The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Overview
- Indicators of Compromise
- How To Respond

I'm Hacked, Now What?

Overview

We know you are concerned about protecting your computer and information and take steps to secure them. However— just like driving a car —no matter how safely you drive, sooner or later you may have an incident. In this newsletter we will teach you what to look for to determine if your computer is hacked, and if so what you can do about it. Ultimately, the quicker you detect your computer has been hacked and the faster you respond, the better you can mitigate any harm to you or your organization.

Guest Editor

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) is Chief Scientist at CSRgroup Computer Security Consultants. He is also the coauthor of the Memory Forensics (FOR526) and Malware Reverse Engineering (FOR610) courses at SANS.

Indicators of Compromise

First, you need to understand that in many cases there is no single step you can take to determine if your computer is hacked. Instead there are usually several indicators. If you identify a combination of these, this implies your computer is hacked. Here are some examples.

- Your anti-virus program has triggered an alert that your computer is infected, particularly if it says that it was unable to remove or quarantine the affected files.
- Your browser's homepage has unexpectedly changed or your browser is taking you to websites that you did not want to go to.
- There are new accounts on your computer that you did not create.
- There are new programs running that you did not install.
- Your computer is continually crashing or running very slow.
- A program on your computer requests your authorization to make changes to your system, although you're not actively installing or updating any of your applications.
- Your firewall alerts you that a program you do not recognize is requesting permission to access the internet.

© The SANS Institute 2014

I'm Hacked, Now What?

How To Respond

If you believe your computer has been compromised, the sooner you respond, the better. If the computer you are using was provided to you by your employer or is used for work, do not try to fix your computer yourself and do not turn the computer off. Not only you may cause more harm than good, but you could destroy valuable evidence that can be used for an investigation. Instead, report the incident to your employer right away, usually by contacting your help desk, security team or supervisor. If for some reason you cannot contact your organization, or you are concerned about a delay, disconnect your computer from the network and then put it in sleep, suspend or hibernation mode. Even if you are not sure if you have been hacked, it is far better to report now just in case. Your organization most likely has processes and a team in place to handle situations like this, let them handle it. If the computer is your own for personal use, here are some steps you can take on your own.

Sooner or later your computer may be compromised, the faster you detect an incident and the sooner you respond, the better.

- Backups: The most important step you can take is to prepare ahead of time with backups. Specifically backup your data regularly and periodically check that you are able to restore files from your backup. Quite often when a computer is compromised, the only option you have is wiping the system hard drive and reinstalling the operating system, or purchasing a new computer. Either way you need your backups to recover your personal data.
- Change Your Passwords: Be sure to change all your passwords. This includes not only the passwords on your computers and mobile devices, but all of your online passwords. Be sure you change all your online passwords from a different computer that you know is trusted and secure.
- Anti-virus: If your anti-virus software informs you of an infected file, you can follow the actions it recommends. This usually can include quarantining the file, cleaning the file or deleting the file. Most anti-virus software will have links which you can follow to learn more about the specific infection. When in doubt, quarantine the file. If that is not possible, then delete it.
- Re-installing: If you are unable to clean the computer with anti-virus, one of the most secure ways to recover is to rebuild the computer from scratch. First disconnect your computer from the network. Then follow your system's manufacturer's instructions, in most cases that means using the built-in recovery partition to reinstall

© The SANS Institute 2014

I'm Hacked, Now What?

the operating system. If the recovery partition is missing, corrupted or infected, then contact your manufacturer and request that they send a recovery DVD. Do not reinstall the operating system from backups. Your backups may have the same vulnerabilities that allowed the hacker to originally gain access. The only thing you should use your backups for is recovering your personal data. Also, if your computer is old or outdated, it may be simpler (and perhaps even cheaper) to purchase a new computer than attempting to spend hours rebuilding it.

- Professional Help: If you are concerned you have been hacked, but feel like you do not have the skills or knowledge to fix it, you may want to turn your computer over to a professional. For example, after being hacked you may realize that your backups are incomplete or outdated. You may be tempted to transfer critical files such as photos, documents or videos between your infected machine and a new machine. However by doing this you can inadvertently transfer malware and infect your new computer at the same time. A far safer alternative is to take the infected computer to a qualified technician who can safely recover these files without risking transferring the infection.

Become a Security Professional - SANSFIRE 2014

SANSFIRE 2014 will be held in Baltimore, MD on June 21st - 30th, with over 40 of SANS's top security courses taught by top-rated instructors. In addition, this is our annual "Internet Storm Center Powered" event. Each evening, the ISC handlers will share riveting talks on their most interesting experiences and the latest cyber threats. For more information, please visit http://www.sans.org/event/sansfire-2014/welcome/.

Resources

OUCH! Backups:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! What Is Malware:	http://www.securingthehuman.org/ouch/2014#february2014
Detecting Evil Poster:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

License

OUCH! is published by SANS Securing The Human and is distributed under the Creative Commons BY-NC-ND 3.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify the newsletter. For past editions or translated versions, visit www.securingthehuman.org/ouch. Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus