On December 26, 2018, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). Due to a vulnerability in Microsoft Internet Explorer, which could allow for arbitrary code execution. (No further update)

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

04 January 2019

In The News This Week

Thousands of Google Chromecast Devices Hijacked to Promote PewDiePie

A group of hackers has hijacked tens of thousands of Google's Chromecast streaming dongles, Google Home smart speakers and smart TVs with built-in Chromecast technology in recent weeks by exploiting a bug that's allegedly been ignored by Google for almost five years. The attackers, who go by Twitter handles @HackerGiraffe and @j3ws3r, managed to hijack Chromecasts' feeds and display a pop-up, spreading a security warning as well as controversial YouTube star PewDiePie propaganda. The hackers are the same ones who hijacked more than 50,000 internet-connected printers worldwide late last year by exploiting vulnerable printers to print out flyers asking everyone to subscribe to PewDiePie YouTube channel. This time, the hackers remotely scanned the internet for compatible devices, including Chromecasts, exposed to the internet through poorly configured routers that have Universal Plug and Play [UPnP] enabled by default. The hackers then exploited a design flaw in Chromecast that allowed them to access the devices and hijack their media streams to display a video message (as shown below) on connected televisions without authentication. Besides security warnings, the hackers again took a chance to promote PewDiePie—a famous YouTuber from Sweden who is known for his game commentary and pranks and has had the most subscribers on YouTube since 2013. See more at https://thehackernews.com

Los Angeles Accuses Weather Channel App of Covertly Mining User Data

The Weather Channel app deceptively collected, shared and profited from the location information of millions of American consumers, the city attorney of Los Angeles said in a lawsuit filed on Thursday. One of the most popular online weather services in the United States, the Weather Channel app has been downloaded more than 100 million times and has 45 million active users monthly. The government said the Weather Company, the business behind the app, unfairly manipulated users into turning on location tracking by implying that the information would be used only to localize weather reports. Yet the company, which is owned by IBM, also used the data for unrelated commercial purposes, like targeted marketing and analysis for hedge funds, according to the lawsuit. The city's lawsuit cited an article last month in The New York Times that detailed a sprawling industry of companies that profit from continuously snooping on users' precise whereabouts. The companies collect location data from smartphone apps to cater to advertisers, stores and investors seeking insights into consumer behavior. The Times found that at least 75 companies collected precise location data — on at least one occasion logging a person's whereabouts more than 14,000 times in just one day. Yet many of the pop-up notices that apps showed to prompt consumers to enable location services only partly disclosed how their data would be shared and used. The Los Angeles lawsuit says such incomplete messages are "fraudulent and deceptive" and violate California's Unfair Competition Law. "If the price of getting a weather report is going to be the sacrifice of your most personal information about where you spend your time day and night," said Michael N. Feuer, the Los Angeles city attorney, "you sure as heck ought to be told clearly in advance." An IBM spokesman, Saswato Das, said, "The Weather Company has always been transparent with use of location data; the disclosures are fully appropriate, and we will defend them vigorously." The lawsuit was filed amid mounting public concern and government scrutiny over how tech companies collect, use and share consumers' personal details. After a spate of scandals — including Facebook's sharing of user data with third parties — federal lawmakers are preparing to introduce consumer privacy legislation this year. Read the full story in the New York Times - www.nytimes.com

Chromium Browser Virus – Getting unwanted pop-up's?

The Chromium Browser Virus

What is it? - The Chromium browser is actually the "alpha" version of the modern Google Chrome browser. It was designed as an open source project, meaning that developers or hackers for that matter, can change and tweak it in all sorts of ways. Unfortunately, it is nowadays most often misused as a platform for malicious web browsers categorized as adware and potentially unwanted programs (PUP). Most infiltrate systems without users' permission. In addition, these apps continually track Internet browsing activity, generate intrusive advertisements, and cause unwanted browser redirects. Clicking on one of the links may redirect you to a malicious website and your computer could be infected with all sorts of viruses, even ransomware.

How do I know if my machine is infected? - You may notice strange behaviour when browsing the web and all sorts of unwanted pop-ups and adverts suddenly starts appearing. Sometimes a browser window will just pop up while you are doing some other stuff or playing games and so on. You may find that sometimes your machine just "wakes up" and play a loud audible advert or video in the middle of the night. More often than not, the adverts feature strong adult and offensive content that you don't want your kids to be exposed to. The easiest way to see if you have it is to open your "Task Manager" and see if there are any "Chromium (32bit)" processes running. There could be several entries as the program replicates itself constantly which makes it difficult to get rid of. (Shortcut to Task Manager: Type Ctrl+Alt+Delete and select Task Manager). Some other variants of the rogue Chromium browser include names such as Olcinium, eFast, Qword, BrowserAir, Chedot, MyBrowser, Fusion, BeagleBrowser, Tortuga, and Torch.

How did the rogue Chromium browser install on my computer? - Most of these rogue Chromium-based browsers are distributed using a deceptive software marketing method called 'bundling' - stealth installation of additional programs with regular software/apps. Research shows that many users do not expect potentially unwanted programs to be concealed within the 'Custom' or 'Advanced' settings. They rush the download and installation processes, skip most/all steps, and often inadvertently install rogue applications.

How do I get rid of it? – Most of the reputable anti-virus vendors boast that their products will clean up or prevent being infected with a rogue Chromium Browser but in my experience, since the rogue program replicates itself constantly, they don't always do the job, or it gets rid of it only temporary. To get rid of it effectively, the root Chromium program needs to be deleted. Here are the steps that worked for me:

1) Open up Task Manager,
2) Now look for the first instance of the "Chromium (32bit)" process (remember it could be called something else as suggested above),
3) Right-click on the running processes and select "Open file location", this will open a new window showing the root program.
4) Keep this window open and go back to the Task Manager. Now select and right-click on the instances of the rogue program one-by-one and select "End task" for each one. This process needs to be done as quickly as possible since the program will replicate itself again in a short space of time.
5) Once all the instances of the rogue program were stopped, go back to the window that shows the location of the core program, right-click on it and select "delete" or drag it to the recycle bin. Now select all the files in that directory and delete them all, also delete the directory.
6) Now empty the recycle bin and you are good to go.

If you are struggling to follow the steps, get one of your tech guys to help or download and try freely available virus and adware cleaning tools such as Malwarebytes's "adwcleaner" or Kaspersky's "Virus Removal Tool", etc.

TOP local Infections registered for last week in the USA

#	KNOWN AS	(%)
1	DangerousObject.Multi.Generic	19.52%
2	Trojan.Script.Generic	7.37%
3	Trojan-Ransom.AndroidOS.Svpeng.ah	4.43%
4	Trojan-Downloader.MSOffice.SLoad.gen	3.71%
5	Hoax.Win32.Uniblue.gen	2.38%
6	HackTool.Win64.HackKMS.b	1.69%
7	Hoax.MSIL.Optimizer.a	1.45%
8	Trojan-PSW.Win32.Mimikatz.ln	1.44%
9	Hoax.Win32.PCFixer.b	1.29%
10	Trojan-Downloader.OSX.Shlayer.a	1.28%

Source: Kaspersky Labs

For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Estimated Crime Revenue Generated in 2018

Illegal online markets $860 Billion

Trade secret, IP theft $500 Billion

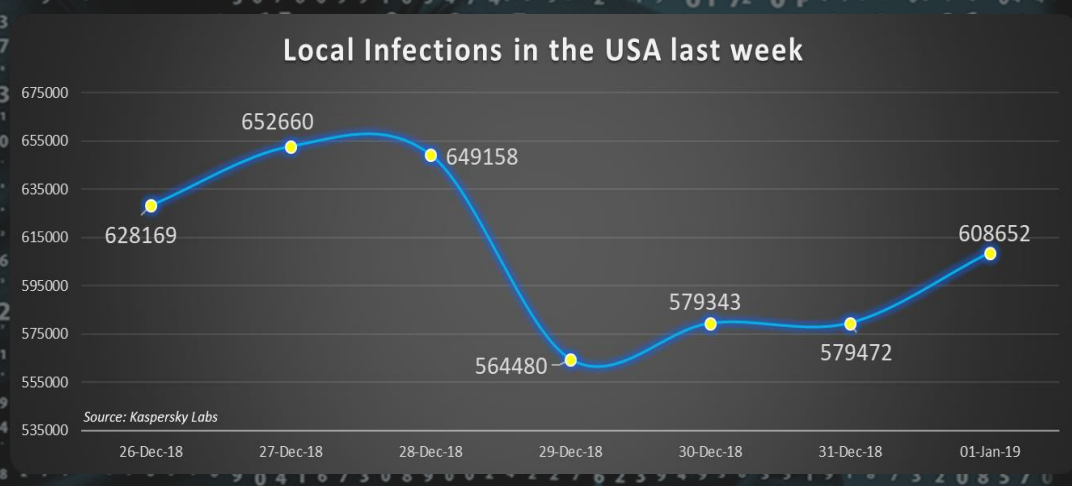
Data Trading $160 Billion

Crime-ware/CaaS $1.6 Billion

Ransomware $1 Billion

Total Cybercrime Revenues $1.5 Trillion

See HashedOut newsletter @ https://www.thesslstore.com/blog/2018-cybercrime-statistics/



Author: Chris Bester