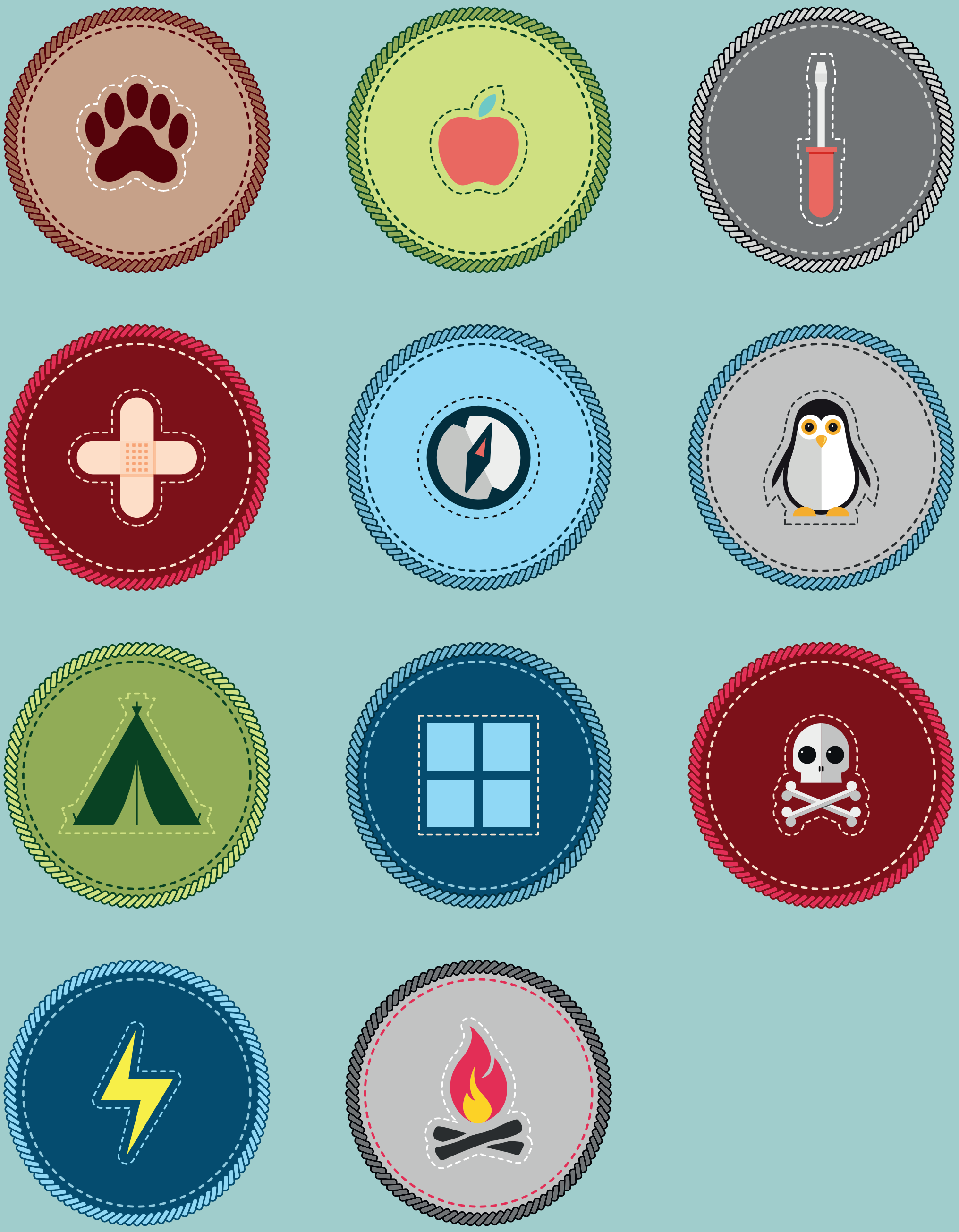


Whitepaper:

I patch. Do you?

Patching for businesses – from manual to automated

GFI LanGuard™

Network security scanner and patch management

No single piece of software is flawless. Be it an operating system, your favourite office suite, accounting applications or a computer game, somewhere in that codebase are errors that slip through the Q&A net. Unfortunately, these errors are often found by hackers and cybercriminals who write malware to exploit those weaknesses.

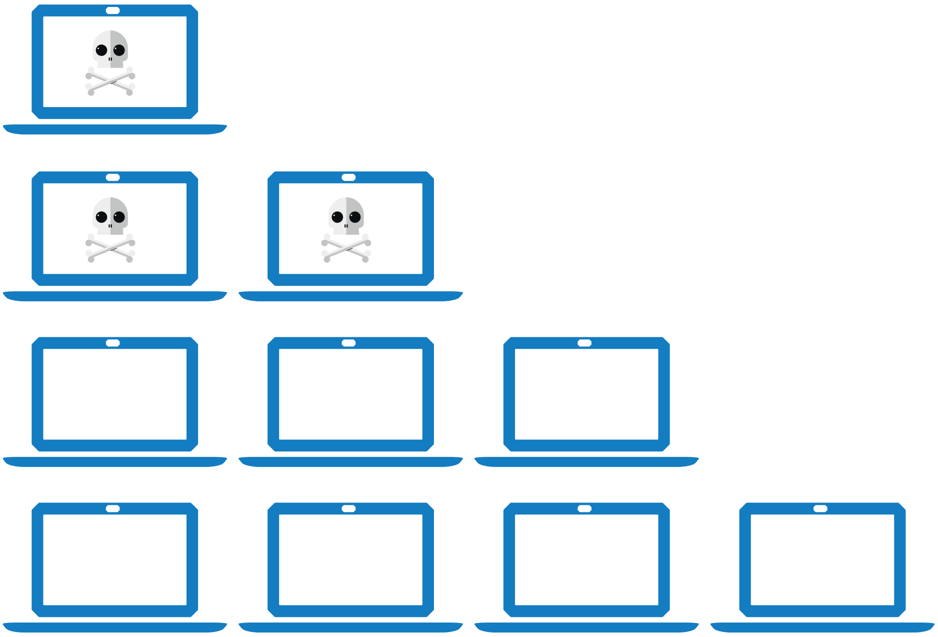
It's really a cat-and-mouse game between the vendors and the bad guys. The latter find a hole, while the former rush to release a fix or patch to close it before some organization feels the brunt of a malware infection.

The key to limiting the damage and preventing the bad guys from taking advantage of known exploits is to make sure that every OS and piece of software on a computer network has the latest patches and fixes. While having a firewall and antivirus installed network-wide is important, they can be rendered almost ineffective if the software used is not updated and has an 'enter here' written all over it.

Not only is patching and vulnerability management a recommended defense against malware attacks by leading organizations and governments but patching is a must-do on the checklist of various regulations and laws, like Sarbanes-Oxley.

Despite fair warning, widely available tools and best practices, many businesses continue to fall victim to cyberattacks. They are often surprised that incidents happen because they have a firewall, AV and other security measures in place and think that they are fully protected.

Unfortunately, a single email with links to compromised servers is enough to open up a backdoor for a hacker to come in and probe the network for weaknesses.



Firewalls, antivirus and even expensive Intrusion Detection/ Prevention Systems are only effective about 70% of the time.[i] That means that malware is making its way on desktop machines and servers three times out of 10.

This is extremely frustrating for system administrators and security professionals who feel they are given no respite and are faced with continuous threats of a cyberattack. A number of recent incidents, such as the Target breach, are believed to have exploited weaknesses in either the operating system or one of many software packages that are in use by businesses (and home users) worldwide.

> “Firewalls, antivirus and even expensive Intrusion Detection/ Prevention Systems are only effective about 70% of the time.”

And these attacks are successful not because their AV or firewall failed them but because THEY failed to patch known holes in the most common software products. Looking for vulnerabilities and applying a patch to fix it is a must in this day and age, yet many companies do not even perform basic patch management.

The sad reality is unpatched systems have led to some of the largest data breaches with severe economic consequences for those organizations.

Take for instance "Paunch" (the alleged creator of the BlackHole Exploit Kit), who was recently arrested by Russian Police. His BlackHole Kit is commercial crimeware designed to be stitched into hacked or malicious sites in order to exploit a variety of Web-browser vulnerabilities. His clients can then choose what malware they want to have installed on the target machines. A more recent version of BlackHole attacked known vulnerabilities in Java, Flash, Windows OS, Adobe Reader and Internet Explorer. Those organizations with systems that are not patched and updated, can easily become another victim of the BlackHole Exploit Kit. The statistics don't lie: it is estimated that Paunch and his gang earned more than $2.3 million USD.[ii]

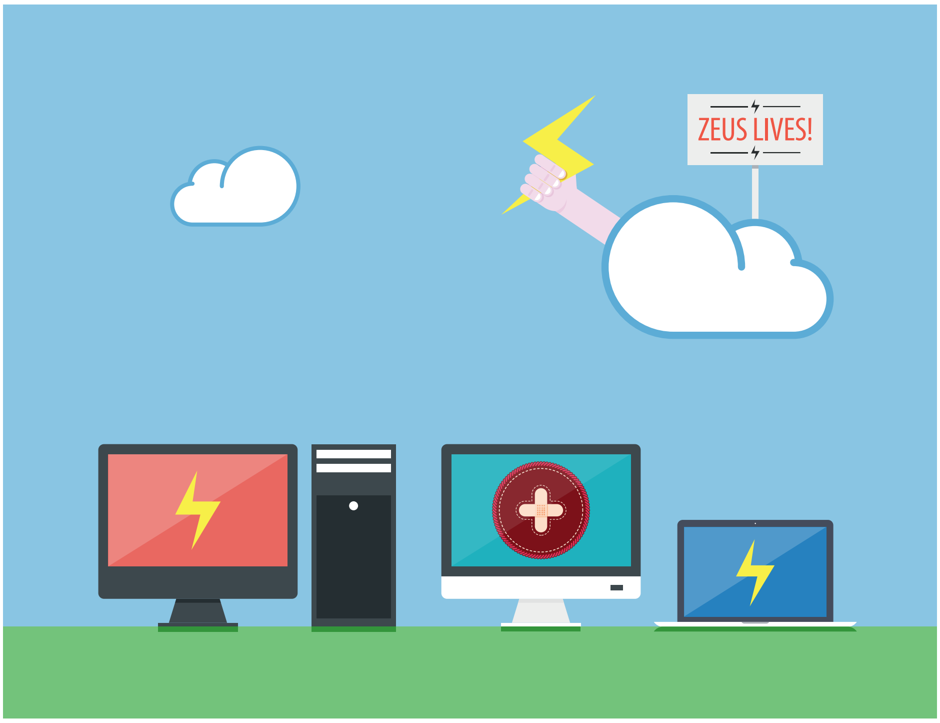
Exploiting a machine is the first step. Once their foot is in the door, it's time to wreak havoc. Most cybercriminals are not interested in 'destroying' anything – they are more interested in collecting stuff that could make money for them.

> “In 2012, Microsoft said Zeus had infected more than 13 million machines, 3 million of which are U.S.-based computers.”

For example, Zeus, also known as Zbot, is the name of an underground toolkit used to create information-stealing Trojans. The bots created by the kit run silently in the background on compromised computers, harvesting information and sending it back to the cybercriminal. The main focus is to steal online banking details and other login credentials however the tool kit has many additional features. In 2010, more than 100 people were arrested on charges of conspiracy to commit bank fraud and money laundering. Members of the ring had stolen $70 million.[iii]

In 2012, Microsoft said Zeus had infected more than 13 million machines, 3 million of which were U.S.-based computers.[iv] Microsoft researchers found that once a computer is infected with Zeus, the malware automatically starts key logging when a person types in the name of a financial or e-commerce institution, allowing criminals to gain access to people's online accounts from that point forward.[v]

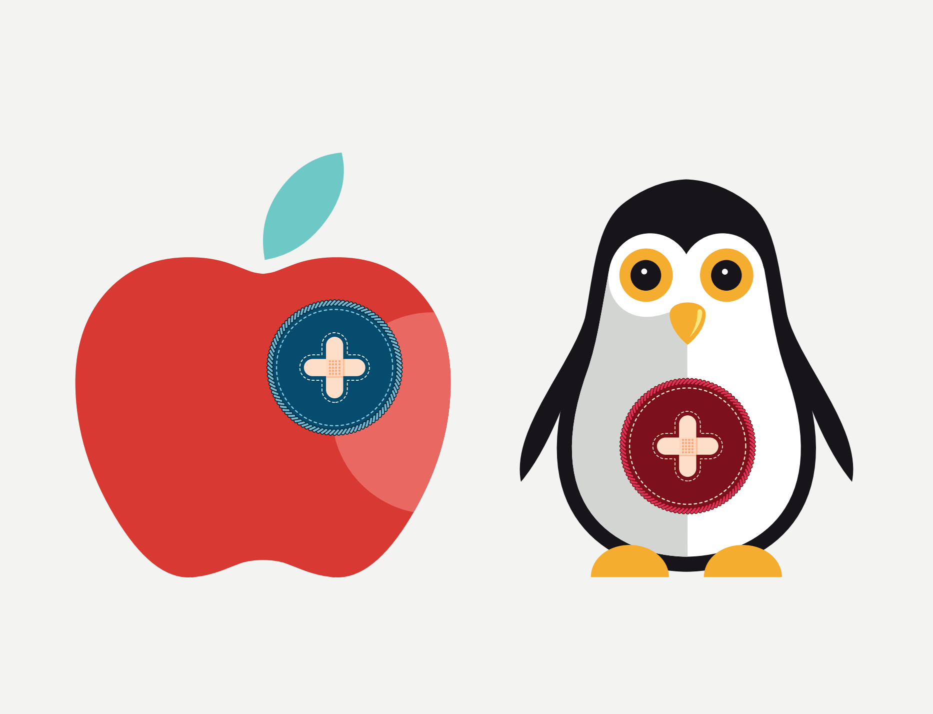
Trojans like Carberp, Citadel, SpyEye, and especially Zeus are among the most dangerous pieces of malware on the internet and most infections start because of an innocent user on an unpatched system visited a dangerous site infected with BlackHole, or some other exploit kit. [vi]



Trojans like Carberp, Citadel, SpyEye, and especially Zeus are among the most dangerous pieces of malware on the internet

The severity of these malware attacks has put the onus on vendors to develop tools that "auto-update" applications and the various Microsoft operating systems and products. Businesses should not rely on these features alone. Windows Software Update Service, also known as WSUS, is Microsoft's free answer to automated patching and updating of corporate system, but unfortunately it is not reliable, or robust enough to handle the modern day threats. Although it does a good job with MS products, it does not allow admins to patch third-party products like Java or Adobe.

Many organizations are reluctant to patch, or find it a time-consuming exercise that places productivity at risk because of a bad patch or incompatibility. IT admins are not happy allowing a piece of software to auto update when the vendor releases a patch or firmware update. And rightly so; because they have no assurance that the applications have been patched, and if they have, correctly or not. Another concern with auto updates is that if something goes wrong, can the admin reverse the changes without causing even more problems?



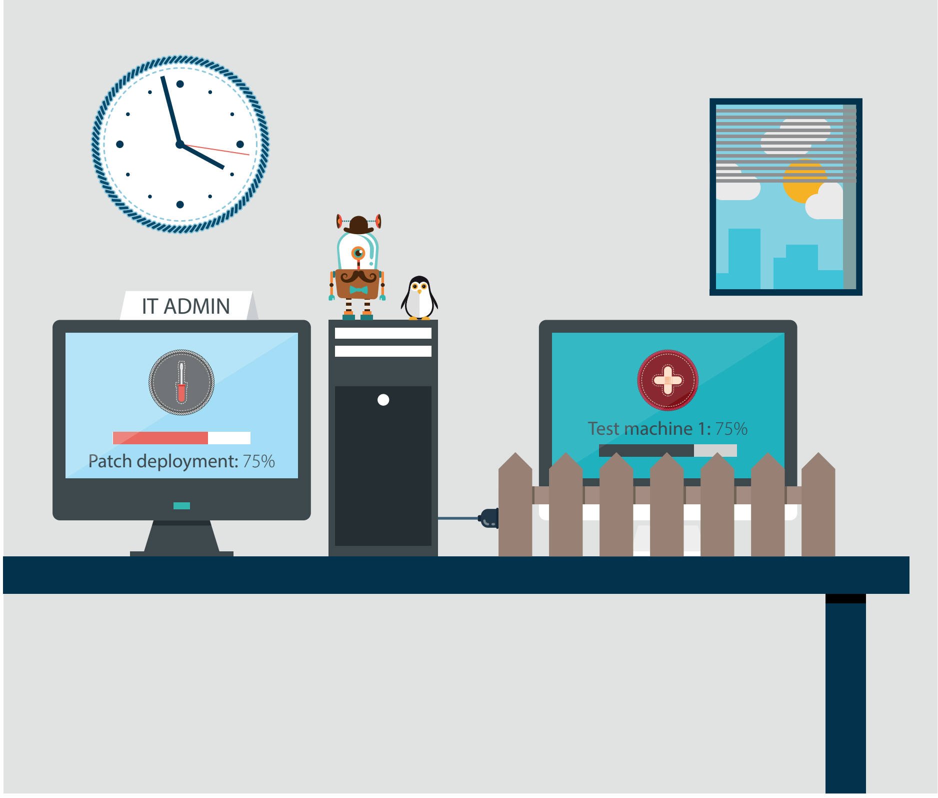
> “Criminals exploiting a vulnerability in Apple's OS X software built a botnet of at least 550,000 infected Macs”

The popularity of Apples Mac machines in the workplace, along with open source solutions like Linux present unique security challenges and corresponding need for a Apple or Linux skillset. Mac and Linux have patching requirements as well; and cyber criminals are targeting the Mac platform with Mac malware. Criminals exploiting a vulnerability in Apple's OS X software built a botnet of at least 550,000 infected Macs, according to research from a Russian security firm.[vii] The vulnerability was found in the Mac's Java version. So, just like Windows machines, Macs can be infected via bundled software belonging to 3rd party vendors.

Depending on the auto update feature is a bad mistake. There is an option, however. Using a scanning tool that identifies vulnerabilities and missing patches, informs the admin which patches are missing, and then automates the whole process of distributing the required patches to those machines that need updating.

Automation makes a huge difference when it comes to software patching. There is much less risk of human error, all actions are scheduled and predictable, and the admin benefits from extensive reporting functionality. All this is not available if an IT department is dependent on WSUS and auto-updates from the vendors (and applied by users).

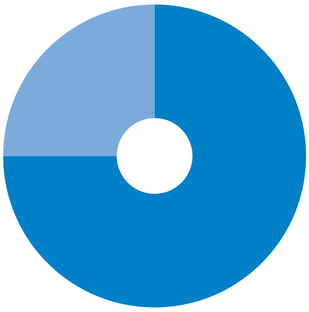
Patch testing is another advantage. One of the main advantages of a patch management tool is that it enables the admin to selectively deploy patches to just one or two workstations and see whether the patched worked or not. If it works fine, then the tool can be used to push the patch to all the machines on the network.



Another advantage of granular control of patch deployment is the ability to control which workstations receive which patches and when. You cannot do this with auto-updates.

To underscore just how important patching is, James A. Lewis, in his "Raising the Bar for Cybersecurity" suggests: "75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching."[viii] Regular vulnerability scanning (once a week) is important because it enables the admin to stay on top of changes to the network, to the software installed and user activity (deployment of authorized software).

Another advantage of regular scanning is that it can detect the presence of new software or configuration changes, which IT did not authorize. The machines of those employees with elevated privileges should be given particular attention. Changes they make to their machine or software they install could compromise the whole network.



75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching.

Of the top four things the Australian Government requires of all departments and contractors to do when it comes to Information Security, two of them directly relate to patch management and patch deployment. At least 85% of the intrusions that the Australian Signals Directorate (ASD) responded to in 2011 involved adversaries using unsophisticated techniques that would have been prevented if the top 4 mitigation strategies - application whitelisting, patching applications and operating systems and using the latest versions, and minimizing administrative privileges – was applied.[ix]

According to the Australian Department of Defense, "the top four mitigation strategies are highly effective in helping achieve a defense-in-depth ICT system. The combination of all four strategies, correctly implemented, will help protect an organization from low to moderately sophisticated intrusion attempts. Put simply, they will make it significantly more difficult for an adversary to get malicious code to run on your systems, or continue to run undetected. This is because the Top 4 strategies enable multiple lines of defense against cyber intrusions"[x]

Although the majority of SMBs do not face the same threat level as the Australian government does, it doesn't mean they cannot be attacked or will not be attacked at some point. Cybercriminals take the path of least resistance and most attacks are successful because systems are poorly secured. From a cybercriminal's perspective, the stronger the defenses, the tougher the target.

Cybercriminals are always probing systems for weaknesses and backdoors. It only takes one breach to cripple a company, and that is why the argument in favor of a patch management tool is so strong. A couple of thousand dollars is nothing compared to losing millions and the organization's credibility.

If you don't have a proper patch management strategy in place, it's high time you did something about it. Invest in a proper tool. Scan your network regularly. Apply patches as soon as possible after they are released.

Options for small and medium businesses (SMBs)

GFI LanGuard is an award-winning automated vulnerability scanning and patching platform. It's a powerful, one-stop shop for automated network security management, that provides vulnerability assessment, patch management, asset audit and management and problem remediation, all from the same powerful console. To further enhance security for small to mid-sized businesses, it can integrate with anti-virus/malware, anti-spyware and personal firewall, as well as GFI EventsManager which provides log management, and GFI EndPointSecurity which provides device blocking.

A proper patch management strategy

1. Invest in a proper tool

2. Scan your network regularly

3. Apply patches as soon as possible after they are released

About GFI Software

GFI Software™ develops quality IT solutions that enable businesses to monitor, manage and secure their networks with minimal administrative overheard. Serving an expanding customer base of tens of thousands of companies, GFI focuses on scalable communications and security platforms comprising network security, web management, anti-spam, patch and vulnerability management, faxing and archiving solutions. GFI is a channel-focused company with thousands of partners worldwide. The company has received numerous awards and industry accolades, and is a longtime Microsoft® Gold ISV Partner.

i. http://www.v3.co.uk/v3-uk/news/1946978/rsa-2010-encryption-anti-virus-failing
ii. http://beta.slashdot.org/story/195323
iii. http://abcnews.go.com/Blotter/fbi-crime-ring-stole-70-million-computer-virus/story?id=11777873
iv. http://phys.org/news/2012-03-hacker-servers-seized-microsoft.html
v. http://transition.fcc.gov/cyber/cyberplanner.pdf
vi. http://blog.kaspersky.com/the-big-four-banking-trojans/
vii. http://www.pcpro.co.uk/news/security/373942/criminals-build-mass-mac-botnet
viii. http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf
ix. http://www.asd.gov.au/infosec/top35mitigationstrategies.htm
x. http://citadel-information.com/wp-content/uploads/2012/08/top-4-mitigation-strategies-to-protect-sensitive-information-2011-australian-defense-2011.pdf

www.gfi.com

For a full list of GFI offices/contact details worldwide,
please visit: www.gfi.com/contact-us

Disclaimer.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.