Ten Ways to Dodge CyberBullets: Reloaded

Revised 12-08-2011

David Harley, FBCS, CITP, CISSP

eset

Table of Contents

Introduction

From time to time, ESET's research teams across the globe revisit their ideas for a "top ten things that people can do to protect themselves against malicious activity" list. While the threat landscape changes all the time as criminals and security companies introduce new techniques and countermeasures, the basic principles of self-defense stay constant, so even while detail changes, as it has here, the underlying advice hasn't changed much.

David Harley, CITP, FBCS, CISSP
ESET Senior Research Fellow
December 12, 2011

1. Don't let AutoRun be AutoInfect

We've been explaining for a long time why AutoRun has presented such a problem in recent years. INF/AutoRun is ESET's generic detection system covering a wide range of malware families that install or modify autorun.inf files in order to infect systems. It consistently appears in the top three in ESET's **ThreatSense.Net®** monthly figures. [1]

In recent years, Microsoft has taken steps to address this loophole: First, by turning off AutoRun by default in Windows 7, then by **making patches available** [2] for XP, Vista and Windows Server, and finally by **pushing the changes out** [3]through Windows Update so that many more systems would then be updated automatically. Better late than never, some would say: In fact, ESET's former director of technical education, Randy Abrams, has described it as "a very late response to a well-known problem that had a very predictable response." [4]

Still, that change has greatly reduced the volume of malware infections exploiting the AutoRun facility, though it hasn't (and can't) make the problem disappear completely. Microsoft tells us that it saw infections on XP and Vista reduced by 1.3 million in the first few months after the changes to Windows update, but we still see high volumes of AutoRun infection attempts [4], indicating that there are other factors at play.

Consider, for instance, the fact that XP SP2 is out of support, so that the figures for machines that aren't updated beyond that show only a small drop. But that doesn't, of course, mean that they aren't a channel for infection attempts. Don't assume, either, that this single precaution will save you from every example of this type of threat. Most malware uses more than one technique to infect targeted systems.

It's not all about INF/AutoRun, of course: Many threats that are detected by more specific names (some versions of Win32/Conficker [5], for example) make use of the same vector.

Here's the description of INF/AutoRun based on the one we use currently in our monthly threat reports:

> This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/AutoRun, unless it is identified as a member of a specific malware family.

What does this mean for the end user?

Removable devices are useful and very popular. Of course, malware authors are well aware of this, as INF/AutoRun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default AutoRun setting in an unpatched version of Windows (apart from Windows 7) will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices. While this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

2. Catch the patch batch

Speaking of patches...Keep applications and operating system components up to date with automated updates and patches and by regularly reviewing the vendors' product update sections on their websites.

This point is particularly relevant given the volumes of Conficker [5] that we're continuing to see, long after its heyday. It's important to note that it's possible to avoid most Conficker infection risks generically by practicing "safe hex." Keep up to date with system patches, disable AutoRun and don't use unsecured shared folders. In view of all the publicity Conficker has received, and its extensive use of **vulnerabilities** [6] that have been remediable literally for years, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions, but clearly it isn't happening.

Sometimes it seems that the whole world assumes that the only vendor that suffers from vulnerabilities in its operating system and other software is Microsoft. To see how misleading claims like this can be, check out the weekly "Consensus Security Vulnerability Alert" published by SANS (see http://portal.sans.org), which summarizes some of the most important vulnerabilities and exploits identified in the preceding week. Even during a week that includes "Patch Tuesday," you'll typically find that problems are flagged with a frightening number of applications from other vendors. Certainly, all system administrators should consider making use of this resource.

In recent years, vulnerabilities in applications have become a serious threat (arguably more so than operating system vulnerabilities). Third-party applications are expected to continue to bear the brunt of vulnerability attacks for a good while yet, as security improvements in operating systems will continue to drive vulnerability research to applications like web browsers, various app stores, practically anything made by Adobe or Oracle, many IM clients and other applications. In addition, there's an increasing interest in SCADA (Supervisory Control and Data Acquisition) [7] systems exploitation [8], though that's not typically something the everyday user can do much about.

Unfortunately, users are far less savvy about patching third-party applications than they are about patching the operating system. However, this vector will also decline in impact as application vendors learn to tighten their quality control and patching methodologies.

3. Do you need administrative privileges?

Log on to your computer with an account that doesn't have "Administrator" privileges to reduce the likelihood and severity of damage from self-installing malware. Multiuser operating systems (and nowadays, few operating systems assume that a machine will be used by a single user at a single level of privilege) allow you to create an account for everyday use that allows you fewer privileges than are available to an administrator.

Most competent system administrators are familiar with (and adhere to) this "principle of least privilege"—simplistically, the more privileges you have as a user, the more damage you can do—and use a privileged account only when it is needed to perform a specific task. Following their lead will give an extra layer of protection. However, as always, you shouldn't think of this as any sort of magic bullet. Apart from the fact that there is no magic bullet, some modern operating systems have somewhat diluted the least-privilege model, making it rather easy for a user with little knowledge of the security implications of administrative privilege to use it inappropriately, exposing the system to threat.

4. Good password practice

Use different passwords for your computer and online services. Also, it's good practice to change passwords on a regular basis and avoid simple passwords, especially those that are easily guessed.

It's debatable whether enforced, frequent changes of hard-to-remember passwords are always constructive (they can force the user to write down passwords, for example, which may well swap one security problem for another).

However, you should certainly be aware that if some miscreant guesses or cracks one of your passwords, using different passwords for other services and for your system passwords drastically limits the damage that he or she can do. If, on the other hand, you use the same password for different accounts, you run the risk that one lucky guess will give the cracker the keys to the kingdom. Indeed, it's likely that one of the reasons that quite trivial accounts are sometimes phished is that they give a cracker a head start on guessing the password for other, more profitable and more easily plundered accounts.

You might find this paper by David Harley and Randy Abrams on good password practice useful (**http://www.eset.com/download/whitepapers/EsetWP-KeepingSecrets20090814.pdf**), as well as some other ESET articles, including:

- **Password strategies: Who goes there?** [9]
- **Good passwords are no joke** [10]
- **No chocolates for my passwords please!** [11]
- **Choosing your password** [12]

You might also find this SANS newsletter on keeping your passwords safe interesting and useful: **http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201105_en.pdf**.

5. Trust people, not addresses

Don't trust unsolicited files or embedded links, even from friends.

It's easy to spoof e-mail addresses, for instance, so that an e-mail appears to come from someone other than the real sender (who/which may in any case be a spam tool rather than a human being). Basic SMTP (Simple Mail Transfer Protocol) doesn't validate the sender's address in the "From" field, though well-secured mail services do often include such functionality.

I remember years ago one of my colleagues at a medical research charity in the UK sent an e-mail as a joke using someone else's address, a trick that's easily performed using telnet and an unsecured mail server, especially when you and the victim on the same network. On that occasion, I was able to identify the real sender immediately by his IP address (much to his surprise), but the nature of the 21st-century Internet means that there are many ways of concealing such information if you really want to stay hidden. to stay hidden.

It's also possible for mail to be sent from your account without your knowledge, by malware, though malware that works in this way is far rarer than it used to be. It's far more effective for a spammer to hire the services of a bot-herder nowadays, and malware that manages to infect your system doesn't have to use your mail account or client software to send spam, scams and malware on to other victims.

There are also many ways to disguise a harmful link so that it looks like something quite different, whether it's in e-mail, chat or whatever. The disguising of malicious links in phishing e-mails so that they appear to go to a legitimate site has obligated developers to reengineer browsers to make it easier to spot such spoofing.

However, too many people forget to make use of elementary precautions such as passing the mouse cursor over the link so that the real link shows up. In any case, it's not always easy to distinguish a genuine site from a fake site just from the URL, even if the URL is rendered correctly. (Early phishing e-mails tended to rely on exploiting bugs in popular browsers to hide the real target link.) DNS cache poisoning, for instance, allows an attacker to redirect a web query to an IP address under the attacker's control.

6. Social networks can be very anti-social

Don't disclose sensitive information on websites like Facebook or LinkedIn if you can't be sure that you can limit access to those data. Even information that in itself is innocuous can be combined with other harmless information and used in social engineering attacks.

In recent years, we've seen increased targeting of social networks: notably Facebook, LinkedIn and Twitter in the United States, and Orkut and Hi5 in South America. Attackers are looking for data they can exploit from a social engineering standpoint, but also for cross-site scripting and replicable malware attacks on the websites as well as their APIs (Application Programming Interfaces).

Data mining (both legitimate and criminal) is having a wider range of effects on individuals, and some of those effects are far from beneficial. A notable example is Facebook's lack of commitment to a realistic security model, which would be a very significant supplement to its rather generic security center advice. It seems to me that Facebook is encouraging its users to share as much information as possible, while essentially making them responsible for the security of their own data. This isn't unique to Facebook, of course, or even to Web 2.0 providers in general. But some such services are grooming us to accept that it's legitimate for an ever-wider pool of data to be used to monitor our behavior. It's becoming harder to distinguish between appropriate and illicit use of personal data, in terms of targeting both advertised content and services, and of monitoring for security purposes by financial and governmental institutions, for instance. Lines are sometimes quite blurred between legitimate and criminal data mining in some of these areas, and there are questions to be asked about validation.

Privacy tends to diminish where it's in the way of commercial rather than political interests. So, ironically enough, there is particular and ongoing interest and even indignation regarding data leakage where it affects public bodies, but selling of information at the back door by more or less legal means continues, though it attracts more attention these days. This may be less true in Europe, where data protection and other directives already give some formal weight to the principle that organizations should only hold as much personal data as they need, rather than what they want. On the other hand, the libertarian lobby in the United States may eventually take more notice of this issue, and its potential influence is considerable.

Paul Laudanski has written a couple of lengthy blog articles addressing Facebook and LinkedIn privacy issues:

- **Facebook Privacy: An Easy How-to Guide to Protecting Yourself** [13]
- **LinkedIn Privacy: An Easy How-to Guide to Protecting Yourself** [14]

7. Call for backup

If sensitive information is stored on your hard drive (and if you don't have something worth protecting on your system, you're probably not reading this paper), protect it with encryption.

Furthermore, when you copy or move data elsewhere, through removable media or electronic transfer, it's important to protect/encrypt it. Even if the target storage device is secure from malware or hacking, you need to be aware of other dangers such as physical risks, transit risks, business-related risks (such as an escrow site going out of business) and so on.

Consider (seriously) regularly backing up your data to a separate disk (as a bare minimum) and, where possible, to a remote site or facility. Sounds extreme? Think about it:

You can't rely on backing up to another partition on the same disk as the original; if the disk dies, chances are all partitions will be lost.

You can't rely on backing up to another disk on the same system. If the system is stolen, or there's a fire, for instance, then in the immortal words of Tom Lehrer, they will "all go together." In the latter instance, chances are you'll lose your thumb drives, CD-RWs and so on.

And if you're working in a corporate environment, you might want to avoid doing what one site I know of did: back up data to a server, but forget to back up the server itself.

Aryeh Goretsky has a white paper on backing up your data at **http://www.eset.com/fileadmin/Images/US/Docs/Home/Staying_Secure/2205_19_0_EsetWP-OptionsBackingUpComputer.pdf**. [15]

I'm sure I don't need to remind you to take care of your passwords as well, do I?

8. Antivirus isn't total security

Don't expect antivirus alone to protect you from everything.

Use additional measures such as a personal firewall, antispam and anti-phishing toolbars, but be aware that there is a lot of fake security software out there. This means that you need to take care to invest in reputable security solutions, not malware that claims to fix nonexistent problems, or toolbars that are designed to divert you away from the sites you want to visit and toward the ones that generate revenue for adware providers.

Apart from that, even the best protection might not protect you as well as common sense and caution. There is no silver bullet in protection from malware, which is why we always advocate multi-layering or defense in depth. Specifically, don't fall for the "I can do anything and click on anything because my antivirus will protect me" trap. There seems to be a temptation for people to cluster at one of two extremes.

Some people have such touching faith in their AV that they assume it will catch everything malicious that's thrown at their system, so they don't run anything else and are convinced that they don't need to think about their own security. When they eventually find that their system has been infected, whether it's by something they've clicked on incautiously or something a little more subtle, like a zero-day vulnerability or a drive-by download, they feel betrayed and angry. That's understandable, but it comes from a misunderstanding of the limitations of all security software. For every technical solution (not just AV), there is at least one way of getting around it.

Others take the view that antivirus is no use at all because it only detects malware it already knows about. That isn't the case; only the most primitive modern antimalware relies purely on signatures of known malware variants. Good antimalware products incorporate tools like generic detection, advanced heuristics, sandboxing, whitelisting and so on into an integrated product that catches a high percentage of all malware, not just viruses.

The danger in both scenarios is that the individual is tempted to substitute one partially successful solution for another. (Some marketing departments may overstate the effectiveness of a product, but that problem isn't restricted to the antimalware industry, or even the security industry!)

The trick is not to rely solely on one solution at all. A diverse spread of partially successful solutions (aka "multilayering") may be more successful...However, note that word: diverse. For most people, half a dozen antivirus packages on a single desktop machine are likely to cause more problems than they solve. By multilayering, I mean using a diversity of product types. Using multiple antivirus products may catch more specific malicious programs, but the increased detection may not be worth the additional strain on resources and risk of program conflicts, false positives and so on.

Also, please bear in mind that malware gangs spend a lot of development time tweaking binaries so that they will evade specific scanners. The more effective a scanner is, the likelier it becomes that it will be targeted in this way. Of course, we monitor these tricks closely and enhance our own detection accordingly, but there is always a risk that such a tweaked binary will reach you before we've received a sample and updated our detection.

For this reason, we're always grateful to receive samples of malware (or indeed false positives) that have evaded our products. For details on how to do this, take a look at: **http://kb.eset.com/esetkb/index?page=content&id=SOLN141**.

9. Be wireless, not careless

Don't connect to just any free Wi-Fi access point; it might alter your DNS queries or be the "evil twin" of a legitimate access point, set up to intercept your logins and online transactions. (When I have occasion to see what networks are being offered to me in hotels, airports, even on the apartment block where I live, I have to wonder how many of them are legitimate.)

Our colleagues in Bratislava have posted a useful article called "Summer Surfing on Free Wi-Fi: Work or Play, but stay secured" (see **http://www.eset.eu/press/summer-surfing-on-free-wifi**). Of course, many of the points made there are just as valid at any time of year. Here's a summary of some of them:

Be aware of some common security issues with hot spots:

- "Evil twin" login interception, a scenario where a network is set up by hackers to resemble legitimate Wi-Fi hot spots in order to intercept your login credentials for legitimate networks and sites.
- Previously unknown (zero-day) attacks exploiting operating system or application vulnerabilities.
- Sniffing, or using computer software and/or hardware to intercept and monitor traffic passing over a network.
- Other forms of data leakage using man-in-the-middle attacks.

Also be aware of ways to reduce your attack surface and protect your computer:

- Ensure VPN pass-through ports are enabled, but don't allow a high port free-for-all; professional system administrators open only necessary ports. This doesn't stop all attacks, but it does reduce them.
- Use HTTPS to access webmail.
- Wherever possible, avoid protocols that don't include encryption.
- Disable sharing of files, folders, services.
- Avoid connecting to sites that transfer sensitive data—your banking information, for instance—when connected to an untrusted access point.
- Ensure you're using sound firewalling, antimalware, HIPS and so on.

10. Don't be a pirate

Don't use cracked/pirated software. Such programs provide an easy avenue for introducing malware into (or exploiting weaknesses in) a system. The illegal P2P (peer-to-peer) distribution of copyrighted audio and video files is dangerous. Some of these are counterfeited or modified so that they can be used directly in the malware distribution process.

Even if a utility seems to come from a trusted and trustworthy source rather than Mrs. Miggins' Warez Emporium, it pays to verify, as best you can, that it's genuine.

Win32/GetCodec.A is a type of malware that modifies media files. This trojan converts all audio files found on a computer to the WMA format and adds a field to the header that includes a URL pointing the user to malicious content, claiming that the fake "codec" has to be downloaded so that the media file can be read.

WMA/TrojanDownloader.GetCodec.Gen is a downloader that facilitates infection by GetCodec variants like Win32/GetCodec.A.

Passing off a malicious file as a new video codec is a long-standing social engineering technique exploited by many malware authors and distributors. The victim is tricked into running malicious code he believes will do something useful or interesting. While there's no simple, universal test to indicate whether what appears to be a new codec is a genuine enhancement or a trojan of some sort, we would encourage you to be cautious and sceptical about any unsolicited invitation to download a new utility. Even if the utility seems to come from a trusted site (see **http://www.eset.com/threat-center/blog/?p=828**, for example), it pays to verify as best you can that it's genuine.

Author Biography

David Harley, CITP, FBCS, CISSP, is an IT security researcher, author and consultant living in the United Kingdom, known for his books on and research into malware, Mac security, anti-malware product testing and management of e-mail abuse [16]. He is a Fellow of the BCS Institute [17], CEO of Small Blue-Green World [18], a Director of the Anti-Malware Testing Standards Organization [19] and Senior Research Fellow at ESET.

References

[1] http://www.eset.com/us/threat-center/threatsense-net

[2] Randy Abrams, *Now you can fix Autorun*: http://blog.eset.com/2009/08/25/now-you-can-fix-autorun

[3] Dan Goodin, *Microsoft finally says adios to Autorun*: http://www.theregister.co.uk/2011/02/08/microsoft_windows_autorun_retirement/

[4] http://www.eset.com/us/resources/threat-trends/Global_Threat_Trends_June_2011.pdf

[5] http://blog.eset.com/?s=conficker

[6] http://technet.microsoft.com/en-us/security/dd452420

[7] http://blog.eset.com/?s=SCADA

[8] http://www.eset.com/us/resources/white-papers/Scared-for-Scada-Post-Infosec.pdf

[9] http://www.scmagazineus.com/password-strategies-who-goes-there/article/203519/

[10] http://www.scmagazineus.com/good-passwords-are-no-joke/article/204675/

[11] http://blog.eset.com/2011/05/19/no-chocolates-for-my-passwords-please

[12] http://www.securingourecity.org/resources/pdf/choosing_your_password.pdf

[13] http://blog.eset.com/2011/05/25/facebook-privacy

[14] http://blog.eset.com/2011/06/22/linkedin-privacy

[15] Aryeh Goretsky, *Options for backing up your computer:* http://www.eset.com/fileadmin/Images/US/Docs/Home/Staying_Secure/2205_19_0_EsetWP-OptionsBackingUpComputer.pdf

[16] http://en.wikipedia.org/wiki/David_Harley

[17] http://www.bcs.org/

[18] http://www.smallblue-greenworld.co.uk/

[19] http://www.amtso.org/

www.eset.com

ESETDCBWP20111208