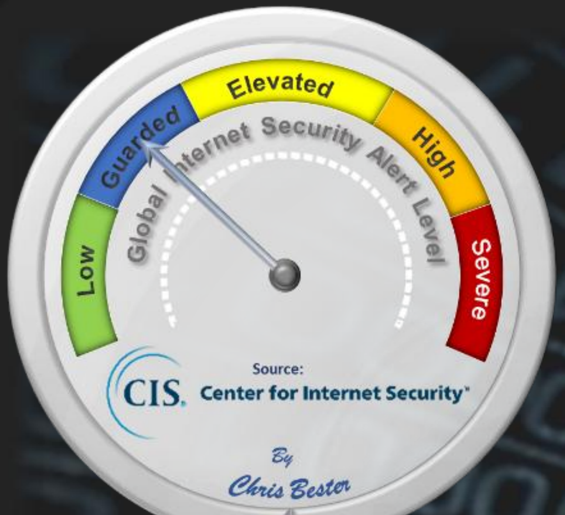

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

**On August 18, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google Chrome.**
**See [Latest Advisory](#) 18 AUG 2021**

Covid-19 Global Stats

| Date | Confirmed Cases | Total Deaths |
|---|---|---|
| 13 Aug | 210,846,773 | 4,417,500 |

## 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

20 August 2021

## In The News This Week

### Critical IoT security camera flaw allows attackers to remotely watch live video

Mandiant, CISA and ThroughTek disclose a vulnerability in millions of devices that could let attackers watch live camera feeds, create botnets or use hacked devices as a stepping stone to further attacks. - Security vulnerabilities in millions of Internet of Things (IoT) devices, including connected security cameras, **smart baby monitors** and other digital video recording equipment, could allow cyber attackers to compromise devices remotely, allowing them to watch and listen to live feeds, as well as compromise credentials to prepare the ground for further attacks. The vulnerabilities in IoT devices that use the ThroughTek Kalay network have been disclosed by cybersecurity company Mandiant in coordination with the Cybersecurity and Infrastructure Security Agency (CISA) and ThroughTek. . Read more here: ZDNet

### 40 million T-Mobile customers hit by US data breach

More than 40 million T-Mobile customers have been hit by a US data breach, the company has admitted. It blamed the breach on a "highly sophisticated cyberattack" - It said it is "taking immediate steps to help protect all of the individuals who may be at risk from this cyberattack". The firm said that while criminals stole personal information, no financial details were leaked as a result. The breach only came to light following online reports last weekend that criminals were attempting to sell a large database containing T-Mobile customer data online. The US telecom giant confirmed that hackers had gained access to its systems on Monday. "Late last week we were informed of claims made in an online forum that a bad actor had compromised T-Mobile systems," it said. "We immediately began an exhaustive investigation into these claims and brought in world-leading cybersecurity experts to help with our assessment. "We then located and immediately closed the access point that we believe was used to illegally gain entry to our servers." The company said its investigations identified approximately 7.8 million current T-Mobile postpaid customer accounts' information in the stolen files, as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile. Read more here: BBC

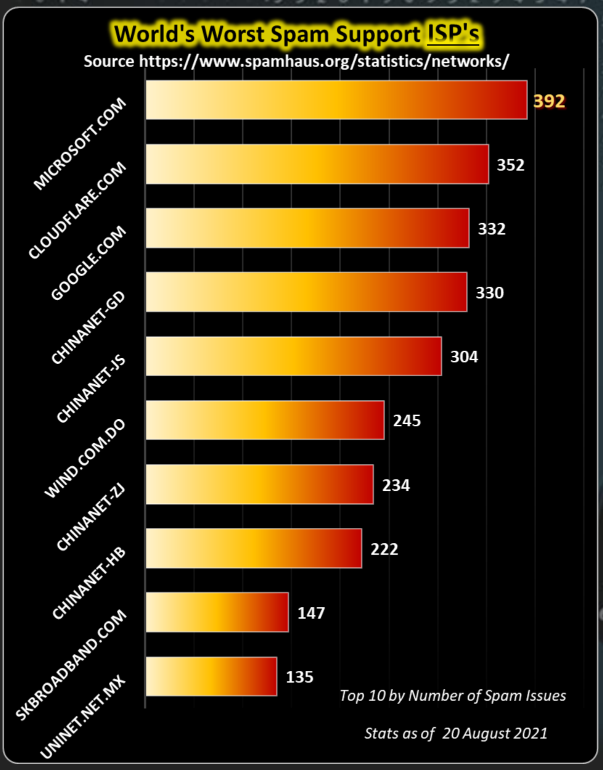
### Liquid cryptocurrency exchange loses $94 million following hack

Japan-based cryptocurrency exchange Liquid has suspended deposits and withdrawals after attackers have compromised its warm wallets. Liquid is one of the largest cryptocurrency-fiat exchange platforms worldwide (based on daily traded spot volume). The exchange has more than 800,000 customers from over 100 countries and says that it reached a $1.1B+ daily trade volume this year. After discovering that its warm wallets were hacked, the crypto exchange moved its assets into a cold wallet. "We are currently investigating and will provide regular updates. In the meantime deposits and withdrawals will be suspended," Liquid said. Current status of Liquid services: (1) To ensure safety of funds, please do not deposit any crypto assets to your Liquid wallets until further notice. (2) Liquid has halted all crypto withdrawals while we assess the impact. (3) Fiat withdrawals and deposits remain available. (4) Other services on Liquid, including trading and Liquid Earn, remain available.
Read the story here: BleepingComputer

### Botnet Generates One of the Largest DDoS Attacks on Record

Last month, someone attempted to launch one of the largest Distributed Denial of Service (DDoS) attacks on record to take down a financial website, according to Cloudflare, an internet infrastructure provider. The attack involved generating a flood of internet traffic via HTTP browser-based requests. At its peak, the bombardment reached 17.2 million requests per second. "For perspective on how large this attack was: Cloudflare serves over 25 million HTTP requests per second on average," the company wrote in a blog post on Thursday. "So peaking at 17.2 million rps, this attack reached 68% of our Q2 average rps rate of legitimate HTTP traffic." In total, the attack bombarded the company's servers with 330 million requests in less than one minute. However, Cloudflare says its automated systems were able to automatically detect and mitigate the flood of traffic. According to Cloudflare, the incident represented the largest application layer-based DDoS attack publicly known. The previous record holder was a 6 million request-per-second attack Google detected last year. In 2017, Google also fended off a separate 2.5Tbps DDoS attack believed to be the largest one in history. However, the assault leveraged a different method to bombard the company's network, so it's measured differently. Read the story here: PCMag

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



*Top 10 by Number of Spam Issues*

*Stats as of 20 August 2021*

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

Oh no!!, hard drive failure.. ?! … and I was just going to do a backup this week!

## Cryptocurrency jargon you should know

By now, most of you know or have an idea what cryptocurrency is. Some of you are already trading or thinking of trading in cryptocurrency. Security-wise, though, the media report on breaches or cryptocurrency thefts almost every week, as we saw once again this week, leaving you to wonder how safe it really is. However, making your own assessment is not so easy, since you get bombarded with a tonne of technical jargon most of us don't really understand. To that point, I decided to list some of the jargon here to make it a bit easier to understand what they are talking about in the countless media reports. Or, if you are dabbling with the thought of investing in cryptocurrency, the information and links could help you a great deal. (The list below is not comprehensive and specifically not in alphabetical order to try and share the most relevant information within a limited space. Please explore the links provided for more in-depth detail)

**Cryptocurrency -** Cryptocurrency is not a legal tender, and not endorsed or backed by any government. A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology (See Blockchain below). More than 10,000 different cryptocurrencies are traded publicly, according to CoinMarketCap.com, a market research website. And cryptocurrencies continue to proliferate, raising money through initial coin offerings, or ICOs. The total value of all cryptocurrencies on Aug. 18, 2021, was more than $1.9 trillion

**Fiat Currency -** Fiat is just mainstream legal tender, or official national currency, issued by governments. This includes the US Dollar, Canadian Dollar, Euro, Japanese Yen, etc. Fiat isn't backed by any commodity like gold (so when the USD used to be on the gold standard, it wasn't fiat). And the material it's made from isn't worth anything in and of itself. Instead, the value of fiat currency is determined by supply and demand — and because the government says it's legal money.

**Fiat to Crypto -** "Fiat to crypto" means buying cryptocurrency with fiat money … so, for example, buying Bitcoin with USD. The reason this is even a thing is because a few years ago, many online trading platforms only allowed you to trade crypto for crypto. So if you had Bitcoin you could trade it for Litecoin, or if you had Litecoin you could trade it for Ether. But you couldn't just buy Ether or Litecoin with USD.

**Bitcoin -** The first and most valuable cryptocurrency, launched on Jan. 3, 2009. While its value has climbed steadily since then, it has seen wild fluctuations. In the past months alone, the price of Bitcoin has fluctuated from a record high of $60,000 to below $30,000.

**Altcoin -** Any coin that's not Bitcoin. Altcoins can be anything from the second-most popular coin, Ethereum, to any of the thousands of coins with very minimal market value. Experts say you should largely stick to the bigger, more mainstream cryptocurrencies as an investment.

**Blockchain -** A digital form of record keeping, and the underlying technology behind cryptocurrencies. A blockchain is the result of sequential blocks that build upon one another, creating a permanent and unchangeable ledger of transactions (or other data).

**Initial Coin Offering (ICO)**
A way that funds are raised for a new cryptocurrency project. ICOs are similar to Initial Public Offerings (IPOs) of stocks.

**Wallet -** A place to store your cryptocurrency holdings. Many exchanges offer digital wallets. Wallets may be **HOT** or **COLD**. A hot wallet is a software-based cryptocurrency wallet connected to the Internet. While more convenient for quickly accessing your crypto, these wallets are a bit more susceptible to hacking and cybersecurity attacks than offline wallets. A cold wallet is a secure method of storing your cryptocurrency completely offline. Many cold wallets (also called hardware wallets) are physical devices that look similar to a USB drive. This kind of wallet can help protect your crypto from hacking and theft, though it also comes with its own risks; like losing it, along with your crypto.

**Ethereum -** The second largest cryptocurrency by trade volume, Ethereum is a crypto network and software platform that developers can use to create new applications, and has an associated currency called ether.

**Decentralized Applications (DApps) -** Applications designed by developers and deployed on a blockchain to carry out actions without intermediaries. Decentralized finance activities are often completed using decentralized apps. Ethereum is the main network supporting activities in decentralized finance.

**Decentralized Finance (DeFi) -** Financial activities conducted without the involvement of an intermediary, like a bank, government, or other financial institution.

**Gas -** A fee that developers have to pay to the Ethereum network in order to use the system. Gas is paid in ether, the native cryptocurrency of Ethereum.

**Mining -** Mining is the process of verifying new transactions on a blockchain. When someone donates computer power to a miner to complete an encryption challenge, that donor is then awarded in cryptocurrency.

**Non-fungible tokens (NFTs) -** Non-fungible tokens are units of value used to represent the ownership of unique digital items like art or collectibles. NFTs are most often held on the Ethereum blockchain.

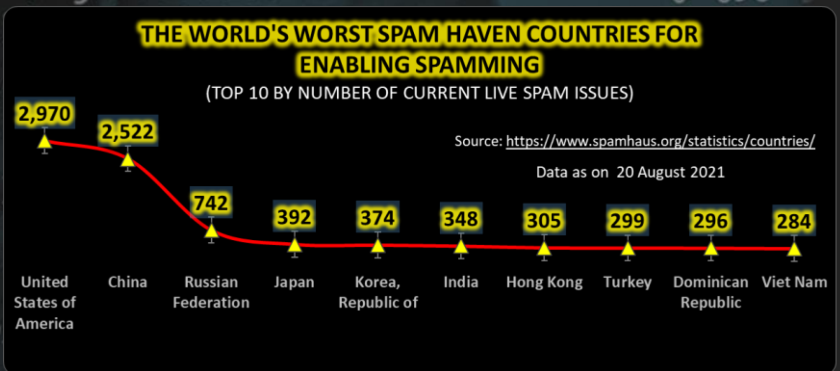
**Tokens -** Unlike altcoins, tokens are created and given out through an Initial Coin Offering, or ICO, very much like a stock offering. They can be represented as: • Value tokens (Bitcoins), • Security tokens (to protect your account) or • Utility tokens (designated for specific uses). They are not so much meant to be used as money as they are used to describe a function. Like American dollars, they represent value but they are not in themselves of value.

That is all we have space for in this edition, please click on the following links to get more info. NextAdvisor, NerdWallet, Dummies, SoFi, One37PM

## Other Interesting News and Cyber Security bits:

- Physicists Levitate a Glass Nanosphere, Pushing It Into The Realm of Quantum Mechanics
- Best Home Security Systems of 2021
- Cryptocurrency Heist: Poly Network Offers Hacker Top Security Job, Insists on Him Keeping $500,000 Reward

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 20 August 2021

*Thank you once again to my good friends Graeme Cartwright and Yazan Shapsugh for the constant contributions*

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