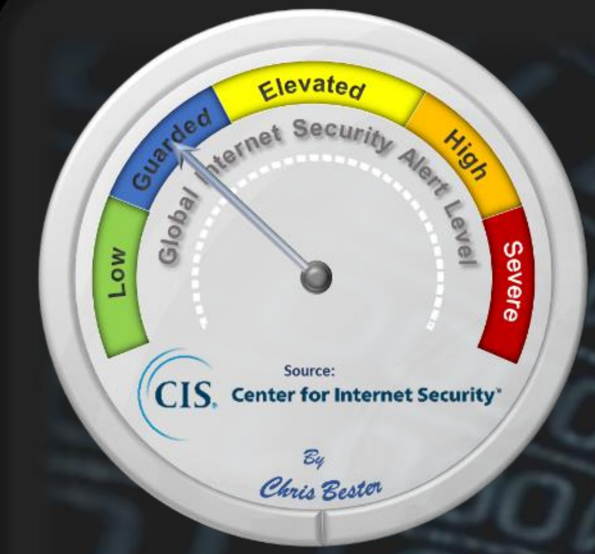

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On February 2, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Samba, and Google products. CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
04 Feb	388,909,416	5,732,814

Deaths this week: 75,709

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 February 2022

In The News This Week

Scammers are posting fake job ads on networking sites to steal your money and identity

The FBI's Internet Crime Center (IC3) is warning that scammers are exploiting verification weaknesses in job-focused networking sites to post legitimate looking ads, capture personal information and steal money from job seekers. Scammers "continue to exploit security weaknesses on job recruitment websites to post fraudulent job postings in order to trick applicants into providing personal information or money," the FBI warns in a new public service announcement. The bogus ads threaten to damage the impersonated firm's reputation and financial loss for the job seeker. According to IC3's complaint reports, the average reported loss from this scheme since early 2019 has been **$3,000** per victim. Read the rest of the story by Liam Tung here: ZDNet

Cyber Security Market is Expected to Reach $478.68 Billion by 2030: Says AMR

According to the report published by Allied Market Research, the global cyber security market was estimated at $197.36 billion in 2020 and is expected to hit $478.68 billion by 2030, registering a CAGR of 9.5% from 2021 to 2030. The report provides an in-depth analysis of the top investment pockets, top winning strategies, drivers & opportunities, market size & estimations, competitive scenario, and varying market trends. An increase in malware & phishing threats among enterprises, rise in adoption of IoT & BYOD trends and surge in demand for cloud-based cybersecurity solutions drive the growth of the global cyber security market. On the other hand, budget constraints among organizations restrain the growth to some extent. However, growth in the adoption of mobile device applications & platforms and an increase in the need for strong authentication methods is expected to create lucrative opportunities in the industry. Read the rest of the story here : GlobalNewsWire

Critical Cisco Bugs Open VPN Routers to Cyberattacks

Critical security vulnerabilities in Cisco's Small Business RV Series routers could allow privilege escalation, remote code execution (RCE) with root privileges on the devices and more. The RV series is a set of affordable VPN appliances that enable remote workers to connect to a company network. They come with built-in firewalls, advanced encryption and authentication features. The critical bugs are part of 15 total vulnerabilities affecting the RV product line that Cisco disclosed this week. Some of the issues are exploitable on their own, while others must be chained together, the networking giant said – but they all could lead to a concerning cornucopia of bad outcome. Read the story by Tara Seals here: ThreatPost

Russian Gamaredon Hackers Targeted 'Western Government Entity' in Ukraine

The Russia-linked Gamaredon hacking group attempted to compromise an unnamed Western government entity operating in Ukraine last month amidst ongoing geopolitical tensions between the two countries. Palo Alto Networks' Unit 42 threat intelligence team, in a new report publicized on February 3, said that the phishing attack took place on January 19, adding it "mapped out three large clusters of their infrastructure used to support different phishing and malware purposes." The threat actor, also known as Shuckworm, Armageddon, or Primitive Bear, has historically focused its offensive cyber attacks against Ukrainian government officials and organizations since 2013. Last year, Ukraine disclosed the collective's ties to Russia's Federal Security Service (FSB).
Read the rest of the story by Ravie Lakshmanan here: TheHackerNews

Exposed corporate credentials threatening the pharma sector

Constella Intelligence released a report which includes new and additional findings pertaining to exposures, breaches, and leakages within the pharma sector, specifically focusing on employees and executives from the top twenty pharma companies on the Fortune Global 500 list. By analyzing identity records from data breaches and leakages found in open sources and on the surface, deep, and dark web, the threat intelligence team identified 9,030 breaches/leakages and 4,549,871 exposed records—including attributes like email addresses, passwords, phone numbers, addresses, and even credit card and banking information—related to employee corporate credentials from the companies analyzed.
Read the rest of the article here: HelpNetSecurity

Choosing and sizing a UPS for your home office

An integral part of information security is data integrity, and a sudden power loss can compromise your data integrity, or even cause data to be lost. We are not even talking about the inconvenience or frustration, and the impact on your productivity.
Since the world around us changed dramatically in the last two years and most folks were forced to set up a home office, the normal infrastructure safeguards the corporate office provided disappeared. Most of us were not really prepared, and setting up these safeguards costs money. Most organizations are also not interested in footing the bill for home office safeguards like a simple UPS (Uninterrupted Power Supply). The reality is that you need these things to ensure a stable environment for your home office. The question is, however, what do you buy and how do you size it for your specific needs. Today I want to share a high-level and very basic overview of how to size and choose the correct UPS for your needs.

The 2 most common power problems

Blackout – A power outage lasting anywhere from seconds to days. These are most commonly caused by severe weather, utility power shortages (load shedding), accidents, and power grid failures.
Surge – A brief, but intense, spike in the electric current supply commonly caused by lightning. Surges can damage and destroy electronics, and the intense "spike in electricity" or spike in voltage and current harms circuit boards and components.

What is a UPS System?

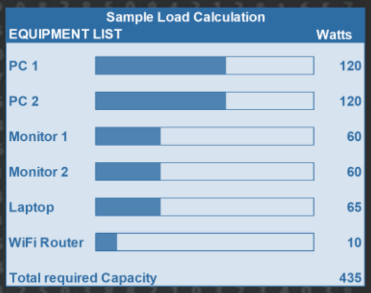
An Uninterrupted Power Supply or UPS is essentially a battery backup system. It can range from a most basic system that supplies power long enough for equipment to properly shut down, to a highly sophisticated system that provides several hours of power when utility power fails. A UPS system helps to prevent loss of data and minimizes the stress a hard shutdown causes on your electronic equipment. In general, a UPS system also acts as a surge protector that protects connected devices from sudden power surges or abnormal voltage fluctuations. If this occurs frequently it can reduce the lifespan or performance of electronic devices. A sudden power surge or fluctuation can be caused by a lightning strike or an electrical short circuit, and so on.

What types of UPS Systems are there?

UPS systems have three different topologies, or categories, based on what type of power protection you need. These are:
(1) Standby UPS - An offline unit that can detect an electrical failure and switch to battery power automatically.
(2) Line-Interactive UPS - A Line-interactive UPS is one type of uninterruptible power source that can regulate voltage automatically. The line-interactive technology responds to high and low voltage conditions. Units also support systems during outages without battery drainage.
(3) Online UPS – A system that utilizes either **double or delta conversion** technology. With double conversion, network equipment does not receive electricity directly from the AC outlet. Instead, AC power travels to a DC rectifier first, then to the battery, and then inverted to AC power delivered to equipment. With delta conversion, a certain amount of power is sent to run computers, routers, and other equipment directly. The Online UPS option is probably the most efficient but it also comes with a higher price tag.

How Big Does My UPS Need to Be?

For the UPS system to supply adequate power, it must have enough capacity to support all the equipment you want to plug into it. "Capacity" is how much power a UPS system can provide (measured in Watts). The higher the capacity, the more electronic devices it can support. To determine the UPS's capacity, you will need to calculate the load first. The Load is the combined amount of power each of the devices use. To identify the load, make an equipment list, and jot down the total watts each one requires to run. Include all of the devices the UPS will need to support. If a piece of equipment has a redundant power supply, only count the wattage of one power supply. If you are unsure how many watts your equipment requires, check the power supply specifications in the user manual or on the sticker tag , or consult the manufacturer.


Sample Load Calculation

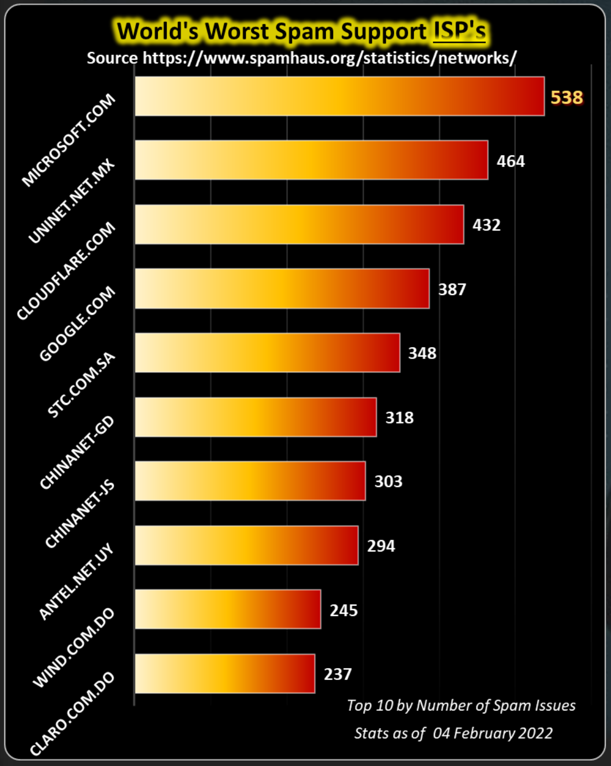
EQUIPMENT LIST	Watts
PC 1	120
PC 2	120
Monitor 1	60
Monitor 2	60
Laptop	65
WiFi Router	10
Total required Capacity	435

How long do I need the UPS to supply power for?

You must now determine runtime. **Runtime** is the number of minutes a UPS system can support the attached devices with electricity during a blackout. This will determine the battery size. The minimum runtime is the time you need to complete proper equipment shutdown. If you want the UPS to supply power for at least 2 hours, for example, you will need a system with a bigger battery or even an array of batteries.

This is unfortunately all I have space for in this bulletin but please check out the resources below to learn more.

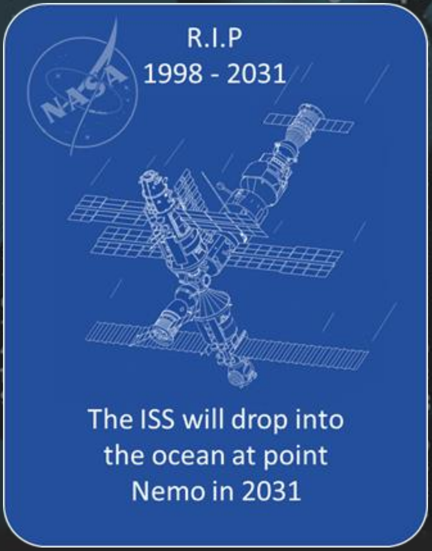
Resources: CyberPower, APC, CommsExpress, Alpha, Riello, WilTronics


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

ISP	Spam Issues
MICROSOFT.COM	538
UNINET.NET.MX	464
CLOUDFLARE.COM	432
GOOGLE.COM	387
STC.COM.SA	348
CHINANET-GD	318
CHINANET-JS	303
ANTEL.NET.UY	294
WIND.COM.DO	245
CLARO.COM.DO	237

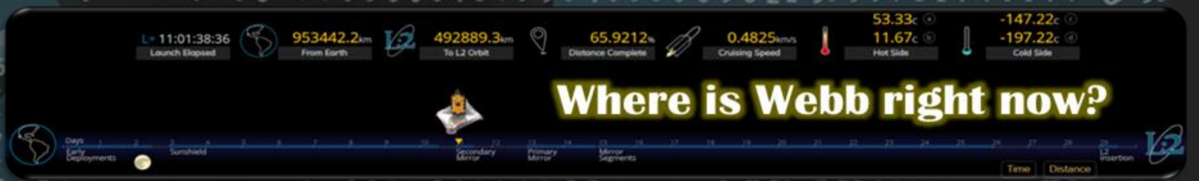
Top 10 by Number of Spam Issues
Stats as of 04 February 2022

For Reporting Cyber Crime in the USA go to the Internet Crime Complaint Center (IC3)



R.I.P
1998 - 2031

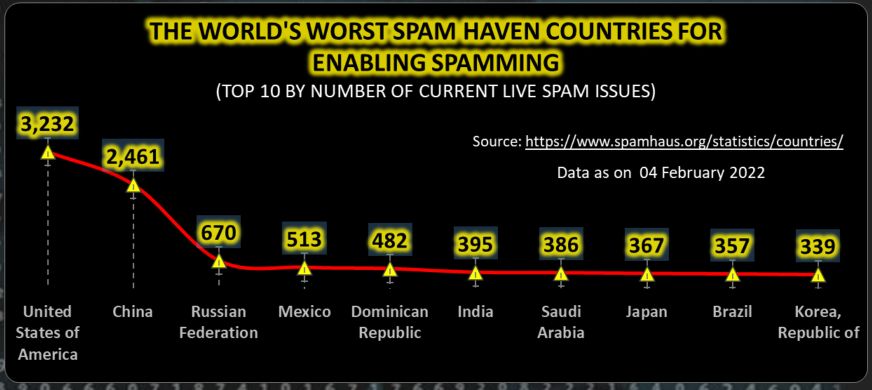
The ISS will drop into the ocean at point Nemo in 2031



Where is Webb right now?

Other Interesting News and Cyber Security bits:

- Cyber crooks are racing ahead of businesses' security plans
- Kaspersky debuts [Dis]connected – a game that teaches cyber security
- NASA Plans to Crash the International Space Station Into the Ocean
- SANS Daily Network Security Podcast (Stormcast)


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 04 February 2022

Country	Spam Issues
United States of America	3,232
China	2,461
Russian Federation	670
Mexico	513
Dominican Republic	482
India	395
Saudi Arabia	386
Japan	367
Brazil	357
Korea, Republic of	339

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