On November 10, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla and Microsoft products.
See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
12 Nov	252,651,684	5,095,673

Deaths this week: 50,596

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
12 November 2021

In The News This Week

McAfee skuffs a buyer on the dance floor

An investor group consisting of six investment firms announced today that they had bought cybersecurity software firm, McAfee, **for 14 billion**, thus far the biggest deal in its history. The purchase price is based on a stock price of 26 per share, which the company claims represents a 22.6 percent premium over the stock's closing value on Thursday. The group is made up of Advent International, Permira Advisers, Crosspoint Capital Partners, Canada Pension Plan Investment Board, GIC Private Limited, and a wholly-owned subsidiary of the Abu Dhabi Investment Authority. According to the firm, Advent and Permira were behind today's purchase. The investment group gained a consumer security firm that has operated in various guises since 1987 when it acquired McAfee. The firm doled out 4 billion for the sale of its business arm earlier this year. Despite McAfee's age, it still has a developing consumer security business. The firm announced net sales of 491 million in its most recent earnings report, up 24% year over year with 640,000 new subscribers for a total of over 20 million subscribers, which is certainly an impressive number and one that needed to pique the interest of the investors in the investor group.
Read the full story by Sam Square here: Pirate press

This prolific hacker-for-hire operation has targeted thousands of victims around the world

Cybersecurity researchers at Trend Micro lift the lid on Void Balaur, a financially motivated cyber-crime group that has targeted politicians, journalists, human rights activists, medical professionals and others since 2015. - A hacker-for-hire operation offered by cyber mercenaries has targeted thousands of individuals and organisations around the world, in a prolific campaign of financially driven attacks that have been ongoing since 2015. Human rights activists, journalists, politicians, telecommunications engineers and medical doctors are among those who have been targeted by the group, which has been detailed by cybersecurity researchers at Trend Micro. They've dubbed it Void Balaur, after a multi-headed creature from Slavic folklore. The cyber-mercenary group has been advertising its services on Russian-language forums since 2018. The key services offered are breaking into email and social media accounts, as well as stealing and selling sensitive personal and financial information. The attacks will also occasionally drop information-stealing malware onto devices used by victims. It doesn't appear to matter who the targets are -- as long as those behind the attacks get paid by their contractors. Only a handful of campaigns are run at any one time, but those that are being run command the full attention of Void Balaur for the duration...
Read the story by Danny Palmer here: ZDNet

Queensland - Sunwater targeted in months-long undetected cyber security breach

Queensland's largest regional water supplier, Sunwater, says it was targeted by hackers in a cyber security breach that went undetected for nine months. It has been revealed that hackers left suspicious files on a webserver to redirect visitor traffic to an online video platform last year. Sunwater admitted the cyber breach after the tabling of a Queensland's Audit Office report into the state's water authorities, which mentioned the incident but did not say which authority was targeted. Following questions from the ABC, Sunwater confirmed it was the authority affected by the breach revealed in the Audit Office's report... Read the full story by Rory Callinan here: ABC News

Hackers claim they have cracked the PS5 and obtained all symmetric root keys

A hot potato: Jailbreaking, modding, pwning, whatever you want to call it—hackers delight in making a device do something that the manufacturer did not intend. Over the years, the process has grown more complicated, but the hackers always seem to find a way. It seems that as we near the first anniversary of the PlayStation 5, someone has already cracked the system. Over the weekend, hackers from Fail0verflow claimed to have rooted the PS5. A Sunday tweet states the group has obtained all symmetric PlayStation 5 root keys. It allegedly got the key by decrypting the PS5's firmware. The tweet included an image of the cracked software highlighting the system's supposedly exposed secure loader (secldr). More often than not, jailbreaking a PlayStation console requires modification of the hardware. Although Fail0verflow did not reveal its exploit, it did say that the keys were "obtained from software," suggesting that no hardware modifications were necessary.
Read the full story by Cal Jeffrey here: TECHSPOT

Software Piracy

Despite the millions spent in time and money in an attempt to curb software piracy, it seems that software developers are still on the short end of the stick. Although massive technology advances have been made in recent years to block and track software piracy, the torrent seeding community is still largely unregulated. The incumbent rules of privacy laws around the world also add to the complexity of law enforcement agencies taking effective action against copyright infringement. However, in some countries, more and more individual lawsuits are filed against individuals for downloading software illegally via torrent seeding sites. With that said, I came across an article this week talking about real action against piracy in Denmark that could pave the way for other countries to do the same. Below is a short extract of the article.

Criminal Copyright Complaint Filed Against BitTorrent Seedbox Provider

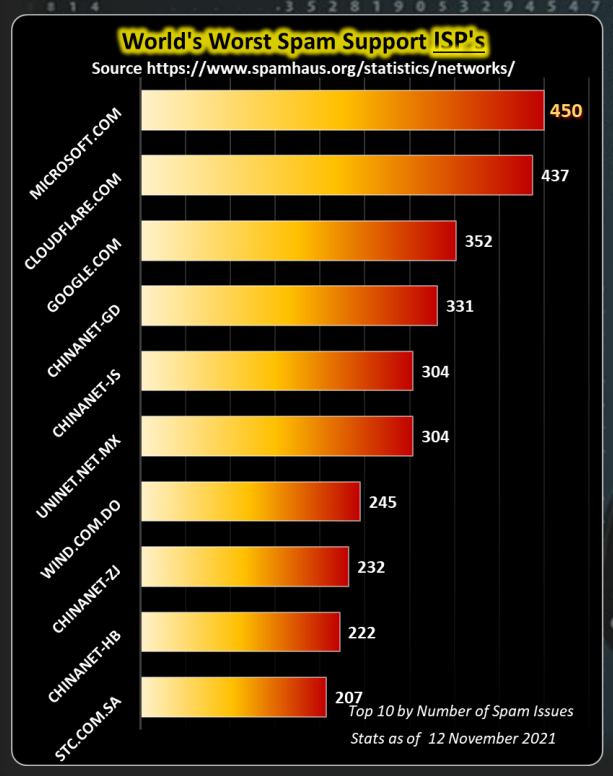
Three seedbox providers have announced that they will block their users from sharing on at least three named trackers. While one appears to have decided to act voluntarily, TorrentFreak is informed that a company operating under two brands is now being investigated for criminal copyright infringement.
Over the past year in particular, anti-piracy group Rights Alliance has been applying maximum pressure to various players in the piracy ecosystem.
Through detailed investigations that are ultimately referred to local law enforcement, one of the group's main aims is to disrupt and ultimately disassemble the private torrent site scene in Denmark. With the shutdown of several major private trackers in recent months, Rights Alliance clearly has the momentum but that isn't to say that clearing-up operations aren't needed.
Last week news broke that six people had been arrested following criminal referrals by Rights Alliance relating to private torrent sites ShareUniversity, DanishBytes, and potentially others. An aspect of the operation last week will be of interest to private tracker users all over Europe and potentially even the United States.

Seedboxes Providers and Sellers Under Pressure
The revelation came from the Public Prosecutor for Special Economic and International Crime (SØIK) which indicated that one of the arrested men reportedly sold access to seedboxes, a BitTorrent-related term for specially-configured servers that allow people to share content remotely.
These servers were reportedly rented by BitTorrent users for use on one or more of the private trackers to share around 3,800 copyrighted works.
It's important to note that seedboxes aren't illegal per se but if they are used to share infringing content then there are implications for users and seedboxes providers alike, when certain conditions are met. The circumstances surrounding last week's arrests will become clearer in the coming weeks and months but in the meantime, some providers are already taking action.

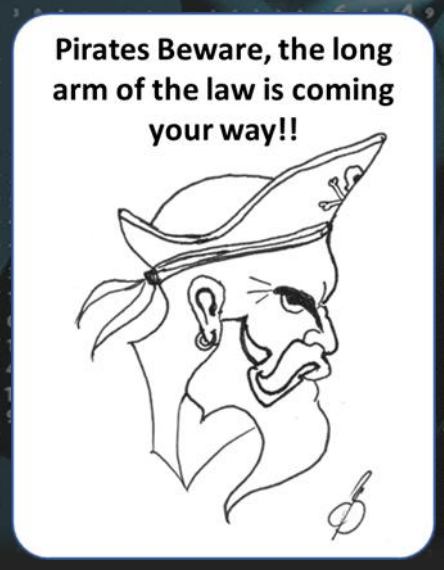
Announcement from Seedbox.io and Walkerservers
In an announcement posted to its portal on November 6, 2021, seedbox provider Seedbox.io said that due to the recent raids in Denmark, it would no longer allow its customers to seed (share) content on three named private trackers.
"Due to recent events in Denmark on November 3rd we have decided to take our precautions and as a result we have blocked access to the below domains from our servers. The trackers in question are: https://superbits.org, https://danishbytes.org (And all subdomains/alternative domains) [and] https://cynicalgen.org. The sites have been blocked on the network level," the provider explained.
Walkerservers, which is operated by the same company as Seedbox.io, later confirmed that the same announcement is true for its business too.

Criminal Complaint Was Filed By Rights Alliance
Given that Rights Alliance is behind most if not all pressure in Denmark that can lead to this type of response, TorrentFreak asked the anti-piracy company what it knows about these announcements. As it turns out, it knows quite a lot.
"The Rights Alliance filed a criminal complaint against HNielsen Networks, the Danish company behind Seedbox.io and Walkerservers, in March this year for facilitating copyright infringements by providing seedbox servers pre-installed with software for torrenting and providing customer support for using their services on illegal torrent sites," explained Ditte Rie Agerskov, Head of Communications at Rights Alliance.
"Seedboxes greatly increase the efficiency of illegal torrent activity. This facilitation is similar in nature to the Filmspeler service that the European Court of Justice has looked at in its case law."
The Filmspeler case involved Dutch anti-piracy group BREIN and Netherlands-based Filmspeler.nl (Movie Player). The online store sold piracy-configured media players that came with pre-installed add-ons containing hyperlinks to websites from where copyrighted works such as movies, TV shows and live broadcasts were made available without copyright holders' permission.
Filmspeler lost that fight after the battle went all the way to the European Court of Justice. As a result, the case has been cited in many separate copyright infringement discussions since, sometimes with references to how those devices were marketed and the sellers' stated aim of allowing customers to access content for free.
Rights Alliance also highlights the existence of criminal precedents in Denmark stating contributory infringement related to "illegal infrastructure." These include the convictions of men who provided detailed instructions on how to use the piracy app 'Popcorn Time'... Read the rest of the article here: Torrentfreak

Other resources – New Media Rights, FOSS, National Law Review,

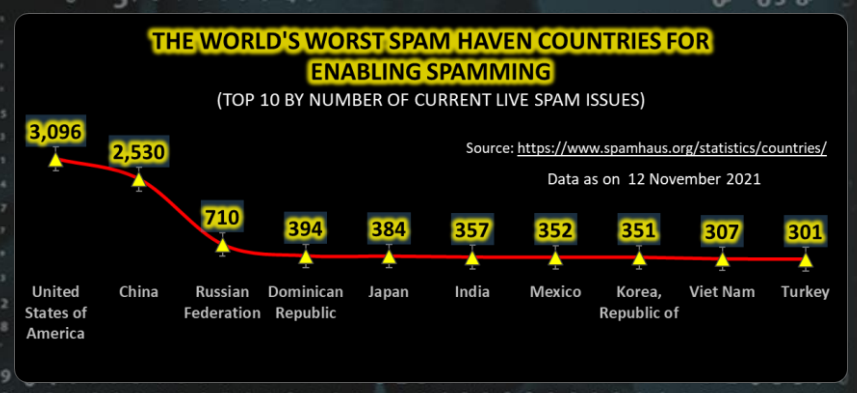


For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov



Other Interesting News and Cyber Security bits:

- In a quantum future, our economy needs to be protected. A cybersecurity expert explains why
- Swiss set to drop criminal probe of VW emissions scandal
- An expired domain caused issues launching games



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com