

InfoWorld DeepDive

11 sure signs you've been hacked

**REDIRECTED NET
SEARCHES, UNEXPECTED
INSTALLS, ROGUE MOUSE
POINTERS: HERE'S WHAT TO
DO WHEN YOU'VE
BEEN OWNED**

Deep Dive

11 sure signs you've been hacked



Redirected Net searches, unexpected installs, rogue mouse pointers: Here's what to do when you've been Owned BY ROGER A. GRIMES

In today's threatscape, antivirus software provides little piece of mind. In fact, antimalware scanners on the whole are horribly inaccurate, especially with exploits less than 24 hours old. After all, malicious hackers and malware [can change their tactics at will](#). Swap a few bytes around, and a previously recognized malware program becomes unrecognizable.

To combat this, many antimalware programs monitor program behaviors, often called heuristics, to catch previously unrecognized malware. Other programs use virtualized environments, system monitoring, network traffic detection, and all of the above at once in order to be more accurate. And [still they fail us](#) on a regular basis.

Here are 11 sure signs you've been hacked and what to do in the event of compromise. Note that in all cases, the No. 1 recommendation is to completely restore your system to a known good state before proceeding. In the early days, this meant formatting the computer and restoring all programs and data. Today, depending on your operating system, it might simply mean clicking on a Restore button. Either way, a [compromised computer](#) can never be fully trusted again. The recovery steps listed in each category below are the recommendations to follow if you don't want to do a full restore -- but again, a full restore is always a better option, risk-wise.

Sure sign of system compromise No. 1: Fake antivirus messages

In slight decline these days, fake antivirus warning messages are among the surest signs that your system has been compromised.

What most people don't realize is that by the time they see the fake antivirus warning, the damage has been done. Clicking No or Cancel to stop the fake virus scan is too little, too late.

The malicious software has already made use of unpatched software, often the Java Runtime Environment or an Adobe product, to completely exploit your system.

Why does the malicious program bother with the "antivirus warning"? This is because the fake scan, which always finds tons of "viruses," is a lure to buy their product. Clicking on the provided link sends you to a professional-looking website, complete with glowing letters of recommendation. There, they ask you for your credit card number and billing information. You'd be surprised how many people get tricked into

Deep Dive



Most browsers allow you to review installed and active toolbars. Remove any you didn't absolutely want to install. When in doubt, remove it.

providing personal financial information. The bad guys gain complete control of your system and get your credit card or banking information. For bad guys, it's the Holy Grail of hacking.

WHAT TO DO: As soon as you notice the fake antivirus warning message, power down your computer. (Note: This requires knowing what your legitimate antivirus program's warning looks like.) If you need to save anything and can do it, do so. But the sooner you power off your computer, the better. Boot up the computer system in Safe Mode, No Networking, and try to uninstall the newly installed software (oftentimes it can be uninstalled like a regular program). Either way, follow up by trying to restore your system to a state previous to the exploitation. If successful, test the computer in regular mode and make sure that the fake antivirus warnings are gone. Then follow up with a complete antivirus scan. Oftentimes, the scanner will find other sneak remnants left behind.

Sure sign of system compromise No. 2:

Unwanted browser toolbars

This is probably the second most common sign of exploitation: Your browser has multiple new toolbars with names that seem to indicate the toolbar is supposed to help you. Unless you recognize the toolbar as coming from a very well-known vendor, it's time to dump the bogus toolbar.

WHAT TO DO: Most browsers allow you to review installed and active toolbars. Remove any you didn't absolutely want to install. When in doubt, remove it. If the bogus toolbar isn't listed there or you can't easily remove it, see if your browser has an option to reset the browser back to its default settings. If this doesn't work, follow the instructions listed above for fake antivirus messages. You can usually avoid malicious toolbars by making sure that all your software is fully patched and by being on the lookout for free software that installs these tool bars. Hint:

Read the licensing agreement. Toolbar installs are often pointed out in the licensing agreements that most people don't read.



Sure sign of system compromise No. 3:

Redirected Internet searches

Many hackers make their living by redirecting your browser somewhere other than you want to go. The hacker gets paid by getting your clicks to appear on someone else's website, often those who don't know that the clicks to their site are from malicious redirection.

You can often spot this type of malware by typing a few related, very common words (for example, "puppy" or "goldfish") into Internet search engines and checking to see whether the same websites appear in the results -- almost always with no actual relevance to your terms. Unfortunately, many of today's redirected Internet searches are well hidden from the user through use of additional proxies, so the bogus results are never returned to alert the user. In general, if you have bogus toolbar programs, you're also being redirected. Technical users who really want to confirm can sniff their own browser or network traffic. The traffic sent and returned will always be distinctly different on a compromised computer vs. an uncompromised computer.

WHAT TO DO: Follow the same instructions as above. Usually removing the bogus toolbars and programs is enough to get rid of malicious redirection.

Deep Dive

Sure sign of system compromise No. 4:

Frequent random popups

This popular sign that you've been hacked is also one of the more annoying ones. When you're getting random browser pop-ups from websites that don't normally generate them, your system has been compromised. I'm constantly amazed about which websites, legitimate and otherwise, can bypass your browser's anti-pop-up mechanisms. It's like battling email spam, but worse.

WHAT TO DO: Not to sound like a broken record, but typically random pop-ups are generated by one of the three previous malicious mechanisms noted above. You'll need to get rid of bogus toolbars and other programs if you even hope to get rid of the pop-ups.

Sure sign of system compromise No. 5:

Your friends receive fake emails from your email account

This is the one scenario where you might be OK. It's fairly common for our email friends to receive malicious emails from us. A decade ago, when email attachment viruses were all the rage, it was very common for malware programs to survey your email address book and send malicious emails to everyone in it.

These days it's more common for malicious emails to be sent to some of your friends, but not everyone in your email address book. If it's just a few friends and not everyone in your email list, then more than likely your computer hasn't been compromised (at least with an email address-hunting malware program). These days

malware programs and hackers often pull email addresses and contact lists from social media sites, but doing so means obtaining a very incomplete list of your contacts' email addresses. Although not always the case, the bogus emails they send to your friends often don't have your email address as the sender. It may have your name, but not your correct email address. If this is the case, then usually your computer is safe.

WHAT TO DO: If one or more friends reports receiving bogus emails claiming to be from you, do your due diligence and run a complete antivirus scan on your computer, followed by looking for unwanted installed programs and toolbars. Often it's nothing to worry about, but it can't hurt to do a little health check when this happens.



Sure sign of system compromise No. 6:

Your online passwords suddenly change

If one or more of your online passwords suddenly change, you've more than likely been hacked -- or at least that online service has been hacked. In this particular scenario, usually what has happened is that the victim responded to an authentic-looking phishing email that purportedly claimed to be from the service that ends up with the changed password. The bad guy collects the login information, logs on, changes the password (and other information to



If one or more friends reports receiving bogus emails claiming to be from you, do your due diligence and run a complete antivirus scan on your computer.

Deep Dive



If the compromised logon information is used on other websites, immediately change those passwords. And be more careful next time. Websites rarely send emails asking you to provide your logon information.

complicate recovery), and uses the service to steal money from the victim or the victim's acquaintances (while pretending to be the victim).

WHAT TO DO: If the scam is widespread and many acquaintances you know are being reached out to, immediately notify all your contacts about your compromised account. Do this to minimize the damage being done to others by your mistake. Second, contact the online service to report the compromised account. Most online services are used to this sort of maliciousness and can quickly get the account back under your control with a new password in a few minutes. Some services even have the whole process automated. A few services even have a "My friend's been hacked!" button that lets your friends start the process. This is helpful, because your friends often know your account has been compromised before you do.

If the compromised logon information is used on other websites, immediately [change those passwords](#). And be more careful next time. Websites rarely send emails asking you to provide your logon information. When in doubt, go to the website directly (don't use the links sent to you in email) and see if the same information is being requested when you log on using the legitimate method. You can also call the service via their phone line or email them to report the received phishing email or to confirm its validity. Lastly, consider using online services that provide two-factor authentication. It makes your account [much harder to steal](#).

Sure sign of system compromise No. 7:

Unexpected software installs

Unwanted and unexpected software installs are a big sign that your computer system has likely been hacked.

In the early days of malware, most programs were computer viruses, which work by modifying other legitimate programs. They did this to better hide themselves. For whatever reason, most

malware programs these days are Trojans and worms, and they typically install themselves like legitimate programs. This may be because their creators are trying to walk a very thin line when the courts catch up to them. They can attempt to say something like, "But we are a legitimate software company." Oftentimes the unwanted software is legally installed by other programs, so read your license agreements. Frequently, I'll read license agreements that plainly state that they will be installing one or more other programs. Sometimes you can opt out of these other installed programs; other times you can't.

WHAT TO DO: There are many free programs that show you all your installed programs and let you selectively disable them. My favorite for Windows is [Autoruns](#). It doesn't show you every program installed but will tell you the ones that automatically start themselves when your PC is restarted. Most malware programs can be found here. The hard part is determining what is and what isn't legitimate. When in doubt, disable the unrecognized program, reboot the PC, and reenable the program only if some needed functionality is no longer working.

Sure sign of system compromise No. 8:

Your mouse moves between programs and makes correct selections

If your mouse pointer moves itself while making selections that work, you've definitely been hacked. Mouse pointers often move randomly, usually due to hardware problems. But if the movements involve making the correct choices to run particular programs, malicious humans are somewhere involved.

Not as common as some of the other attacks, many hackers will break into a computer, wait for it to be idle for a long time (like after midnight), then try to steal your money. Hackers will break into bank accounts and transfer money, trade

Deep Dive



If you notice that your antimalware software is disabled and you didn't do it, you're probably exploited.

your stocks, and do all sorts of rogue actions, all designed to lighten your cash load.

WHAT TO DO: If your computer “comes alive” one night, take a minute before turning it off to determine what the intruders are interested in. Don't let them rob you, but it will be useful to see what things they are looking at and trying to compromise. If you have a cell-phone handy, take a few pictures to document their tasks. When it makes sense, power off the computer. Unhook it from the network (or disable the wireless router) and call in the professionals. This is the one time that you're going to need expert help.

Using another known good computer, immediately change all your other logon names and passwords. Check your bank account transaction histories, stock accounts, and so on. Consider paying for a credit-monitoring service. If you've been a victim of this attack, [you have to take it seriously](#). Complete restore of the computer is the only option you should choose for recovery. But if you've lost any money, make sure to let the forensics team make a copy first. If you've suffered a loss, call law enforcement and file a case. You'll need this information to best recover your real money losses, if any.

Sure sign of system compromise No. 9:

Your anti-malware software, Task Manager, or Registry Editor is disabled and can't be restarted

This is a huge sign of malicious compromise. If you notice that your antimalware software is disabled and you didn't do it, you're probably exploited -- especially if you try to start Task Manager or Registry Editor and they won't start, start and

disappear, or start in a reduced state. This is very common for malware to do.

WHAT TO DO: You should really perform a complete restore because there is no telling what has happened. But if you want to try something less drastic first, research the many methods on how to restore the lost functionality (any Internet search engine will return lots of results), then restart your computer in Safe Mode and start the hard work. I say “hard work” because usually it isn't easy or quick. Often, I have to try a handful of different methods to find one that works. Precede restoring your software by getting rid of the malware program, using the methods listed above.

Sure sign of system compromise No. 10:

Your bank account is missing money

I mean lots of money. Online bad guys don't usually steal a little money. They like to transfer everything or nearly everything, often to a foreign exchange or bank. Usually it begins by your computer being compromised or from you responding to a fake phish from your bank. In any case, the bad guys log on to your bank, change your contact information, and transfer large sums of money to themselves.

WHAT TO DO: In most cases you are in luck because most financial institutions will replace the stolen funds (especially if they can stop the transaction before the damage is truly done). However, there have been many cases where the courts have ruled it was the customer's responsibility to not be hacked, and it's up to the financial institution to decide whether they will make restitution to you.

If you're trying to prevent this from happening in the first place, turn on transaction alerts that send text alerts to you when something unusual is happening. Many financial institutions allow you to set thresholds on transaction amounts, and if the threshold is exceeded or it goes to a foreign country, you'll

Deep Dive

be warned. Unfortunately, many times the bad guys reset the alerts or your contact information before they steal your money. So make sure your financial institution sends you alerts anytime your contact information or alerting choices are changed.

Sure sign of system compromise No. 11:

You get calls from stores about nonpayment of shipped goods

In this case, hackers have compromised one of your accounts, made a purchase, and had it shipped to someplace other than your house. Oftentimes, the bad guys will order tons of merchandise at the same time, making each business entity think you have enough funds at the beginning, but as each transaction finally pushes through you end up with insufficient funds.

WHAT TO DO: This is a bad one. First try to think of how your account was compromised. If it was one of the methods above, follow those recommendations. Either way, change all your logon names and passwords (not just the one related to the single compromised account), call law enforcement, get a case going, and start monitoring your credit. You'll probably spend months trying to clear up all the bogus transactions committed in your name, but you should be able to undo most, if not all, of the damage.

Years ago you could be left with a negative credit history that would impact your life for a

decade. These days, companies and the credit reporting agencies are more used to cyber crime, and they deal with it better. Still, be aggressive and make sure you follow every bit of advice given to you by law enforcement, the creditors, and the credit-rating agencies (there are three major ones).

Malware vector trifecta to avoid

The hope of an antimalware program that can perfectly detect malware and malicious hacking is pure folly. Keep an eye out for the common signs and symptoms of your computer being hacked as outlined above. And if you are risk-averse, as I am, always perform a complete computer restore with the event of a breach. Because once your computer has been compromised, the bad guys can do anything and hide anywhere. It's best to just start from scratch.

Most malicious hacking originates from one of three vectors: unpatched software, running Trojan horse programs, and responding to fake phishing emails. Do better at preventing these three things, and you'll be less likely to have to rely on your antimalware software's accuracy -- and luck. ■

Roger A. Grimes is contributing editor of the *InfoWorld Test Center*. Roger holds over 40 computer certifications and has authored eight books on computer security. He has been fighting malware and malicious hackers since 1987, beginning with disassembling early DOS viruses. He currently runs eight honeypots to track hacker and malware behavior and consults to companies from the *Fortune 100* to small businesses. A frequent industry speaker and educator, Roger currently works for Microsoft as a Principal Security Architect. He also writes the [Security Adviser blog](#).



Most malicious hacking originates from one of three vectors: unpatched software, running Trojan horse programs, and responding to fake phishing emails. Do better at preventing these three things, and you'll be less likely to have to rely on your anti-malware software's accuracy — and luck.

Deep Dive

5 signs you've been hit with an advanced persistent threat



Do you have valuable data on your network? Noticing odd network behavior? You could be the victim of an APT attack BY ROGER A. GRIMES

Hackers who employ APTs ([advanced persistent threats](#)) are a different breed. A real and constant threat to the world's companies and networks, APT hackers tend to be well organized, working together as part of a professional team. Their goal, typically, is to steal valuable intellectual property, such as confidential project descriptions, contracts, and patent information.

Generally, APT hackers employ familiar methods, using phishing emails or other tricks to fool users into downloading malware. But the ultimate objective tends to be very ambitious. If you discover a break-in where the only apparent intent was to steal money from your company, then it probably wasn't an APT hack. Those who deal in APTs are trying to be your company.

Because APT hackers use different techniques from ordinary hackers, they leave behind different signs. Over the past decade, I've discovered the following five signs are most likely to indicate that your company has been compromised by an APT. Each could be part of legitimate actions within the business, but their unexpected nature or the volume of activity may bear witness to an APT exploit.

APT sign No. 1: Increase in elevated log-ons late at night

APTs rapidly escalate from compromising a single computer to taking over the whole environment. They do this by reading an authentication database, stealing credentials, and reusing them. They learn which user (or service) accounts have elevated privileges and permissions, then go through those accounts to compromise assets within the environment. Often, a high volume of elevated log-ons occur at night because the

attackers live on the other side of the world. If you suddenly notice a high volume of elevated log-ons while the legitimate work crew is at home, start to worry.

APT sign No. 2: Finding widespread backdoor Trojans

APT hackers often install backdoor Trojan programs on compromised computers within the exploited environment. They do this to ensure

Deep Dive

they can always get back in, even if the captured log-on credentials get changed when the victim gets a clue. Another related trait: Once discovered, APT hackers don't go away like normal attackers. Why should they? They own computers in your environment, and you aren't likely to see them in a court of law.

These days, Trojans deployed through social engineering provide the avenue through which most companies are exploited. They are fairly common in every environment -- and they proliferate in APT attacks.

APT sign No.3: Unexpected information flows

If I could pick the single best way to detect APT activities, this would be it: Look for large, unexpected flows of data from internal origination points to other internal computers or to external computers. It could be server to server, server to client, or network to network.

Those data flows may also be limited, but targeted -- such as someone picking up email from a foreign country. I wish every email client had the ability to show where the latest user logged in to pick up email and where the last message was accessed. Gmail and some other cloud email systems already offer this.

Of course, in order to detect a possible APT, you have to understand what your data flows look like before your environment is compromised. Start now and learn your baselines.

APT sign No. 4: Discovering unexpected data bundles

APTs often aggregate stolen data to internal collection points before moving it outside. Look for large (we're talking gigabytes, not megabytes) chunks of data appearing in places where that data should

not be, especially if compressed in archive formats not normally used by your company.


APT sign No. 5: Detecting pass-the-hash hacking tools

Although APTs don't always use [pass-the-hash attack tools](#), they frequently pop up. Strangely, after using them, hackers often forget to delete them. If you find [pass-the-hash attack](#) tools hanging around, it's OK to panic a little or at least consider them as evidence that should be investigated further.

If I had to think of a sixth indicator -- there's no charge for this one -- it would be focused spear-phishing campaigns against a company's employees using malformed Adobe Acrobat PDF files. This is the original causative agent in the vast majority of APT attacks. I didn't include it in the original five signs above because [Adobe Acrobat is exploited](#) all over the place. But if you hear of a focused spear-phishing attack, especially if a few [executives have reported being duped](#) into clicking on an attached PDF file, start looking for the other five signs and symptoms. It may be your canary in the coal mine.

That said, I hope you never have to face cleaning up from an APT attack. It's one of the hardest things you and your enterprise can do. [Prevention](#) and early detection will reduce your suffering. ■

Roger A. Grimes is contributing editor of the InfoWorld Test Center. Roger holds over 40 computer certifications and has authored eight books on computer security. He has been fighting malware and malicious hackers since 1987, beginning with disassembling early DOS viruses. He currently runs eight honeypots to track hacker and malware behavior and consults to companies from the Fortune 100 to small businesses. A frequent industry speaker and educator, Roger currently works for Microsoft as a Principal Security Architect. He also writes the [Security Adviser blog](#).



I hope you never have to face cleaning up from an APT attack. It's one of the hardest things you and your enterprise can do. Prevention and early detection will reduce your suffering.