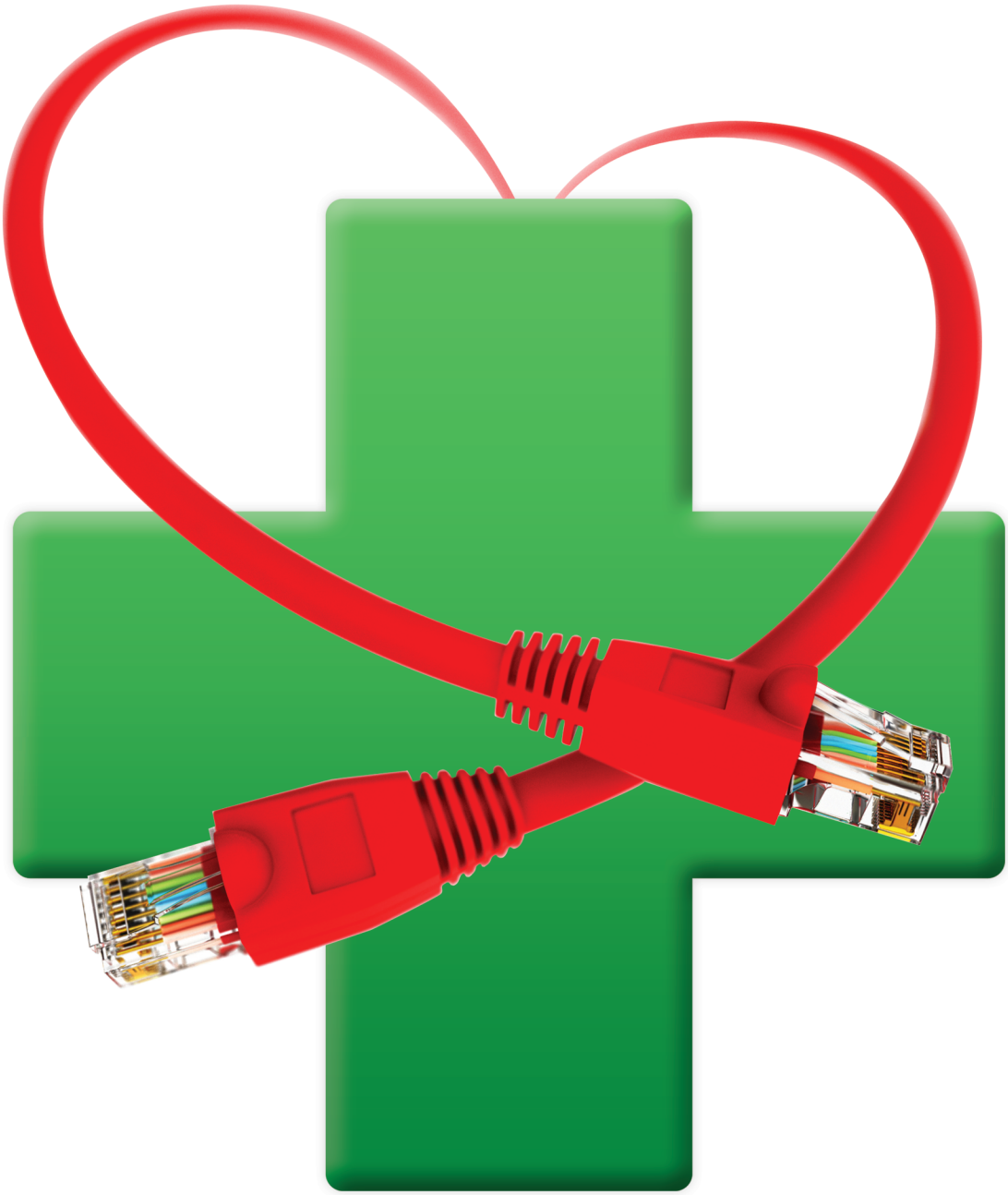
FIRST AID KIT
FOR SYS ADMINS



GFI LanGuard™

e-book: A GFI Software™ publication

First aid kit for sys admins

Sys admins have to deal with network and security emergencies every so often, so here's a first aid kit with a number of tips on how to handle various emergency scenarios and the necessary steps to take.

Contents

When disaster strikes

You've found a virus running on your server. You discover logon IDs on your network that you don't recognize and you can't delete them. The logs say someone accessed the payroll admin's computer and copied the master earning report. A hacker emails you saying they have your credit card database. Any one of these is enough for you to hit the panic button and lose it – don't. These things happen, and when they do, just keep a cool head on your shoulders and follow the established procedure for dealing with issues.

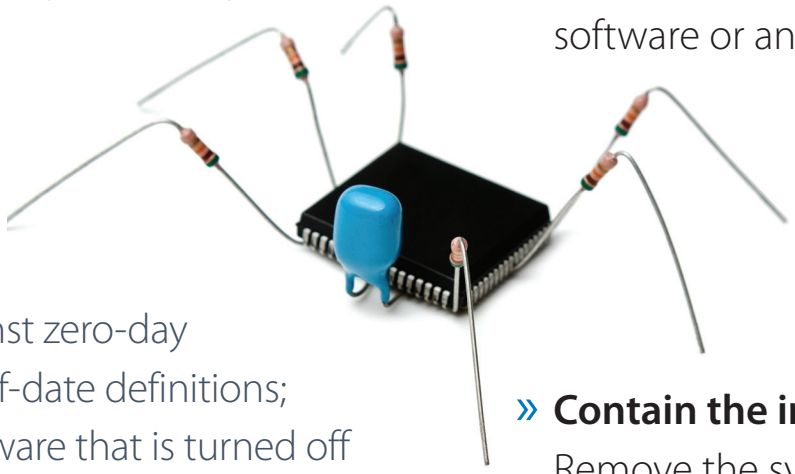
In our *First aid kit for sys admins*, we're going to give you the steps you need to take to provide immediate aid to hacked systems, infected workstations, compromised services and other computer emergencies that will come up from time to time in any network. There are eight steps to take for any incident:

1. Don't panic
2. Assess the situation
3. Keep the team informed
4. Take steps to minimize the damage
5. Determine the appropriate remediation response
6. Follow the appropriate steps for the situation
7. Learn from the incident
8. KEEP CALM AND CARRY ON

Like us on Facebook

Malware infection

Even companies that have antivirus running on all their servers and workstations may eventually experience a malware infection. A network that is not secured against zero-day attacks; out-of-date definitions; antivirus software that is turned off to speed up performance can all, in turn, lead to a malware infection – and that's without even talking about infected attachments in email, malicious files on USB drives, etc. Microsoft has a six-step incident response plan that works very well for most companies. Here are the highlights, along with a seventh critical step:



» **Confirm the infection.** Not everything that looks strange is caused by a virus. Confirm that the system is infected by scanning with your antivirus software or an emergency boot disk. If there is any doubt, err on the side of caution.

» **Contain the infection.** Remove the system from the network. Disconnect the Ethernet cable, disable the Wi-Fi and then shut the computer down until you can boot from known good media to proceed with remediation. You don't want the virus destroying other data on the PC, trying to spread to other systems on your network or spewing out spam to the Internet.

» **Determine the course of action.** Many IT professionals prefer to nuke a machine from high orbit, just to be sure, rather than attempting to clean an infection. However, there may be critical data on the hard drive which you have to back up first. If it is an application server you may not have the option to rebuild, so you will need to decide whether to clean the malware or restore from backup.

» **Attempt to clean the system.** Boot the system from a USB key or optical media that you have your antivirus software installed upon, with updated definitions, in case you cannot get network access. Some antivirus applications have the ability to create an emergency boot disk for cleaning infected systems, so check your chosen solution for that. Check whether you can clean the system this way, so that you don't have to rely upon the software on the PC that was already breached by the malware.

» **Attempt to restore the system state.** If you cannot clean the machine but you have a good backup, try restoring from that backup or disabling system restore.

» **Rebuild the system.** If you cannot clean or restore, you have no choice but to rebuild the system from scratch. Back up any critical files first, and then completely wipe the drive before beginning the install.

» **Conduct a post-attack review.** Fix the problem. Discuss how the malware got past your current defenses, and address the shortcomings to reduce the chance of this happening again.

Follow us on Twitter

You can **read the entire Microsoft article** that details these steps, and you can download useful supplemental content. You can also see **how to create a bootable Windows 7 USB key**.

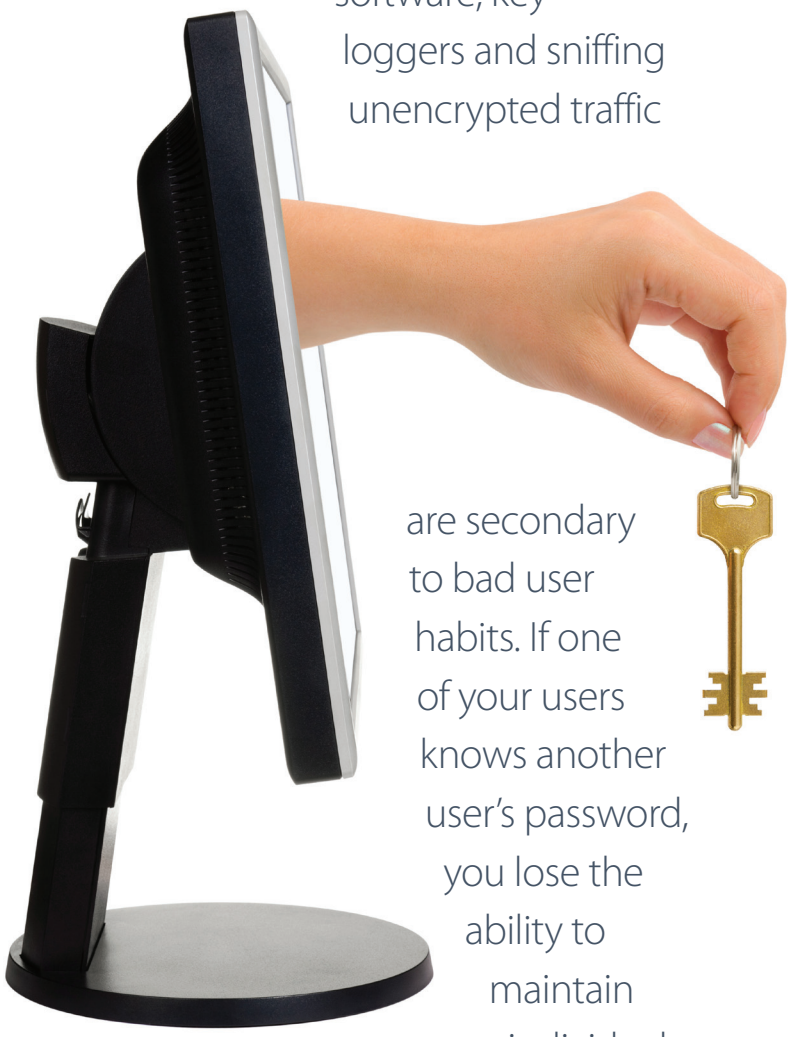
Helpful tools

Here are some helpful tools to assist you when dealing with an infected system:

- **PsTools** – This collection of tools can help you identify running processes, and more importantly, kill the ones that you don't want but cannot stop.
- **Netstat** – This article may be old, but the steps to use netstat to identify what processes are using the network are effective all the way through Windows 8.
- **What Process** – This website has a useful database of Windows processes to help you figure out what is running on your system.

Cracked passwords

There are lots of ways that passwords can be "cracked" and not all of them involve technology. Users write passwords down, share them with others and pick ones that can be easily guessed. Password cracking software, key loggers and sniffing unencrypted traffic are secondary to bad user habits. If one of your users knows another user's password, you lose the ability to maintain individual accountability, and you may have a situation where someone can now access data that they shouldn't. Here's how to handle this:



- **Force all users who might be impacted to change their passwords.** You can do this in AD (Active Directory) by simply ticking a box to require users to change their password at next logon.
- **Implement a strong password policy. Microsoft provides recommendations** as to what makes a strong password, as well as how to implement this with AD.
- **Remind users about your policy regarding securing passwords.** This may require more of a training approach than a conversational one.

Follow us on YouTube

- **Consider setting up logon auditing to prevent this from happening again in the future.** Microsoft offers **information on how to do this**.

Helpful tools

Here are some tools to help you with account lockout issues:

- **The account lockout tools** – This set of tools includes the Event Log Parser EventCombMT.exe and other tools to find which domain controller is processing a lockout event, so you can then locate the source.
- **How to create a strong password** – Simple steps you can share with users to help them create strong, easy-to-remember passwords.
- **KeePass** – One of the many very good open source password tools, which are infinitely better than writing passwords down or reusing the same password for different purposes.

Defaced website

This is the technical equivalent of someone spray painting graffiti on your building, but it's visible around the world. You will want to restore your website to normal operation as soon as possible, but you will also want to make sure this doesn't happen again.

- Take the web server offline and put up a simple "Under Maintenance" page on another server so your visitors know you will be back soon.
- Perform a vulnerability scan against your website to see how the person got access to your system in the first place.
- Remediate any vulnerabilities and apply any missing patches.
- Restore your website content from backup.
- Rescan your server with the restored content before returning it to service.
- Make sure the entire team understands what happened so you can reduce the chance of it happening again.

Helpful tools

Here are some tools to assist you with keeping an eye on your website:

- **Wget** – A great command line tool for mirroring websites. Use it to grab a copy of all the static content on your website.
- **Site 24x7** – Not only can the web-based service monitor your services; it can also alert you if any page changes on your website.
- **Google Webmaster Tools** – Use these free tools from Google to scan your site for malware and identify other issues.

Unauthorized access to critical data

Whether an internal user was just poking around or an attacker gained access to your network and started looking for data to steal, when unauthorized access to critical data occurs, you must respond swiftly and completely. In some cases, you must also disclose the incident in compliance with the law.

- Determine what data was accessed. Use access logs, when possible, to determine whether data was simply touched, copied or altered.
- Determine how the data was accessed and remediate this immediately. Open FTP servers, peer-to-peer software, websites with improper permissions or open shares on the internal network can all easily be exploited by others to gain access to data.
- Work with the data owner and the people who have authorized access to confirm your findings.
- Determine whether the data access was done with malicious intent or not. If it was accessed by an attacker, assume malicious intent. If by an employee, work with HR to determine the intent.
- Consult your legal counsel to determine whether you should notify customers, consumers or a regulatory agency.
- Scan your network for other instances of the same problem that led to this unauthorized access and fix those issues.

Helpful tools

Here are some tools to help you review access to data:

- **Logparser** – This powerful log mining tool can help you parse through several different log formats.
- **Cacls** – This tool can dump and/or modify file system access control lists.

Compromised DNS

This is one of the worse things that can happen to a company, since it means the attacker can redirect all email, website visits and other traffic destined for that network. Because this happens to companies large and small, it's critical for you to keep an eye on things and to act swiftly if an attacker does manage to compromise your DNS.

- Immediately contact your service provider or registrar to cut off the unauthorized access to your DNS records.
- Restore your zone files from backup.
- Be open and honest about what happened. Notify your customers and vendors so that they are aware that anything that they might have been redirected to was inadvertent.
- Determine how the unauthorized access occurred. Were passwords guessed, were they reset with new credentials sent to a compromised email account, or was a change request sent from a spoofed email account? However it happened; implement procedural changes to ensure it doesn't happen again.

Helpful tools

Use these tools to help you with DNS:

- **Dig for Windows** – Much more powerful than nslookup.
- **DNS Stuff** – A premium collection of DNS tools on the Internet.
- **DNS Lint** – A great tool for diagnosing and testing DNS both for AD and other purposes.

Licensing violations

Licensing violations can cost even small businesses tens of thousands of dollars to remediate. When users install software that they don't have a license for, it's the company that is on the hook to the vendor for this; so preventing this from happening is critical.

- Uninstall unapproved software from all systems immediately.
- Close open network shares to software if users were installing from the network.
- Work with the vendor to obtain licenses for software you cannot uninstall as quickly as possible.
- Educate your users on the importance of complying with licensing requirements, and train them on the proper way to request licensed software for business purposes.

Read our blog posts

Stolen hardware

Hardware theft can cost a company a significant part of its annual IT budget, but it can also go undetected for weeks or even months. Maintaining a complete, accurate and current inventory of your hardware assets is crucial. Properly securing servers in a locked server room, using security cables to lock laptops down when users travel, and ensuring users sign agreements for any hardware they take out of the office will help to reduce the likelihood of hardware loss.

- Maintain a complete inventory of all hardware purchased, including serial numbers and who is responsible for the hardware.
- Train users on the importance of securing laptops, portable storage media and other hardware both at their desk, in their car and when travelling.
- Notify law enforcement of any hardware thefts.
- Ensure that all storage media is encrypted to prevent data loss if the hardware is stolen.
- Encourage users to use backpacks or other "less obvious" ways to transport their laptops; also avoid displaying company logos on bags as these will attract attention and temptation.

Conclusion

Of course, prevention is better than cure. Implementing the right tools on your network to help you patch your systems, deploying antivirus software, performing security scans and maintaining an inventory, could prevent or at least help with most of the incidents outlined in the e-book.

If you're looking for a virtual security consultant that provides the tools you need to perform patch management, vulnerability assessments, network audits and more, take a look at **GFI LanGuard®**. You can get a fully functional **30-day trial** so you can see for yourself how powerful this application is, and how much it can help you with your preventative efforts.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

33 North Garden Ave, Suite 1200, Clearwater, FL 33755, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

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