SUPERCOM COMPUTER CLUB TECH TIMES

Volume 22 December 8, 2018

Objective:

To bring the latest technology news to you, our members. Tips and suggestions will help you to keep your device(s) running smoothly and help you be aware of threats. Technical tips will be coming to you through our Technical Committee.

Committee Members: (Pictured Below)

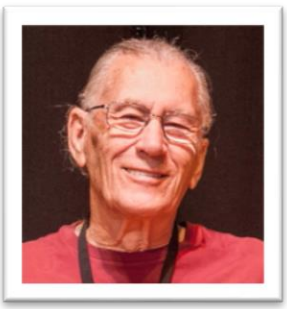
Ben Tarbell, Mike Gerkin, Peggy Bullock, Jim Mills, Rick Heesen, Lowell Lee, Steve Andreasen (Apple/Mac) and Mike Smith. Jim Oliver and Dick Strong.









Dick Strong is on "time off" for season 2018-2019.

Greetings

This is the first Tech Times for the 2018-2019 Season. Don't forget to check out the Website.

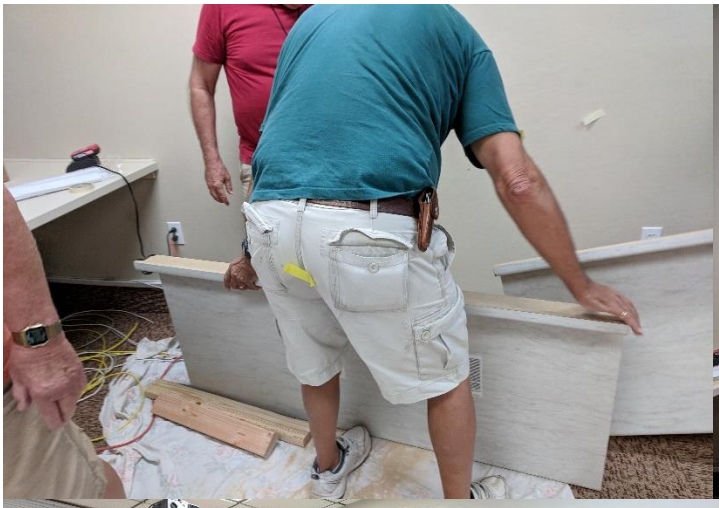
Welcome back to several of our previous members of the SuperCom Computer Club and a big welcome to our new members. We are growing each week! Hope to see many of you at our Friday Meetings at 9:00am in the Ballroom (with the exception of some holidays – see website or bulletin board in the Hallway of the Main Building).

We have been scheduling Open Labs (where you can bring your computer in to the Geeks and they can help you with most all of your problems) from 10:30am – 12:00 noon on Fridays after the club meeting (exception – 2nd Friday and Holidays). Geeks are still available for home visits until 5pm, Monday – Friday.

Many of you may have already seen the new Lab 2 which was reconstructed prior to your arrival and the painting and carpeting of Lab 1. Lab 2 will be used for classes where you bring your own personal computer with you.

Not only have we gotten great new looking Labs, but Rick Heesen and Jim Mills put in countless hours to rewire all the cable from the main input to the Labs, install wireless antennas throughout the main building so that SIG groups can have better access to the internet and classes using downloads have a high quality of speed. Their summer planning and fall work has been a tremendous help to our club! A BIG THANK YOU guys!!!

Here are some pictures of the "work in progress". Sorry, I don't have any of the finished project. Guess you will have to come check it out!





Classes and some SIG's are in full swing. Classes were held in November and are going strong for the month of December. Check out the website for a current Calendar of classes and times. Be sure to come to a Friday meeting to sign up for a class either before or after the meeting. During the time of the actual meeting, there will be no class registration. This enables those helpful people to listen to the program along with everyone else.

We are always looking for new classes to teach and new instructors. We **KNOW** with a membership the size we have, there has to be many of you that can teach us all something. If you are interested or have an idea for a class, please contact the Education Committee, Judy Lee or Marny Dadson.

Short-term volunteerism is the best!!! Change is GOOD!!

Remember – Our Club Website is: www.supercomcc.org.

All links in our newsletter are safe to click on.

Some of the following articles were received right after I published the last Tech Times, so they might be a little behind, but I am sure they are always relevant to what we need to be aware of.

Submitted by Mike Gerkin:

(This article does not have a great sense of urgency simply because the immediate threat is over, but it should provide you a very good educational experience).

Mean Ransomware Hides in Legitimate Site

One of the anti-malware/anti-spyware programs that the SuperCom techs have recommended to our membership for several years is an excellent one called SuperAntiSpyware. A rather strange thing happened just the other day.

The Kraken Cryptor Ransomware is a newer ransomware that was released in August 2018. A new version, called Kraken Cryptor 1.5, was recently released that was masquerading as the legitimate SuperAntiSpyware anti-malware program in order to trick users into installing it. What makes it worse, though, is that somehow the attackers were able to gain access to the superantispyware.com site and distribute the ransomware from there.

The file name for the legitimate SuperAntiSpyware Free installer is called SUPERAntiSpyware.exe. The Kraken Cryptor installer spotted by VirusTotal was called SUPERAntiSpywares.exe. The only difference between the two names is the addition of a s to the malicious executable. **This malicious executable is no longer available** from superantispyware.com, so any new download should be safe. But the moral lesson to be learned here is that the bad guys are getting even more tricky and sneaky. Always be extra alert, and, even then, bad things can happen.

It is important to note that the SUPERAntiSpyware.exe executable was not compromised and continued to install the legitimate version of SuperAntiSpyware. So, users who installed SuperAntiSpyware via the normal links were not affected. At this point, we do not know how users were being directed to the malicious SUPERAntiSpywares.exe executable.

In order to protect yourself from Kraken Cryptor, or from any ransomware, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

Last, but not least, make sure you practice the following good online security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them.
- Scan attachments with tools like Malwarebytes.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore, it is important to keep them updated.
- Make sure you use have some sort of security software installed (contact one of the SuperCom Tech Geeks if in doubt).
- Use hard passwords and never reuse the same password at multiple sites.

If you want to read more on this topic go to this source: Bleeping Computer

Submitted by Rick Heesen:

Windows Defender Now Offers Ultra Secure Sandbox Mode, Here's How To Turn It On


Chris Hoffman
@chrisbhoffman
October 26, 2018

Windows 10's built-in antivirus can now run in a sandbox. Even if an attacker compromises the antivirus engine, they wouldn't have access to the rest of the system. As Google's Tavis Ormandy puts it, "this is game changing."

In fact, Windows Defender is the first complete antivirus product that can run in a sandbox. None of the paid (or free) antivirus products you can download boast this feature.

This news comes from the official Microsoft Secure blog. As Microsoft puts it:

Security researchers both inside and outside of Microsoft have previously identified ways that an attacker can take advantage of vulnerabilities in Windows Defender Antivirus's content parsers that could enable arbitrary code execution. While we haven't seen attacks in-the-wild actively targeting Windows Defender Antivirus, we take these reports seriously…

Running Windows Defender Antivirus in a sandbox ensures that in the unlikely event of a compromise, malicious actions are limited to the isolated environment, protecting the rest of the system from harm.

In other words, the Windows Defender antivirus process that analyzes downloaded files and other content will run with very few permissions. Even if there was a bug in the antivirus process and a maliciously crafted file managed to compromise the antivirus itself, that now-dangerous antivirus process wouldn't provide any access to the rest of your system. The attack would have failed.

Sure, an antivirus still needs a lot of access to your system. But the main antivirus process that runs with a lot of permissions won't analyze files. It hands content off to a low-privilege sandboxed process, which does the dirty and dangerous work in a secure area.

Microsoft's blog post goes on to describe how this feature was implemented without any noticeable performance drops:

Performance is often the main concern raised around sandboxing, especially given that antimalware products are in many critical paths like synchronously inspecting file operations and processing and aggregating or matching large numbers of runtime events. To ensure that performance doesn't degrade, we had to minimize the number of interactions between the sandbox and the privileged process, and at the same time, only perform these interactions in key moments where their cost would not be significant, for example, when IO is being performed.

There's much more detail than that in Microsoft's blog post, so check it out if you're interested.

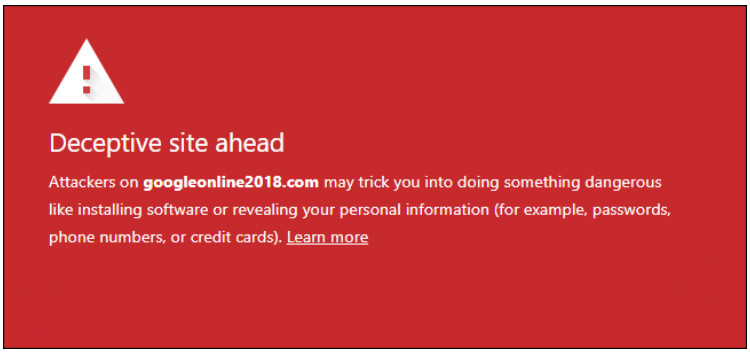
When Will You Get It?

To finish reading the article, Ctrl+Click on the title at the beginning of the article.

Submitted by Rick Heesen: ALWAYS CHECK YOUR URL ADDRESS TO MAKE SURE IT IS GOING TO WHERE YOU WANT IT TO GO!!!

Bing Is Pushing Malware When You Search for Chrome

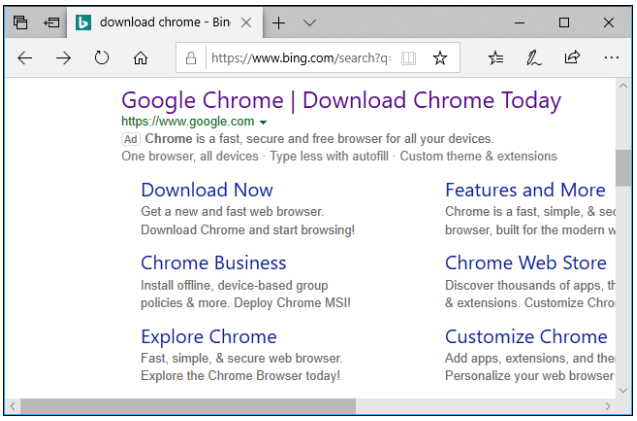

Chris Hoffman
@chrisbhoffman
October 26, 2018



You launch Edge on your new PC, search for “download Chrome,” and click the first result headed to “google.com” on Bing. You’re now on a phishing website pushing malware, disguised to look like the Chrome download page.

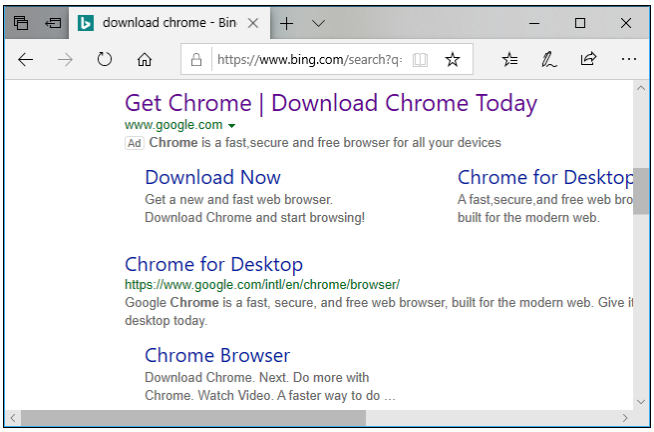
That’s the story Gabriel Landau tells on Twitter:

We were able to reproduce this problem, although it doesn’t happen every time. Usually, you’ll end up seeing an ad for “https://www.google.com”. That goes to the real Chrome download page, and everything is fine.



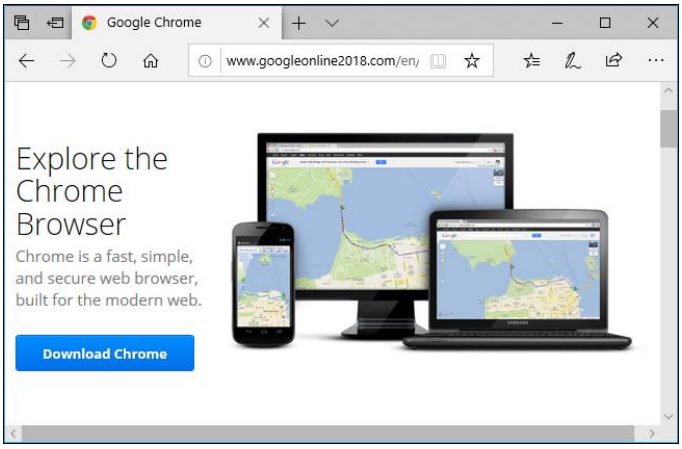
But, sometimes, you’ll see an ad for “google.com”. Guess what—that doesn’t actually go to Google.com. This ad was created by a scammer and goes elsewhere.

Microsoft is apparently not verifying the web address the advertisement actually goes to. Bing is letting this advertisement lie to people.

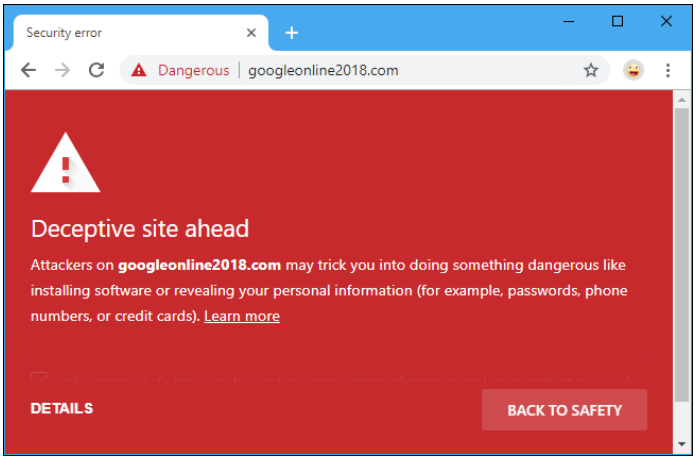


If you click the link, you’ll be taken to a Google Chrome download page that looks like the real one. But it didn’t take you to Google.com. It takes you to “googleonline2018.com”, a scam website.

We didn’t actually download Chrome from here, of course. But we’re certain that this website is pushing malware or something malicious.



Chrome actually blocks this site as “deceptive,” but Bing and Edge don’t.



It’s worth noting that we could reproduce this on some systems, but not others. The advertisement may be targeted geographically. We could also only reproduce this in Microsoft Edge.

If you’d like to try it yourself, head to this search address in Microsoft Edge and refresh a few times.

This is crazy. Scammy advertisements pop up everywhere now and then, but they always have a nasty-looking URL that acts as a giveaway. Bing isn’t even checking the URL here.

Update: It’s even worse than we thought. Bleeping Computer reported almost the exact same advertisement in April, over six months ago. Microsoft removed the ad at the time, but it’s now back in a nearly identical form. Bing is still letting this advertisement lie about going to “google.com”, too. Thanks to @killyourfm on Twitter for noticing this.

Update: Microsoft has now removed the ad. Here’s what a Microsoft spokesperson told us:

Protecting customers from malicious content is a top priority, and we have removed the ads from Bing and banned the associated account. We encourage users to continue to report this type of content so we can take appropriate action.

However, Microsoft has not explained how the ad was marked as from “google.com”, nor have it said if the underlying issue was properly fixed. Without a real fix that prevents advertisers from lying, this problem will just pop up again in the near future.

Bing already has problems with horrifying search suggestions, so this is yet another problem on the pile. Microsoft really needs to clean Bing up.

Submitted by Mike Gerkin:

With the significant increase of scams of all types appearing with regularity, here is an excellent Microsoft web site that does a really good job of spelling out warnings and some common-sense solutions to most scams. I suggest including it or members who want to learn more from a good source.
https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams

---

Submitted by Rick Heesen:

PSA: You Have Less Than a Month to Get Your iPhone Battery Replaced for Cheap


Craig Lloyd
@craig_lloyd
December 3, 2018

If you still have an older iPhone and have not yet gotten the battery replaced, you have until December 31 to get it replaced by Apple for just $29.

Last year, it was discovered that Apple was unknowingly throttling iPhone performance in order to prevent unexpected shutdowns on devices with old, degraded batteries. The fix was rather easy: just replace the battery.

RELATED: ***You Can Speed Up Your Slow iPhone by Replacing the Battery***

As a goodwill to keep customers happy, Apple started offering discounted battery replacements for devices as old as the iPhone SE and as new as the iPhone X. Normally $69, you can get the battery replaced in your iPhone for just $29, but you only have until the end of the year. Afterward, the cost will likely jump back up to $69 for out-of-warranty service.

If you're not sure if your iPhone needs a battery replacement, you can check the battery health by going to Settings > Battery > Battery Health. Anything over 80% is pretty good, but if the percentage is lower than that, you would likely benefit greatly from a battery replacement.

You can also replace the battery in your iPhone yourself if you feel up to the task. In older iPhones, it's not terribly difficult—it just takes a bit of time and patience.

Submitted by Peggy Bullock:

I just received this email alert from SRP on Friday, December 7. Some of you may also have gotten it. This is the season…..and it isn't always the Jolly Holly Season!!!

SRP Delivering water and power™

Stay alert this holiday season! Scammers are on the prowl.

We have received new reports of scams targeting SRP customers. Especially around the holidays, scammers may try to retrieve your account or credit card information by:

- **Identifying themselves as SRP employees in calls, emails or text messages and demanding that you make an immediate payment or face same-day disconnection. Do not pay.**
- **Insisting that you purchase prepaid credit cards and call them back to pay. The callback number they provide is not an SRP number and may include a recording that attempts to sound like our automated voice system. Do not comply.**

Don't become a victim. Always remember:

- **We never demand immediate payments.**
- **We never threaten same-day disconnection.**
- **We don't accept bitcoin or prepaid cards such a MoneyPack, Green Dot or Vanilla.**
- **When in doubt, give us a call 24/7 at (602) 236-8888.**

Stay alert

If you feel you have been the target of a scam, contact your local law enforcement or the Arizona Attorney General's Office.

Submitted by Peggy Bullock:

Update now! Adobe issues emergency Flash update for a serious flaw

By Francis Navarro, Komando.com

Do you still use Adobe's Flash Player? Maybe not as much as before, right? Browser makers are all trying their best to finally lay Flash on its deathbed. Its decline has been a slow but steady downward spiral since it is a perennial target for hackers and it is a known computer resource hog that crashes computers regularly.

And yet, Flash is still alive and kicking and plenty of websites still use it to display their content. So, stop us if you've heard this one before, if you're still a Flash holdover, update it now!

Adobe rushed another emergency patch to fix a zero-day vulnerability, and it's critical that you update your Flash software as soon as you can.

Note: Zero-day vulnerabilities are dangerous since they are previously unknown software exploits that are already being used by hackers even before the software makers are made aware of them.

Another zero-day Flash flaw

Adobe has recently issued another out-of-band emergency patch for its infamous Flash software for a critical zero-day bug that it is already being exploited by hackers.

Security researchers from Chinese cybersecurity firm Qihoo 360 discovered the flaw after spotting a targeted Advanced Persistent Threat Attack (APT) aimed at a Russian medical clinic. This facility is known for providing health-care and cosmetic services to high-level Russian Federation employees and famous Russian scientists and artists.

Codenamed "Operation Poison Needles" by Qihoo, the zero-day attack sneaks in via a RAR-compressed Word document disguised as a seven-page job application questionnaire. Embedded within the document is a Flash Active X object which harbors the exploit.

The method of distribution for this attack? The booby-trapped document is sent via phishing emails to the intended targets. If a target opens the document and allows the embedded Flash Active X object

to execute, the malicious code will then escalate its system privileges via the zero-day exploit and download a remote spying tool.

The bugs

The critical vulnerability is now known as "use after free" bug (CVE-2018-15982), and Adobe warns that a successful exploit could lead to remote code execution.

Another important fix is also included in the emergency patch (CVE-2018-15983), and this one addresses a privilege escalation vulnerability due to DLL hijacking.

Who's responsible for the attacks?

Qihoo 360 said that the source of the attacks is still under investigation but due to the clientele of the targeted Russian polyclinic, it is likely that it is political in nature.

The zero-day exploit's code also has similarities with the hacking exploits deployed by the Italian spyware developer HackingTeam which interestingly, had its tools leaked back in 2015.

This suggests that this current Flash attack may be from a separate hacking group who gained possession of HackingTeam's leaked exploits and is now using the tools for political ends.

However, the main thing you need to know about this incident is that the zero-day flaw is out there and other enterprising cybercrooks will inevitably exploit it too. If you're still using Flash on a regular basis, update your software now!

How to update Flash

If you still rely on using Flash Player for websites (*you shouldn't*), it's important that you update to the latest version 32.0.0.101 immediately.

Here's how to update your system's Flash software:

For Chrome, Internet Explorer 11 and Microsoft Edge browsers, the updates should be applied automatically after a restart. For other browsers, you may need to update the Flash plugin manually.

--> Click here to use our Adobe Flash Update Tool guide for download and install instructions.

The latest Flash Player version for Windows, Mac, Chrome, Microsoft Edge and Internet Explorer 11 and Linux is 32.0.0.101. The latest Adobe Flash Player Windows installer is version 31.0.0.122.

Your Techs for this time: Mike Gerkin, Rick Heesen, and Peggy Bullock