

[Cybersecurity 101: The Fundamentals of Cybersecurity](#) > [What Is a Cyberattack?](#) > **Backdoor Attacks**

BACKDOOR ATTACKS

Bart Lenaerts-Bergmans - July 17, 2023

What is a backdoor attack?

A **backdoor attack** is a clandestine method of sidestepping normal authentication procedures to gain unauthorized access to a system.

Typically, executing a backdoor attack involves exploiting system weaknesses or installing **malicious software** that creates an entry point for the attacker. A backdoor attack can result in **privilege escalation**, **lateral movements** to other systems, the **exfiltration of sensitive data**, and disruptions to operations. Because of this, understanding backdoor attacks is essential to a **robust cybersecurity strategy**.



EXPERT TIP

Think of a backdoor attack like a secret entrance that a burglar can use to get into a house — but instead of a house, it's a computer or a network.

Definition How It Works Prevention

Backdoor attacks leverage existing vulnerabilities or deliberately install uncontrolled access points in a computer system or network. The most effective backdoors are cleverly hidden, providing unauthorized users with an entry point that is difficult to detect. Once an attacker has found their way into a system through a backdoor, they can steal information, change how your system works, or simply sit back and watch. Their access and presence may continue for a long time unnoticed.

Common techniques

Let's consider some of the most common techniques used to create backdoors.

Maintenance hooks

Maintenance hooks are features or commands intentionally built into systems or applications by developers for testing,

Common techniques

Let's consider some of the most common techniques used to create backdoors.

Maintenance hooks

Maintenance hooks are features or commands intentionally built into systems or applications by developers for testing, troubleshooting, or maintenance. These are developer conveniences, often providing permissions and privileged access while bypassing normal authentication measures. These same conveniences are what make maintenance hooks attractive backdoors for malicious attackers.

After discovering a maintenance hook, a malicious attacker gains unauthorized access to a system. From here, the attacker might change settings, install malicious software, or even establish another backdoor to leverage in case this one is discovered and closed.

Maintenance hooks are often installed by **DevOps teams**, IT asset owners, or developers during initial implementation, testing, and deployment, but creators sometimes forget to remove them once they're no longer needed. Sometimes, a maintenance hook is only meant to be accessible in development or staging environments, but a misconfiguration exposes the maintenance hook in the production environment, too.

Covert channels

Networks and operating systems have standard protocols and mechanisms — legitimate channels — designed for the transmission of data from one component to another. Malicious attackers may execute backdoor attacks by leveraging a covert channel. A covert channel is used to transmit information using parts of a network or an operating system that weren't ordinarily designed for that purpose. For example, an attacker may embed data in network packet headers to transmit secret messages out of a system.

Kernel-level or application-level installations

An operating system kernel manages system resources and facilitates communication between hardware and software. If a malicious attacker can install malicious code at the kernel level — sometimes called a kernel **rootkit** — the system becomes critically vulnerable.

An application-level backdoor is malicious code that is installed in — or secretly disseminated and installed by — a software application. Because operating systems typically limit the access that a software application has to other parts of a system, the impact of an application-level backdoor attack may not be as devastating as that of a kernel-level backdoor. However, the potential for unauthorized data access or unwanted activities is still significant.

The image shows the cover of the 'CrowdStrike 2025 Threat Hunting Report'. The cover is dark with a glowing red 'X' shape. Text on the cover includes 'proLine', 'CrowdStrike', and '2025 THREAT HUNTING REPORT'.

**CrowdStrike 2025
Threat Hunting Report**

Adversaries weaponize and target AI at scale.

[Download report →](#)

Risks and implications of backdoor attacks

Now that we've covered the how of backdoor attacks, let's consider the potential damage and scope of backdoor threats.

Risks and implications of backdoor attacks

Now that we've covered the how of backdoor attacks, let's consider the potential damage and scope of backdoor threats.

The implications of backdoor attacks are wide-ranging and significant. First and foremost, **unauthorized access to sensitive information** is a primary risk. As cyberattackers prowl through your systems unnoticed, they have free rein to access, corrupt, or steal sensitive data.

In addition, backdoor attacks can lead to **malicious changes or damage to your system operations**. An attacker with access to your system can delete files, change configurations, disable system components, or even completely lock down your system. The results of such an attack can include system downtime, lost revenue, and a breach of customer trust.

Perhaps the most insidious aspect of backdoor attacks is their ability to **remain undetected for a long period of time**. A backdoor attack may not result in an obvious, one-time event like an arsonist burning down a building. It's more akin to an enemy living secretly and undetected in a home for months or years. Access to systems — accompanied by data theft and potential damage — may be prolonged and undetected.

Potential impact on corporations and governments

When viewed narrowly, a backdoor attack directly affects an individual computer or network. However, the scope of a backdoor attack can quickly extend beyond individual systems or organizations. If a backdoor is installed on hardware or software that is widely used, it could provide unauthorized access to business or government systems. Because of this, backdoor attacks can lead to corporate espionage or national security threats.

A well-known real-world example of a backdoor attack was the insertion of malicious code into third-party dependencies used by the SolarWinds Orion Platform. This opened a backdoor for malicious users to access files on systems that used the Orion Platform. The Orion Platform was widely used by corporations and government agencies, including the U.S. Treasury Department. In addition to the damages suffered by organizations that used the Orion Platform and were breached, the direct cost of the breach to SolarWinds was around \$40 million USD, according to [news reports](#).

Strategies for prevention and mitigation

Although backdoor attacks present a considerable threat, software organizations can adopt best practices that are effective in preventing and mitigating them.

Perform regular security audits

Regular security audits, which involve a thorough review and testing of a system's security measures, can identify potential vulnerabilities that can be exploited as backdoors. Incorrect configurations or unused but accessible entry points are just some of the vulnerabilities that an attacker can exploit but an audit can expose. In addition, an audit may uncover suspicious activity, which can lead to the detection of backdoor attacks already in progress. Audits should be regularly scheduled and comprehensive, and any vulnerabilities that surface should be immediately addressed.

LEARN MORE

Read this post to learn some of the most common vulnerabilities and exposures you should keep an eye on to ensure patching before they are exploited.

LEARN MORE

Read this post to learn some of the most common vulnerabilities and exposures you should keep an eye on to ensure patching before they are exploited.

Common Vulnerabilities & Exposures >

Harden your system security

Hardening the security of your systems will also help you safeguard against backdoor attacks. This includes taking some of the following measures:

- Remove unused or unnecessary software applications on a system
- Keep all software updated by applying the latest patches
- Turn off any unnecessary features or services that might offer points of entry for an attacker
- Implement strong access controls

Leverage intrusion detection systems

An intrusion detection system (IDS) monitors network traffic and system activities for signs of suspicious behavior. When patterns of activity might indicate the exploitation of a backdoor, an IDS will alert the security team. Advanced IDS tools can take automated remediation action.

With constant monitoring and immediate action through an IDS, you significantly shorten the window of time during which a malicious actor can leverage a backdoor to cause harm. **CrowdStrike endpoint detection and response (EDR)** monitors end-user devices across your system to detect and respond to the presence of malware or ransomware.

I Stay Protected

Backdoor attacks can result in data theft or crippled operations, but they are especially dangerous because a malicious attacker's access to a computer or network system can go undetected for a long period of time. If a backdoor attack makes its way into a piece of software that is then distributed and installed widely, a cyberattacker could gain broad access to multiple systems across corporations and governments. Software organizations must understand, prevent, and mitigate backdoor attacks.

In addition to basic best practices such as performing regular security audits and hardening system security, organizations should employ robust and reliable tools that help with intrusion detection. The cloud-based CrowdStrike Falcon® platform brings endpoint protection, real-time threat detection, and proactive threat hunting into a single, centralized interface. Sign up for a **free trial** today.



Bart is Senior Product Marketing Manager of Threat Intelligence at CrowdStrike and holds +20 years of experience in threat monitoring, detection and intelligence. After starting his career as a network security operations analyst at a Belgian financial organization, Bart moved to the US East Coast to join multiple cybersecurity companies including 3Com/Tippingpoint, RSA Security, Symantec, McAfee, Venafi and FireEye-Mandiant, holding both product management, as well as product marketing roles.



Bart is Senior Product Marketing Manager of Threat Intelligence at CrowdStrike and holds +20 years of experience in threat monitoring, detection and intelligence. After starting his career as a network security operations analyst at a Belgian financial organization, Bart moved to the US East Coast to join multiple cybersecurity companies including 3Com/Tippingpoint, RSA Security, Symantec, McAfee, Venafi and FireEye-Mandiant, holding both product management, as well as product marketing roles.

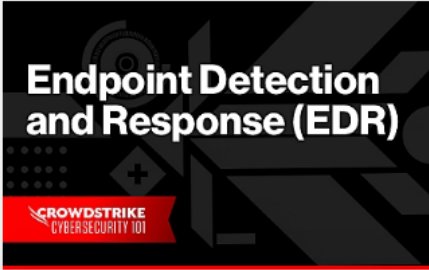
Featured Articles



Types of Cyberattacks



Types of Malware



Endpoint Detection and Response (EDR)

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			



Types of Cyberattacks



Types of Malware



Endpoint Detection and Response (EDR)

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			