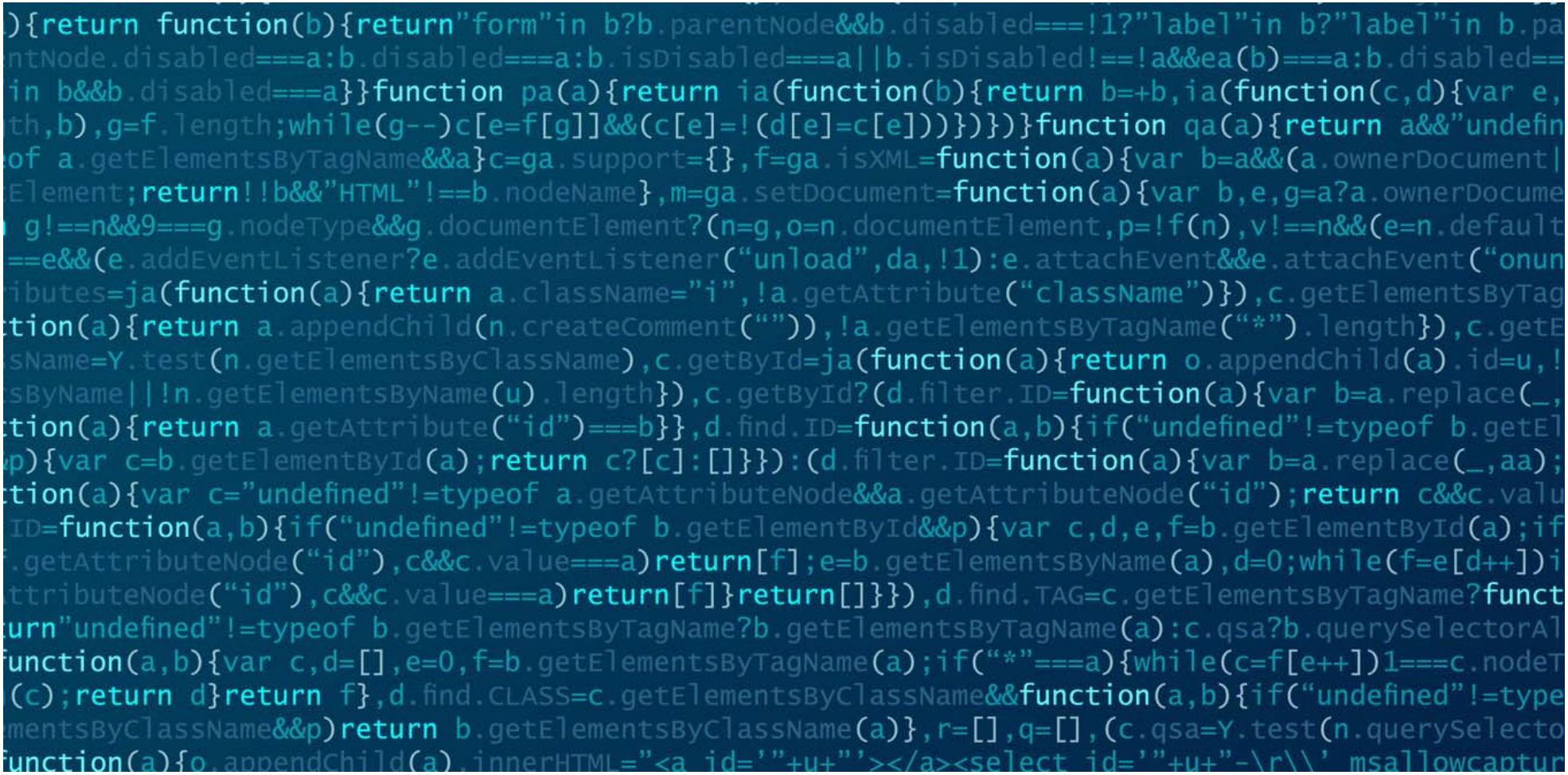
THE CONVERSATION
Academic rigor, journalistic flair



From botnet to malware: a guide to decoding cybersecurity buzzwords

May 31, 2017 4.09pm EDT

Cybersecurity jargon can be intimidating, but it needn't be. www.shutterstock.com

Words like worm, trojan horse and zombie may seem like the stuff of science fiction, but they're part of the reality of life online.

Now that we communicate, work and entertain ourselves on the internet, these familiar terms start to take on new meaning. They're just a few of the cybersecurity threats we face.

While most of us would rather leave the problem to the IT department, it's essential we all have an understanding of cybersecurity so we can protect ourselves, and that means understanding some key terms.

This glossary, which is by no means exhaustive, is a first step.

The cybersecurity glossary

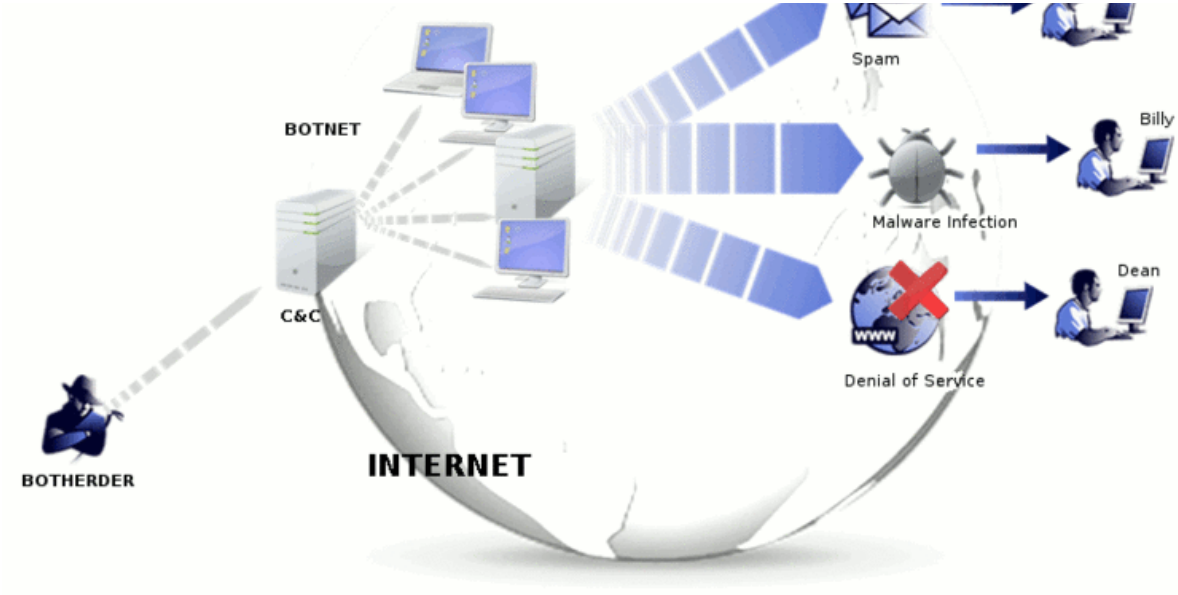
Backup: Ensuring all important data is stored in a secure, offline location to protect it from being lost, if a computer is hacked. It's important to routinely copy files to a USB flash drive, for example, or secure them in cloud storage.

Blackhat hacker: A person who uses programming skills to cause damage to a computer system, steal data and in general conduct illegal cyber activities.

Botnet: A grouping of computer systems, potentially anywhere in the world, that has been infected by a malicious piece of software. This software allows them to be networked together by the hacker (or bot-herder), giving them full control of all the "bots" in the network to conduct malicious tasks, including denial of service attacks (see below).

Author

Nicholas Patterson
Teaching Scholar, Deakin University

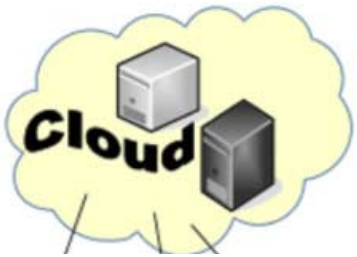


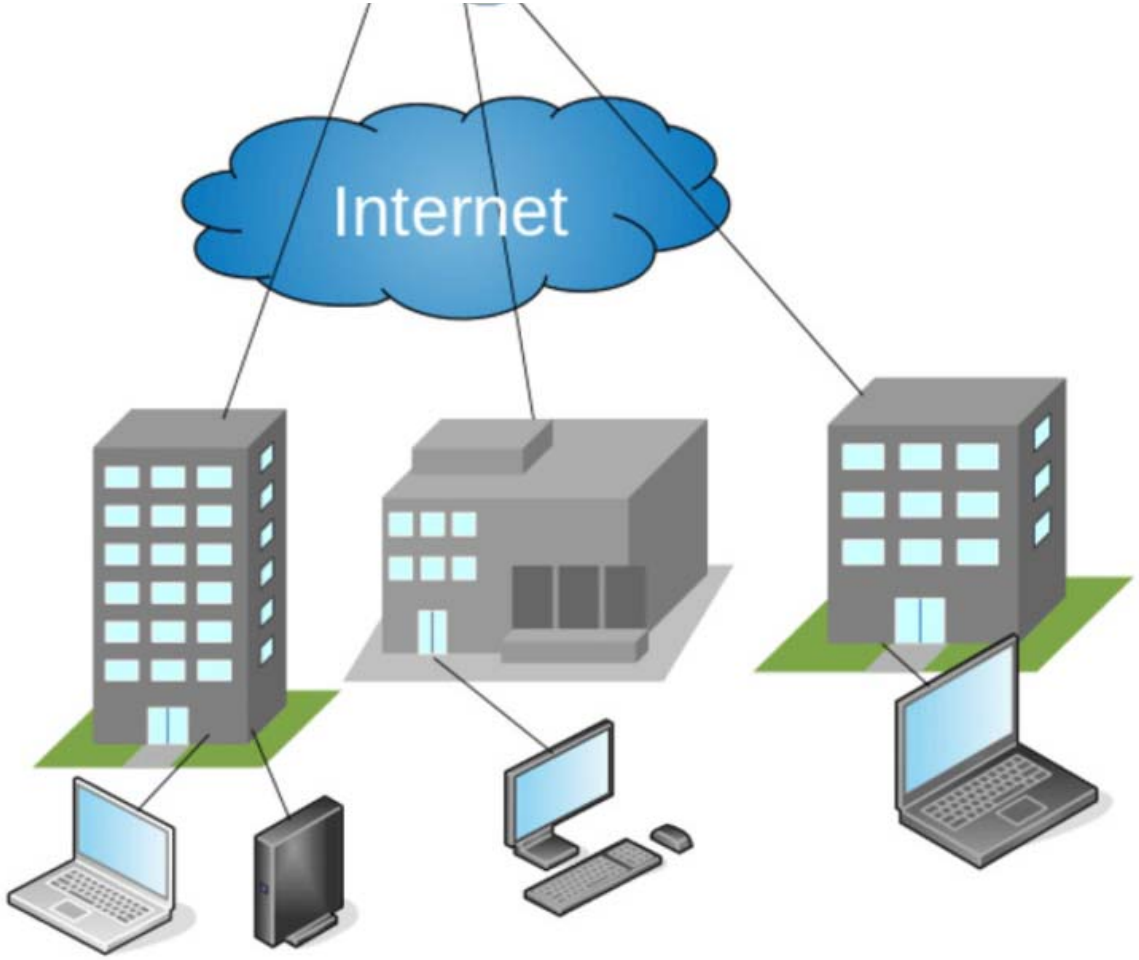
Botnet's can be used for all kinds of malicious activities. JeroenT96/Wikimedia Commons, CC BY

Breach: The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.

Brute force attack: A technique a hacker can use to break into a computer system. They do this by trying to "guess" its password (either manually or with a computer application).

Cloud: A technology that allows us to access our files through the internet from anywhere in the world. More technically, it is a collection of computers with large storage capabilities that remotely serve customer file requests.





Cloud computing lets you access your data from anywhere in the world. Rr 750~commonswiki/Wikimedia Commons, CC BY-SA

Command-and-control server: An application that controls all bots in a botnet (see above). The hacker will send a command through this server, which then relays it to all compromised computers in the network.

DDoS: An acronym that stands for distributed denial of service – a form of cyber attack. This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from

multiple sources (often botnets).

Domain: The networking of computers and devices. A domain is a group of computers, printers and devices that are interconnected and governed as a whole. Your computer is usually part of a domain at your workplace.

Encryption: An algorithmic technique that takes a file and changes its contents into something unreadable to those outside the chain of communication. If we use a Caesar cipher on the word "hello", for example, we can replace each letter with a fixed number of places in the alphabet. The encrypted form of "hello" would become "ifmmp".

The Caesar cipher.

Exploit: A malicious application or script that can be used to take advantage of a computer's vulnerability.

Firewall: A defensive technology focused on keeping the bad guys out. A "wall" or filter is created that judges each attempted interaction with a user's computer and internet connection to determine "should this be allowed entry or not?" Firewalls can be hardware or software-based.

Firewalls put a filter between you and the public internet. Luis F. Gonzalez/Wikimedia Commons

Honeypot: A defensive cybersecurity technique. This technology is essentially a computer (server) that is set up to look like a legitimate and high value target on a network. The aim is to entice hackers to focus on this computer and not on actual high value computers or data. The bonus is that administrators can watch hackers in the act and learn to protect against their techniques.

https:// versus http:// Two online standards that allow computers to communicate.

HTTP is defined as Hypertext Transfer Protocol. Its most popular use is online to help internet browsers communicate. For example, to send you web pages from the associated computer hosting the web site you're visiting.

HTTPS is similar, but it adds security, hence the "S". It encrypts all data by creating a secure tunnel between you and the website you're visiting, and is commonly seen in online shopping stores where security is required.

IP Address: An internet version of a home address for your computer, which identifies it when it's connected to the internet.

Patch or Update: Most software requires thousands of lines of programming language to create, so it's difficult for a developer to ensure all possible vulnerabilities are covered. When entry points are discovered by hackers or the developer themselves, software vendors will often release new pieces of software as a fix.

Phishing or spear phishing: A technique used by hackers to obtain sensitive information, including passwords, bank accounts or credit cards.

Often an unexpected email is received disguised as being from a legitimate source. In many cases, the hacker will attempt to trick you into either replying with the information they seek, like bank details,

or tempt you to click a malicious link or run an attachment.

Spear phishing is a variant of this technique, but the hacker targets a business or person specifically, instead of taking a blanket approach.

What is phishing.

Malware: An umbrella term that describes all forms of malicious software designed to cause havoc on a computer. Typical forms include viruses, trojans, worms and ransomware.

Ransomware: A form of malware that deliberately prevents you from accessing files on your computer. If a computer is infected by malware designed for this purpose, it will typically encrypt files and request that a ransom be paid in order to have them decrypted.

Spoofing: A technique hackers use to hide their identity, pretend to be someone else or simply try to fool you over the internet.

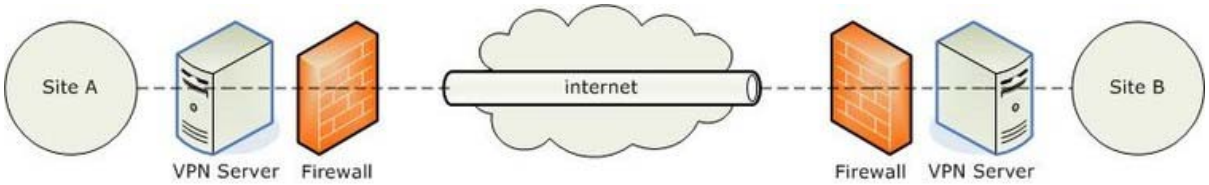
There a number of spoofing methods, such as making a hack look like it's coming from another source, sending emails that appear to come from a different person, and website spoofing, where hackers set up a fake website to trick users into entering sensitive information.

Software: A set of instructions that tell a computer to perform a task. These instructions are compiled into a package that users can install and use. Software is broadly categorised into system software like Microsoft Windows and application software like Microsoft Office.

Trojan horse: A piece of malware that often allows a hacker to gain remote access to a computer. The system will be infected by a virus that sets up an entry point for the perpetrator to download files or watch the user's keystrokes.

Virtual Private Network: A tool that allows the user to remain anonymous while using the internet. It does this by masking location and encrypting traffic as it travels between the user's

computer and the website they're visiting.

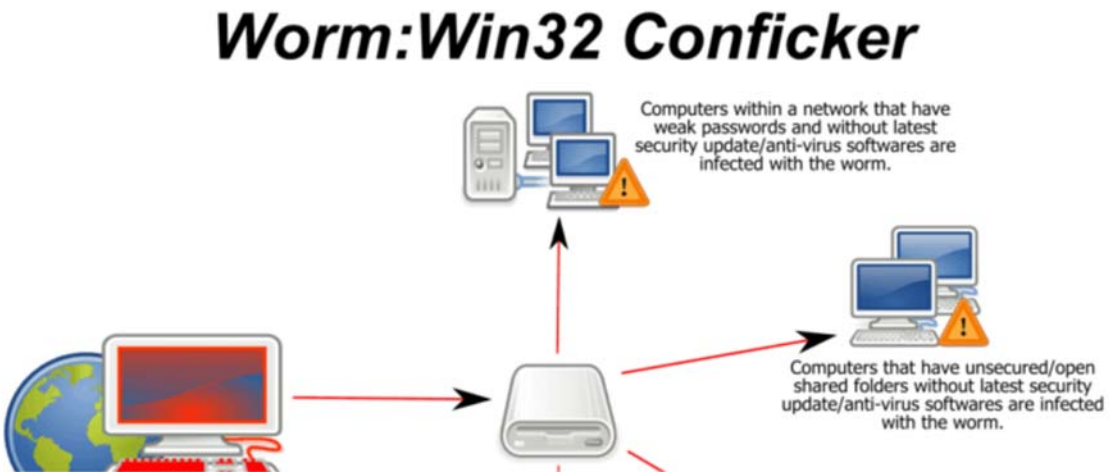


Demonstration of where a VPN operates in a normal internet connection. Wikimedia Commons/Philippe Belet

Virus: A type of malware for personal computers, dating back to the days of floppy disks. Viruses typically aim to corrupt, erase or modify information on a computer before spreading to others. However, in more recent years, viruses like Stuxnet have caused physical damage.

Vulnerability: A weakness in computer software. Eventually, if you do not keep your systems up to date, you will have vulnerabilities. Say you're using Microsoft Windows 7 but are failing to install updates – your system could exhibit vulnerabilities that can be attacked by a hacker because security safeguards are out of date.

Worm: A piece of malware that can replicate itself in order to spread the infection to other connected computers. It will actively hunt out weak systems in the network to exploit and spread. Below is an example of a common worm, named the Win32 Conficker.



Example of how the Win32 Conficker worm operates. Gppande/Wikimedia Commons, CC BY-SA

Whitehat hacker: A person who uses their hacking skills for an ethical purpose, as opposed to a blackhat hacker, who typically has a malicious intent. Businesses will often hire these individuals to test their cybersecurity capabilities.

Zero Day: A particular form of software exploit, usually malware. What makes a zero day exploit unique is that they are unknown to the public or the software vendor. In other words, because few people are aware of the vulnerability, they have "zero days" to protect themselves from its use.

Zombie: A computer system that has been infected by malware and is now part of a hacker's botnet.

There are still many cybersecurity terms to tackle, but this will get you started. Next time someone mentions "phishing", you'll know they are not talking about the water-related hobby.

Encryption **Cybersecurity** **Hackers** **data** **Viruses** **botnet** **VPNs** **Phishing** **Great Firewall of China** **Distributed Denial of Service (DDoS) Attack** **Technology explainer**