Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On November 17, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Palo Alto, Apple, and Google products.
See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
19 Nov	256,349,268	5,147,173

Deaths this week: 51,500

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
19 November 2021

In The News This Week

Bad form: FBI server sending fake emails taken offline and fixed

Far from complex, the sender manipulated a POST request to send an email from FBI infrastructure, and automated it. - The FBI has placed the blame for a weekend fake email incident on a misconfiguration in its Law Enforcement Enterprise Portal (LEEP) that allowed emails to be sent from the ic.fbi.gov domain. "LEEP is FBI IT infrastructure used to communicate with our state and local law enforcement partners," it said. "While the illegitimate email originated from an FBI operated server, that server was dedicated to pushing notifications for LEEP and was not part of the FBI's corporate email service. No actor was able to access or compromise any data or PII on the FBI's network." The FBI said it initially took the "impacted hardware" quickly offline, and later said it quickly remediated the "software vulnerability" as well as confirmed its network integrity. Spamhaus said it saw two waves of email being sent… Read the full story by Chris Duckett here: ZDNet

Dark web crooks are now teaching courses on how to build botnets

Security researchers are warning that the botnet threat could increase as more would-be crooks learn how to build their own. - Botnets are one of the key drivers of cyberattacks, used to distribute malware, ransomware and other malicious payloads – and dark web forums are now offering lessons on how to make money from them, a move that is likely to increase the threat over time. Infected computers and devices in a cyber criminal-controlled botnet can be used to send phishing emails or malware to even more devices. It's common for botnet operators to lease out their collection of unwittingly controlled machines – which can number in the thousands – to other cyber criminals. For example, TrickBot malware ropes machines into a botnet, providing the attacker with a backdoor into them. That access is often sold to cyber criminals who can then use them to deploy ransomware, using that access to encrypt files and demand a significant ransom payment. Many botnets are used to steal usernames and passwords, while others will take the processing power of the machines they control and lease them out to launch DDoS attacks in order to overflow websites with traffic and take them down.
Read the story by Danny Palmer here: ZDNet

Revealed: The 200 Most used and Worst Passwords of 2021

If you are one of those who believed in the myth that ”123456” or ”QWERTY” were reliable passwords, it is time you get the facts right because NordPass, a password management service, has debunked this myth once and for all. Read on to find out the worst passwords of 2021. According to a report from NordPass, people haven't yet stopped relying on done-to-death passwords such as ”123456,” ”12345,” ”password,” and ”qwerty,” while research reveals that these three are the weakest passwords nowadays and can easily make you vulnerable to hacking. The password 123456 appeared over 103 million times in NordPass's research. (See: List of 2021 most used passwords) The study involved around fifty countries, and researchers conducted gender comparisons to reach a fair conclusion. As many as 222,287 females used ”iloveyou” as their password in the US, while 96,785 men used the same… Read the full article by Waqas here: Hackread; Select your country in the NordPass Report here

How Iran Tried to Undermine the 2020 US Presidential Election

From faked emails to a hacked voter registration database, a new indictment offers fresh details on the attempted interference. – Less than two weeks before the 2020 US presidential election, tens of thousands of emails purportedly from the far-right group Proud Boys threatened to "come after" Democrats if they didn't vote for Trump. As officials warned at the time, the messages were part of a broader Iranian disinformation and influence campaign meant to sow division in the US and undermine confidence in the electoral process. Now, the US Department of Justice has unsealed an indictment that charges two Iranian nationals with carrying out those email blasts and more, providing new details on an audacious election interference scheme. Seyyed Mohammad Hosein Musa Kazemi, 24, and Sajjad Kashian, 27, face charges of conspiracy, transmission of interstate threats, computer fraud, and voter intimidation. The two allegedly worked for the Iranian cybersecurity company Emennet Pasargad, which Justice Department officials say has contracted with the Iranian government…
Read the full story by Lily Hay Newman here: Wired

Online video meetings, how secure are you?

With the advent of the Covid-19 pandemic in early 2020, the world as we knew it changed dramatically. With various stages of lock-down across the world, face-to-face meetings, physical conference attendance, and even school attendance had to make way for an electronic alternative. As "Work from Home" (WFH) and virtual schooling became the norm, the adoption of video conferencing and meeting solutions soared. The three most prominent solutions are Zoom, Google Meet, and Microsoft Teams. With Zoom's free edition in the mix, it became by far the most popular solution for the man in the street with a whopping 49% market share. Other chatroom solutions with similar capabilities like Discord and Hangouts are also gaining huge popularity among the younger generation.

With that being said, let's look at the security spectrum and the risks associated with video meetings. In a previous bulletin, I reported how a stalker managed to work out exactly what the address of a young Japanese actress was by just studying the social media photos she shared. The unfortunate outcome of that episode was a physical assault on the young lady. Now with video conferencing and meetings, you have to bear the same in mind. We all heard of the term gate crashing in video meetings, where uninvited guests manage to join the meeting. Sometimes the intention of these so-called gate crashers is just to disrupt the meeting or to spy or gather information not intended for them. But, sometimes these guys will silently observe and analyze the surroundings or background of the participants whose videos are on. Sometimes these perpetrators are actually invited guests or worse, someone masquerading as an invited guest.

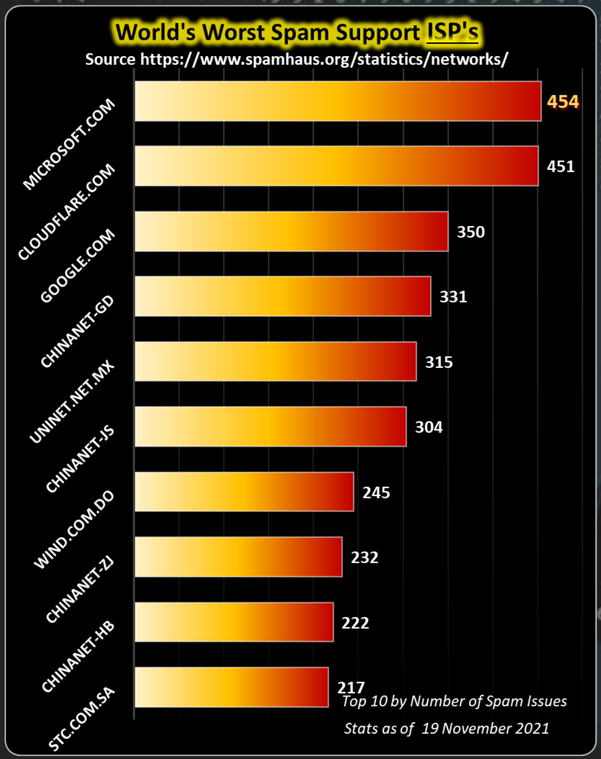
Now, what are these service providers offer in the line of security? For this post, I'll use Zoom as an example but the security concerns are related to all video conferencing solutions. According to a recent post in Tom's Guide, "Zoom went from 10 million daily users in December 2019 to 300 million daily users in April 2020 (a number that was disputed but recent polls indeed reflect that Zoom has in the excess of 300 million daily users). At the time, Zoom's security and privacy practices came under sharp scrutiny — and experts didn't like what they found." Since then Zoom has made a number of improvements to its security posture with better controls available for the meeting host to reduce the possibility of gate crashing and other illicit information sharing/leaking. Zoom published an updated Security Guide in February this year to assist users and meeting hosts with secure meeting protocols. As far as I can see, however, end-to-end encryption is still only an option and is not applied by default, so meeting hosts, keep that in mind.

However, the software and service providers can only do so much to ensure a secure meeting, but as per the nature of online meetings, you share and converse and most of the time, this includes a live streaming video camera. The onus of being vigilant is on you. What you say and what you show and what others see on your camera footage can reveal many things about you, your surroundings, and maybe your travel itinerary. The nature of online meetings is less formal than in-person meetings or gatherings and in general, people are more relaxed as the meetings are mostly attended from the comfort of their homes or another informal venue, like a coffee shop. Naturally, the more relaxed you are, the easier it is to let your guard down. On the other side of the coin, In a post written in "The Conversation", they give 5 reasons why Zoom meetings can be utterly exhausting. Both of these scenarios are conducive to a situation where safety and security are not at the forefront of your mind and "things" can slip through.

Now, with that in mind, let's look at simple steps you can follow to keep you safer during your Zoom session.

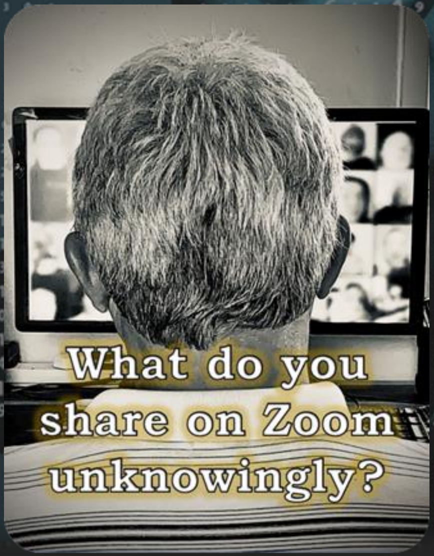
1. Be mindful of your background, that family photo on the wall behind you can reveal more than what you want to share. Sitting on your veranda or balcony on a hot day sounds great, but what can others see in the background, a street name? , a distinctive feature in a garden? In general, be aware of your surroundings when your video is on. Make sure others don't see things you do not want to share. Make sure that security apparatus like surveillance cameras, alarm panels, or motion sensors are not visible in the background. Most video conferencing solutions support virtual backgrounds,
2. Do not overshare in your conversations, especially if some of the participants are not close relatives or friends. Even in a work meeting, some of the participants might come up with some sinister ideas if the opportunity presents itself. Do not advertise the fact that you will be on holiday and your house will be uninhabited for some time if you do not personally know the participants. Although we sometimes desperately want to share the fact that we just acquired something new, but it is mostly better to keep it to ourselves, especially if it is something of great value or even something like a firearm.
3. Distribute your Zoom meeting link only to those individuals who will be attending your meeting. Do not share your meeting link on social media or other public platforms, anyone who sees the link will be able to join your meeting (unless you set a password for your meeting and share that privately with invited guests, but that sounds like double work to me)
4. A note on screen sharing, make sure all the windows that contain information you do not want to share is closed before you share your screen. Firstly, it can be quite embarrassing if you start sharing your screen and some private photos are open, but more importantly, a confidential report that is open can accidentally be shared, and once it is seen, it cannot be "unseen".
5. Make it a habit to stay on mute unless you actually speak. That side-line conversation you have with a family member or colleague can reveal many things you do not want to share with the rest of the world. Especially if you tell your wife you are going to walk over to the bank through the park to deposit the ten grand in your pocket. (exaggerated, but you get my point). Sharing is not necessarily caring if it comes to video meetings.
6. Unless you really need it, turn off the Annotation option, participants can "Zoom bomb" your screen share.
7. Follow Zoom's Security Guide to minimize the opportunity for uninvited guests and shares.

References: Tom's Guide, Zoom, VdoCipher, ProofHub,


World's Worst Spam Support ISP's
Source https://www.spamhaus.org/statistics/networks/

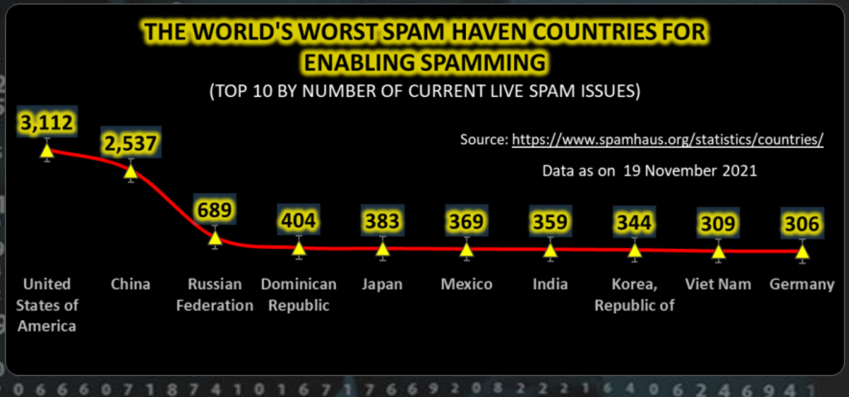
Top 10 by Number of Spam Issues
Stats as of 19 November 2021

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



Other Interesting News and Cyber Security bits:

- New York City mayor-elect says he'll take his first three pay checks in Bitcoin
- Apple is working to build a fully autonomous electric car
- Microsoft now has one of the world's fastest supercomputers (and no, it doesn't run on Windows)


THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)
Source: https://www.spamhaus.org/statistics/countries/
Data as on 19 November 2021

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