Vicious attack steals millions of Facebook and Google passwords

Researchers have discovered a huge new virus called the Pony Botnet Controller. It is swiping account information from millions of computers worldwide.

So far, the virus has stolen nearly 2 million user names and passwords for Facebook, Google, Yahoo, Twitter, LinkedIn, a Russian social network and the ADP payroll software. If your computer is infected with Pony Botnet, you won't even know it because this nasty virus runs undetected!

If left unchecked, this virus will eventually report back every password and account you have to the hackers behind it.

To stay safe, you need to update your security, download several program patches and change your passwords!

The first thing to do is to make sure your security software is up to date. I have several free programs in my Security Center that will secure your computer. Click here to get the best antivirus software now!

The Pony Botnet Controller is technically a keylogger, which makes it a bit harder to find and remove. Learn more about keyloggers and how to remove them.

You should make sure your Internet browsers are up to date. An older browser might not have the most recent security in place and let the virus through. See if your browser needs updating (BELOW)

Web browsers can be a confusing topic. There are several you could be using, and each one can have multiple versions.

How do you know which one you use? How do you know it's up to date?

Well, now you can see with just a click. It's that easy. Just visit this site

whatbrowser.org

It tells you what browser you're using and if it's the latest version. Plus, there are links to other browsers if you want to give them a try.

Adobe Flash and Java are two programs notorious for letting viruses on to your system. Make sure you have the most recent updates. In the case of Java, you might not even need it. Just when the scary Java headlines had died down, Java came out of nowhere with an update that fixed almost 50 security issues. Of course, a few hours later hackers were bragging about finding a hole in Java that the update missed. So, it's off to the races once more.

For those who haven't been following this, Java is a programming language required for certain programs and websites. It runs many chat sites, online games and programs like LibreOffice.

Hackers have spent the last few months finding security flaws in Java that can help them take over your computer and steal your information.

It seems like every time Oracle, the company that develops Java, patches a security flaw, hackers find another one. That's bad news since Java comes on most computers by default.

Now that hackers have found another new crack in Java, what should you do?

The best thing to do, as always, is uninstall Java completely. This avoids all the security problems. For help deleting Java or any other program you don't want, check out this must-read tip.

Unfortunately, as I said above, some programs and websites require Java to work. If you use one of those, then uninstalling Java isn't an option.

Fortunately, that isn't the end of your security options.

First I should explain that there are two ways Java can run. It can run with standalone programs on your system, or it can run as a plug-in in your Web browser.

The standalone version really isn't dangerous. It doesn't communicate with the Internet so hackers have a much harder time taking control of it. That means using a program like LibreOffice isn't really a security threat.

The real danger is the Java browser plug-in. All you have to do is visit a malicious site with it enabled and hackers can use it to invade your system. Thankfully, you can turn it off.

To start, make sure you have the most-recent version of Java. Once you've installed it, go to Start>>Computer and type "Javacpl.exe" in your search bar. When it shows up, double-click on it to run it.

On some computers "Javacpl.exe" won't show up, so you'll have to look for it manually. Go to Start>>Computer>>Local Disk (C:). If you have a 64-bit computer, go to Program Files (x86)>>Java>>jre7>>bin. On 32-bit computers, you'll find it in Program Files>>Java>>jre7>>bin.

Double-click Javacpl.exe and find the Security tab. Uncheck the box that says "Enable Java content in the browser." Restart any browsers you have open for the change to take effect.

If you're on a Mac with OS X 10.7 or later, Java is already turned off in your browser. If you want to double check, you can find the Java Control Panel on your Mac by going to System Preferences and clicking on the Java icon. It looks like a piping-hot cup of coffee.

If you need Java to make some sites work, you'll have to leave the Java plug-in enabled. There is a way to do this without hurting your security.

Go back to the Java Privacy menu and set the security slider to "Custom level." Then select "Prompt User," "Single-click confirmation prompt" and "Prompt user" in the menu that pops up.

If you think your information was compromised, or your security software finds the virus, you should immediately change your online account passwords. You can manage your passwords with these helpful programs.

Now all sites that use Java will ask for permission before running it. Only give permission to sites you trust! On all other sites, tell Java not to run.

If you still aren't comfortable having Java installed, you can try finding some alternatives to the sites and programs that require it. Take a look through my Cool Sites and Free Downloads sections.

Your computer isn't completely safe just yet, though. Use these three ideas to boost your computer's security even more.

- You can boost your computer's security just by knowing how to avoid scams. Here are a few telltale signs of a scam.
- The more you know about different viruses, the better off you are. Learn 12 different virus terms you need to know.

- See more at: http://www.komando.com/tips/index.aspx?id=15679&utm_medium=nl&utm_source=alerts&utm_content=2013-12-05-article-1-title-a&page=2#sthash.PtpwYmii.dpuf