May 2014

Microsoft REGISTERED Refurbisher

Charlotte County Computer Group

30th YEAR Anniversary

1984 - 2014

The Next General Meeting of CCCGC will be

May 6, 2014

See us on the Web
www.cccgc.net

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

VOL. XXVI

No. V

The President's Platform by Ron Wallis, President CCCGC

Inside this issue:

Well, we have said goodbye to Windows XP, along with many of our snowbirds. The difference is the snowbirds, God willing, will be back, XP won't.

It is also the end of our chilly weather and the busy season. Summer is the time when the Northerners go home, the locals take vacations, and we just sit back and enjoy the hot weather and the break from the busy winter season.

The stores aren't so crowded, the traffic is less, and the pace gets slower. It's a pleasant change. I'm looking forward to it. I hope you will enjoy it as much as I intend to.
With the schools closed there isn't a big demand for computers, so we can get a little break in the back room.

There will be no president's message in the June Bytes as I am taking a short vacation and I don't want to write this while I'm on the road.

Remember, your computer doesn't know it is summer, so keep up your maintenance and backups. You'll be glad you did.

Please note: Our office phone number has changed to 941-585-0356

Ron

Charlotte County Computer Group

2280 Aaron Street
Port Charlotte, FL 33952

Phone: 941-585-0356
941-625-4175 x244
E-**mail:**
office@cccgc.net

Charlotte Bytes

Computer Drawing

Chuck Wright wins again! Chuck had the winning ticket and packed up the computer and all its parts and took it home.

Thanks to everyone who participated. Good luck next time.

50/50 Winner

Charles Crawford won the money.

As you can tell by his picture, Charles is pleased he was the winner.

Off he goes with the cash. To all the ticket purchasers, better luck

Door Prize Winners

Left To Right

Louis Rendano

Salvatore Leto

Rosemary Craemer

Linda Hudson

Pam Stern

WELCOME

New Members

Nancy Sincock	**Robert Fike**	**Ted Robedee**
James King	**Rolf Egelandsdal**	**Marti Orr**
Joan Brocher	**Ian Anderson**	**Edward Sullivan**
Dorothy Keefe	**Joseph Harshman**	**Lynn Keating**
Louis Sabatini	**Thomas Blackman**	**Cheryl McCullough**

The Executive Board and Members of CCCGC welcome each of you to the group. We're Here To Help. Membership Has Its Privileges.

If you have any questions, concerns or need computer help, please contact us at the office. We will endeavor to help you any way we can.

Scott Baty's presentation was on Cloud Computing.

From the ground to the cloud, we use a computer connected to the internet. You can open accounts with the different suppliers for cloud storage. Log onto any computer and get into your cloud account. Think of it as an external hard drive where your information is stored, not in your computer. You can take many pictures and upload them and then supply a link to family or friends and share the pictures. This process applies to documents as well.

Microsoft has SkyDrive that is now named One Drive. Another cloud storage facility is Google Drive or Drop box . Use any one or all of them.

Create documents without having the software on your computer to do so. For instance, One Drive offers Microsoft products like Word, Excel or Power Point. You create the document and store in the cloud without having to buy the software. Google Drive also offers software to create documents or spreadsheets. Google goes one step further and actually opens different file extensions.

When you use web mail, the mail is stored in the cloud, (on their servers) not your computer. This is no different than what we have been doing all along.

You are able to use these storages even if you have a tablet with an android operating system and share these files with a specific person or group.

Happy Cloud Computing

L ydia

Program High-Lights

Charlotte Bytes

Charlotte County Computer Group

Information: (941) 295-7672

(941) 625-4175 x244

Official publication of the Charlotte County

Computer Group Corporation

2280 Aaron Street

Port Charlotte, FL 33952

www.cccgc.info

www.cccgc.net

May Program

Ron Wallis and Yvette Pilch will team up to provide a combination of Backup and a Maintenance excursion for our May presentation.

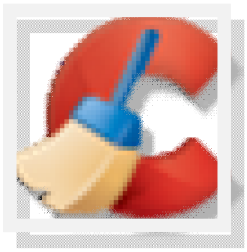
The Backup portion of the presentation will include how to download the free Easeus To Do program and how to complete the backup. Also, included will be the paid program of Acronis for those members who still use it.

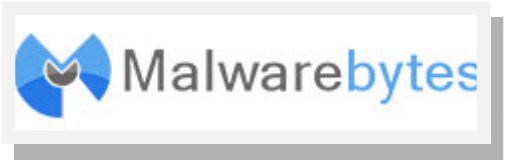
Ron will go through the entire Maintenance process which will include virus and malware protection and cleaning the registry.

Acronis True Image

Other various free or paid Virus Protection

EaseUs To Do Workstation





Microsoft® REGISTERED Refurbisher

For more information go to www.cccgc.info

View/download Bytes

Please be sure to register online for classes

Charlotte County Computer Group

30th YEAR Anniversary 1984 - 2014

Classes & Events Calendar

May 2014 CCCGC Events Calendar

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				1 Classes Canceled	2	3
4	5 Libre Office 2 to 4 PM John Palmer	6 General Meeti 7:15 PM Classes 5:00 PM 6:00 PM	7 Maintenance 2 to 4 PM Ron Wallis	8 Classes Cancele	9	10
11 	12	13 Windows 8.1 2 to 4 PM Ron Wallis	14 World of Google 2 to 4 PM Larry Hurley	15 Back To Basics 2 to 4 PM Dick Evans	16	17
18	19 Libre Office 2 to 4 PM John Palmer	20	21	22 Back To Basics 2 to 4 PM Dick Evans	23	24
25	26 Memorial Day 	27 AndroidTablets 2 to 4 PM Yvette Pilch	28 Home Inventory 2 to 4 PM Larry Hurley	29 Back To Basics 2 to 4 PM Dick Evans Board Meeting 6:30 PM	30	31
		NOTICE All Non Meeting Night Classes will be held in **Our New CCCGC Office.**			**Notes:** OFFICE HOURS: 10:00 AM-2:00 PM MONDAY -FRIDAY **Please sign up for classes ONLINE:** http://www.cccgc.info	

CCCGC

Charlotte County Computer Group

30th YEAR Anniversary

1984 - 2014

The Charlotte County Computer Group Corp.

Is a non-profit 501(c)3 organization as classified by the Internal Revenue Service.

Donations, gifts, bequests, legacies, devices and transfers are deductible under federal laws.

Officers and Board of Directors for 2014

President: Ron Wallis

Vice President: A Yvette Pilch

Secretary: Ron Muschong

Treasurer: Larry Hurley

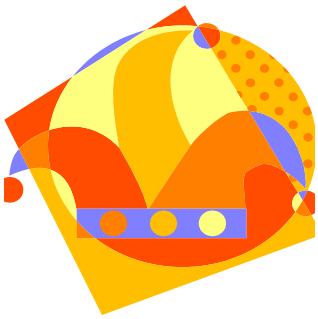
Director: John Hegard

Director: Grover Mudd

Director: Lydia Rist

Director: Frank Messina

Director: Mava Graves



We're on the Web
www.cccgc.net

What is the Internet Of Things?

the How-To Geek
Computer Help from your Friendly How-To Geek

If you read any tech news, you've probably seen "the Internet of Things" mentioned over and over. It's supposedly one of the next big things — but what exactly does it mean? Isn't the Internet already made up of things?

In a nutshell, the Internet of things involves bringing more devices and sensors onto the network, connecting them to the Internet and allowing them to communicate without human interaction.

The Internet of Things Explained

The Internet of Things refers to more devices, objects, and even living beings — people, plants, and animals — being given unique identifiers and the ability to automatically transfer data without human interaction. For example, let's say you own a farm and want to track the soil conditions. You'd have to measure them and enter them into a computer by hand. In the Internet of things scenario, you'd use a sensor that automatically measures the soil conditions and reports them over the network. If these sensors become cheap enough, you might attach a unique sensor to every single plant on the farm to measure its conditions and transfer them over a network automatically. In effect, this would be giving each plant a unique identifier and bringing these plants online.

The Internet of things refers to networking all these different types of "things." This includes everything from smart appliances to health implants that can communicate over a network. Imagine giving more and more things an IP address and connecting them to the Internet using some sort of sensor.

What's the Point?

Right now, most of the data on the Internet comes from human beings. To put a photo online, someone has to take and upload it. To measure a piece of data and get it on the Internet, a person has to get the data and enter it into a computer. But there are only so many human beings, and they only have so much time. The Internet of things would provide us with much more data — imagine if each component in a car could monitor and report its own status in real time. Or imagine a farmer being able to sit down and see the health of each plant in their field along with historical conditions.

Continued on page 15

Sorting out the revolution in PC backups: Part 2

By Fred Langa

In Part 1 of this two-part series, I gave an overview of the five major types of backup technologies available today for Windows PCs. This month, Part 2 shows the enormous speed differences in backup methods; it also includes some real-life scenarios to help you pick the best method for your needs.

Beyond the theories: Backups in real-life

As discussed in Part 1, today's primary backup options include a second internal drive; optical discs (DVDs/CDs); USB-connected external drives; a standalone, network-attached drive or another PC; and cloud-based data-storage services.

Each of those backup types offers its own mix of cost, security, and ease of use. If you haven't read Part 1 yet, I suggest taking a moment to go through it — it'll put each backup type into context, and it might help you better understand the terminology and concepts discussed in this article.

For the five backup types listed above, the most important usability factor is speed. Depending on the size of the data set and the method used, a single back-up (or restore) session can take seconds or days. Obviously, speed is a significant component of your backup-method choice. So this Part 2 of the series includes a Windows Secrets exclusive: real-world timing tests that show how long it takes to back up file sets of different sizes — from a modest 10MB to a hefty 300GB.

Part 2 also includes a closer look at backup usability and applicability to help you make a fully informed decision about your back-up options.

Factors affecting backup speeds and times

Some of the elements of backup speeds are obvious. For example, backing up to an internal drive is clearly going to be faster than backing up to a cloud service via the Internet. Other backup speed factors, such as the innate speed of your PC and its subsystems, are less obvious.

There are also some subtle aspects. For example, backup times will vary depending on whether the source and destination drives are defragged. The amount of background activity, the effects of file caching and compression, whether files are processed serially or in parallel, the proximity of a cloud-storage service's data centers, and so forth can further impact backup speed.

Given all those factors taken together, your backup speeds won't match mine. In fact, your own backup times will vary from day to day. Local factors always win.

While the times posted below have little absolute value, they serve as a perfectly good reference for the relative speeds offered by the different backup types — and these relative differences should hold fairly true across different PC/network/Internet configurations.

Setting up real-world backup-speed tests

To get a solid handle on relative backup speeds, I ran a series of 14 timing tests, using my daily-use systems.

For the first seven tests, I simulated a small backup. For each test, I timed how long it took to back up a single 10MB test file to the following:

- A freshly defragged, conventional, secondary internal drive;
- 16x DVD burner and an empty DVD disc, using the standard live file system (info) format;
- Defragged USB 3.0 conventional external drive;
- Defragged networked drive on a second PC, connected by 802.11g Wi-Fi;
- Defragged networked drive on a second PC, connected by 100Mbs Ethernet;

Continued on next page

CCCGC

Charlotte Bytes

Sorting out the revolution in PC backups: Part 2 Continued

Two cloud-storage services — Google Drive and Microsoft's OneDrive/SkyDrive — accessed via a standard cable Internet connection (Comcast in Boston, Massachusetts).

I then simulated a 1GB backup made up of separate 10MB files, repeating the backup destinations and conditions I used for the 10MB tests.

Finally, as a convenience to readers, I extrapolated those initial 14 tests to post the time it might take to back up 15GB (the approximate size of a small Windows 7 or 8 setup — or a modest disk image) and 300GB (the size of a large Windows system replete with numerous documents, music files, and/or digital images).

A brief technical aside (Skip this paragraph and the next if you don't want the details.) To reduce the possibility of human error, the timing tests were run via automated scripts, with start and stop times recorded by software. To homogenize the file sets (i.e., to minimize any bias toward a specific file type), I used a random-character generator to create a standardized 10MB data file containing 10,000 strings of 1,000 characters each.

The 10MB file's random characters also helped minimize any data-compression bias potentially introduced by the different backup types. For the 1GB test, I used multiple copies of the base 10MB file. I gave each copy a unique name to defeat any local file caching that might skew the results.

To further ensure the real-life quality of these tests, the PCs had configurations that were typical of daily-use systems, and they were run with minimal — but normal — background activity. For example, I kept my antivirus apps (Microsoft Security Essentials and MalwareBytes Pro) active during the tests, so the files were scanned as they passed to and from my systems — just as they would in a real backup.

Quantum differences between the backup options

Table 1 shows the results of the timed 10MB and 1GB backup tests using different destinations — plus the extrapolated times for 15GB and 300GB backups.

	10MB (Seconds)	1GB (Minutes)	15GB (Hours)	300GB (Hours)
Internal hard drive	0.2	1.9	0.5	9.3
External USB 3.0 drive	1.1	2.1	0.5	10.3
Networked drive, 100Mbs Ethernet	1.3	2.7	0.7	13.3
Networked drive, 802.11g Wi-Fi	4.5	3.7	0.9	18.4
Google Drive	6.9	14.7	3.7	73.3
Microsoft OneDrive/SkyDrive	8.1	12.3	3.1	61.7
16x DVD	12.0	6.3	1.6	31.3

To use the table, estimate the likely size(s) of your backup sets. (As one example, use Windows/File Explorer to see how large your Documents folder is.) Find the table's column with a heading closest to the size of your likely backup, and then read down to see the relative backup times for file sets of that approximate size.

Table 1. Real-life backup times for differently sized file sets and destinations

At a glance, it's apparent that large, whole-system data sets will be problematic with cloud-based services. You might be able to live with their 60+ hours to complete a full backup, but two-plus days to restore a system with a few hundred gigabytes of data is probably unacceptable.

On the other hand, backup speeds to internal hard drives, external USB drives, and networked drives are close enough that relative speed is not much of an issue.

Backing up to DVDs has two problems: the time to burn the disc and the time and inconvenience of swapping media for any backup that requires multiple discs.

Weighing all the factors, calling the shot

While backup speed is important, you need to weigh other factors to choose the best backup option or options for yourself. Along with speed, there are the pros and cons discussed in Part 1. And you need to consider the types of files you regularly back up.

These options quickly become clearer once you start applying real-life scenarios.

Continued on next page

CCCGC

Charlotte Bytes

Sorting out the revolution in PC backups: Part 2 Continued

To start, I'll use myself as an example. Here's how I settled on the several backup options I use.

I make my living online, so my backup needs are admittedly more extreme than most people's. But this will show how the various backup techniques apply to different needs.

Take cloud storage, for example. Both Google Drive and Microsoft's OneDrive/SkyDrive would take between two and three full days to back up or restore my complete 300GB Windows setup. To my mind, that's a ridiculous amount of time. For my needs, cloud services are impractical for full-system backups.

But as noted in Part 1, cloud backups are an excellent form of offsite storage that can be further secured with third-party apps that create virtually hack-proof encryption. In other words, cloud storage offers an extremely high degree of both physical and anti-snooping security. That makes them great for long-term storage of extremely important documents and files — ones that you simply can't afford to lose.

For instance, I store copies of sensitive files such as my tax and health records in the cloud. These are files I need to store safely for at least several years — and sometimes more or less permanently. Putting them in the cloud means that, no matter what happens to my PC or my local copies of the files, the cloud-based copies will still be available. The files are generally small, so backup and restore times aren't an issue.

Cloud services offer their own built-in security measures, but for sensitive materials, I add one — and sometimes two — extra levels of third-party encryption. I pre-encrypt the files with tools such as Boxcryptor (free and paid; site) as a second layer of defense. (See the Dec. 12, 2013, Top Story, "Pre-encryption makes cloud-based storage safer.")

For my most sensitive files, I'll add a third layer of defense by encrypting the files with a tool such as 7-Zip (free; site) — before they're encrypted again by Boxcryptor. With three separate layers of security and encryption, these cloud-stored files are essentially uncrackable by hackers or other parties.

I also use cloud storage for copies of my processed photos and videos — again, files that I access infrequently. I keep the raw, full-resolution originals on a fast, local drive, where editing is quick and easy and space isn't an issue. (My local system also has full-strength, image-editing tools instead of the typically limited tools offered by cloud-based photo-storage services.)

Again, the finished, edited photos go into the cloud — where they'll be preserved, no matter what happens to my local systems. I don't use extra security on my cloud-stored photos because there's nothing unusually sensitive about them (how dull, I know), and because I usually want others to see them. Cloud storage makes photo sharing easy; I just send or post the URL of the photos I want to share.

As for regular, whole-system backups — the ones that would take an unacceptably long time via cloud storage — I use a fast, local medium. Once a month or so, I make an image backup using an inexpensive, external, USB drive. (See the Jan. 16 Top Story, "Keep a healthy PC: A routine-maintenance guide.") I then disconnect that drive and store it locally in a safe place. This protects the backups from anything that might compromise my primary drive — such as malware, mechanical or electrical malfunction, fire, etc.

In between full backups, I keep a second, inexpensive USB drive connected to my PC at all times, and I let Windows 8's File History make continuous, near–real time backups. (See the July 11, 2013, Top Story, "Understanding Windows 8's File History.")

I also have a spare PC that I keep on hand and ready to go — a sort of data lifeboat I can call into immediate service if my main PC goes down for any reason. I keep that spare PC up to date and in sync with my main PC by copying files via my local network. For routine synching, I'll use Wi-Fi because it's easy and convenient. If I'm in a hurry, I'll dig out an Ethernet cable and connect the PCs that way. I sync my files with KarenWare's Replicator (site), but there are others — such as Microsoft's SyncToy 2.1 (site) and SourceForge's FreeFileSync (site).

I rarely, if ever, use optical media for backups. As Part 1 discusses, DVDs and CDs are slow, bulky, and expensive for handling large amounts of data. That said, they're still good for creating bootable repair or rescue discs. See, for example, the April 11, 2013, Top Story, "A dozen tools for removing almost any malware."

It's now your turn to choose the backup option

To find the best type of backup for yourself, read Part 1 **(in April Bytes)** if you haven't done so already. Familiarize (or refamiliarize) yourself with the available options.

Charlotte Bytes

See us on the Web
www.cccgc.net

the How-To Geek
Computer Help from your Friendly How-To Geek

CCCGC

Who is Making All This Malware — and Why?

We've come a long way since the days of infected floppy disks moving between DOS computers. Malware isn't about messing with you, joking around, or just causing damage — it's all about profit.

To understand why all this malware is out there and why people are making it, all you have to keep in mind is the profit motive. Criminals make malware and other nasty software to make money.

Early Malware

If you used computers in the 90s, you remember the first mainstream computer viruses. They were often practical jokes of just proofs of concepts, created to mess with your computer and cause damage by people with too much time on their hands. Getting infected by a piece of malware meant that your desktop might be taken over by a pop-up proudly proclaiming that you've been infected. Your computer's performance might deteriorate as a worm tried to send as many copies of itself out onto the Internet as possible. A particularly vicious piece of malware might try to delete everything from your hard drive and make your computer unbootable until you reinstalled Windows.

For example, the Happy99 worm, considered the first virus to spread itself via email, existed only to spread itself. It emailed itself to other computers, caused errors on your computer while doing so, and displayed a "Happy New Year 1999 !!" window with fireworks. This worm didn't do anything beyond spreading itself.

Keyloggers and Trojans

Malware creators are almost purely motivated by profit these days. Malware doesn't want to inform you that you've been compromised, degrade your system performance, or damage your system. Why would a piece of malware want to destroy your software and force you to reinstall Windows? That would only be inconveniencing you and the malware's creator would have one less infected computer.

Instead, the malware wants to infect your system and hide quietly in the background. Often, malware will function as a keylogger and intercept your credit card numbers, online banking passwords, and other sensitive personal data when you type it into your computer. The malware will send this data back to its creator. The malware's creator may not even use these stolen credit card numbers and other personal information. Instead, they may sell it cheaply on a virtual black market to someone else who will take the risk of using the stolen data.

Malware may also function as a Trojan, connecting to a remote server and waiting for instructions. The Trojan will then download whatever other malware the creator wants it to. This allows a malware's creator to keep using those infected computers for other purposes and update them with new versions of malware.

Botnets and Ransomware

Many types of malware also create a "botnet." In effect, the malware turns your computer into a remotely-controlled "bot" that joins with other bots in a large network. The malware's creator can then use this botnet for whatever purpose it likes — or, more likely, the botnet's creator may rent access to the botnet to other criminal enterprises. For example, a botnet could be used to perform a distributed denial-of-service (DDoS) attack on a website, bombarding it with traffic from a huge amount of computers and causing the servers to become unresponsive under the load. Someone could pay for access to a botnet to perform a DDoS attack, perhaps of a competitor's website.

A botnet could also be used to load web pages in the background and click on advertising links on a huge number of different PCs. Many websites make money each time a page loads or an advertising link is clicked, so these page loads and advertising link clicks — designed to look like real traffic from many different computers — can make the website money. This is known as "click fraud."

Continued on page 16

CCCGC

Charlotte Bytes

Warning: Your Browser Extensions Are Spying On You

the How-To Geek
Computer Help from your Friendly How-To Geek

The internet exploded with the news that Google Chrome extensions are being sold and injected with adware. But the little-known and much more important fact is that your extensions are spying on you and selling your browsing history to shady corporations. HTG investigates.

TL;DR version:

Browser add-ons for Chrome, Firefox, and probably other browsers are tracking every single page you visit and sending that data back to a third-party company that pays them for your information.

Some of these add-ons are also injecting ads into the pages that you visit, and Google specifically allows this for some reason as long as it is "clearly disclosed".

Millions of people are being tracked this way and they don't have a clue.

Are we officially calling it spyware? Well… it's not quite that simple. Wikipedia defines spyware as "software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent". That doesn't mean that all software that gathers data is necessarily spyware, and it doesn't mean that all software that sends data back to their servers is necessarily spyware.

But when the developer of an extension goes out of their way to hide the fact that every single page you visit is being stored and sent to a corporation that pays them for that data while burying it in the settings as "anonymous usage statistics", there is a problem, at least. Any reasonable user would assume that if a developer wants to track usage stastics they are only going to be tracking the usage of the extension itself — but the opposite is true. Most of these extensions are tracking everything else you do except using the extension. They are just tracking you.

This becomes even more problematic because they call it "anonymous usage statistics"; the word "anonymous" implies that it would be impossible to figure out who that data belongs to, as if they are scrubbing the data clean of all your information. But they aren't. Yeah, sure, they are using an anonymous token to represent you rather than your full name or email, but every single page you visit is tied to that token. For as long as you have that extension installed.

Track anybody's browsing history long enough, and you can figure out exactly who they are.

How many times have you opened your own Facebook profile page, or your Pinterest, Google+, or other page? Have you ever noticed how the URL contains your name or something that identifies you? Even if you never visited any of those sites, figuring out who you are is possible.

I don't know about you, but my browsing history is mine, and nobody should have access to that but me. There's a reason why computers have passwords and everybody older than 5 knows about deleting their browser history. What you visit on the internet is very personal, and nobody should have the list of pages I visit but me, even if my name is not specifically associated with the list.

I'm not a lawyer, but the Google Developer Program Policies for Chrome extensions specifically say that an extension developer should not be allowed to publish any of my personal information:

We don't allow unauthorized publishing of people's private and confidential information, such as credit card numbers, government identification numbers, driver's and other license numbers, or any other information that is not publicly accessible.

Exactly how is my browsing history not personal information? It's definitely not publicly accessible!

Yep, Many of These Extensions Insert Ads Too

The problem is compounded by a large number of extensions that are injecting ads into many of the pages you visit. These extensions are just putting their ads wherever they randomly choose to put them into the page, and they are only required to include a tiny piece of text identifying where the ad came from, which most people will ignore, because most

CCCGC
Microsoft REGISTERED Refurbisher
Charlotte Bytes
the How-To Geek
Computer Help from your Friendly How-To Geek

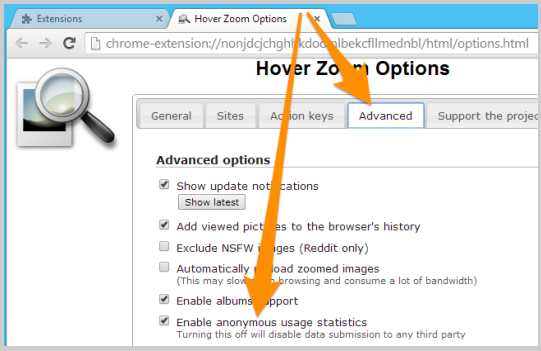
Warning: Your Browser Extensions Are Spying On You Continued

This Spying is Hidden Behind EULAs and Privacy Policies

These extensions are "allowed" to engage in this tracking behavior because they "disclose" it on their description page, or at some point in their options panel. For instance, the HoverZoom extension, which has a million users, says the following in their description page, at the very bottom:

Hover Zoom uses anonymous usage statistics. This can be disabled in the options page without losing any features as well. By leaving this feature enabled, the user authorize the collection, transfer and use of anonymous usage data, including but not limited to transferring to third parties.

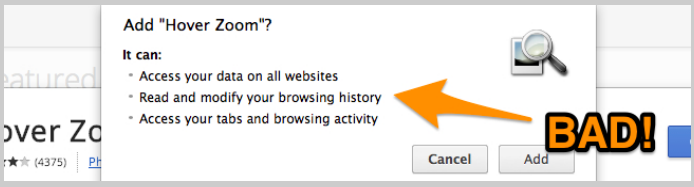
Where exactly in this description does it explain that they are going to track every single page you visit and send the URL back to a third party, which pays them for your data? In fact, they claim everywhere that they are sponsored through affiliate links, completely ignoring the fact that they are spying on you. Yeah, that's right, they are also injecting ads all over the place. But which do you care more about, an ad showing up on a page, or them taking your entire browsing history and sending it back to somebody else?



Hover Zoom's Excuse Panel

They are able to get away with this because they have a tiny little checkbox buried in their options panel that says "Enable anonymous usage statistics", and you can disable that "feature" — though it's worth noting that it is defaulted to be checked.

This particular extension has had a long history of bad behavior, going back quite some time. The developer has recently been caught collecting browsing data including form data… but he was also caught last year selling data on what you typed in to another company. They've added a privacy policy now that explains in further depth what is going on, but if you have to read a privacy policy to figure out that you are being spied on, you've got another problem.



To sum up, a million people are being spied on by this one extension alone. And that's just one of these extensions — there are a lot more doing the same thing.

This extension is asking for way too many permissions. Deny!

There is absolutely no way to know when an extension has been updated to include spyware, and since many types of extensions need a ton of permissions to even operate properly in the first place before they turn into ad-injecting pieces of spycraft, so you won't be prompted when the new version comes out.

To make matters worse, many of these extensions have changed hands over the last year — and anybody who has ever written an extension is being flooded with requests to sell their extension to shady individuals, who will then infect you with ads or spy on you. Since the extensions don't require any new permissions, you'll never have the opportunity to go figure out which ones added secret tracking without your knowledge.

In the future, of course, you should either avoid installing extensions or addons entirely, or be very careful about which ones you do install. If they ask for permissions to everything on your computer, you should click that Cancel button and run.

CCCGC

Charlotte Bytes

Warning: Your Browser Extensions Are Spying On You Continued

Hidden Tracking Code with a Remote Enable Switch

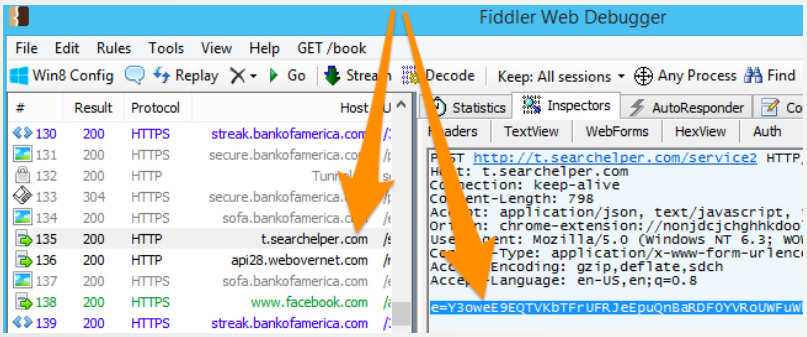
There are other extensions, in fact, a ton of them, that have complete tracking code built right in — but that code is currently disabled. Those extensions ping back to the server every 7 days to update their configuration. These ones are configured to send even more data back — they calculate exactly how long you have each tab open, and how long you spend on each site.

We tested one of these extensions, called Autocopy Original, by tricking it into thinking that the tracking behavior was supposed to be enabled, and we were able to immediately see a ton of data sent back to their servers. There were 73 of these extensions in the Chrome Store, and some in the Firefox add-ons store. They are easily identifiable because they are all from "wips.com" or "wips.com partners".

Wondering why we are worried about tracking code that isn't even enabled yet? Because their description page doesn't say a word about the tracking code — it's buried as a checkbox on each of their extensions. So people are installing the extensions assuming they are from a quality company.

And it's only a matter of time before that tracking code is enabled.

Investigating this Spying Extension Awfulness



The average person isn't going to ever even know that this spying is going on — they won't see a request to a server, they won't even have a way to tell that it is happening. The vast majority of those million users won't be affected in any way… except that their personal data was stolen out from under them. So how do you figure this out for yourself? It's called Fiddler. Fiddler is a web debugging tool that acts as a proxy and caches all the requests so you can see what is going on. This is the tool that we used — if you want to duplicate at home, just install one of these spying extensions like Hover Zoom, and you'll start seeing two requests to sites similar to t.searchelper.com and api28.webovernet.com for every single page that you view. If you check on the Inspectors tag you'll see a bunch of base64-encoded text… in fact, it's been base64-encoded twice for some reason. (If you want the full example text before decoding, we stashed it in a text file here).

They'll track any site your visit, even the HTTPS ones

Once you've successfully decoded that text, you'll see exactly what is going on. They are sending back the current page that you are visiting, along with the previous page, and a unique ID to identify you, and some other information. The very scary thing about this example is that I was on my banking site at the time, which is SSL encrypted using HTTPS. That's right, these extensions are still tracking you on sites that should be encrypted.

s=1809&md=21&pid=mi8PjvHcZYtjxA&sess=23112540366128090&sub=chrome&q=https%3A//secure.bankofamerica.com/login/sign-in/signOnScreen.*go%3Fmsg%3DInvalidOnlineIdException%26request_locale%3Den-us%26lpOlbResetErrorCounter%3D0&hreferer=https%3A//secure.bankofamerica.com/login/sign-in/entry/signOn.go&prev=https%3A//secure.bankofamerica.com/login/sign-in/entry/signOn.go&tmv=4001.1&tmf=1&sr=****https%3A//secure.bankofamerica.com/login/sign-in/signOn.go***

You can drop api28.webovernet.com and the other site into your browser to see where they lead, but we'll save you the suspense: they are actually redirects for the API for a company called Similar Web, which is one of many companies doing this kind of tracking, and selling the data so other companies can spy on what their competitors are doing.

If you're the adventurous type, you can easily find this same tracking code by opening up your chrome://extensions page and clicking on the Developer mode, and then "Inspect views: html/background.html" or the similar text that tells you to inspect the extension. This is going to let you see what that extension is running all the time in the background.

Continued Next Page

Charlotte Bytes

the How-To Geek
Computer Help from your Friendly How-To Geek

See us on the Web
www.cccgc.net

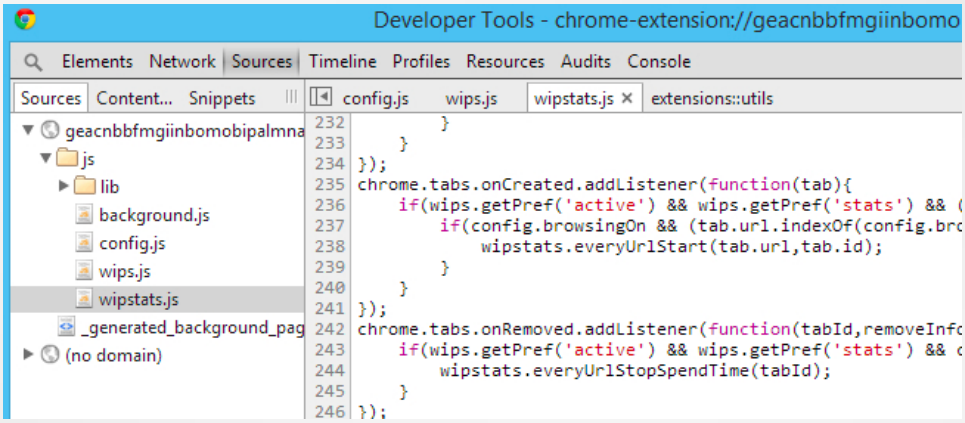
CCCGC

Warning: Your Browser Extensions Are Spying On You

Conclusion

That trash can icon is your friend

Once you click to inspect, you'll immediately see a list of source files and all sorts of other stuff that will probably be greek to you. The important thing in this case are the two files named tr_advanced.js and tr_simple.js. These contain the tracking code, and it's safe to say that if you see those files inside of any extension, you are being spied on, or will be spied on at some point. Some extension contain different tracking code, of course, so just because your extension doesn't have those, doesn't mean anything. Scammers tend to be tricky.



(Note that we wrapped the source code to fit into the window)

You'll probably notice that the URL on the right-hand side isn't quite the same as the one earlier. The actual tracking source code is pretty complicated, and it appears that each extension has a different tracking URL.

Preventing an Extension from Updating Automatically (Advanced)

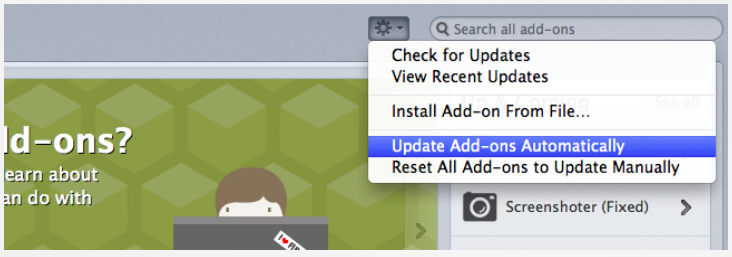
If you have an extension that you know and trust, and you've already verified that it doesn't contain anything bad, you can make sure that the extension never secretly updates on you with spyware — but it is really manual and probably not what you'll want to do.

If you still want to do so, open the Extensions panel, find the ID of the extension, then head to %localappdata%\google\chrome\User Data\default\Extensions and find the folder that contains your extension. Change the update_url line in the manifest.json to replace clients2.google.com with localhost. Note: we haven't been able to test this with an actual extension yet, but it should work.

So Where Does This Leave Us?

We've already established that loads of extensions are being updated to include tracking / spying code, injecting ads, and who knows what else. They are being sold to untrustworthy companies, or the developers are being bought with a promise of easy money.

Once you have an add-on installed, there's no way to know that they aren't going to be including spyware down the road. All we do know is that there are a lot of add-ons and extensions that are doing these things.

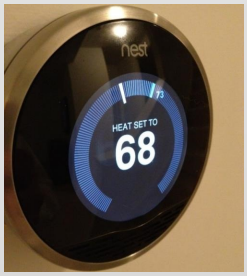


People have been asking us for a list, and as we've been investigating, we've found so many extensions doing these things, we're not sure that we can make a full list of all of them. We'll add a list of them to the forum topic associated with this article, so we can have the community help us generate a bigger list.

CCCGC

Charlotte Bytes

What is the Internet Of Things? Conclusion from page 6



Nest Smart Thermostat

The Internet of things also refers to other, more everyday scenarios. We have this today with Philips Hue light bulbs that connect to the network so you can control them from smartphones, network-enabled thermostats like the Nest, and other devices. Imagine if every appliance in your house was "smart" so you could have the information at your fingertips. You'd be able to see when the laundry will be done, how long until coffee is ready, whether you left the lights on at home, and more. Because more devices become "smart" and networked, you could have your house automatically turn on the lights and turn up the heat when you come home by detecting where your smartphone is. This is the dream of the "smart home," but it's also related to the Internet of things — it refers to networking more devices and objects.

IPv6 and Addressability

RELATED ARTICLE

HTG Explains: Why The Internet Is Running Out of IPv4 Addresses and Why IPv6 Is Important

http://www.howtogeek.com/119619/htg-explains-why-the-internet-is-running-out-of-ipv4-addresses-and-why-ipv6-is-important/

IPv4 addresses on the public Internet are running low. Microsoft paid $7.5 million for Nortel's 666,624 IP addresses when Nortel... [Read Article]

Currently, most devices use IPv4 to connect to the Internet. We're quickly running out of IPv4 addresses. IPv6 solves this problem by providing a larger number of possible addresses we can use. Once we've actually migrated to IPv6, it will be possible for every object on the planet to have its own IP address. Some have said that there will be more IPv6 addresses than there are atoms on Earth. Whether this is true or not, we'll have a huge amount of addresses to work with. This means that everything on the planet could be publically addressable. In other words, everything on the planet could communicate with each other without worrying about network address translation and port forwarding.

Security

RELATED ARTICLE

Secure Your Wireless Router: 8 Things You Can Do Right Now

http://www.howtogeek.com/173921/secure-your-wireless-router-8-things-you-can-do-right-now/

A security researcher recently discovered a backdoor in many D-Link routers, allowing anyone to access the router without knowing the... [Read Article]

Security will be a challenge as we bring more and more devices online. After all, we can't even secure all the network-connected devices we have today. Home routers are notoriously insecure and router companies have failed over and over, whether it's a backdoor in a D-Link router or an Asus router sharing your private files with everyone on the Internet. How could we secure every appliance an average person would have at home? Do we really expect the manufacturers of $15 appliances to support them all with timely security patches and solid, secure code? And we're not even worrying about all the other sensors and networked devices we might have.

There's no easy answer here. We'll need a new model for security to move forward without the Internet of things being a complete security mess.

Everything on the planet won't be connected any time soon, but the "Internet of things" is gradually taking form as more and more "smart devices" join the network and sensors become cheaper and cheaper. The Internet of the future won't just be about people communicating; it'll be about things communicating with each other.

Microsoft REGISTERED Refurbisher

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

CCCGC

Sorting out the revolution in PC backups: Part 2 Conclusion

Windows Secrets
Everything Microsoft forgot to mention.

Next, look at the timing information presented above, and apply that information to the anticipated size of your backup file sets.

Finally, think about the kinds of files you need to back up. Find the option — or like me, the options — that will give you the best mix of speed, security, and convenience for your needs.

As illustrated by my real-life, personal examples, if you have large numbers of different kinds of files, you'll probably end up with more than one backup method — some in the cloud (with or without extra encryption), some on a secondary drive, others on a spare PC, and so on.

Be flexible: mix and match backup types as you see fit. But most important, maintain your well-honed backup habits over the coming months and years. With five major backup types to choose from, you can easily achieve that long-sought Holy Grail of backups: a virtual guarantee that you'll never again lose important files or other data!

Who is Making All This Malware — and Why? Conclusion

Ransomware like CryptoLocker is an extreme example of this trend taken to its logical extreme. When it infects you, CryptoLocker will encrypt the personal files it finds on your computer with a secret encryption key and delete the originals. It will then pop up a polite, professional wizard asking you to spend money to get your files back. If you don't pay, you'll lose your files — but, don't worry, they'll accept several different methods of payment to make it convenient for you. You apparently will get your files back when you pay them — of course, because otherwise word would spread and no one would pay them. Performing regular backups can defeat CryptoLocker and we don't recommend paying criminals their ransom, but this is a clear example of malware being for-profit. They want to cause just enough trouble for you that you'll pay up to get them to go away.

Phishing and Social Engineering Attacks

Online threats aren't just about malware, either. Phishing and other social-engineering attacks are now also a huge threat. For example, you might get an email claiming to be from your bank that might take you to an imposter website designed to look like your bank's. If you enter your banking information, the attacker will be able to gain access to your bank account on your bank's website.

These attacks are profit-driven in the same way malware is. The attacker isn't performing a phishing attack just to mess with you — they're doing it to gain access to your sensitive financial information so they can make a profit.

This lens can also help you understand other obnoxious types of software, like adware that displays advertisements on your computer and spyware that spies on your browsing information and sends it over the Internet. These obnoxious types of software are made for the same reason — profit. Their creators make money by serving you advertisements and tailoring them to you.

Image Credit: Sean MacEntee on Flickr, Happy99 worm from Wikimedia Commons, Szilard Mihaly on Flickr

HTG Explains:

Online Security: Breaking Down the Anatomy of a Phishing Email http://www.howtogeek.com/58642/online-security-breaking-down-the-anatomy-of-a-phishing-email/

What is Social Engineering and How Can You Avoid It? http://www.howtogeek.com/180186/htg-explains-what-is-social-engineering-and-how-can-you-avoid-it/

Keyloggers Explained: What You Need to Know

http://www.howtogeek.com/180615/keyloggers-explained-what-you-need-to-know/

Ransomeware: Why This New Malware is So Dangerous and How to Protect Yourself

http://www.howtogeek.com/174343/ransomware-why-this-new-malware-is-so-dangerous-and-how-to-protect-yourself/