The Fulcrum Group, Inc.
(817) 337-0300

3 Big Bugs Of The Past Year: *Cryptolocker, Heartbleed and Bash*

What they are, and what to do
to ensure your systems are safe.

This White Paper is brought to you by your friends at The Fulcrum Group, Inc.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5600 Egg Farm Rd., Suite 452, Fort Worth TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

3 Big Bugs of the Past Year

Cryptolocker

In fall of 2013, **Cryptolocker** ransomware came to light. *Ransomware* is a software that locks you out of something until you give it what it wants (usually money).

Spread via malicious email attachments, or deployed by hacked and malevolent web sites, ransomware scans the drives of your PC (hard drives, flash drives, even network shares) for certain file types and encrypts them – think of it as the malevolent version of similar techniques that encrypt files for your safety. Cryptolocker left its victims with nothing but a notice about the foul act it just performed. The notice allowed for about 3 days to pay up, or the virus deleted their side of the encryption key.

While the original Cryptolocker infection was effectively brought down in late May, 2014, malware variants and imitators within this category continue to flourish, and not only in Windows Operating Systems – but also targeting popular Network Attached Storage (NAS) systems and smart phones and tablets that use the Android Operating System. Companies are beginning to develop programs which may be used to decrypt ransomware encrypted files, however there is no single silver bullet yet.

Your best defense against this type of brute force attack is to:
keep all of your systems ***patched and updated****, making sure your* ***antivirus is active*** *and up to date as well; regularly* ***back up*** *your system files; and please always use (and make sure your employees use)* ***good online safety protocol*** *such as avoiding opening unexpected attachments.*

Heartbleed

In April, 2014, we first alerted you to the **Heartbleed** bug, the name given to the massive OpenSSL exploit that left huge portions of the web, and thus its users, vulnerable.

Attackers could grab important information from a susceptible server, including encryption keys that could unlock access to usernames, passwords and other data that should be encrypted.

The bug sat dormant for nearly two years before being uncovered in April.
By June 2014, reports by security researchers revealed that approximately 300,000 web servers were still in need of remediation.

A solid course of action against Heartbleed remains:

- *If you have Google Chrome configured as your browser, configure it to* ***detect certificate revocation*** *(so you can see still-compromised sites).*
- *Consider the sites, hosted applications and publicly available systems in which the vulnerability was detected and* ***change your passwords*** *(however, don't do it from a compromised device).*
- *Go through public systems and* ***remediate*** *(if a patch is available).*
- *Go through any private network systems and* ***remediate*** *(if a patch is available).*

Bash/Shellshock

Our most recent blog on the latest of these 3 big bugs, the **Bash Bug (aka, "Shellshock")** explains it well: Bash stands for Bourne-Again SHell. In simplest terms, a computer program that allows users to type commands and executes them. Shellshock is a nickname for a bug in the Bash (Bourne Again SHell) command-line interpreter, also known as a shell.

The quarter-century-old security flaw allows malicious code execution within the bash shell (commonly accessed through Command Prompt on PC or Mac's Terminal application) to take over an operating system and access confidential information. The Bash shell can also be found on many other systems, from Windows to Android. However it is not installed and/or used by default on these systems.

Bash/Shellshock Action Items:

You can find a list of links to common vendors and their remediation efforts on our blog at ***http://www.fulcrum.pro/bash-shellshock-resources/*** *.*

Red Hat has an excellent guide on how to determine if your system is unpatched and vulnerable at ***https://access.redhat.com/articles/1200223*** *.*

If you cannot patch Bash, or a patch is not available for your platform, consider switching to another shell.

Be sure to check out the Security page on our website at **http://www.fulcrum.pro/resources/security/** for an always updated wealth of general security resources. If you don't already have an IT security team in place, we urge you to reach out for expert assistance.   As always, if you have any questions or would like to speak to someone in person (or try out the live chat feature on our website), you'll find us here at The Fulcrum Group, ready to assist you.