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

On October 20, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla and Oracle products.
See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
22 Oct	240,388,930	4,947,528

Deaths this week: 50,127

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

22 October 2021

In The News This Week

Acer hit with second cyberattack in less than a week, Taiwanese authorities notified

Acer has confirmed yet another cyberattack on its servers in Taiwan after their offices in India were hit less than a week ago by the same group. The Desorden Group -- which claimed responsibility for both attacks -- contacted ZDNet and said part of why they conducted the second attack was to prove their point "that Acer is way behind in its cybersecurity effects on protecting its data and is a global network of vulnerable servers." Acer spokesman Steven Chung told ZDNet that the company recently detected "an isolated attack on our local after-sales service system in India and a further attack in Taiwan." "Upon detection, we immediately initiated our security protocols and conducted a full scan of our systems. We are notifying all potentially affected customers in India, while the attacked Taiwan system does not involve customer data," Chung said. Read the full story here: ZDNet

Olympus Hit by a Second Cyber Attack a Month After the Ransomware Incident in EMEA

Japanese medical tech giant Olympus suffered a subsequent cyber attack, almost exactly one month after hackers disrupted its European, Middle East, and Africa (EMEA) operations. On its website, the company said it was investigating a "potential cybersecurity incident" detected on Oct 10, 2021. The cyber attack shut down the company's IT systems in the Americas, affecting the U.S., Canada, and Latin America with no impacts on other parts of the world, the company said. Olympus said it was working with "appropriate third parties" and had taken necessary steps to protect its customers. Read the full story here: CPO Magazine

Microsoft asks admins to patch PowerShell to fix WDAC bypass

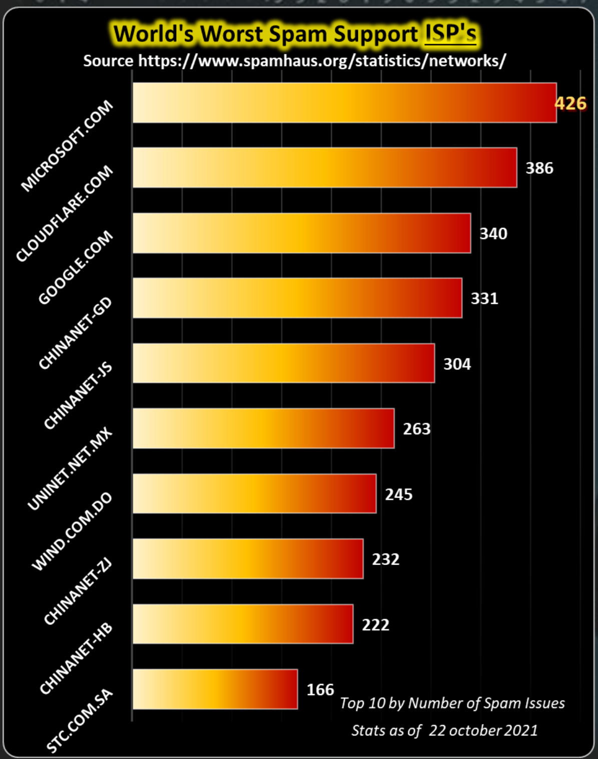
Microsoft has asked system administrators to patch PowerShell 7 against two vulnerabilities allowing attackers to bypass Windows Defender Application Control (WDAC) enforcements and gain access to plain text credentials. PowerShell is a cross-platform solution that provides a command-line shell, a framework, and a scripting language focused on automation for processing PowerShell cmdlets. Redmond released PowerShell 7.0.8 and PowerShell 7.1.5 to address these security flaws in the PowerShell 7 and PowerShell 7.1 branches in September and October. Leaked passwords and WDAC bypass - WDAC is designed to protect Windows devices against potentially malicious software by ensuring that only trusted apps and drivers can run, thus blocking malware and unwanted software from launching. When the software-based WDAC security layer is enabled in Windows, PowerShell automatically goes into constrained language mode, restricting access to only a limited set of Windows APIs. By exploiting the Windows Defender Application Control security feature bypass vulnerability tracked as CVE-2020-0951, threat actors can circumvent WDAC's allow list, which allows them to execute PowerShell commands that would otherwise be blocked when WDAC is enabled. Read the full story here: Bleeping Computer

Privacy breach: 7-Eleven secretly scanned customer faces

Australia - 7-Eleven violated its customers' privacy by secretly collecting their facial images at 700 stores over the last year for demographic profiling and data verification, the regulator has determined after a seven month investigation. The convenience store chain claims its actions did not constitute a privacy breach and will face no punishment beyond being asked to destroy the images, despite the regulator describing the breach as "serious" and having to the power to issue fines. Privacy experts said the determination still sends a clear message about businesses' privacy obligations but more clarity in Australia's legislation would help prevent similar incidents. Read the full story here: Innovation AUS

BLACKMATTER RANSOMWARE ACTORS TARGETING CRITICAL INFRASTRUCTURE

Federal authorities are warning that BlackMatter ransomware actors are targeting critical infrastructure operators, including two organizations in the food supply chain, in the last few months. BlackMatter emerged over the summer and officials from the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and NSA said Monday that actors affiliated with the group had been going after various critical infrastructure (CI) organizations.. The group targets not only Windows machines, but also Linux servers, and has been observed wiping or reformatting backup systems to hamper recovery efforts. The group's main initial access technique is using previously compromised, embedded credentials for LDAP and SMB in order to then get into the Active Directory. From there, the actors enumerate all of the machines on the network and encrypts them. Read more here: Decipher


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

Top 10 by Number of Spam Issues
Stats as of 22 october 2021

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

Not that kind of chips, you idiot!
It would be terrible if we can't get any chips... with this chip shortage and all...
CHIPS

The Chip Shortage Explained

In recent months more and more news articles and stories are reported in the media regarding the so-called "Chip Shortage" and how it is affecting our daily lives. Like most industries, the security industry is not exempted from this phenomenon. Surveillance systems, OT monitoring equipment, and even the Firewall industry are also suffering the consequences of short supply. I found many articles giving a rundown of what it is, but mostly lengthy pieces going into the finer details of what, where, and how. However, running in the footpaths of the Internet, I spotted an article by Blue Ridge Technology giving us a simple but precise overview that I am sharing below.

How It Happened and What It Means for Your Business

Have you heard about the global chip shortage? It's a serious problem, affecting everything from cars to iPhones to the equipment you need to keep your business running smoothly. But unless you follow tech news on your own time, you may not have heard about this problem or know what the ramifications might be at work.

Here's what you need to know about the global chip shortage, how we got here, and what your business needs to do to stay equipped.

The Chip Shortage: What Is It?

The global chip shortage is a supply chain problem caused by a lack of sufficient supply of the silicon microchips that power today's electronics. These chips go by a variety of names: semiconductors, semiconductor chips, computer chips, and so on. And right now, manufacturers need more of these chips than the chipmakers can make.

These chips are in nearly everything with a computing component, from household appliances to cars to consumer electronics. As a rule of thumb, if it has a screen, it has one or more chips inside.

The auto industry was one of the first to hit a chip shortage. Ever since the summer of 2020, new vehicles have been in short supply— not because of assembly line shutdowns, but because the automakers can't source the $10 chips for the computer and infotainment modules that the vehicles can't run without.

These chips exist at a variety of performance and price levels, too. The high-performance chips in the latest computers and smartphones are far more complex — and more expensive — than the chips that power a smart toaster or even a smart TV. Various types of chips are faring better or worse, but the shortage is affecting most categories at this point.

How Did This Happen?

So, how did we get here? Well, it's complicated, but in a word, COVID. Most of the global manufacturing capacity for semiconductors is located in Asia, which was the first region to shut down at the beginning of the COVID-19 pandemic. Semiconductor factories sat offline for months, but demand for their chips didn't lag all that much.

Semiconductors are incredibly complex, and they take a long time to make — in the neighbourhood of three months, start to finish. On top of that, building a new plant for manufacturing them is not simple. Some firms have already begun building in Arizona, but their facilities won't even come online until 2022 at the earliest.

COVID also created high levels of demand for certain products that — you guessed it — needed semiconductors. Manufacturers shifted to fill those orders, of course.

Then, when other product manufacturers started ordering semiconductors again after the initial wave of COVID lockdowns, there weren't enough chips to go around. And for any firm that cancelled orders, they found themselves at the back of the line when it was time to order again.

There wasn't (and still isn't) enough surge capacity to create more chips to meet the demand. And no one can build new factories fast enough to fix the problem quickly. The factories are just too complicated, and it's going to take time.

What the Chip Shortage Means for Your Business

If you're just hearing about the chip shortage for the first time, this all might sound a little scary. What does all this mean for your business?

Supply chain bottlenecks caused by the chip shortage may well affect your industry and your business, and prices for electronics and equipment are trending slightly upward.

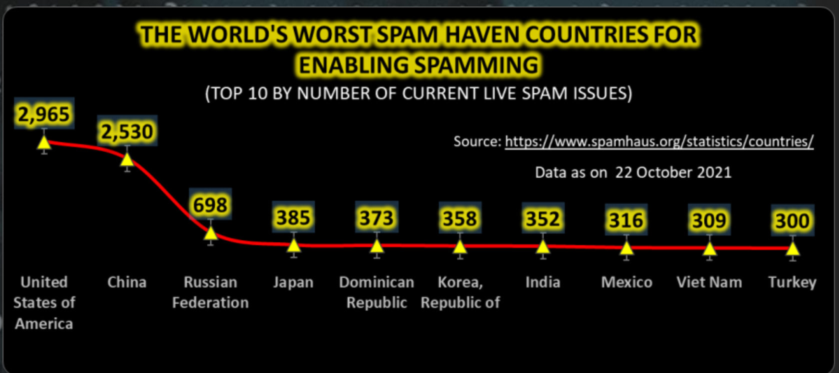
But there's good news here, too. Most businesses that have weathered the pandemic this far should have no issues maintaining normal business operations — so long as they plan ahead.

Sourcing new computers and other electronic equipment is still possible. You just might need more lead time than you would otherwise. If you think you might need any new hardware in the next six months, consider placing your order as soon as you can. That way, if you encounter any delays or supply chain issues, your vendor still has plenty of time to deliver.

If you're not sure whether certain hardware will last, now is the time to proactively order a replacement. Last-minute replacements — especially for specialized hardware — could be a real challenge during this shortage. Blue Ridge Technology, BBC, P&B

Other Interesting News and Cyber Security bits:

- The new MacBook Pro highlights what's gone wrong with Windows laptops
- Raspberry Pi price to increase for the first time ever due to chip shortage
- Qubits Are Coming: Your Quantum Computing Future


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 22 October 2021

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