

[Cybersecurity 101: The Fundamentals of Cybersecurity](#) > [Malware Explained](#) > **Bootkit: Definition, Prevention, and Removal**

BOOTKIT: DEFINITION, PREVENTION, AND REMOVAL

Kurt Baker - January 04, 2023

A strong cybersecurity strategy should not only include reactive approaches to **cyberattacks**, but should also include proactive prevention methods for infections such as bootkit. Mitigating the consequences of a bootkit infection and removing the infection are valuable tools for your cybersecurity team. Bootkits are stealthy, and understanding how they work and how to combat them can help keep your business safe from threat actors.

What Is a Bootkit?

Bootkits are a type of modern **malware** used by a threat actor to attach malicious software to a computer system. Bootkits can be a critical security threat to your business and often involve rootkit tools for evading detection. These attacks target the Unified Extensible Firmware Interface (UEFI), software that connects a PC's operating system with its device firmware.

One example of a **rootkit infection** is the Spicy Hot Pot browser hijacking rootkit from 2020. This changed the user's homepage to one controlled by the threat actor.

Bootkit Vs Rootkit

A **rootkit** is a collection of software tools, or a program designed to give a **threat actor** remote control over a computer system. Rootkits are made to function without being detected by deactivating endpoint antivirus and antimalware software. This enables malicious software to be introduced to the system with the purpose of attacking network or application security.

Bootkits take this process a step further and are designed to infect the volume boot record or master boot record. By doing so, a bootkit can act before the computer's operating system has loaded. In this way, malicious code installed by the bootkit is up and running prior to the computer operating system on boot up.

Bootkit infections go undetected because all components are outside the Microsoft windows filing system, rendering them invisible to standard operating system processes. Some warnings that a computer might have a bootkit infection include system instability resulting in blue screen warnings and being unable to launch the operating system.

The Risk and Impact of Bootkits

A UEFI bootkit can be a serious problem for your business, especially since a well-made one can go virtually undetected. Rootkits such as bootkits are a critical threat to security and open the way for additional malware installation. The consequences of an undetected rootkit can include file deletion and information theft.

I The Risk and Impact of Bootkits

A UEFI bootkit can be a serious problem for your business, especially since a well-made one can go virtually undetected. Rootkits such as bootkits are a critical threat to security and open the way for additional malware installation. The consequences of an undetected rootkit can include file deletion and information theft.

Why Are Bootkits a Critical Security Threat?

A UEFI bootkit is particularly dangerous because it is difficult to get rid of. UEFI firmware is embedded in the motherboard instead of being written to the hard drive and is therefore immune to any hard drive manipulation. These bootkit attacks are generally hard to detect and may be installed alongside free downloads or through malicious websites exploiting browser vulnerabilities.

The consequences of rootkit malware in your system include:

- **File deletion:** Operating system code and other files are vulnerable to rootkits.
- **Remote access:** Changing configuration settings, opening backdoor ports in firewall settings and changing start-up scripts. Any of these enable threat actors to have remote access to the computer for further attacks.
- **Information theft:** Malware installed by rootkits can steal passwords, personal information and sensitive data while remaining undetected.
- **Additional malware:** With a rootkit installed, a threat actor can install additional malicious software and can even function like ransomware, demanding payment to restore your computer.

Bootkit infections have some additional potential consequences, such as persistent corporate espionage. UEFI firmware bootkits can be invisible to standard cybersecurity measures and, since they start before the operating system is loaded, are always active when the system is on. Preventing bootkit infections from happening in the first place is the best safety measure against them.

I Preventing Bootkit Infections

Scanning for suspicious activity with a software program or rootkit scanner can be effective for discovering application rootkits, but these cannot find bootkits, a kernel mode rootkit or firmware attacks. Having multiple layers of scanners can help create a preventative measure if you make sure to understand the limits of your software. However, the best prevention for a bootkit attack is the **secure boot**.

Protection and Risk Mitigation

UEFI secure boot is a security standard that ensures a device boots using only trusted software. The firmware checks the signature of every piece of boot software, including the UEFI firmware, and if all signatures are valid the PC boots. This secure boot can prevent a bootkit infection from causing harm, because if it is found, the PC will not start.

You can also take preventative measures to mitigate the risks of experiencing a bootkit attack in the first place. This involves avoiding activities such as booting the operating system from untrusted media. You can also check for updates to the operating system and firmware to avoid supply chain attacks. Regularly scanning for malicious activity is a good way to identify when you've become vulnerable to a bootkit infection. If a bootkit infection has taken place, the first step to take is to remove it.

I Bootkit Removal

Removing a bootkit is possible and involves specialized malware removal software. Rootkit removal is often easier because you can clean your hard drive to remove them. Finding the right tool is important for removing a bootkit infection on your system.

Welcome to CrowdStrike

What are you looking for today?

CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: [Privacy Notice](#).



taken place, the first step to take is to remove it.

I Bootkit Removal

Removing a bootkit is possible and involves specialized malware removal software. Rootkit removal is often easier because you can clean your hard drive to remove them. Finding the right tool is important for removing a bootkit infection on your system.

How to Get Rid of Bootkits

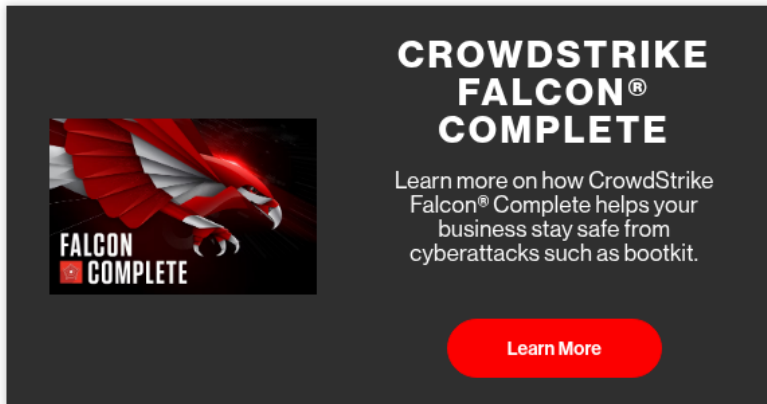
The type of tool you need is a boot repair disk that can clean your master boot record. This software should be used to wipe the master boot record, rather than repairing it. This way you can ensure the bootkit has been removed. Once wiped, you can create a clean master boot record, reformatting the new drive partitions.

Bootkits can be removed from internal hard drives and USB sticks as well as using an SPI flash programmer. These programming devices can erase, program and verify the operations of the storage chips. Because a **rootkit infection** is evasive, if you don't use a specialized tool, it can often protect itself.

I Protect Yourself against Malware Attacks

Protecting your business from bootkit attacks is important so threat actors can't gain secret remote access to your systems. Bootkits are dangerous because they are hard to detect, difficult to remove and they enable easy future malware attacks. Preventing and removing bootkits keeps your business safe.

With **CrowdStrike Falcon® Complete** you can stop breaches on endpoints, workloads and identities with expert management, threat hunting, monitoring and remediation. By keeping your system prepared and aware of even hidden malware threats, you can keep your business safe from bootkits and other rootkit attacks.

A dark-themed advertisement for CrowdStrike Falcon Complete. On the left is a red and white falcon logo with the text 'FALCON COMPLETE' below it. To the right, the text 'CROWDSTRIKE FALCON® COMPLETE' is displayed in large, bold, white letters. Below this, a smaller line of text reads: 'Learn more on how CrowdStrike Falcon® Complete helps your business stay safe from cyberattacks such as bootkit.' At the bottom right is a red button with the text 'Learn More' in white.

**CROWDSTRIKE
FALCON®
COMPLETE**

Learn more on how CrowdStrike Falcon® Complete helps your business stay safe from cyberattacks such as bootkit.

[Learn More](#)



Kurt Baker is the senior director of product marketing for Falcon Intelligence at CrowdStrike. He has over 25 years of experience in various positions, specializing in emerging software companies. He has expertise in cyber threat intelligence, security analysis, and advanced threat protection. Prior to joining CrowdStrike, Baker worked in technical roles at Tripwire and had co-founded several enterprise security solutions to mobile devices. He holds a bachelor of arts degree from the University of Washington in Massachusetts.

Welcome to CrowdStrike

What are you looking for today?

CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: [Privacy Notice](#).



Featured Articles

Featured Articles

Malware Detection



Malware Detection Techniques

What is a Cyberattack?



Cyberattacks

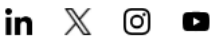
Types of Malware



Types of Malware

Try CrowdStrike free for 15 days

[Start free trial →](#)[Contact us →](#)[View pricing >](#)



Get Started	Company	Partners	Existing Customers	Support
Pricing Sale	About Us	Partner Programs	Support Portal	Call 1 888 512 8006 (US)
Free Trial Guide	Executive Leadership	Service Providers	Developer Portal	<div><div>Welcome to CrowdStrike</div><div>What are you looking for today?</div><div>CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.</div></div>
Falcon Flex	Board of Directors	Strategic Technology		FAQs
Financing	Newsroom	Channel & Distributors		
CrowdStrike Marketplace	Investor Relations	Become a Partner		
Cyber Monday Deals	CrowdStrike Racing & F1			
	Sustainability			



Malware Detection
Techniques

Cyberattacks

Types of Malware

Try CrowdStrike free for 15 days

Start free trial →

Contact us →

View pricing >



Get Started	Company	Partners	Existing Customers	Support
Pricing Sale	About Us	Partner Programs	Support Portal	Call 1-888-512-8906 (US)
Free Trial Guide	Executive Leadership	Service Providers	Developer Portal	Experienced a Breach?
Falcon Flex	Board of Directors	Strategic Technology		Contact Us
Financing	Newsroom	Channel & Distributors		Schedule a Meeting
CrowdStrike Marketplace	Investor Relations	Become a Partner		FAQs
Cyber Monday Deals	CrowdStrike Racing & F1			
	Sustainability			



Welcome to CrowdStrike

What are you looking for today?

CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: [Privacy Notice](#).