

Forum:[Hack Forums](#)

Thread: [How to remove a rootkit/firmware malware](#)

ForgeSMTP - April 2, 2025, 3:45 pm

So my buddy's PC got hacked by a Russian hacker few weeks ago and ever since he's been trying to take out the malware. At first, we both found out that the windows MoUsocoreWorker.exe was infected and a fake service was created at a different path instead of C:/Windows/System32/MoUsocoreWorker.exe. We had to do some firewall and app whitelisting at first because according to him, he wanted to find out the malware file and do a reverse engineering attack to the hackers server and take down all his/her botnets. None of this could solve the problem because the signs of a hacked PC was still there. So he had to re-install his OS only to later discover that we was dealing with a rootkit/firmware malware. So I'm asking does anyone know how to analyse rootkit/firmware processes? We actually want to find out the malware file and explore with it.

Biggy_Asian - April 2, 2025, 3:45 pm

Reformat your HDD/SSD best way to do it.

DramaKing - April 2, 2025, 5:10 pm

(Apr 2, 2025 03:45 PM)ForgeSMTP Wrote: [\[CITE\]](#) So my buddy's PC got hacked by a Russian hacker few weeks ago and ever since he's been trying to take out the malware. At first, we both found out that the windows MoUsocoreWorker.exe was infected and a fake service was created at a different path instead of C:/Windows/System32/MoUsocoreWorker.exe. We had to do some firewall and app whitelisting at first because according to him, he wanted to find out the malware file and do a reverse engineering attack to the hackers server and take down all his/her botnets. None of this could solve the problem because the signs of a hacked PC was still there. So he had to re-install his OS only to later discover that we was dealing with a rootkit/firmware malware. So I'm asking does anyone know how to analyse rootkit/firmware processes? We actually want to find out the malware file and explore with it.

First of all, did you really identify a command-and-control server in Russia? It doesn't really mean that the hacker is Russian, so don't assume. Second, there is no such thing as a reverse engineering attack.

Now as for the rootkit, what you need to do is open up the computer and locate the EEPROM chip on the motherboard. Carefully desolder the chip from the board. You'll now need to connect it to a firmware debugger (costs a few hundred bucks or so). This will allow you to dump the firmware and sift through unintelligible UEFI code. Or you could just make sure that Secure Boot is enabled, and the latest BIOS/UEFI update is applied (updating will wipe out any rootkit).

Having said all that, you'll want to have your buddy download and run the Farbar Recovery Scan Tool and Malwarebytes Anti-Rootkit. [Tha Sneak](#) or [Bastille](#) can review the generated log files.

Pr0m3th3us - April 2, 2025, 5:49 pm

(Apr 2, 2025 05:10 PM)DramaKing Wrote: [\[CITE\]](#) First of all, did you really identify a command-and-control server in Russia? It doesn't really mean that the hacker is Russian, so don't assume. Second, there is no such thing as a reverse engineering attack.

Now as for the rootkit, what you need to do is open up the computer and locate the EEPROM chip on the motherboard. Carefully desolder the chip from the board. You'll now need to connect it to a

firmware debugger (costs a few hundred bucks or so). This will allow you to dump the firmware and sift through unintelligible UEFI code. Or you could just make sure that Secure Boot is enabled, and the latest BIOS/UEFI update is applied (updating will wipe out any rootkit).

Having said all that, you'll want to have your buddy download and run the Farbar Recovery Scan Tool and Malwarebytes Anti-Rootkit. [Tha Sneak](#) or [Bastille](#) can review the generated log files. Also check this thread out, the group is here to help, free of charge.

<https://hackforums.net/showthread.php?tid=6292276>

ForgeSMTP - April 3, 2025, 9:25 am

(Apr 2, 2025 03:45 PM)Biggy_Asian Wrote: [\[CITE\]](#) Reformat your HDD/SSD best way to do it. Doesn't the drive get formatted properly when the option to format the disk get selected during Windows OS installation?

(Apr 2, 2025 05:10 PM)DramaKing Wrote: [\[CITE\]](#) First of all, did you really identify a command-and-control server in Russia? It doesn't really mean that the hacker is Russian, so don't assume. Second, there is no such thing as a reverse engineering attack.

Now as for the rootkit, what you need to do is open up the computer and locate the EEPROM chip on the motherboard. Carefully desolder the chip from the board. You'll now need to connect it to a firmware debugger (costs a few hundred bucks or so). This will allow you to dump the firmware and sift through unintelligible UEFI code. Or you could just make sure that Secure Boot is enabled, and the latest BIOS/UEFI update is applied (updating will wipe out any rootkit).

Having said all that, you'll want to have your buddy download and run the Farbar Recovery Scan Tool and Malwarebytes Anti-Rootkit. [Tha Sneak](#) or [Bastille](#) can review the generated log files. Well according to him, the hacker is Russian. It all started in a TG group where he dare a Russian hacker. Soon after he gained access to his PC and started social engineering him. He did couple of manipulative tricks and leaked his info and projects on the TG group.

By reverse engineering attack, our intention is simple find out the stub/malware file, analyze the file and figure out the command-and-control server so we can explore further. This is absolutely possible and does exist but the issue right now is figuring out the rootkit/firmware malware file. Recently, the hacker went as far as writing a text on the UI of the HP startup screen. That was a clear indication of a firmware malware or probably a CVE that got exploited.

Isn't it possible todo this "Now as for the rootkit, what you need to do is open up the computer and locate the EEPROM chip on the motherboard. Carefully desolder the chip from the board." without having to tamper with the hardware? "Secure Boot is enabled, and the latest BIOS/UEFI update is applied" we have done this to mitigate the hackers control. "Farbar Recovery Scan Tool and Malwarebytes Anti-Rootkit" we will get this done but can this give information about the rootkits/firmware processes? Also, how effective can it be with secure boot enable?

(Apr 2, 2025 05:49 PM)Rustoleum Wrote: [\[CITE\]](#) Also check this thread out, the group is here to help, free of charge.

<https://hackforums.net/showthread.php?tid=6292276>

Okay thanks waiting to hear from @DramaKing before we proceed. But clearly this is a really complicated malware.

Biggy_Asian - April 3, 2025, 10:35 am

(Apr 3, 2025 09:25 AM)ForgeSMTP Wrote: [\[CITE\]](#) Doesn't the drive get formatted properly when the

option to format the disk get selected during Windows OS installation?

Yes but its best you just wipe the drive pre-installation anyway.

ForgeSMTP - April 3, 2025, 10:39 am

(Apr 3, 2025 10:35 AM)Biggy_Asian Wrote: [\[CITE\]](#) Yes but its best you just wipe the drive pre-installation anyway.

Okay thanks

DramaKing - April 3, 2025, 10:47 am

(Apr 3, 2025 09:25 AM)ForgeSMTP Wrote: [\[CITE\]](#) Doesn't the drive get formatted properly when the option to format the disk get selected during Windows OS installation?

Absolutely. Formatting the disk using in Windows Setup is like any other format. The sectors with the malware will be unallocated.

(Apr 3, 2025 09:25 AM)ForgeSMTP Wrote: [\[CITE\]](#) Well according to him, the hacker is Russian. It all started in a TG group where he dare a Russian hacker. Soon after he gained access to his PC and started social engineering him. He did couple of manipulative tricks and leaked his info and projects on the TG group.

Finally someone who gives actual evidence.

(Apr 3, 2025 09:25 AM)ForgeSMTP Wrote: [\[CITE\]](#) By reverse engineering attack, our intention is simple find out the stub/malware file, analyze the file and figure out the command-and-control server so we can explore further. This is absolutely possible and does exist but the issue right now is figuring out the rootkit/firmware malware file. Recently, the hacker went as far as writing a text on the UI of the HP startup screen. That was a clear indication of a firmware malware or probably a CVE that got exploited.

Malware analysis can identify a command-and-control server. This is not an attack. I would not advise attempting to hack the hacker, especially one located in the dark depths of Russia where international law dares not enter. Best you'll likely be able to do is get the IP address blacklisted if that hasn't happened already. And maybe block all Russian IPs and get a good antivirus. There must be a download or some code that the hacker got your friend to run. However, he may have cleared his tracks.

Modifying the boot splash screen is a clear sign of a BIOS rootkit. Secure Boot should prevent the system from booting if enabled.

(Apr 3, 2025 09:25 AM)ForgeSMTP Wrote: [\[CITE\]](#) Isn't it possible todo this "Now as for the rootkit, what you need to do is open up the computer and locate the EEPROM chip on the motherboard. Carefully desolder the chip from the board." without having to tamper with the hardware? "Secure Boot is enabled, and the latest BIOS/UEFI update is applied" we have done this to mitigate the hackers control. "Farbar Recovery Scan Tool and Malwarebytes Anti-Rootkit" we will get this done but can this give information about the rootkits/firmware processes? Also, how effective can it be with secure boot enable?

That was not meant to encourage you to do this. BIOS/UEFI analysis should only be done by a computer hardware expert. Resoldering the chip is tricky at best, even if you get it removed and can afford the proper equipment. Reading the firmware is not something that can be done without hardware tampering according to my research.

Maybe there is a way to do it in software. Try this Charon tool.

<https://github.com/ch3rn0byl/Charon/releases/tag/1.0.1>

ForgeSMTP - April 3, 2025, 11:57 am

(Apr 3, 2025 10:47 AM)DramaKing Wrote: [\[CITE\]](#) Absolutely. Formatting the disk using in Windows Setup is like any other format. The sectors with the malware will be unallocated.

Finally someone who gives actual evidence.

Malware analysis can identify a command-and-control server. This is not an attack. I would not advise attempting to hack the hacker, especially one located in the dark depths of Russia where international law dares not enter. Best you'll likely be able to do is get the IP address blacklisted if that hasn't happened already. And maybe block all Russian IPs and get a good antivirus. There must be a download or some code that the hacker got your friend to run. However, he may have cleared his tracks.

Modifying the boot splash screen is a clear sign of a BIOS rootkit. Secure Boot should prevent the system from booting if enabled.

That was not meant to encourage you to do this. BIOS/UEFI analysis should only be done by a computer hardware expert. Resoldering the chip is tricky at best, even if you get it removed and can afford the proper equipment.

Maybe there is a way to do it in software. Try this Charon tool.

<https://github.com/ch3rn0byl/Charon/releases/tag/1.0.1>

Alright, thanks alot. We will look further and may revert.

ttbr0 - April 3, 2025, 10:46 pm

im still waiting to see some evidence. all text, no images or videos.

cosmocheats - April 4, 2025, 4:14 am

(Apr 2, 2025 03:45 PM)ForgeSMTP Wrote: [\[CITE\]](#) So my buddy's PC got hacked by a Russian hacker few weeks ago and ever since he's been trying to take out the malware. At first, we both found out that the windows MoUsoCoreWorker.exe was infected and a fake service was created at a different path instead of C:/Windows/System32/MoUsoCoreWorker.exe. We had to do some firewall and app whitelisting at first because according to him, he wanted to find out the malware file and do a reverse engineering attack to the hackers server and take down all his/her botnets. None of this could solve the problem because the signs of a hacked PC was still there. So he had to re-install his OS only to later discover that we was dealing with a rootkit/firmware malware. So I'm asking does anyone know how to analyse rootkit/firmware processes? We actually want to find out the malware file and explore with it.

Dealing with a rootkit/firmware malware is tricky. You'll need to check firmware integrity (UEFI/BIOS) using tools like CHIPSEC or GMER for deep scans. Best bet is to flash BIOS, replace storage drives, and reinstall OS on a clean system.

ForgeSMTP - April 5, 2025, 11:27 am

(Apr 3, 2025 10:46 PM)ttbr0 Wrote: [\[CITE\]](#) im still waiting to see some evidence. all text, no images or videos.

Evidence of what exactly?

(Apr 4, 2025 04:14 AM)cosmocheats Wrote: [\[CITE\]](#) Dealing with a rootkit/firmware malware is tricky. You'll need to check firmware integrity (UEFI/BIOS) using tools like CHIPSEC or GMER for deep

scans. Best bet is to flash BIOS, replace storage drives, and reinstall OS on a clean system.

We initially wanted to flash the BIOS, but the previously installed BIOS was outdated with 2 CVE vulnerabilities so we did an update. Does updating the BIOS and not flashing it retain any malware in it?

DramaKing - April 5, 2025, 11:41 am

(Apr 5, 2025 11:27 AM)ForgeSMTP Wrote: [\[CITE\]](#) Evidence of what exactly?

We initially wanted to flash the BIOS, but the previously installed BIOS was outdated with 2 CVE vulnerabilities so we did an update. Does updating the BIOS and not flashing it retain any malware in it?

There is no difference. You flashed a clean image. Everything should be normal now. Case closed.

ForgeSMTP - April 5, 2025, 11:45 am

(Apr 5, 2025 11:41 AM)DramaKing Wrote: [\[CITE\]](#) There is no difference. You flashed a clean image. Everything should be normal now. Case closed.

AhhhHaann thought as much. Thanks DramaKing. Would like to come under your mentorship you seem really good.

Tyr - April 6, 2025, 12:03 pm

(Apr 5, 2025 11:45 AM)ForgeSMTP Wrote: [\[CITE\]](#) AhhhHaann thought as much. Thanks DramaKing. Would like to come under your mentorship you seem really good.

He's better than I am; can say that. Unfortunately one of the most knowledgeable and dedicated WH members to this forum is secluded (or simply doesn't want to join) the malware removal team here which is supposed to consist of group members whom actually possess the skillset of [DramaKing](#), yet seem to overlook their talent. Such a shame because he's probably one of the most qualified individuals on this forum.

Anyway, for rootkit removal, you're gonna want to check up on that every few often as fragments can still lay dormant in parts of your EFI

DramaKing - April 6, 2025, 5:03 pm

(Apr 6, 2025 12:03 PM)Tyr Wrote: [\[CITE\]](#) He's better than I am; can say that. Unfortunately one of the most knowledgeable and dedicated WH members to this forum is secluded (or simply doesn't want to join) the malware removal team here which is supposed to consist of group members whom actually possess the skillset of [DramaKing](#), yet seem to overlook their talent. Such a shame because he's probably one of the most qualified individuals on this forum.

Anyway, for rootkit removal, you're gonna want to check up on that every few often as fragments can still lay dormant in parts of your EFI

Huh, thought updating the BIOS was a full overwrite of EEPROM. My only concern would be any infected files remaining on disk that try to reinfect the UEFI. The update hopefully took care of anyvSecure Boot vulnerability, and the computer is Noe secure against this (basically).

Tyr - April 6, 2025, 7:26 pm

(Apr 6, 2025 05:03 PM)DramaKing Wrote: [\[CITE\]](#) Huh, thought updating the BIOS was a full overwrite of EEPROM. My only concern would be any infected files remaining on disk that try to reinfect the UEFI. The update hopefully took care of anyvSecure Boot vulnerability, and the computer is Noe secure against this (basically).

You would think so but while updating the BIOS can help address vulnerabilities related to the EEPROM, the concern about infected files remaining on the disk is still possible. I've seen insane types of malware often go after the EFI System Partition (ESP), (has the bootloader and critical

startup files), effectively compromising the bootup process before the OS even begins to load. Correct if wrong but can even go as far as setting a BIOS password this way(?)

From what I understand, by infecting the EFI boot sector, the malware ensures that it can load early in the boot process, even before security software has a chance to operate. If the malware has infected the ESP, simply updating the BIOS won't necessarily address the issue, as the malware could still persist on the disk and reinfect the UEFI on reboot. Correct?

Even though the BIOS update might have mitigated some risks, it's crucial to also examine the disk, ensuring no remnants of infected files remain, especially within the EFI partition, which could try to reinfect the system and bypass the updated BIOS protections. This is why a comprehensive disk analysis and ensuring Secure Boot is enabled would be important next steps in securing the system. But most importantly, to disable the correct secure boot properties before initializing the actual restoration.

DramaKing - April 7, 2025, 3:02 am

(Apr 6, 2025 07:26 PM)Tyr Wrote: [\[CITE\]](#) You would think so but while updating the BIOS can help address vulnerabilities related to the EEPROM, the concern about infected files remaining on the disk is still possible. I've seen insane types of malware often go after the EFI System Partition (ESP), (has the bootloader and critical startup files), effectively compromising the bootup process before the OS even begins to load. Correct if wrong but can even go as far as setting a BIOS password this way(?)

Eh, I guess if malware can write to system firmware, then it can change settings. What I can say is that a bootkit in the EFI would compromise the secure root-of-trust, resulting in boot failure.

(Apr 6, 2025 07:26 PM)Tyr Wrote: [\[CITE\]](#) From what I understand, by infecting the EFI boot sector, the malware ensures that it can load early in the boot process, even before security software has a chance to operate. If the malware has infected the ESP, simply updating the BIOS won't necessarily address the issue, as the malware could still persist on the disk and reinfect the UEFI on reboot. Correct?

Even though the BIOS update might have mitigated some risks, it's crucial to also examine the disk, ensuring no remnants of infected files remain, especially within the EFI partition, which could try to reinfect the system and bypass the updated BIOS protections. This is why a comprehensive disk analysis and ensuring Secure Boot is enabled would be important next steps in securing the system. But most importantly, to disable the correct secure boot properties before initializing the actual restoration.

A second rootkit in the boot partition wouldn't bypass Secure Boot, and bypassing the patches should require a zero-day.

ForgeSMTP - April 7, 2025, 4:34 pm

(Apr 6, 2025 12:03 PM)Tyr Wrote: [\[CITE\]](#) He's better than I am; can say that. Unfortunately one of the most knowledgeable and dedicated WH members to this forum is secluded (or simply doesn't want to join) the malware removal team here which is supposed to consist of group members whom actually possess the skillset of [DramaKing](#), yet seem to overlook their talent. Such a shame because he's probably one of the most qualified individuals on this forum.

Anyway, for rootkit removal, you're gonna want to check up on that every few often as fragments can still lay dormant in parts of your EFI

Alright, we tried to flash the BIOS earlier today but it seems it just about updating it. The update file from the HP website created a recovery flash drive with the BIOS .bin file in Hewlett-Packard\BIOS\Current when trying to update from local media, it didn't work out so we had to move the bin file to Hewlett-Packard\BIOS\New and it got detected and updated. Are we doing

something wrong or there is just no flashing of the BIOS?

Also, the letter is still on the HP boot screen. How exactly is this letter there? What can be done to remove it? BTW we also installed the latest firmware update from HP website again today. None of this could revert the deeds. How could this fellow write to the HP boot screen UI?

Just so many questions...

(Apr 6, 2025 07:26 PM)Tyr Wrote: [\[CITE\]](#) You would think so but while updating the BIOS can help address vulnerabilities related to the EEPROM, the concern about infected files remaining on the disk is still possible. I've seen insane types of malware often go after the EFI System Partition (ESP), (has the bootloader and critical startup files), effectively compromising the bootup process before the OS even begins to load. Correct if wrong but can even go as far as setting a BIOS password this way(?)

From what I understand, by infecting the EFI boot sector, the malware ensures that it can load early in the boot process, even before security software has a chance to operate. If the malware has infected the ESP, simply updating the BIOS won't necessarily address the issue, as the malware could still persist on the disk and reinfect the UEFI on reboot. Correct?

Even though the BIOS update might have mitigated some risks, it's crucial to also examine the disk, ensuring no remnants of infected files remain, especially within the EFI partition, which could try to reinfect the system and bypass the updated BIOS protections. This is why a comprehensive disk analysis and ensuring Secure Boot is enabled would be important next steps in securing the system. But most importantly, to disable the correct secure boot properties before initializing the actual restoration.

How do we go about examining the disk? Currently, Secure boot, Kernel DMA protection, Enforced virtualization security etc are all enable. Also, something came to my mind today. What are the most possible things a rootkit malware can do? If it can inject code to running processes, does it relate to use the stack processes for this (not sure I'm correct about the stack process but saw somewhere that is had a CVE vulnerability)?

DramaKing - April 7, 2025, 4:48 pm

(Apr 7, 2025 04:34 PM)ForgeSMTP Wrote: [\[CITE\]](#) Alright, we tried to flash the BIOS earlier today but it seems it just about updating it. The update file from the HP website created a recovery flash drive with the BIOS .bin file in Hewlett-Packard\BIOS\Current when trying to update from local media, it didn't work out so we had to move the bin file to Hewlett-Packard\BIOS\New and it got detected and updated. Are we doing something wrong or there is just no flashing of the BIOS?

Also, the letter is still on the HP boot screen. How exactly is this letter there? What can be done to remove it? BTW we also installed the latest firmware update from HP website again today. None of this could revert the deeds. How could this fellow write to the HP boot screen UI?

Just so many questions...

How do we go about examining the disk? Currently, Secure boot, Kernel DMA protection, Enforced virtualization security etc are all enable. Also, something came to my mind today. What are the most possible things a rootkit malware can do? If it can inject code to running processes, does it relate to use the stack processes for this (not sure I'm correct about the stack process but saw somewhere that is had a CVE vulnerability)?

You would think that the boot splash would need to be in the UEFI, but that may not be the case, going off this project: <https://github.com/chnzzh/lenovo-logo-changer>.

ForgeSMTP - April 7, 2025, 4:50 pm

(Apr 7, 2025 03:02 AM)DramaKing Wrote: [\[CITE\]](#) Eh, I guess if malware can write to system firmware, then it can change settings. What I can say is that a bootkit in the EFI would compromise the secure root-of-trust, resulting in boot failure.

A second rootkit in the boot partition wouldn't bypass Secure Boot, and bypassing the patches should require a zero-day.

To a very reasonably extent, I'm quite confident about the secure boot implementation. But still keeping my fingers crossed. Personally, I'm amazed seen that this is possible and idk why I'm quite interested in practically knowing how it was accomplished.

BORA9 - May 22, 2025, 8:47 pm

Okay deep scans suck! We all know this, I suggest a decent security template for malware. Anything bypassing windows defender, your firewall, the GPE is going to require you to remove it manually, WHY? Because your scans are not going to detect them if they are being bypassed! This means cold boots and command lines. For example, boot in safe mode and remove it via CMD prompt and remove it via command line. Red Hat techniques are very PERSISTENT this means the HACKER WILL COME BACK! Reverse engineering is okay to slow these hackers down, but they will always find a way around it! You need to harden your computer with using all of the faulty features Windows and Mac offer! Not all attacks come from outside of corporate networks, SOME ARE INTERNAL!!!!

DROP SOME REP!!!