# Computer Security Series

# Cleaning Infected Machines, Part 1

*By Robert Spotswood*

*with contributions by Modem Bob*

## *An Ounce of Prevention is Worth a Pound of Cure*

The best way to avoid having to deal with a malware (AKA virus/trojan/rootkit/spyware/adware /etc.) infected machine is to not get infected in the first place. While that is far easier said than done, there things you can do to put the odds in your favor. Nothing is fool proof, but every time you raise the bar higher, the chances of getting infected go down. You don't have to make an attack impossible, you just have to make it not worthwhile.

## *Antivirus/Antimalware software*

Get some antivirus (AKA antimalware) software and keep it up to date. For home users, there are multiple free versions to chose from. Currently I recommend either Avast for the "not a computer geek" home user, and Comodo for the more sophisticated user. But if you're happy with what you have, don't change without a good reason.

Malware is constantly evolving, and there is always a gap in the protection between the time a new threat comes out and when the antivirus vendors update their signature databases. There is another gap between when the signature database is updated and when you download the update. Further, no program will catch everything. So don't think you are immune if you have some antivirus software installed. You're not, but you are safer.

Don't forget to update the antivirus program (often referred to as the engine) too when a new version of the program comes out. As threats evolve, the programs have to evolve with them. An older program, even with updated signatures, won't protect you as well as a newer program.

Be warned that not all antivirus programs are created equal, and the effectiveness is constantly changing. It's a marathon race, not a sprint, and there is no one perfect program. Every program has trade-offs. If you're interested in some good comparison data, check out the AV-Comparatives.org site (http://www.av-comparatives.org/). While they don't test every program, they have good data on the ones they do test.

## *Patch, Patch, Patch!*

Stay current on your security patches. Most infection mechanisms that use vulnerabilities/holes use holes already patched. According to Microsoft's Security Intelligence Report volume 11 (http://www.microsoft.com/security/sir/default.aspx), "exploits are relatively rare, and exploits that target recently disclosed vulnerabilities are rarer still." If you back out the numbers from Figure 4 of the report, about 57% of the infections that used vulnerabilities, used holes that were patched over a

year before. Almost all of the remaining vulnerability using infections used holes for which a patch is available, but for less than a year.

A second study (http://www.csis.dk/en/csis/news/3321) found, "...that as much as 99.8 % of all virus/malware infections caused by commercial exploit kits are a direct result of the lack of updating five specific software packages." The five most common pieces of software exploited are: Operating Systems (think Windows, although this does include all the others), Java, Adobe Reader, Adobe Flash, and browser exploits.

There are several free programs that can help you make sure you are up to date. My current favorite is FileHippo.com Update Checker (http://www.filehippo.com/updatechecker/). While it doesn't cover every piece of software you might have, it does check quite a bit, including Java, Flash, Reader, and your web browser. Unlike some other free version checkers, it does not, for now, include any bundled programs, such as adware or toolbars. However, it does not have any mechanism for downloading and installing updates automatically. Very few update checkers do. FileHippo will give you a web page with links to download the programs however.

### *Windows*

Turn on Windows update, and if it wants to install some patches, let it. You don't have to install them right this minute, but do it within a few days at most. The sooner the better.

### *Java*

Unless you need it, don't install it at all. Many other pieces of very useful software do use or even require it, so not installing it may not be an option. OpenOffice.org and LibreOffice are two popular examples. Some software, if it needs it, will install it for you if don't have it, but will install an old, unpatched version. To make matters worse, some java programs/applets only work with a specific version of java, so you may be forced to use an unpatched version.

If you do install it, the latest versions come with an update notifier that sits in your system tray. Don't ignore it. Be warned that the Java installation program does not uninstall old, vulnerable, versions. You have do this yourself, manually. You must go to "Control Panel, then Add/Remove Programs, or for newer Windows like Vista & 7, Programs & Features, and uninstall that older JAVA.

Finally, unless you really need it, you can disable the Java browser plugin. Some sites require Java, but only a few, so you likely don't need it. Firefox users can the NoScript plugin (described in more detail below) to selectively enable Java only for certain sites.

### *Adobe Reader*

Adobe Reader is something to read PDFs. But it is far from the only program out there that does this. Two popular alternatives for Windows are Foxit and Sumatra (my preference). Unfortunately, some websites don't react well if you don't have a PDF plugin available (*cough*State of Texas*cough*), and that means Reader.

You can have Reader and one of the other PDF readers installed too, using Reader only for sites that pretty much require a plugin. The downside is malware distributing sites will likely demand the plugin. Unless you know it's going to cause a problem, I recommend you don't install Reader and try going

with one of the alternatives. You will have to download PDFs you encounter and read them outside your web browser, but that's a small price to pay for the extra security.

Like Java, Reader does come with its own updater that sits in the system tray. If it tells you to update, update. It will remove older version, so its better than the Java updater.

### *Flash*

Flash is one of those programs lots of people wish would die, and HTML 5 may wound it, but it isn't going anywhere soon. So many sites use Flash, even in places they don't need it, that trying to use and enjoy all that the web offers without it isn't realistic for most people.

Thankfully, like Java and Reader, Flash comes with its own update checker program, and unlike Java and Reader, this one is a lot more in your face nagging than the other two, which just sit it system tray and are easily ignored. If it wants to update, then update. For additional security, Firefox users can use the NoScript plugin (see below) to selectively enable and disable flash. Chrome also offers a script blocking mechanism that includes flash (more on that below).

### *Browser Exploits*

For browsers, regardless of which one you use, be sure you are running the latest version available, using whatever update method that browser offers. Beyond that, dealing intelligently javascript is the biggest hurdle to preventing browser exploits. Almost every browser attack involves javascript at some level.

Javascript is designed to make sites more interactive, but the criminals have numerous ways to use javascript to sneak malicious software and exploits onto a site visitor's computer. While you can disable javascript in pretty much any browser, it isn't a viable option. Very few sites work good enough without javascript enabled.

Enabling it manually every time you go to site you trust won't work either. First, you have to remember to disable it afterwards. Even the most patient person will soon give up. Secondly, even if you trust the site, there is no guarantee the site hasn't been compromised, and is now serving up malicious javascript.

There are few options. One of the best is a free Firefox plugin called NoScript. It can selectively block javascript, Java, Flash, and several other items. It includes whitelisting, so you don't have to continually switch things on and off. Whitelisted sites automatically just work, while all other sites are automatically treated as dangerous and scripting is disabled. You can give temporary permissions to a particular site.


*Figure 1: NoScript blocking Flash.*

If NoScript has a flaw, it's you are going to whitelist potentially hundreds of sites. That gets old real fast. There is a work around though. If you go into the NoScript options, under General, check the "Temporarily allow top-level sites by default", then chose "Base 2nd level domains".

While this does sacrifice a small amount of security, according to the NoScript site itself (http://noscript.net/faq#qa1_11), "When a respectable site gets compromised, 99.9% of the times malicious scripts are still hosted on a different domain which is likely not in your whitelist, and gets just *included* by the pages you trust. Since NoScript blocks 3rd party scripts which have not been explicitly whitelisted themselves, you're still safe..." Beats turning NoScript off out of frustration by a long way.

Unfortunately for NoScript users, some sites, not a majority, but enough to be a nuisance, do use scripts that come from another domain. Symptoms that you need to whitelist a "3rd party" script include pictures not displaying, the site search box doesn't work, or clicking on links doesn't do anything. You will have to discover which domain(s) is the correct one to get full functionality from that website. However, once you white list these few, you'll be good to go. Since most people only regularly visit a few sites, it won't take long for you to build up a whitelist of your favorite sites that you trust or need to allow scripts to display, etc.

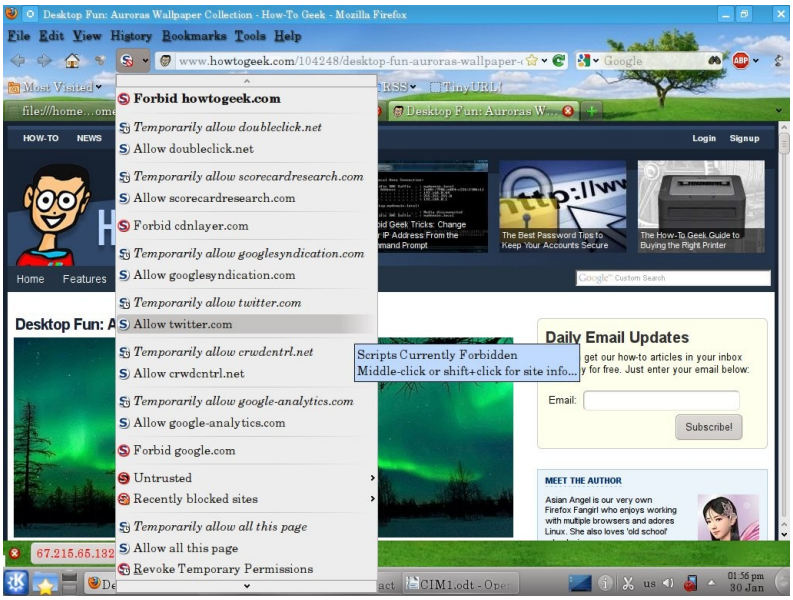


*Figure 2: This site uses lots of 3rd party scripts. In this case, cdnlayer.com must be allowed in order for the pictures to display (already done).*

Chrome includes a similar function to NoScript, but no where near as powerful, nor as useful. You can tell Chrome to block all javascript by default, then selectively whitelist sites. To whitelist sites, click on the box with the red X through it in the upper right corner, then select “Always allow javascript on [site name]”. However, this allows all javascript on that page, even 3rd party scripts and you have to manually refresh the page to see the changes. Because so many sites effectively require javascript, and it doesn't block 3rd party scripts, it offers little protection.

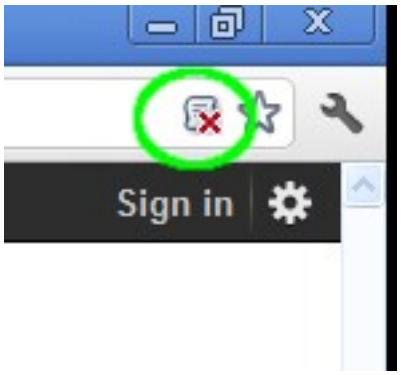


*Figure 3: Chrome's javascript whitelist icon*

Internet Explorer (IE) users are out of luck for javascript protection. You can turn javascript off, on, or prompt. The prompt might sound like a reasonable compromise, but it prompts you on EVERY script on EVERY page. The prompt tells you nothing about the script wanting to execute, so can't selectively block. There is no whitelist feature. You won't last long before you just turn it back on. You can use the different zones to selectively allow javascript on some sites but not others, but then you run into the same problem as Chrome. Too many sites require javascript to function properly.

All modern versions of the browser mentioned, Chrome, Firefox, and Internet Explorer (version 8+) offer built in anti-phishing and anti-malware protection. Chrome and Firefox's are at least partially based off a Google list, while IE uses other source(s). Some researchers give IE the edge currently in blocking the bad sites. If your browser tells you it's a bad site, stay away!

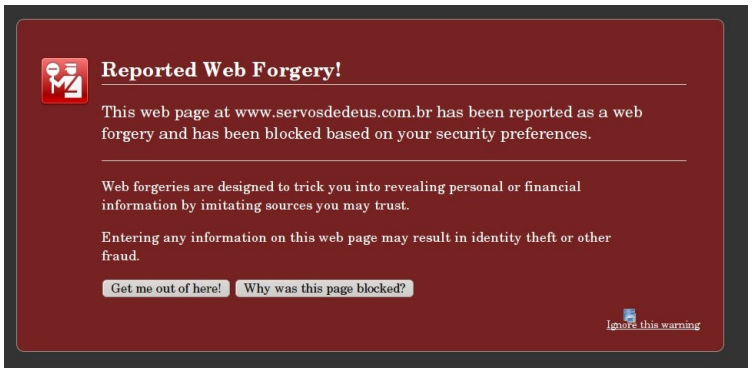


*Figure 4: Firefox's built in phishing protection at work.*

## Firewalls and NAT

Since XP SP2, every version of Windows comes with a free firewall. It's not the fanciest thing in the world, but it works, and should be enabled unless you have a very, very good reason to disable it. If you want to go with a fancier third party firewall, that's fine.

It seems strange that a simple, free with Windows, left with the default settings program can make a difference, but it can. A study by Craig Wright (http://www.sans.org/reading_room/whitepapers/riskmanagement/question-platinum_33579) tested 640 XP SP2 machines. None had any antivirus, nor any users, and automatic updates were turned off (i.e. no patches). They were connected directly to the Internet and monitored to see how soon they were infected.

With Windows firewall turned off, the average time to infection was 18.16 hours. With Windows firewall turned ON, the average time to infection was 336 days, with the first infection happening in 108 days. Thus, the simple act of turning on the firewall made a significant difference.

### OpenDNS

Another simple step you can take to reduce the chances of getting infected is to not visit the websites that distribute malware and are involved in phishing. But how do you know which sites to avoid ahead of time, especially when the list changes constantly? You don't, but then, you don't have to.

Several companies offer a free DNS filter service. These companies maintain realtime blacklists of malware, phishing, and spyware sites. By using their DNS servers, any attempt to reach the bad sites using a domain name will be blocked automatically. A simple, one-time change on your computer or home router can prevent an infection.

One of the biggest names that offers this service is OpenDNS, which also allows customized filters for a small fee. Simply change your DNS servers to 208.67.222.222 and 208.67.220.220 in your computer or router and you're done. HALNET members already have OpenDNS, so they don't have to do anything.

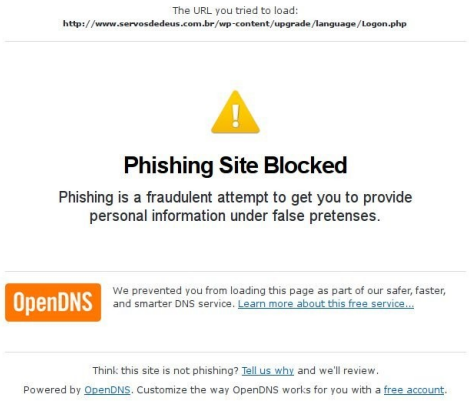


*Figure 5: OpenDNS stopped you from going to a site you really don't want to visit.*

There are a few others that also offer this service. Comodo offers their Comodo Secure DNS (instructions at http://www.comodo.com/secure-dns/), and Symantec offers Norton DNS. Google's DNS service does not filter out malware and phishing sites and is not suitable for this purpose.

Be warned that, especially for people outside the United States, using these services may slow down your downloads and web surfing, despite their claims of speeding things up, so there is a trade-off.

## *This is too much trouble*

Some readers might be thinking to themselves, “This is too much trouble. For starters, I don't know how to do some of things mentioned.” That's no excuse. There are computer user groups that can help you if you just ask, such as HAL-PC if you live in the Houston area. You could also pay someone to do it for you. Not doing these things pretty much guarantees you'll be paying someone to remove the malware later.

In addition to paying to remove the malware, you could be paying in other ways, quite literally. Ask Karen McCarthy, whose company lost $146,000 to malware and may go bankrupt (http://krebsonsecurity.com/2010/02/n-y-firm-faces-bankruptcy-from-164000-e-banking-loss/), or Elie Kassab, who lost around $60,000 (http://krebsonsecurity.com/2010/02/a-tale-of-two-victims/), and the some 3,000 banks accounts in the UK drained of over $1 million (http://techcrunch.com/2010/08/11/new-sophisticated-trojan-which-is-undetectable-has-emptied-bank-accounts-worldwide/).

There are tens of thousands more victims who's names never make the news. You can't afford not to take this seriously. Don't think your bank will protect you or reimburse you. Maybe they will, but you don't really want to take that chance. Karen McCarthy (above) found that out the hard way, as did Patco Construction, who lost $358,000 and the court battle to make the bank pay up (http://www.infosecurity-magazine.com/view/18512/bank-dodges-legal-bullet-over-zeus-trojan-lawsuit/).

## *Response to infections*

Should you find out, or suspect your machine is infected, or one of your passwords is compromised, the clock is ticking. If it's a password compromised, and you can't find a good explanation, such as the

website where you used that password was broken into, you should assume the worst. If you reused that password somewhere else, assume that account is compromised too. If it's not, it soon will be.

First, stop using the computer. Anything you do can be seen by the bad guys. This especially involves anything with usernames and passwords. Stored passwords and usernames can be harvested. It's probably too late, but an off computer can't transmit anything. An off computer also can't be destroyed. The Zeus trojan includes a kill operating system command which the criminals use as a diversion while they drain your accounts.

Second, using another, hopefully clean computer, or live CD, check any financial accounts you access from that computer. This includes, but is not limited to, credit cards, bank accounts, and brokerage accounts. If need be, stop in and see them or call them. If you call them, do not use the infected computer to look up the number. At least one trojan will throw up a fake support number if it detects you searching for one.

Next, check your backups (you do have backups right?) and get your computer cleaned. Just remember that your backups might have the malware included in the backup, and restoring from them could just reinstall the malware.

Finally, never reuse any of the old passwords. My experience at HALNET has taught me the criminals will try the old passwords again from time to time.

## *Coming Soon*

In part 2 of this series, I'll go over how to actually clean an infected computer, including a technique that some to many “professional” places don't use, but really should.

## *Update (03/31/2012)*

In addition to NoScript, there is another, confusingly similar, Firefox extension called RequestPolicy. The difference between the two is subtle. NoScript blocks javascript, Java, and Flash. It can do that whether they come from a third party site, or the site you are visiting itself. NoScript can not block http requests to another site, such as those found in many cross-site request forgery attacks.

RequestPolicy only blocks requests to another site. It can not block any content, such as malicious javascript or plugins coming from the site you are currently visiting. Only if the site calls them from another site, can RequestPolicy block them.

RequestPolicy suffers from the same problem as NoScript in that enough websites do use content from other domains legitimately that you have to go through the same whitelisting headaches. Further, RequestPolicy blocking can really mess up the way a page looks, much more than NoScript does. This is because sites do legitimately use content from third party sites, including content affecting the layout of the page, such as CSS files. When RequestPolicy is blocking content, a little flag in the lower right corner (visible in Figure 6) will be red. Click on that to see what's blocked an unblock it.

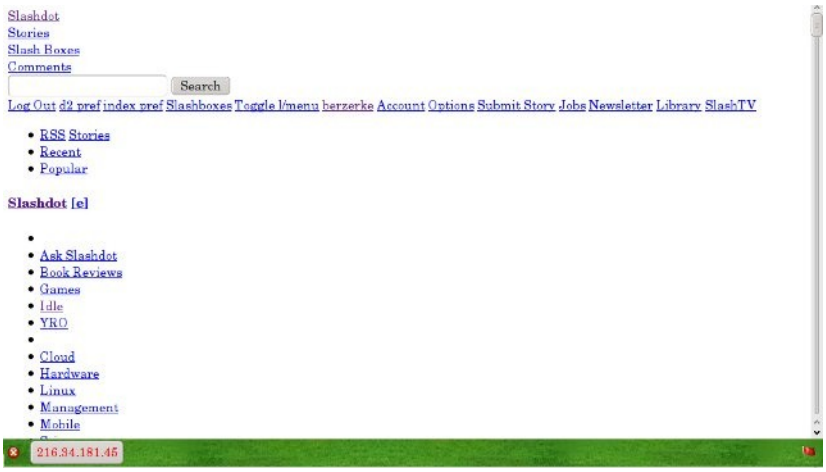


*Figure 6: If you find pages (http://slashdot.org in this example) looking like this, it likely means RequestPolicy is blocking needed content. In this case, content from fsdn.com.*


*Figure 7: The flag shows content (a picture) has been blocked. Hovering over it tells you to what the source is.*

Some blocked content is displayed as a grayed out red flag as shown in Figure 7. If you hover over the flag, you'll see the site you need to unblock in order to see the content. You can then go down to the flag in the lower right corner and click on it (shown in Figure 6). Under blocked destinations will be, in this example, uclick.com. Hover the mouse pointer over that, and a new menu pops up, seen below. Click on the top choice to unblock permanently.


*Figure 8: The first choice is the best.*

You can run both NoScript and RequestPolicy at the same time. It which case, many legitimate cross-site requests must be whitelisted in both extensions. Between the two, NoScript is easier to use and will potentially impact your browsing less. But recognizing that desired content has been blocked is a bit harder and involves some trial and error on the unblocking.

If you are using NoScript as recommended in this article, RequestPolicy will give you better protection. RequestPolicy does make it easier to recognize content has been blocked and get it unblocked, often unblocking needed javascript as a side effect. But, you'll have to do it more often than with NoScript, and you'll be prompted on whenever a page tries to redirect you to another page. Usually, but not always, redirects are harmless and often helpful.

Chrome users have an extension called ScriptNo, which mimics many of NoScript's functions, although it is not affiliated with NoScript. It is recommend for Chrome users for the same reasons NoScript is recommended for Firefox users.