Locking the backdoor: Reducing the risk of unauthorized system access

There are multiple kinds of "backdoors" that can be used to compromise the security and privacy of a system. While many of these secret access methods are put in place by vendors and service providers, some backdoors create a remotely exploitable vulnerability that gives an attacker root system access. These backdoors -- which have existed for most of the modern computing era -- have become a hot security topic in the wake of an NSA scandal.

> A backdoor is a secret way into a network, application or system that nobody else knows about -- at least, in theory.

In this tip, we'll look at the history of IT backdoors, the threats they pose to enterprises and what can be done to mitigate the risks.

How it all began: History of IT backdoors

A backdoor is a secret way into a network, application or system that nobody else knows about -- at least, in theory. Backdoors are often implemented for support purposes, created accidently while debugging or inserted intentionally by an attacker. Examples of backdoors have been found in software, hardware and virtually every other kind of electronic system since the dawn of the computing era.

The first widely acknowledged backdoor was created in 1984 by computer science pioneer Ken Thompson. During his acceptance speech for the Association for Computing Machinery Turing award, Thompson revealed he inserted a virus into a C compiler to create a backdoor when login information was being complied. Dubbed the "Trusting Trust" compiler, Thompson's backdoor ran unnoticed and took advantage of a trusted tool, demonstrating how trust should remain relative in the computing world.

Since then, many other backdoors have emerged. An example of a software backdoor in popular culture was featured in the movie *Wargames*. A user account named Joshua was hardcoded into the system for the creator to use if he needed it; as luck would have it, the account was exploited by Matthew Broderick's character to gain unauthorized system access.

There are frequent questions about potential existence of software backdoors in operating systems, especially when the government is involved. At the 2013 LinuxCon and CloudOpen North America conference, a roundtable discussion of U.S. backdoors led to an interesting response by Linux project coordinator Linus Torvalds. Did he confirm what many security pros have suspected for years? You be the judge.

Yet software backdoors aren't the only topic of concern. While hardware backdoors are less common, they have also made the news. When the Data Encryption Standard was proposed in 1975, it was alleged that the NSA weakened the DES algorithm s-boxes so it would be easier for it to break them. In 1993, there were fears that the NSA created the "Clipper Chip" as a government backdoor to bypass encryption. In 2012, the Chinese government was accused of inserting backdoors in Huawei products.

Not all backdoors are used for malicious acts, however. A number of known backdoors are

put in place by vendors and service providers. These are created for the convenience of support staff and are often shared widely at the vendor level, and are sometimes even publicly known. (For a list of known backdoor support accounts credentials, check here.)

More information on backdoor threats

Good and bad backdoors

Research on Coding Backdoors Presents Ugly Picture

Conducting APT detection when Elirks, other backdoors hide traffic

Promiscuous-mode sniffing backdoor

Backdoors also exist in networks that allow a connection from a certain IP range or using a certain port knocking to bypass network access controls. Even the law enforcement wiretapping capabilities enabled by the Communications Assistance for Law Enforcement Act could be seen as a backdoor because an unauthorized party could use it to eavesdrop on communications by an unauthorized party.

The threats backdoors pose to enterprises

At the risk of stating the obvious, backdoors present significant risks to enterprises because potentially anyone that knows or finds out about one could abuse it and not be easily detected.

Whether an attacker exploits a vendor-created backdoor or inserts his own, he can gain complete access to a system and then use it as a starting point to attack other enterprise resources and completely compromise the security of the enterprise.

Unfortunately, some known backdoors can't be disabled and require additional security measures to reduce threats.

How to minimize the risks

There are many steps IT administrators can take to mitigate the risks from both known and unknown backdoors. One of the most important practices an enterprise should adopt is monitoring.

Monitoring is highly effective for detecting known backdoors, though it can be hard to accomplish. To do this, monitor the processes on a given system and identify which ones are running under an account not contained in the system's password file. Alternative communication channels (e.g., modems) that are not regularly monitored should also be limited or prohibited.

Furthermore, IT admins can reduce the risks of backdoors implanted in products they use in their environment by:

- Using multiple vendors to limit the risk of a common backdoor across different systems
- Changing default passwords on backdoor support accounts to prevent unauthorized access
- Installing open source software
- Checking software integrity signatures
- Scanning for known backdoors
- Monitoring the network for suspicious communications

In addition, it would be wise for admins to employ a vulnerability scanner or configuration

management tool that identifies known backdoors and can potentially detect and disable them. Vendors should be required to use strong software development lifecycles to minimize the chance of an unauthorized backdoor being inserted or a debug functionality being introduced for a backdoor and not removed when released to the customer's production environment.

For enterprises with the highest security requirements, it may be necessary to either perform an internal audit or employ a third-party audit to look for backdoors in source code and closed source products and systems.

Bottom line

The IT supply chain is surprisingly fragile. Consumers and enterprises must trust that there are no known backdoors inserted into their products by their vendors. And to take it a step further, organizations must trust that their service providers and government agencies won't utilize backdoors either. Given the current scope of things, it's easy to understand why IT admins are taking caution.

Backdoors will continue to be a risk to enterprises for as long as computers are used. However, planning early on and securing an enterprise from backdoors of all shapes and sizes can help significantly lower the potential risks.

About the author:
Nick Lewis, CISSP, is the information security officer at Saint Louis University. Nick received his Master of Science in information assurance from Norwich University in 2005, and in telecommunications from Michigan State University in 2002. Prior to joining Saint Louis University in 2011, Nick worked at the University of Michigan and at Boston Children's Hospital, the primary pediatric teaching hospital of Harvard Medical School, as well as for Internet2 and Michigan State University.