

Forum:[Hack Forums](#)

Thread: [question about virustotal](#)

SIM-5515815 - April 19, 2024, 3:33 pm

I have a question about VirusTotal, the online antivirus scan.

I ran across this lastnight, correct me if I'm wrong.

When I was doing some studying about hacking, I discovered the fact that antivirus software depends on signatures to be realized and recognized, and the fact that a hacker can make a RAT that no antivirus software will be able to recognize because the signature has not been recognized, therefore unidentified.

So last night at about 3:00 in the morning, I downloaded the latest greatest version of Windows VirtualBox.

VirtualBox-7.0.16-r162802-Win.exe
2fb44977d3329e55e8b61408ab4af5239ecd3d80c5990fb5cd6bd0c91a854d62

It raises no red flags. But it states 'last modification date: 14 minutes ago.'

Now I'm assuming that it's the software that has been modified and has nothing to do with a modification by VirusTotal.

Which to me raises a red flag. So I do this with several other downloads, all software that is hacking related.

And every one of them has been very recently modified, with less than half an hour ago. And this is at 3:00 a.m.?

So my question is, what is going on?

If I knew what I was doing, and I don't, this is the first time that I even started looking into the hacking industry as a potential way of earning money. So I'm fresher than the sweetest, youngest, noobiest cherry. But if I was involved in nefarious activity, I would have my software being consistently modified via AI, therefore always passing all known antivirus signatures, therefore never being caught, and planting my RAT across machines all across the world?

Unless that's not possible. Again, I have no idea what I'm doing or talking about. However, I do have enough common sense to refrain from moving forward and actually installing these products without first asking why they are consistently being modified every 20 minutes or so.

DramaKing - April 19, 2024, 5:16 pm

(Apr 19, 2024 03:33 PM)GeorgeCarlinRules Wrote: [\[CITE\]](#) I have a question about VirusTotal, the online antivirus scan.

I ran across this lastnight, correct me if I'm wrong.

When I was doing some studying about hacking, I discovered the fact that antivirus software

depends on signatures to be realized and recognized, and the fact that a hacker can make a RAT that no antivirus software will be able to recognize because the signature has not been recognized, therefore unidentified.

So last night at about 3:00 in the morning, I downloaded the latest greatest version of Windows VirtualBox.

VirtualBox-7.0.16-r162802-Win.exe
2fb44977d3329e55e8b61408ab4af5239ecd3d80c5990fb5cd6bd0c91a854d62

It raises no red flags. But it states 'last modification date: 14 minutes ago.'

Now I'm assuming that it's the software that has been modified and has nothing to do with a modification by VirusTotal.

Which to me raises a red flag. So I do this with several other downloads, all software that is hacking related.

And every one of them has been very recently modified, with less than half an hour ago. And this is at 3:00 a.m.?

So my question is, what is going on?

If I knew what I was doing, and I don't, this is the first time that I even started looking into the hacking industry as a potential way of earning money. So I'm fresher than the sweetest, youngest, noobiest cherry. But if I was involved in nefarious activity, I would have my software being consistently modified via AI, therefore always passing all known antivirus signatures, therefore never being caught, and planting my RAT across machines all across the world?

Unless that's not possible. Again, I have no idea what I'm doing or talking about. However, I do have enough common sense to refrain from moving forward and actually installing these products without first asking why they are consistently being modified every 20 minutes or so.

That hash matches the legitimate VirtualBox installer. Even files that have just been created will have a modified date. The file has the modified date as the download time. No metadata can be attached to the file during download.

As for malware signatures, obfuscated malware bypassing static detection is why runtime detection was introduced.

SIM-5515815 - April 19, 2024, 5:48 pm

Thanks for the insight.

I'm pretty certain I understand what you're saying, but please correct me if I'm wrong.

In layman's terms, you're saying that it's all legit and makes total sense in the world of computers, particularly from the perspective of a hacker?

In other words, "Forget about it!" ~ Donnie Brasco

DramaKing - April 19, 2024, 6:15 pm

(Apr 19, 2024 05:48 PM)GeorgeCarlinRules Wrote: [\[CITE\]](#) Thanks for the insight.

I'm pretty certain I understand what you're saying, but please correct me if I'm wrong.

In layman's terms, you're saying that it's all legit and makes total sense in the world of computers, particularly from the perspective of a hacker?

In other words, "Forget about it!" ~ Donnie Brasco

Yep, don't worry about the modified dates. Download directly from virtualbox.org and verify the hash. If the digital signature doesn't match, there should be a warning.

SIM-5515815 - April 19, 2024, 6:49 pm

I was just having a chat with my imaginary friends, and it seems to me that the hash means absolutely nothing within the degree and perspective of my question and concern. As far as the fact that when I checked out VirtualBox, the hash had been changed only 16 minutes prior to me checking it out. So my version of VirtualBox is literally 16 minutes old, so therefore it has a totally different hash than what it did 30 minutes prior? So yeah, my version of VirtualBox may match the most current hash, but that's only because there's been cooperation between two parties, or it could be the exact same entity operating two separate venues in unison. So I would have to put full faith in the creators of VirtualBox, which I don't. Especially due to the fact that the whole system is completely wired and rigged, completely, in absolute entirety. The only positive way to look at this would be that the only 'perpetrators' you would have to worry about are the ones that are inside of VirtualBox, as compared to any Tom, and Harry, Dick on the street. (yes, I am scratching my worthless turd I call a head)

I need to find out the exact definition for 'last modification date' as far as virustotal is concerned.

Only then will this make sense to me. Because it makes sense from both angles. And the only reason it doesn't make sense is because I do not know the exact definition, so I can put it in proper perspective.

If virustotal is claiming 'last modification date' means the last time somebody just passed the exact identical product through virustotal to be scanned, then it makes sense.

However 'last modification date', is a terrible way to express what could have simply been expressed 'last scanned'

DramaKing - April 19, 2024, 8:50 pm

(Apr 19, 2024 06:49 PM)GeorgeCarlinRules Wrote: [\[CITE\]](#) I was just having a chat with my imaginary friends, and it seems to me that the hash means absolutely nothing within the degree and perspective of my question and concern. As far as the fact that when I checked out VirtualBox, the hash had been changed only 16 minutes prior to me checking it out. So my version of VirtualBox is literally 16 minutes old, so therefore it has a totally different hash than what it did 30 minutes prior? So yeah, my version of VirtualBox may match the most current hash, but that's only because there's been cooperation between two parties, or it could be the exact same entity operating two separate venues in unison. So I would have to put full faith in the creators of VirtualBox, which I don't. Especially due to the fact that the whole system is completely wired and rigged, completely, in absolute entirety. The only positive way to look at this would be that the only 'perpetrators' you would have to worry about are the ones that are inside of VirtualBox, as compared to any Tom, and Harry, Dick on the street. (yes, I am scratching my worthless turd I call a head)

I need to find out the exact definition for 'last modification date' as far as virustotal is concerned.

Only then will this make sense to me. Because it makes sense from both angles. And the only reason it doesn't make sense is because I do not know the exact definition, so I can put it in proper perspective.

If virustotal is claiming 'last modification date' means the last time somebody just passed the exact identical product through virustotal to be scanned, then it makes sense.

However 'last modification date', is a terrible way to express what could have simply been expressed 'last scanned'

I finally found where it says "Last Modification Date." Yes, it's the last time that the record was updated. If one bit in the file was changed, it would be a completely different sample, so people with a little background know that it's not the file being modified.

SIM-5515815 - April 20, 2024, 9:35 pm

Okay cool that makes sense. Again "Last Modification Date" is a terrible way to express "Last Scanned". And to think I barely graduated high school and dreaded even thinking about going to college because I was going to have to, not only put up with four more years of this nonsense, but go into debt and pay a small fortune? And yet the jokes still on me because I should have gone to college, maybe then I wouldn't be so worthless. lol. Anyways thanks for the insight.

AnonAlias - April 20, 2024, 9:38 pm

(Apr 20, 2024 09:35 PM)GeorgeCarlinRules Wrote: [\[CITE\]](#) Okay cool that makes sense. Again "Last Modification Date" is a terrible way to express "Last Scanned". And to think I barely graduated high school and dreaded even thinking about going to college because I was going to have to, not only put up with four more years of this nonsense, but go into debt and pay a small fortune? And yet the jokes still on me because I should have gone to college, maybe then I wouldn't be so worthless. lol. Anyways thanks for the insight.

you aint worthless homie, everyone has their thing brother.