April 2012

Feature Article: Now Google Privacy Policy Reaches the Cloud

eset

Table of Contents

Now Google Privacy Policy Reaches the Cloud

If you use the Internet, or an iPhone, or an Android phone, or a Kindle or an iPad, you very likely use Google in some shape or form. And if you take a keen interest in how your personal information is used, you probably know that on March 1, 2012, the world's largest collector of personal data, Google, changed the way it uses information about you. But how big of a deal is this? Well, our blog post on Google privacy changes is the currently the most popular post of the year on the ESET blog.

What, if anything, should you be doing differently today to protect data that Google may be collecting about you? We answered this question in some detail in the blog post but our advice boils down to two points:

1. Read the privacy policy that applies to whatever Google services you are using.

2. Investigate Google's use of data about you and control that use by visiting the Dashboard.

Let's start answering those questions by picturing just how much data about its users Google has the potential to tap. The infographic on the right is titled: "Google Data Mining Bonanza." It shows some, but not all, of the different "pools" of data that Google could potentially access in order to build a picture of you and your interests as you use different Google services.

Just to be clear, we are not saying that Google is actively mining all this data to create detailed profiles of people that are shared inappropriately with third parties. But we are saying that the changes Google made on March 1 have raised numerous questions to which we have not yet found answers.

The most visible sign of those March 1 changes is a "unified privacy policy" that combines over 60 separate privacy policies for different Google services into one. There is much to be said for the benefits of a unified privacy policy, but applying one retroactively is problematic. That is why the folks who first thought about privacy and computer-based information systems chose, as the first privacy principle: Notice/Consent.

To its credit, Google gave plenty of Notice of the March 1 changes, but when you first signed up for something like Gmail I'm guessing you did not give informed consent to what Google is doing with your data today. And millions of users of those scores of Google services have time and data invested in them which make withholding consent, where that is an option, problematic to say the least.

How about Google Search? A quick back-of-the-envelope calculation tells me it is quite possible that I've performed more than 47,000 searches via Google in the same time period. What a picture those search terms could paint! And if it's moving pictures you want, consider the YouTube videos that I have uploaded, commented on, searched for and watched.

Not that I think I am personally of great interest to Google or the world in general, the point is I am valuable to Google as a potential clicker of online advertisements; and Google has found that my value increases each time the company can pipe another source of data about me into the ad targeting mix. Like a lot of people, including many fans of Google, I am now wondering what could happen to my "pooled" Google data.

(See the Annexe: Image 1)

How to recognize a PC support scam

David Harley, ESET Senior Research Fellow

Not content with perpetrating phishing attacks and spreading malware infections, some people who are committed to ripping off computer owners also use the telephone as an attack vector, as documented by numerous posts on the ESET blog. We see these “PC support” scams being reported at least as far back as 2009 when stories started to appear in Australian newspapers. We then saw outbreaks in the UK and more recently the USA.

Many of these callers sound as if they are working from scripts and calling from call centers of some kind. They may offer to help solve your computer problems or sell you a software license and often imply a Microsoft connection. That has led Microsoft to devote resources to educating the public about the problem, warning that once these scam artists have access to your computer, they can do the following:

- Talk you into installing malicious software that could capture sensitive data such as user names and passwords for bank accounts, email accounts, or social media sites (they may even go one step further and try to charge you to remove the software).

- Trick you into executing commands that enable them to take control of your computer remotely and then adjust settings that leave your computer accessible to strangers.

- Convince you to provide credit card information—either over the phone or by directing you to a fraudulent website—so that they can bill you for what turn out to be phony services.

Clearly you want to avoid falling victim to such malfeasance and so I have pulled together these tips for spotting PC support scams. You may want to share them with friends, family and colleagues at work. Given the persistence of this type of threat you can bet these tips will prove helpful for some time to come.

- If you have caller-ID enabled on your phone display, you may see International or Number Withheld. That doesn't, of course, guarantee a scam. But if you're not accustomed to receiving international calls and you share my dislike of businesses that call without showing the number they're calling from, it is at least a warning to be on your guard. On the other hand, it's far from unusual for a scammer to use what looks like a local number (which may or may not be spoofed).

- India is a major provider of legitimate call-centre services to many parts of the world, so you can't assume that a caller with an Indian or Asiatic accent is a scammer, just as you can't assume that all Nigerians are 419 scammers (or even that all 419s are Nigerian in origin). Nonetheless, at the moment, nearly all the reports of support scams that I'm seeing note that the caller sounds Indian, and almost all of the sites and domains we've been able to trace (and in some cases, block) have had an Indian connection.

- If you're on a national "do-not-call" register, pointing that out early in the conversation is a pretty good way of whether a call is likely to be from the same region. If, as often happens, they take no notice, it's probably a good time to put the phone down.

- The caller is likely to claim to represent or to be affiliated with a well-known name - Microsoft, Cisco and Dell (and, more recently, BT) are frequently mentioned, though the nature of the affiliation is often vague. These big brand names are companies that are very unlikely to contact an end-user directly about a virus problem: frankly, it's pretty time-consuming to trace individual users who may have a security issue.

- The fact that the caller may know your correct name, address and telephone does *not* mean they have access to *any* information about your PC. They're guessing, and if you know enough about your own system to ask how they have the information they claim, their answers make no sense at all. And if, as is often the case, they don't have your correct contact details, how can they possibly know anything about the status of your PC?

Most scam calls rely on the scammer "proving" that he or she can identify problems with your system: in a moment, we'll look at the ways in which they misuse and misrepresent standard Windows utilities as some kind of malware diagnostic, but even before that, they may tell you that they already know you have a security problem because:

- Microsoft, or your ISP, or some other "authority" told them so. The circumstances under which this might be true are very limited indeed: if you think it's possible that it might apply to you, check directly with the "authority". It's naive to take the word of someone who just called you out of the blue. If they're evasive about the exact nature of their relationship with Microsoft (or whoever), I'd suggest you save yourself the bother and just put the phone down.

- The details of your system are on some imaginary database.

- There are spam or virus reports associated with your IP address. Or your phone number. Or, more vaguely, "your computer". Take with a very large pinch of salt. If you don't understand the caller's explanation of how they identified your system, assume that you're being misled. If you think you do understand the explanation, that's probably a tribute to the social engineering talents of the scammer, not a reliable indicator of a bona fide support call.

So what about the ways in which they try to prove to you that your machine is infected by walking you through standard Windows utilities? It's likely that scammers will come up with variations on this approach, but these are the ones that we see most often.

- Event Viewer is a tool that keeps a system log. A scammer is likely to tell you to go to the Run menu and type in *eventvwr*. That will take you to a screen that shows you various system events, some of which will indeed be problems, though they're usually transient problems that have already come and gone. When you see the Event Viewer screen, say something rude and put the phone down, if you've let them get that far.

- Microsoft tells us that ASSOC "Displays or modifies file name extension associations." However, scammers tend to use one of the items near the bottom of the list it outputs that looks like this:

.ZFSendToTarget=CLSID\{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}

- What that ASSOC command actually tells us here is that the .zfsendtotarget extension file is associated with the compressed (zipped) folder form in Microsoft windows. However, the scammer will usually tell you that this is the unique identifier of your PC, as proof that he can see that there is a problem uniquely associated with your PC. Or he may tell you that CLSID stands for Computer License ID, and that you need to renew the license. Either way, he's lying to you. Tell him where to stick his license and put the phone down.

- INF and PREFETCH are legitimate system utilities: The "Prefetch" command shows the contents of C:\Windows\Prefetch, containing files used in loading programs. The "INF" command actually shows the contents of a folder normally named C:\Windows\Inf: it contains files used in installing the system. So how are they misused by scammers? By asking a victim to press Windows-R to get the Run dialogue box, then asking them to type in something "prefetch hidden virus" or "inf trojan malware". When a folder listing like those above appears, the victim believes that the system is listing malicious files. In fact, neither of these commands accepts parameters in the Run box. You could type "inf elvish fantasy" or "prefetch me a gin and tonic" and you'd get exactly the same directory listing, showing legitimate files. Time for another rude word.

For the scammer, there are two other critical steps.

- The main point of the exercise (and they'll probably want you to do it before they actually "fix" your system) is to get you to give hand over credit card details. Make it clear from the start that you're not going to give that information to anyone you can't validate as genuine. In some cases, they may simply give up at this point, or they may try to persuade you that they're genuine by giving some information about themselves (or, more to the point, their company). Tell them you'll call them back and get in touch with the authorities, or even us. Unfortunately, there's a good chance that they'll call you back eventually if you don't ring them back: they really do want your money. Tell them you've talked to the police, or to a security company, or even to Microsoft, and the chances are they'll give up sooner or later, though they may bluster for a while.

- The other is to persuade you to download remote control software (most often from logmein.com or ammyy.com) so that he can demonstrate to you that he's downloading utilities (usually these are free versions of genuine software, but of course they could in principle be anything...) and fixing your imaginary problems. Don't go there: why would you give someone who just rang you up out of the blue access to your system?

Of course, I can't guarantee that they'll use any particular approach, and in fact you may get threatening or abusive behaviour before they give up. Nonetheless, the earlier in the process you disengage and make it clear you're not interested, the less hassle they're likely to give you: at least, in terms of that specific phone call. The advantage to that approach, of course is that it tends to work for other scams (some of which may come from the same call centres): mortgage scams, fake surveys (usually a precursor to a sales pitch or even to a follow-

up scam call, tailored according to your responses) and so on.

See also ESET's white paper Hanging on the Telephone, and the blog articles:

- Support Scammers (mis)using INF and PREFETCH
- Facebook Likes and cold-call scams
- Support Desk Scams: CLSID Not Unique

What if you've fallen for the scam and already given them your credit card details? Contact them and tell them you know you've been scammed, you don't want their phony service, and you want your money back. There are occasional reports that this works. More probably, they'll argue and bully: if so, just drop the call. Shut down the system while you're talking to them, or disconnect from the internet. Obviously, talk to the credit card provider, and see if they have advice.

You probably need to get whatever remote access software they used (it mostly seems to be software from ammyy.com or logmein.com) off the compromised system. It's probably not infected as such (they've probably used free versions of legitimate utilities rather than malware, but I can't guarantee that) but I'm not sure how easy it is for these guys to use it without your knowledge. You should be able to do that from the install/uninstall control panel. If you can't, get help from someone knowledgeable: it's worth paying for help, if necessary.

If you don't have AV (or have a product that was installed by the scammer), try one or two online scans: if they come up clean, the chances are that there's nothing actually malicious on there. In general, these guys take your money for doing nothing much, rather than introducing deliberate infection. ESET, like many other reputable companies, has a free online scanner that uses the same detection engine as its commercial AV scanner, but you should install a proper PC-hosted scanner as well. It's probably better to do that after checking with an online scanner. For most people it's probably better to install a full internet security suite rather than just AV. It doesn't have to be ours, of course, but we happen to think it's pretty good.

I can't guarantee this will fix it, but those are approximately the minimum steps that a real, competent support tech would take. It's probably worth getting in a local professional if you're not confident with the technology yourself. And try to get essential data backed up first.

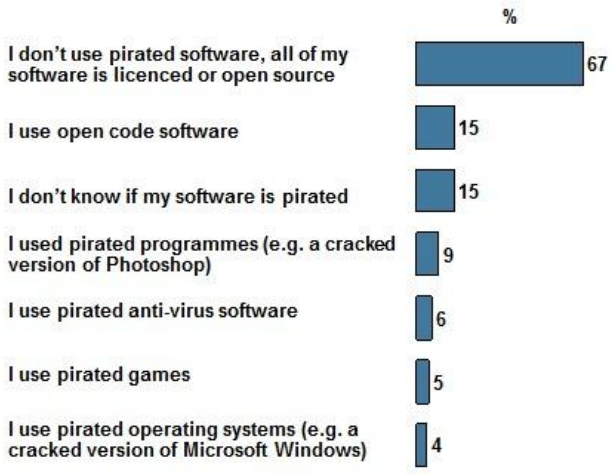
Pirated software: an update from Ireland

Urban Schrott, ESET Ireland

A recent survey commissioned by ESET Ireland indicated that 67% of the people surveyed use legitimate software (or say they do!), men are more likely to pirate than women, and nearly one in five computer users in Munster just doesn't know what they use

Why is a security company like ESET interested in the use of pirated software? Because in our experience the vast majority of pirated software comes with a little something extra attached. A cracked version of a known graphical editing program or a popular computer game isn't made freely available online out of the goodness of someone's heart; more likely it's because someone has an interest in getting a malicious payload installed along with the pirated application.

ESET Ireland, through Amárach research, asked over 1000 people across Ireland about the legitimacy of their software and these are the results:



Since the survey was anonymous, we presume people answered truthfully and it's good news that the vast majority of respondents are users of legal software. The availability of free open source software also makes things easier for many users. But the combined percentage of people using pirated software is still a concern, as is the high number of people that just don't know if their software is legitimate.

The statistical breakdown of the results also offers an interesting picture. The worst offenders with only 51% of their software being legal are in the age group 25-34, while 83% of those over 55 don't use anything pirated. And while most Dubliners know what they use, with only 10% claiming they don't know if it's legitimate, people of Munster seem to be in the dark – 19% answered that they don't know if their software is pirated. And nearly twice as many men (12%) as women (7%) use pirated software.

Statistically Eastern Europe is known for a very high percentage of pirated software in use, and it is no coincidence that they also have by far the highest rates of malware infections: when the Conficker worm raged at its highest volumes, less than one in ten was infected globally, but in Russia and Ukraine it was nearly one in three. Usually the worst-hit victims seem to be the users of pirated operating systems, where malware comes embedded at the heart of their system; and because their software is illegitimate they do not get updated and patched regularly they are vulnerable to most targeted zero-day (and even 30 and 60-day) threats. Attacks via pirated operating systems are closely followed by attacks using pirated security software, with all the irony that involves (wolves guarding sheep, thieves guarding your valuables and so on).

For those companies and consumers who have not yet heard the message and taken it to heart, it bears repeating: Using pirated software does not pay, and the costs can be far higher than buying a license.

The Top Ten Threats

1. HTML/ScrInject.B

Previous Ranking: 1
Percentage Detected: 6.75%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

2. HTML/Iframe.B

Previous Ranking: 3
Percentage Detected: 4.54%

Type of infiltration: Virus

HTML/Iframe.B is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

3. INF/Autorun

Previous Ranking: 2
Percentage Detected: 4.32%

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.

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 Windows 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.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (http://blog.eset.com/?p=94 ; http://blog.eset.com/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

4. JS/Iframe.AS

Previous Ranking: 6
Percentage Detected: 4.14%

JS/Iframe.AS is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

5. Win32/Conficker

Previous Ranking: 4
Percentage Detected: 2.86%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on

Conficker issues: http://blog.eset.com/?cat=145

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 a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

6. Win32/Sirefef

Previous Ranking: 7
Percentage Detected: 1.95%

Win32/Sirefef.A is a trojan that redirects results of online search engines to web sites that contain adware.

7. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 7
Percentage Detected: 1.86%

It is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

8. JS/Agent

Previous Ranking: 5
Percentage Detected: 1.55%

The trojan displays dialogs that ask the user to purchase a specific product/service. After purchasing the product/service, the malware removes itself from the computer. Trojan is probably a part of other malware.

9. Win32/Dorkbot

Previous Ranking: 9
Percentage Detected: 1.53%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX.

The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

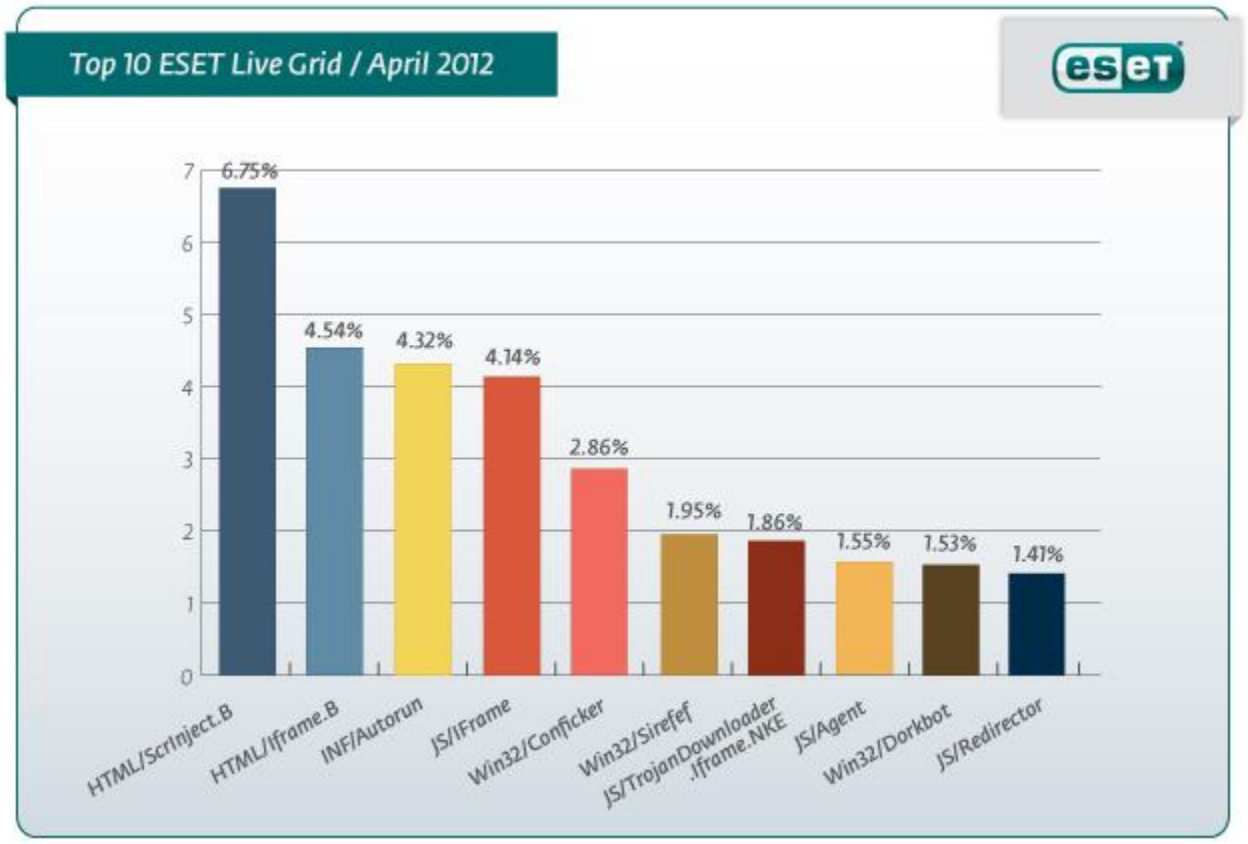
10. JS/Redirector

Previous Ranking: 10
Percentage Detected: 1.41%

JS/Redirector is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

Top Ten Threats at a Glance (graph)

Analysis of ESET Live Grid, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 6.75% of the total, was scored by the HTML/Scrinject.B class of threat.



Annexe

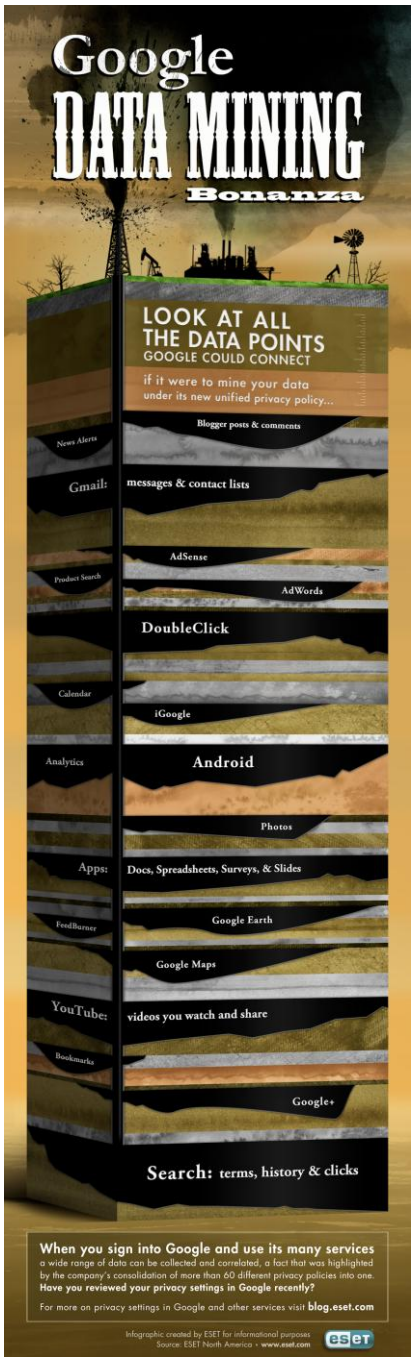


Image 1

About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

Additional resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the ESET Threat Center to view the latest:

- ESET White Papers
- ESET Blog
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation