In the today’s business environment, companies must do everything in their power to prevent network breaches. With attacks coming from nearly all sides, it can sometimes be difficult to ensure that every vector and point of entry is protected.

Recently, there has been an increase in backdoor attacks. Here, we’ll take a look at just what a backdoor attack entails, what makes them such a dangerous risk factor and how enterprises can protect themselves.

**The basics of a backdoor attack**  
According to Trend Micro’s report, “[Backdoor Use in Targeted Attacks](http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-backdoor-use-in-targeted-attacks.pdf),” applications that allow for remote access to computers – known as backdoors – are often used for targeted attacks. In these types of breaches, hackers leverage backdoor programs to access the victim’s network. The benefit of this attack vector is that the backdoor itself can help cybercriminals break into the infrastructure without being discovered.

“Often initially used in the second (point of entry) or third (command-and-control [C&C]) stage of the targeted attack process, backdoors enable threat actors to gain command and control of their target network,” report authors Dove Chiu. Shih-Hao Weng and Joseph Chiu wrote. “In fact, research reveals that many of the backdoors used in targeted attacks have been especially designed with the ability to bypass any kind of intrusion detection system (IDS).”

**Intrusion strategies in backdoor attacks**  
Backdoors not only provide a disguised point of entry for hackers, but can also offer a number of strategies for intrusion. Trend Micro’s report noted that these include:

* *Port binding:* Utilized before firewalls were commonplace, port binding involves specific information configurations to reveal where and how messages are transmitted and delivered within the network.
* *Connect-back:*Once firewalls were put in place on many networks, hackers began using the connect-back approach, where backdoors are leveraged to connect the targeted systems to cybercriminals’ C&C server systems. This also allows for a reverse connection from the servers to the victim platform through ports not under firewall protection.
* *Connect availability use:*This strategy involves the use of several malware samples to not only breach the network, but remain there undetected for long periods of time. This extends the window hackers have to steal sensitive data from the target. The first malware, or “first-line backdoor,” serves as a platform to download the second sample, the “second-line backdoor,” which performs the actual theft of information.
* *Legitimate platform abuse:* The report noted that abusing legitimate platforms has become more common especially as hackers must now work harder to side-step security systems. Within this strategy, cybercriminals abuse a valid platform – like a blog, for example – and utilize it to for the storage of C&C server data.

These are just a few attack strategies that can be carried out with backdoors. Trend Micro noted that other approaches include common services protocol or file header abuse, protocol or port listening, custom DNS lookup use and port reuse.

In addition, Tripwire noted that software isn’t the only system that can have a backdoor. [Hardware components](http://www.tripwire.com/state-of-security/security-data-protection/backdoors-electronic-component-qualification-hardware-attacks-1/) including authentication tokens, network appliances, surveillance systems and certain communication infrastructure devices can also have malicious backdoors allow for cybercriminal intrusion.

**How to protect against backdoor attacks**  
Cloud Security Alliance noted that because many backdoor attacks are known for being able to [prevent detection by many discovery tools](https://blog.cloudsecurityalliance.org/2013/11/20/protecting-your-company-from-backdoor-attacks-what-you-need-to-know/), protecting against them can be difficult. However, there are strategies that can be leveraged to help reduce the risk of a breach of this kind.

First and foremost, companies should have firewalls in place that can block entry points from all but authorized users. This is especially important as execution of a port binding backdoor attack is nearly impossible should a firewall be present.

In addition, Cloud Security Alliance encouraged [robust network monitoring](https://www.trendmicro.com/en_us/business/products/network.html) particularly of any open source-based programs.

“Unlike surpassing huge barriers in influencing (or writing) an industry standard, open-source projects enable someone to choose any of the missions of open-source projects in hundreds of mirroring sites opening up a broad surface of attack,” Cloud Security Alliance stated.

In this way, businesses should be choosy about the open-source applications they use and ensure that they come from a reputable source.

Network monitoring is also key when it comes to protection from backdoor attacks. Monitoring can help guarantee that any suspicious activity – such as information being gathered by a command and control server – is flagged with network administrators. IT staff can then react quickly to get to the root of the issue, stop the attack and mitigate any damage.

Another protection measure involves the use of an anti-malware solution. Trend Micro noted that because some backdoor attacks include the emulation of network traffic, the network activity therefore appears genuine and does not set off any alarms. However, an anti-malware system like [Trend Micro OfficeScan](http://www.trendmicro.com/us/enterprise/product-security/officescan/) is able to detect backdoors if this kind.

Backdoor attacks present a considerable threat to businesses, but understanding how they happen and how they can be prevented can go a long way toward better protection.

In the world of cybersecurity, a [backdoor](https://blog.malwarebytes.com/glossary/backdoor/) refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka [root access](https://en.wikipedia.org/wiki/Superuser)) on a computer system, network, or software application. Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices.

But backdoors aren't just for bad guys. Backdoors can also be installed by software or hardware makers as a deliberate means of gaining access to their technology after the fact. Backdoors of the non-criminal variety are useful for helping customers who are hopelessly locked out of their devices or for troubleshooting and resolving software issues.

Unlike other cyberthreats that make themselves known to the user (looking at you [ransomware](https://www.malwarebytes.com/ransomware/)), backdoors are known for being discreet. Backdoors exist for a select group of people in the know to gain easy access to a system or application.

As a threat, backdoors aren't going away anytime soon. According to the Malwarebytes Labs [State of Malware report](https://blog.malwarebytes.com/malwarebytes-news/ctnt-report/2019/01/2019-state-malware-report-trojans-cryptominers-dominate-threat-landscape/), backdoors were the fourth most common threat detection in 2018 for both consumers and businesses—respective increases of 34 and 173 percent over the previous year.

If you're concerned about backdoors, you heard about backdoors in the news and want to know what the deal is, or you have a backdoor on your computer and need to get rid of it right now, you're in the right place. Read on and get ready to learn everything you've ever wanted to know about backdoors.

“A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application.”

Latest news on backdoors

* [Mac malware combines EmPyre backdoor and XMRig miner](https://blog.malwarebytes.com/threat-analysis/2018/12/mac-malware-combines-empyre-backdoor-and-xmrig-miner/)
* [Mac cryptocurrency ticker app installs backdoors](https://blog.malwarebytes.com/threat-analysis/2018/10/mac-cryptocurrency-ticker-app-installs-backdoors/)
* [Another OSX.Dok dropper found installing new backdoor](https://blog.malwarebytes.com/threat-analysis/2017/05/another-osx-dok-dropper-found-installing-new-backdoor/)

How do backdoors work?

Let's start by figuring out how backdoors end up on your computer to begin with. This can happen in a couple different ways. Either the backdoor comes as a result of malware or by an intentional manufacturing (hardware or software) decision.

**Backdoor malware** is generally classified as a [Trojan](https://www.malwarebytes.com/trojan/). A Trojan is a malicious computer program pretending to be something it's not for the purposes of delivering malware, stealing data, or opening up a backdoor on your system. Much like the [Trojan horse](https://en.wikipedia.org/wiki/Trojan_Horse) of ancient Greek literature, computer Trojans always contain a nasty surprise.

Trojans are an incredibly versatile instrument within the cybercriminal toolkit. They come under many guises, like an email attachment or file download, and deliver any number of malware threats.

To compound the problem, Trojans sometimes exhibit a [worm](https://blog.malwarebytes.com/detections/worm/)-like ability to replicate themselves and spread to other systems without any additional commands from the cybercriminals that created them. Take, for example, the [Emotet](https://www.malwarebytes.com/emotet/) banking Trojan. [Emotet](https://blog.malwarebytes.com/cybercrime/2019/03/emotet-revisited-this-pervasive-persistent-threat-is-still-a-danger-to-businesses/) got its start in 2014 as an information stealer, spreading across devices and stealing sensitive financial data. Since then [Emotet has evolved](https://blog.malwarebytes.com/cybercrime/2018/09/emotet-rise-heavy-spam-campaign/) into a delivery vehicle for other forms of malware. Emotet helped make the Trojan the top threat detection for 2018, according to the State of Malware report.

[In one example](https://blog.malwarebytes.com/cybercrime/2016/07/new-mac-backdoor-malware-eleanor/) of backdoor malware, cybercriminals hid malware inside of a free file converter. No surprise—it didn't convert anything. In fact, the download was designed solely to open up a backdoor on the target system. [In another example](https://blog.malwarebytes.com/threat-analysis/2018/12/mac-malware-combines-empyre-backdoor-and-xmrig-miner/), cybercriminals hid backdoor malware inside of a tool used for pirating Adobe software applications (let that be a lesson on software piracy). And in one final example, a seemingly legitimate cryptocurrency ticker app called [CoinTicker](https://blog.malwarebytes.com/threat-analysis/2018/10/mac-cryptocurrency-ticker-app-installs-backdoors/) worked as advertised, displaying information about various forms of cryptocurrency and markets, but it also opened a backdoor.

Once cybercriminals have their foot in the door, they might employ what's known as a [rootkit](https://blog.malwarebytes.com/glossary/rootkit/). A rootkit is a package of malware designed to avoid detection and conceal Internet activity (from you and your [operating system](https://blog.malwarebytes.com/glossary/os/)). Rootkits provide attackers with continued access to infected systems. In essence, the rootkit is the doorstopper that keeps the backdoor open.

“Backdoors were the fourth most common threat detection in 2018 for both consumers and businesses—respective increases of 34 and 173 percent over the previous year.”

**Built-in or proprietary backdoors** are put in place by the hardware and software makers themselves. Unlike backdoor malware, built-in backdoors aren't necessarily conceived with some criminal purpose in mind. More often than not, built-in backdoors exist as artifacts of the software creation process. Software developers create these backdoor accounts so they can quickly move in and out of applications as they're being coded, test their applications, and fix software bugs (i.e. mistakes) without having to create a "real" account. These backdoors aren't supposed to ship with the final software released to the public, but sometimes they do. It's not the end of the world, but there's always the chance a proprietary backdoor will fall into the hands of cybercriminals.

While the majority of built-in backdoors that we know about fall into the former category (i.e. the "whoops, we didn't mean to put that there" category) members of the [Five Eyes](https://en.wikipedia.org/wiki/Five_Eyes) intelligence sharing pact (the US, UK, Canada, Australia, and New Zealand) have asked Apple, Facebook, and Google to install backdoors in their technology to aid in evidence gathering during criminal investigations. Though all three companies have declined, all three do provide [downstream](https://www.eff.org/pages/upstream-prism) data to the extent required by law.

The Five Eyes nations have stressed that these backdoors are in the best interest of global security, but there's a lot of potential for abuse. CBS News found dozens of police officers all over the country used currently available criminal databases to help themselves and their friends harass their exes, creep on women, and harass journalists who took umbrage with their harassing and creeping.

That being said, what if government agencies decided they weren't going to take no for an answer?

This brings us to the supply chain backdoor. As the name suggests, a supply chain backdoor is inserted surreptitiously into the software or hardware at some point in the supply chain. This could happen as raw materials are shipped from supplier to manufacturer or as the finished product makes its way from manufacturer to consumer. For example, a government agency could intercept completed routers, servers and miscellaneous networking gear on its way to a customer, then install a backdoor into the [firmware](https://en.wikipedia.org/wiki/Firmware). And, by the way, the US National Security Agency (NSA) actually did that, as revealed in the 2013 Edward Snowden global [surveillance disclosures](https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)).

Supply chain infiltrations could also happen in software. Take open source code, for example. Open source code libraries are free repositories of code, applications, and development tools that any organization can dip into instead of coding everything from scratch. Sounds great, right? Everyone working together for the greater good, sharing the fruits of their labor with each other. For the most part, it is great. Any contribution to the source code is up for scrutiny, but there have been instances where malicious code has made its way to the end user.

To that point, in July of 2018 [cryptomining malware](https://blog.malwarebytes.com/security-world/2018/07/5-ways-find-fix-open-source-vulnerabilities/) was found inside of an app (or "snap," as they call it in the world of Linux) for [Ubuntu](https://blog.malwarebytes.com/glossary/ubuntu/) and other [Linux](https://blog.malwarebytes.com/glossary/linux/)-based operating systems. Canonical, the developers of Ubuntu admitted, "It's impossible for a large-scale repository to only accept software after every individual file has been reviewed in detail."

Are backdoors and exploits the same?

Malwarebytes Labs defines [exploits](https://www.malwarebytes.com/exploits/) as, "known vulnerabilities in software that can be abused to gain some level of control over the systems running the affected software." And we know a backdoor works like a secret entrance into your computer. So are backdoors and exploits one in the same?

While backdoors and exploits seem awfully similar at first glance, they are not the same thing.

Exploits are accidental software vulnerabilities used to gain access to your computer and, potentially, deploy some sort of malware. To put it another way, exploits are just software bugs that researchers or cybercriminals have found a way to take advantage of. Backdoors, on the other hand, are deliberately put in place by manufacturers or cybercriminals to get into and out of a system at will.

“Exploits are accidental software vulnerabilities used to gain access to your computer and, potentially, deploy some sort of malware…. Backdoors, on the other hand, are deliberately put in place by manufacturers or cybercriminals to get into and out of a system at will.”

What can hackers do with a backdoor?

Hackers can use a backdoor to install all manner of malware on your computer.

* [Spyware](https://www.malwarebytes.com/spyware/) is a type of malware that, once deployed on your system, collects information about you, the sites you visit on the Internet, the things you download, the files you open, usernames, passwords, and anything else of value. A lesser form of spyware called [keyloggers](https://www.malwarebytes.com/keylogger/) specifically track every keystroke and click you make. Companies may use spyware/keyloggers as a legitimate and legal, means of monitoring employees at work.
* [Ransomware](https://www.malwarebytes.com/ransomware/) is a type of malware designed to encrypt your files and lock down your computer. In order to get back those precious photos, documents, etc. (or whatever file type the attackers choose to target) you have to pay the attackers via some form of [cryptocurrency](https://blog.malwarebytes.com/101/2017/11/cryptocurrency-works-cybercriminals-love/), usually [Bitcoin](https://blog.malwarebytes.com/glossary/bitcoin/).
* Use your computer in a [DDoS](https://www.malwarebytes.com/ddos/) attack. Using the backdoor to get super user access on your system, cybercriminals can take command of your computer remotely, enlisting it in a network of hacked computers, aka a [botnet](https://blog.malwarebytes.com/threats/botnets/). With this zombie computer botnet, criminals can then overwhelm a website or network with traffic from the botnet in what's known as a distributed denial of service attack (DDoS). The flood of traffic prevents the website or network from responding to legitimate requests, effectively taking the site out of service.
* [Cryptojacking](https://www.malwarebytes.com/cryptojacking/) malware is designed to use your system's resources to mine cryptocurrency. In short, every time someone exchanges cryptocurrency the transaction is recorded on an encrypted virtual ledger known as the blockchain. Cryptomining is the process of validating these online transactions in exchange for more cryptocurrency and it takes an enormous amount of computing power. Instead of buying the expensive hardware required for cryptomining, criminals have found that they can simply enlist hacked computers in a botnet that works the same as expensive cryptomining farms.

What is the history of backdoors?

Here's a look back at some of the most (in)famous backdoors, both real and fictional since the dawn of computers.

One could argue backdoors entered the public consciousness in the 1983 science fiction film *[WarGames](https://en.wikipedia.org/wiki/WarGames)*, starring Matthew Broderick (in what feels like a test run for *Ferris Bueller*). Broderick as mischievous teenage hacker David Lightman uses a built-in backdoor to gain access to a military supercomputer designed to run nuclear war simulations. Unbeknownst to Lightman, the schizophrenic computer can't tell reality from simulation. And also some genius decided to give the computer access to the entire United States nuclear arsenal. Hilarity ensues as the computer threatens to blow up the entire world.

In 1993 the NSA developed an encryption chip with a built-in backdoor for use in computers and phones. Supposedly, the chip would keep sensitive communications secure while allowing law enforcement and government agencies to decrypt and listen in on voice and data transmissions when warranted. Hardware backdoors have big advantages over the software kind. Namely, they are harder to remove—you have to rip the hardware out or re-flash the firmware to do so. The chip, however, was derailed over privacy concerns before seeing any kind of adoption.

In 2005 Sony BMG got into the business of backdoors when they shipped millions of music CDs with a harmful copy protection rootkit. Little did you know, while rocking out to the latest edition of [*Now That's What I Call Music!*](https://en.wikipedia.org/wiki/Now_That%27s_What_I_Call_Music!) your CD included a rootkit, which would install itself automatically once inserted into your computer. Designed to monitor your listening habits, the Sony BMG rootkit would also stop you from burning CDs and left a gaping vulnerability in your computer that cybercriminals could take advantage of. Sony BMG paid out millions to settle lawsuits related to the rootkit and recalled even more millions of CDs.

In 2014 several Netgear and Linksys routers were found to have built-in backdoors. SerComm, the third-party manufacturer that put the routers together, denied putting the backdoors in their hardware on purpose. But when the patch SerComm released ended up hiding the backdoor instead of fixing it, it became clear the company was up to no good. Exactly what SerComm was trying to accomplish with the backdoor remains unclear.

That same year software developers working on a spinoff of Google's Android operating system (called Replicant) discovered a backdoor on Samsung mobile devices, including Samsung's Galaxy series of phones. The backdoor allegedly allowed Samsung or anyone else who knew about it remote access to all of the files stored on affected devices. In response to the discovery, Samsung referred to the backdoor as a "feature" that posed "no security risk."

The other famous phone maker, Apple, refuses to include backdoors in its products, despite repeated requests from the FBI and US Department of Justice to do so. Pressure mounted following the 2015 San Bernardino terrorist attacks in which the FBI recovered an iPhone owned by one of the shooters. Instead of compromising the security of their iOS devices, Apple doubled down on privacy and made their iPhones and iPads even harder to crack. The FBI eventually withdrew their request when they were able to hack the older, less secure iPhone with the help of a mysterious third party.

Plugins containing malicious hidden code for WordPress, Joomla, Drupal and other [content management systems](https://en.wikipedia.org/wiki/Content_management_system) are an ongoing problem. In 2017 security researchers uncovered an [SEO](https://blog.malwarebytes.com/glossary/seo-2/) scam that affected more than 300,000 WordPress websites. The scam centered around a WordPress [CAPTCHA](https://blog.malwarebytes.com/cybercrime/2015/02/logging-in-and-captcha/) plugin called Simply WordPress. Once installed, Simply WordPress opened up a backdoor, allowing admin access to the affected websites. From there, the hacker responsible embedded hidden links to his sketchy payday loan website (other websites linking back to your website is great for SEO).

2017 also bore witness to the destructive [NotPetya](https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/) ransomware. The apparent patient zero in this case was a backdoor Trojan disguised as a software update for a Ukrainian accounting app called [MeDoc](https://blog.malwarebytes.com/cybercrime/2017/06/petya-esque-ransomware-is-spreading-across-the-world/). When questioned, MeDoc denied being the source for NotPetya. The real question—why would someone choose a wildly suspect Ukrainian accounting app called MeDoc?

In a 2018 news story that sounds like the setup for a straight-to-video, B-movie thriller, *Bloomberg Businessweek* reported state sponsored Chinese spies had infiltrated server manufacturer Supermicro. The spies allegedly installed spy chips with hardware backdoors on server components destined for dozens of American tech companies and US government organizations—most notably Amazon, Apple, and the CIA. Once installed in a data center, the spy chips were said to communicate back with Chinese [command and control](https://blog.malwarebytes.com/glossary/cc/) (C&C) servers, giving Chinese operatives unrestricted access to data on the network. Amazon, Apple, and various US government officials have all refuted the claims made in the *Bloomberg* story. Supermicro, in their defense, called the story "virtually impossible," and no other news organization has picked it up.

Finally, as an example of a situation where a company wishes they had a backdoor, Canadian cryptocurrency exchange QuadrigaCX made news in early 2019 when the company founder died abruptly while vacationing in India, taking the password to everything with him. QuadrigaCX claims all $190 million in client cryptocurrency holdings are irretrievably locked away in "cold storage," where they will sit for decades and eventually be worth zillions of dollars—or nothing, depending on how cryptocurrency goes.

How can I protect against backdoors?

Good news bad news. The bad news is that it's difficult to identify and protect yourself against built-in backdoors. More often than not, the manufacturers don't even know the backdoor is there. The good news is that there are things you can do to protect yourself from the other kinds of backdoors.

**Change your default passwords.** The hardworking people in your company's IT department never intended for your actual password to be "guest" or "12345." If you leave that default password in place, you've unwittingly created a backdoor. Change it as soon as possible and enable [multi-factor authentication](https://blog.malwarebytes.com/101/2017/01/understanding-the-basics-of-two-factor-authentication/) (MFA) while you're at it. Yes, keeping track of a unique password for every application can be daunting. A Malwarebytes Labs [report on data privacy](https://blog.malwarebytes.com/security-world/2019/03/labs-survey-finds-privacy-concerns-distrust-of-social-media-rampant-with-all-age-groups/) found that 29 percent of respondents used the same password across numerous apps and devices. Not bad, but there's still room for improvement.

**Monitor network activity.** Any weird data spikes could mean someone is using a backdoor on your system. To stop this, use firewalls to track inbound and outbound activity from the various applications installed on your computer.

**Choose applications and plugins carefully.** As we've covered, cybercriminals like to hide backdoors inside of seemingly benign free apps and plugins. The best defense here is to make sure whatever apps and plugins you choose come from a reputable source. Android and Chromebook users should stick with apps from the Google Play store, while Mac and iOS users should stick to Apple's App Store. Bonus related tech tip—when a newly installed app asks for permission to access data or functions on your device, think twice. [Suspect apps](https://blog.malwarebytes.com/cybercrime/2017/11/new-trojan-malware-discovered-google-play/) have been known to make it through Google and Apple's respective app vetting processes. Referring back to the data privacy study, most respondents did well to track app permissions, but 26 percent said, "I don't know." Take some time, possibly right now, to review app permissions on your devices (Malwarebytes for Android will do this for you). As for WordPress plugins and the like. Check user ratings and reviews and avoid installing anything with a less than stellar score.

**Use a good cybersecurity solution.** Any good anti-malware solution should be able to stop cybercriminals from deploying the Trojans and rootkits used to open up those pesky backdoors. Malwarebytes, for example, has cybersecurity solutions for [Windows](https://www.malwarebytes.com/premium/), [Mac](https://www.malwarebytes.com/mac/), and [Chromebook](https://www.malwarebytes.com/chromebook/). Not to mention [Malwarebytes for Android](https://www.malwarebytes.com/android/) and [Malwarebytes for iOS](https://www.malwarebytes.com/ios/), so you can stay protected on all your devices. Business users—we've got you covered too. Check out all of [Malwarebytes business solutions](https://www.malwarebytes.com/business/solutions/).

And if your interest in backdoors goes beyond what you've read here, be sure to read and subscribe to the [Malwarebytes Labs blog](https://blog.malwarebytes.com/). There you'll find all the latest news on backdoors and everything else that matters in the world of cybersecurity.

“We often get in quicker by the back door than the front” — Napoleon Bonaparte

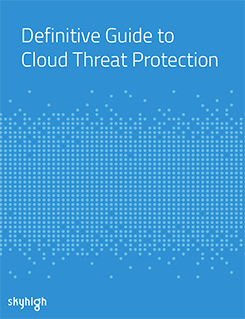
A rare example of a backdoor planted in a core industry security standard has recently come to light. It is now widely believed that the NSA compromised trust in NIST’s encryption standard ([called the Dual EC DRBG standard](http://web.archive.org/web/20060930163233/http:/csrc.nist.gov/publications/nistpubs/800-90/SP800-90_DRBG-June2006-final.pdf)) by adding the ability for NSA to decipher any encrypted communication over the Internet. This incident brings to fore the question of how much trust is warranted in the technologies that enable business over the Internet today.

There are only a few organizations in the world (all with 3 letter acronyms) that can pull off a fundamental backdoor coup such as this. More commonly entities undertaking backdoor attacks do not have that level of gravitas or such far reaching ambitions – instead the majority of these entities tend to leverage backdoors to undertake cybercrime missions ranging from advanced persistent threats on specific target companies, to botnet and malware/adware networks for monetary gains. In these instances, Cloud services are a favorite vector for injecting backdoors into the enterprise.

Definitive Guide to Cloud Threat Protection

Learn about the most common threats to corporate data in the cloud and how to protect against them.

[**Download Now**](https://info.skyhighnetworks.com/WP_Definitive-Guide-to-Cloud-Threat-Protection-eBook_BannerCloud-MFE.html?Source=website&LSource=website)



**What can we really trust?**

In his 1984 Turing Award acceptance speech, [Ken Thompson](http://en.wikipedia.org/wiki/Ken_Thompson) points out that trust is relative in what is perhaps the first major paper on this topic titled Reflections on Trusting Trust which describes the threat of backdoor attacks. He describes a backdoor mechanism, which relies on the fact that people only review source (human-written) software, and not compiled [machine code](http://en.wikipedia.org/wiki/Machine_code). A [program](http://en.wikipedia.org/wiki/Software) called a [compiler](http://en.wikipedia.org/wiki/Compiler) is used to create the latter from the former, and the compiler is usually trusted to do an honest job. However, as he demonstrated, this trust on the compiler to do an honest job can, and has, been abused.

**Inserting backdoors via compilers**

As an example, Sophos labs discovered a virus attack on Delphi in August 2009. The W32/Induc-A virus infected the program compiler for [Delphi](http://en.wikipedia.org/wiki/Delphi_(programming_language)), a Windows programming language. The virus introduced its own code to the compilation of new Delphi programs, allowing it to infect and propagate to many systems, without the knowledge of the software programmer. An attack that propagates by building its own [Trojan horse](http://en.wikipedia.org/wiki/Trojan_horse_(computing)) can be especially hard to discover. It is believed that the Induc-A virus had been propagating for at least a year before it was discovered.

While backdoors in compilers are more frequent than backdoors in standards, they are not as prevalent as backdoors in open-source software. Enterprises freely trust closed- and open-source software as evidenced by its extensive use today. In our experience, we have not come across any corporate enterprise that does not use (and hence trust) at least some open-source software today.

**The open-source conundrum**

The global software contributor base and publicly reviewable source code are both hallmarks of an open-source ecosystem that actually provides transparency and value for free. Yet, these are the same characteristics that pose the biggest risk of backdoor exploits into enterprises by malicious actors intent on capturing competitive advantage. Unlike surpassing huge barriers in influencing (or writing) an industry standard, open-source projects enable someone to choose any of the millions of open-source projects (> 300,000 hosted in SourceForge alone, at last count) in hundreds of mirror sites opening up a broad surface area of attack.

One of the earliest known open-source backdoor attacks occurred in none less than the Linux kernel — exposed in November 2003. This example serves to show just how subtle such a code change can be. In this case, a two-line change appeared to be a typographical error, but actually gave the caller to the sys\_wait4 function root access to the system.

**Hiding in plane sight***Given the complexity of today’s software, it is possible for backdoors to hide in plain sight.*

More recently, there have been many backdoors exposed including an incident last September with an official mirror of SourceForge. In this attack, users were tricked into downloading a compromised version of phpMyAdmin that contained a backdoor. The backdoor contained code that allowed remote attackers to take control of the underlying server running the modified phpMyAdmin, which is a web-based tool for managing MySQL databases. In another case that came to light as recently as August, 2013, a popular open-source ad software (OpenX) used by many Fortune 500 companies including was determined to have a backdoor giving hackers administrative control of the web server. Worse than the number of these backdoors is the time elapsed between the planting of the backdoor and the actual discovery of the backdoor. These backdoors often go unnoticed for months.

**How to prevent backdoor attacks**

The reality in today’s enterprise is that software projects/products that have little or unknown trust are leveraged every day. We have found that many of these backdoors elude malware detection tools because there are no executables, Enterprises must now look for new ways to track the open-source projects that enter their enterprise from external untrusted sources, such as open-source code repositories and must be able to rapidly respond to any backdoors discovered in these projects. If not, these backdoors have the potential to inflict serious and prolonged harm on the enterprise.