startup (but without realizing all these different names are all linked together, that might have been more difficult to see than it will be now that you know). If you like WinPatrol for how it helps manage startup programs, you may find the free Secunia PSI http://secunia.com/vulnerability_scanning/personal/ also interesting in terms of keeping all the various programs on your system updated either automatically or by notification when they are no longer the most current version. I find it saves me a lot of time and helps keep me from missing some I rarely use and keeping them updated is extremely important to your security as unpatched programs leave vulnerabilities on your defenses that can be exploited despite using excellent AV products and keeping Windows Updates current. Anyway, I thought I'd throw that in because I remember installed WinPatrol and Secunia PSI on the same day when I first discovered them.

Good luck!

> MVP(7/2012-6/2015),MCSE,MCSA,MCC2011,x-CMM,x-CAM,MCP+Int,x-Yammer Admin,Influencer. More in Profile.

3 people found this helpful

Helpful Reply

All replies (7)

TO TommyKerans replied on October 3, 2011

In reply to Kosh Vorlon's post on October 2, 2011

Thanks! That's just what I needed to know.

Helpful Reply

Kosh Vorlon replied on October 3, 2011

Insider , , , , Wiki Contributor

In reply to TommyKerans's post on October 3, 2011

Hi Tommy,

You're quite welcome. It was my pleasure - glad it helped.

We're here anytime you have any further questions or problems. I'd rather hear an easy question before you do something than face a hard problem after you've done something rather than asking first.

Good luck and best wishes!

P.S. While WinPatrol is great for managing startup-programs, for me it's a tad short on details (far better than MSCONFIG, but still not all I'd like to know - perhaps the Pro version offers more). I use Autoruns http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx (which doesn't offer real-time surveillance and is not as easy to use) for far more detailed information about just about everything concerning boot and startup. When I'm working to truly pare things down and get them nice and trim (not often, but once in a blue moon or if I'm having a problem) that's what gives me the extra details I need to know and also keeps me from having to look elsewhere or tells me where to look for some of the information if I can't figure out what something means. Just another FYI.

> MVP(7/2012-6/2015),MCSE,MCSA,MCC2011,x-CMM,x-CAM,MCP+Int,x-Yammer Admin,Influencer. More in Profile.

1 person found this helpful

Helpful Reply

MI MichelleGrand replied on November 2, 2011

In reply to Kosh Vorlon's post on October 2, 2011

Hi Tommy,

1. If you open MSE and go to the History tab and check detected items, you'll see the history of what has happened in the last 30 days (because that record is retained in the system for only 30 days and then it is automatically deleted). There's no way to save the information longer or extend the retention period or download it to keep a record. It's there for 30 days and then it's gone (though Event Viewer and some logs may provide some level of information for a longer period). You can check event viewer for every event that showed up in history for as far back as you have Event Viewer configured to retain information. For the other logs (which are drastically harder to read and interpret), see: http://social.answers.microsoft.com/Forums/en-US/msescan/thread/b9feaa4d-7300-4a76-97cb-fda4393ac50f and http://social.answers.microsoft.com/Forums/en-US/msescan/thread/e7ed7b1a-9015-4851-b550-3c013f8d1d44.

2. The first time represents when MSE cleared the history from 30 days ago. The second time represents the time of the information that was removed automatically. This is perfectly normal and no reason to be concerned about. It will occur from

time-to-time as the history file is automatically maintained current. It may not occur every day if there isn't anything to clear from 30 days prior in the history report.

there is one for Microsoft Antimalware and that's what makes MSE work. If you check C:\Program Data\ Microsoft, you'll find folders for Microsoft Antimalware, Microsoft Security Client, and Microsoft Security Essentials. All are part of MSE and work together to make it operate properly. If you open Task Manager (for all users if applicable), you'll find a process called MsMpENG.exe with a description of "Antimalware Service Executable." This is the process that manages your real-time scanning protection and also does most of the work during scans. You'll also find a process called msseces.exe with a description of "Microsoft Security Client User Interface". My point is that there are many different parts of MSE that are called different things that work together to make MSE function. Unfortunately, it's hard to find detailed reference materials on such things as I'm not aware of anything formally published to this level of detail though some of the threads in this forum do sometimes go that far.

I hope that helps. And BTW, I too use WinPatrol (but found the free version perfectly adequate) and if you were wondering, it has absolutely nothing to do with any of this. It does advise you of programs and services related to MSE that are checked to begin at startup (but without realizing all these different names are all linked together, that might have been more difficult to see than it will be now that you know). If you like WinPatrol for how it helps manage startup programs, you may find the free Secunia PSI http://secunia.com/vulnerability_scanning/personal/ also interesting in terms of keeping all the various programs on your system updated either automatically or by notification when they are no longer the most current version. I find it saves me a lot of time and helps keep me from missing some I rarely use and keeping them updated is extremely important to your security as unpatched programs leave vulnerabilities on your defenses that can be exploited despite using excellent AV products and keeping Windows Updates current. Anyway, I thought I'd throw that in because I remember installed WinPatrol and Secunia PSI on the same day when I first discovered them.

Good luck!

Hello. GREAT explanation. I saw this message "Microsoft Antimalware has removed history of malware and other potentially unwanted software 1013" as well.

My question is ---> Is "history" different from "Remove quarantined files after.....:"? Under "Settings" ---> "Advanced", I have that tick box unchecked. So I have it as "Quarantined files remain disabled until you allow them or remove them". I was thinking if that was not checked, the history will stay there for a long as I want. Or are they 2 different things?

Thank you,
Michelle

Be the first person to mark this helpful

Helpful Reply

Kosh Vorlon replied on November 2, 2011
Insider ★, , , , Wiki Contributor

In reply to MichelleGrand's post on November 2, 2011

Hi Michelle,

History includes three parts: detected history, quarantined items, and allowed items.

First, having "Remove quarantine files after" unchecked simply means it uses the default of removing them after 30 days. If you check the box, then you can choose other options but the longest is 3 months. You cannot choose to leave them indefinitely or until you decide what to do. Some removal timeframe limit must apply. Checking the box gives you some options - unchecking the box makes it occur in 30 days.

As far as detected history goes, it is set and locked at 30 days and cannot be changed in any way. It's 30 days and that's that. After 30 days it is removed. But keep in mind detected history is simply a list - you cant do anything with anything there except clear the list (which doesn't affect any of the files on the list in the slightest). Think of it as "read only."

A

potentially be removed as might occur if a timeframe was set and MSE then responded to what it once again saw as a threat when you still wanted to allow it. So all three categories operate a bit differently.

I hope this helps.

Good luck!

> MVP(7/2012-6/2015),MCSE,MCSA,MCC2011,x-CMM,x-CAM,MCP+Int,x-Yammer Admin,Influencer. More in Profile.

1 person found this helpful

Helpful Reply

MI MichelleGrand replied on November 2, 2011

In reply to Kosh Vorlon's post on November 2, 2011

> Hi Michelle,
>
> History includes three parts: detected history, quarantined items, and allowed items.
>
> First, having "Remove quarantine files after" unchecked simply means it uses the default of removing them after 30 days. If you check the box, then you can choose other options but the longest is 3 months. You cannot choose to leave them indefinitely or until you decide what to do. Some removal timeframe limit must apply. Checking the box gives you some options - unchecking the box makes it occur in 30 days.
>
> As far as detected history goes, it is set and locked at 30 days and cannot be changed in any way. It's 30 days and that's that. After 30 days it is removed. But keep in mind detected history is simply a list - you cant do anything with anything there except clear the list (which doesn't affect any of the files on the list in the slightest). Think of it as "read only."
>
> Allowed items will remain indefinitely because MSE doesn't want to cause those items to potentially be removed as might occur if a timeframe was set and MSE then responded to what it once again saw as a threat when you still wanted to allow it. So all three categories operate a bit differently.
>
> I hope this helps.
>
> Good luck!

Kosh,

That explanation helps a lot. Thank you. So seeing that in the event viewer is nothing to be concerned about. I was just curious since I do not have the box checked. I just thought it would just stay in the "history" until I delete it manually. I wasn't aware there was a "default" setting of 30 days.

Michelle

Be the first person to mark this helpful

Helpful Reply

TA taylorjw2 replied on April 4, 2015

I found these remarks when I searched msmpeng.exe. I am running Win8.1. Why; is this
program identified in a couple of places asa "Windows-defender-service"? Why do you
h differen
identified as published by MS?

Be the first person to mark this helpful

Helpful Reply