

DEFINITION

backdoor (computing)

Ben Lutkevich, Technical Features Writer

Brien Posey

What is a backdoor?

A backdoor attack is a way to access a computer system or encrypted data that bypasses the system's customary security mechanisms. A developer may create a backdoor so that an application, operating system (OS) or data can be accessed for troubleshooting or other purposes. Attackers make use of backdoors that software developers install, and they also install backdoors themselves as part of a [computer exploit](#).

Whether added as an administrative tool, a means of attack or a mechanism allowing the government to access encrypted data, all backdoor installation is a security risk. [Threat actors](#) are always looking for these sorts of vulnerabilities to take advantage of.

What is Cybersecurity? Cybersecurity Threats, Methods, and Technology



What is a backdoor attack?

A backdoor attack occurs when threat actors create or use a backdoor to gain remote access to a system. These attacks let attackers gain control of system resources, perform network reconnaissance and install different [types of malware](#). In some cases, attackers design a [worm](#) or [virus](#) to take advantage of an existing backdoor created by the original developers or from an earlier attack.

To illustrate how backdoors undermine security systems, consider a bank vault that is protected with several layers of security. It has armed guards at the front door, sophisticated locking mechanisms and biometric access controls that make it impossible to access without proper authorization. However, a backdoor that bypasses these measures, such as a large ventilation shaft, makes the vault vulnerable to attack.

The malicious actions threat actors perform once they access a system include the following:

- stealing sensitive information;
- performing fraudulent transactions;
- installing spyware, keyloggers and Trojan horses;
- using rootkits;
- launching denial of service ([DoS](#)) attacks;
- hijacking servers; and
- defacing websites.

The consequences of a backdoor attack vary. In some cases, they can be immediate and severe and result in a data breach that harms customers and the business. In other cases, the effect shows up later, as the attacker uses the backdoor first for reconnaissance and returns later to execute a series of direct attacks.

Backdoor attacks can be large-scale operations, targeting government or enterprise IT infrastructure. However, [smaller attacks](#) are used to target individuals and personal computing implementations.

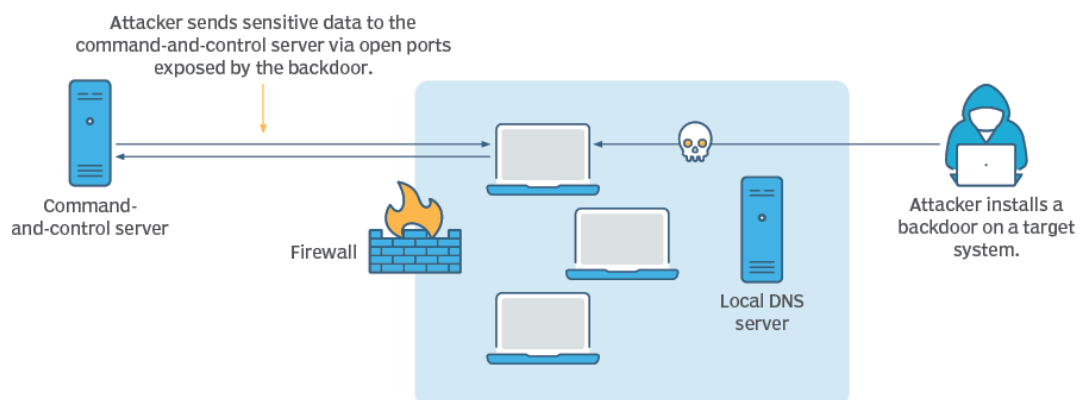
[Advanced persistent threats](#) are sophisticated cyber attacks that might use a backdoor to attack a system on multiple fronts. With these sorts of attacks, the backdoor could remain in the system for a long time.

How do backdoors work?

In the context of an attack, backdoors are hidden mechanisms attackers use to access a system without authentication. However, vendors sometimes create backdoors for legitimate purposes, such as restoring a user's lost password or providing government entities with access to encrypted data. Other backdoors are created and installed nefariously by hackers. Developers sometimes use backdoors during the development process and don't remove them, leaving them as a potential vulnerability point.

Malware can also act as a backdoor. In some cases, malware is a first-line backdoor, where it provides a staging platform for downloading other malware modules that perform an actual attack. With this type of attack, threat actors install a web shell to establish a backdoor on targeted systems and obtain remote access to a server. The attacker uses a [command-and-control server](#) to send commands through the backdoor to sensitive data or otherwise cause harm.

How a backdoor attack works



 Hackers use backdoors to communicate with a command-and-control server and bypass security.

Encryption algorithms and [networking protocols](#) can contain backdoors. For example, in 2016, researchers described how the prime numbers in encryption algorithms could be crafted to let an attacker factor the primes and break the encryption.

In 2014, an approach to random number generation called Dual Elliptic Curve Deterministic Random Bit Generator, or Dual_EC_DRBG, was found to contain a fault that made its resulting random seed numbers predictable. Some security experts speculated that the U.S. National Security Agency (NSA) allowed Dual_EC_DRBG to be used, even though it knew about the weakness, so the agency could use it as a backdoor. This accusation has not been proven.

Types of backdoor attacks

Various types of malware are used in backdoor attacks, including the following:

- **Cryptojacking** occurs when a victim's computing resources are hijacked to mine cryptocurrency. [Cryptojacking](#) attacks target all sorts of devices and systems.
- **DoS attacks** overwhelm servers, systems and networks with unauthorized traffic so that legitimate users can't access them.
- **Ransomware** is [malware that prevents users from accessing a system](#) and the files it contains. Attackers usually demand payment of a ransom for the resources to be unlocked.
- **Spyware** is [malware that steals sensitive information](#) and relays it to other users without the information owner's knowledge. It can steal credit card numbers, account login data and location information. Keyloggers are a form of spyware used to record a user's keystrokes and steal passwords and other sensitive data.
- **Trojan horse** is a malicious program that's often installed through a backdoor and appears harmless. A backdoor Trojan includes a backdoor that enables remote administrative control of a targeted system.

What is a Keylogger? What Does it Do?



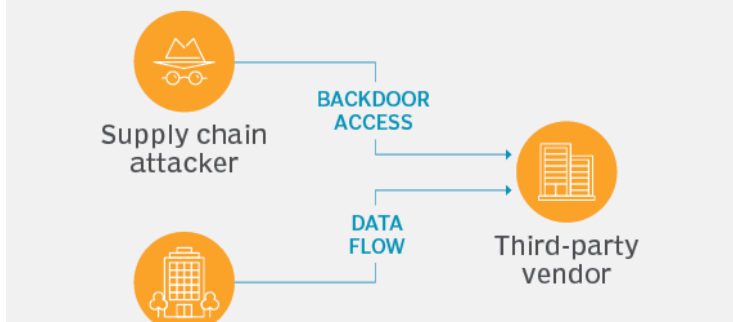
Various attack vectors are used to install backdoors, such as the following:


- **Federated learning.** [This decentralized method of machine learning](#) trains models locally on edge devices, as opposed to collecting data and training it in a centralized location. Edge devices have limited communication with the centralized servers. This lets threat actors poison a training data set and embed a backdoor on the central server when it does communicate with the edge device.
- **Hardware.** Attackers use modified chips, processors, hard drives and USBs to create backdoors.
- **Internet of things (IoT).** Components of these systems, such as security cameras, drones and smart thermostats, can act as backdoors and turn into [security vulnerabilities](#). IoT devices often come equipped with default passwords that function as a backdoor. Administrators often don't change them, and hackers can easily guess them.
- **Island hopping.** [These types of attacks](#) target an organization's third-party business partners to gain unauthorized access to the larger organization being targeted. Supply chains can be compromised using island hopping.
- **Phishing.** Seemingly legitimate emails are used to trick users into giving hackers sensitive information and can be used to install backdoor malware.
- **Steganography.** Malware is concealed in the bitmap of an image file. These files would normally not be considered a security threat, but [steganography](#) turns them into one.

Detection and prevention

Backdoors are designed to be hidden from most users. They are hidden using alias names, code obfuscation and multiple layers of encryption. This makes backdoors difficult to detect. Detection and prevention methods include the following tools and strategies:

Supply chain attack




 Supply chains are vulnerable to island hopping attacks because third parties provide a path into target organizations or access to the target organization's data.

- **Antimalware.** Some [antimalware](#) software can detect and prevent a backdoor from being installed.
- **Firewalls.** Ensure a firewall protects every device on a network. [Application firewalls](#) and web application firewalls can help prevent backdoor attacks by limiting the traffic that can flow across open ports.
- **Honeypots.** These security mechanisms lure attackers to a fake target. [Honeypots](#) are used to protect the real network and study the behavior of an attacker without their knowledge.
- **Network monitoring.** IT professionals use a protocol monitoring tool or [network analyzer](#) to inspect network packets. Malicious traffic can contain signatures that indicate the presence of a backdoor, and abnormal spikes in traffic can signal suspicious activity.
- **Security best practices.** Standard security measures and a layered cybersecurity strategy help prevent attackers from creating backdoors. If a backdoor is created for a legitimate purpose, its attack surface should be minimized. It also must be monitored and removed once its legitimate use is finished.
- **Allowlisting.** Use [allowlisting](#) to avoid untrusted software and only allow trusted user access with proper authentication. Choose applications and plugins with caution, as cybercriminals often hide backdoors in free applications and plugins.

4 steps to building a cybersecurity strategy

1. Understand your cyber threat landscape	2. Assess your cybersecurity maturity	3. Determine how to improve your cybersecurity program	4. Document your cybersecurity strategy
<ul style="list-style-type: none">■ Examine types of threats facing your organization■ Determine which threats affect your organization most often and most severely■ Get up to speed on cyber threat trends (e.g., rise in ransomware)	<ul style="list-style-type: none">■ Select a cybersecurity framework (e.g., NIST Cybersecurity Framework)■ Determine your organization's current level of maturity for all categories and subcategories (e.g., policies, governance, security technologies, incident recovery capabilities)■ Use same framework to determine the maturity level goals for next 3-5 years	<ul style="list-style-type: none">■ Determine improvements needed to reach maturity objectives■ Brainstorm options for achieving the objectives, with pros and cons for each option■ Present options to upper management for review, feedback and support	<ul style="list-style-type: none">■ Write and/or update cybersecurity plans, policies, guidelines, procedures, etc.■ Spell out each person's responsibility in carrying out the strategy■ Update your cybersecurity awareness and training initiatives

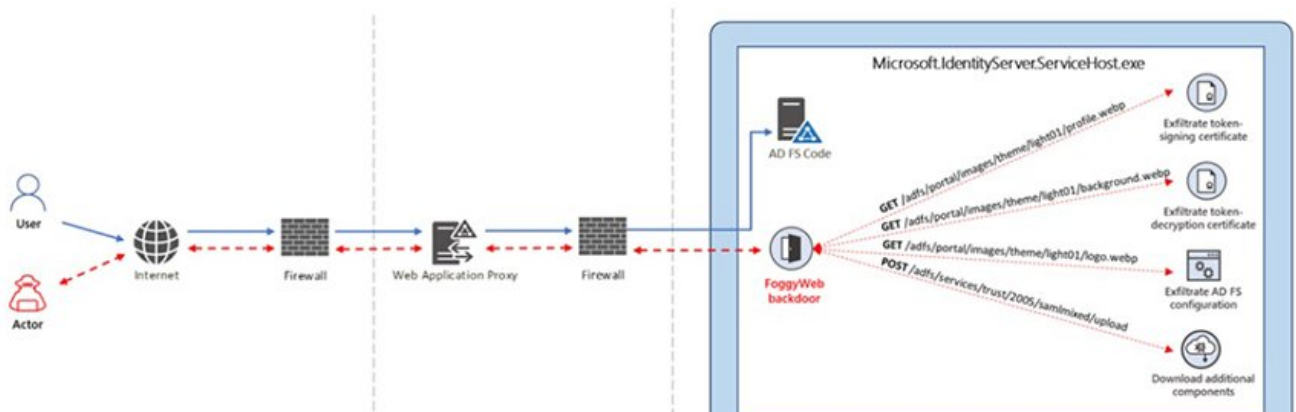
 One principle of a strong cybersecurity strategy is to hold software and system developers accountable for backdoors they create as part of the development process so that they aren't forgotten and left for attackers to exploit.


Famous backdoor attacks

There have been a number of high-profile backdoor attacks in recent years, including the following:

- **SolarWinds.** In late 2020, cybersecurity company FireEye discovered a dangerous backdoor hidden in updates for SolarWinds' Orion network management software. The attackers are suspected to be nation-state actors. They [secretly modified the SolarWinds software](#) to facilitate island hopping attacks that installed malware on Orion customer networks. The U.S. [Cybersecurity and Infrastructure Security Agency](#) said the attack began as early as March 2020 and that not all compromised organizations were actually targeted by the attacker for follow-up actions.

In late 2021, Microsoft security researchers identified a backdoor exploit, called [FoggyWeb](#), that the SolarWinds attackers are thought to have created. It let them access SolarWinds' Active Directory server and steal user credentials.



 The FoggyWeb backdoor gave hacker group Nobelium a persistent entry point to the internal network, bypassing firewalls, the DMZ and other external-facing security measures.

- **Zyxel.** In early 2021, a Dutch cybersecurity firm discovered a backdoor secret account hardcoded in Zyxel firewalls and access point (AP) controllers. The secret account let attackers give themselves administrative privileges, including the ability to change firewall settings and intercept traffic. The backdoor exploited a vulnerability in the credentials used to update firewall and AP controller firmware.
- **Back Orifice.** The hacker group Cult of the Dead Cow created this malware in 1998 to take advantage of vulnerabilities in the Windows OS. It installed backdoors that allowed remote control of Windows computers.

Backdoors aren't always software-based, and they aren't always created by rogue hackers. In 2013, the German news outlet *Der Spiegel* reported that the NSA's Tailored Access Operations unit maintained a catalog of backdoors to implant in firewalls, routers and other devices to be used overseas. The NSA also allegedly incorporated backdoor capabilities into individual hardware components, such as hard drives and even USB cables.

Malware and ransomware are two common cyber threats used in backdoor attacks. [Learn more about these two attack types](#) and why ransomware is so pervasive.

This was last updated in January 2023

Continue Reading About backdoor (computing)

- [How the SolarWinds vulnerability affects networking](#)
- [Encryption myths versus realities of Online Safety Bill](#)

- Securing AI during the development process
- Prepare for ransomware attacks on critical infrastructure
- Quiz: Web application security threats and vulnerabilities

Related Terms

antivirus software (antivirus program)

Antivirus software (antivirus program) is a security program designed to prevent, detect, search and remove viruses and other ...

[See complete definition](#) ⓘ

cyberwarfare

The generally accepted definition of cyberwarfare is a series of cyber attacks against a nation-state, causing it significant ...

[See complete definition](#) ⓘ

quantum supremacy

Quantum supremacy is the experimental demonstration of a quantum computer's dominance and advantage over classical computers by ... [See complete definition](#) ⓘ

🔍 Dig Deeper on Threats and vulnerabilities

supply chain attack

By: Alexander Gillis

Mandiant spots new malware targeting VMware ESXi hypervisors

By: Rob Wright

blended threat

By: Kinza Yasar

Networking

Top 9 SD-WAN benefits for businesses

Make the case for an SD-WAN implementation, and explore the benefits and main use cases for SD-WAN in enterprises, beyond ...

White box networking use cases and how to get started

Rising cloud costs have prompted organizations to consider white box switches to lower costs and simplify network management. ...

[About Us](#) [Editorial Ethics Policy](#) [Meet The Editors](#) [Contact Us](#) [Videos](#) [Photo Stories](#)

[Definitions](#) [Guides](#) [Advertisers](#) [Partner with Us](#) [Media Kit](#) [Corporate Site](#)

[Contributors](#) [CPE and CISSP Training](#) [Reprints](#) [Events](#) [E-Products](#)

All Rights Reserved,
Copyright 2000 - 2023, TechTarget

[Privacy Policy](#)

[Do Not Sell or Share My Personal Information](#)