On December 8, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in HP, Mozilla, Google, and WebHMI products. CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
10 Dec	268,769,794	5,303,574

Deaths this week: 53,504

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

10 December 2021

In The News This Week

Cuba Ransomware Gang Hauls in $44M in Payouts

The "Cuba" ransomware gang has settled into a groove, compromising at least 49 entities in five critical sectors in the U.S. as of November, the FBI has warned. In a flash alert, the Feds attributed a rash of attacks on U.S. entities in the financial, government, healthcare, manufacturing and information technology sectors to the group. Collectively, the hits resulted in the extortion of $44 million in ransom payments. That's a little more than half of the $74 million that the Cuba gang actually demanded across the attacks, indicating that companies remain split on whether or not to pay up. The FBI didn't name specific victims, but last month the bureau also warned that the group is targeting tribal casinos throughout the U.S... Read the rest of the story by Tara Seals here: ThreatPost

BitMart CEO Says Stolen Private Key Behind $196M Hack

The crypto exchange's CEO said the company will compensate affected users out of its own funds. - Hackers were able to drain $196 million of crypto from crypto exchange BitMart by stealing a private key that opened two hot wallets, BitMart CEO Sheldon Xia tweeted on Monday. Hackers stole $100 million worth of various cryptocurrencies on the Ethereum blockchain and $96 million on Binance Smart Chain, crypto security firm PeckShield revealed on Dec. 5. BitMart has completed an initial security check and identified affected assets, and it plans to compensate users out of its own pocket, Xia said. The exchange will announce a timetable to gradually continue deposits and withdrawals, he said, adding that he is "confident" they will resume on Dec. 7. The hackers used decentralized exchange aggregator 1inch to swap stolen tokens for ether, and deposited ether funds to privacy mixer Tornado Cash to hide their identities, PeckShield said.. Read more here: CoinDesk

Criminal hackers are now going after phone lines, too

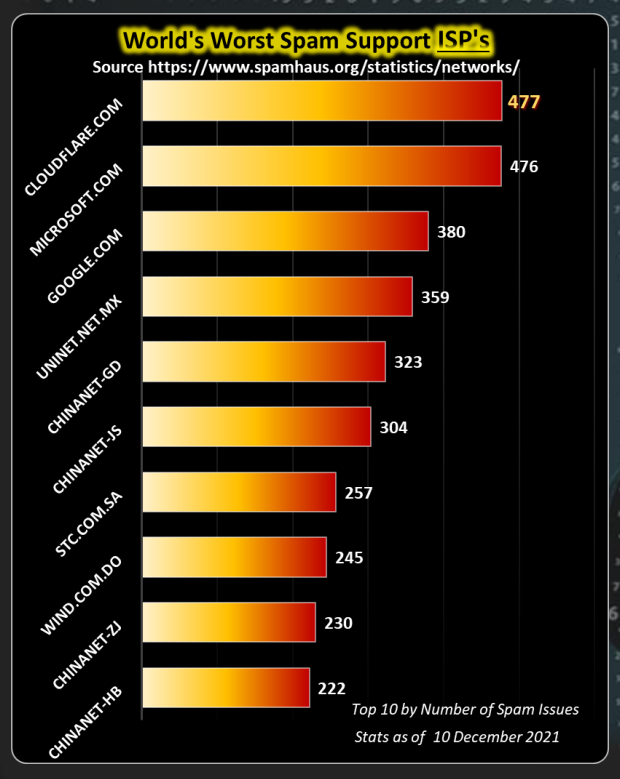
Criminal groups have been sending threatening messages in the past couple of months to companies that manage broadband phone services all over the world, promising they'll flood the digital phone lines with traffic and take them offline unless the targets pay a ransom. What those extortionists have discovered is that the number of phone calls that take place at least partially over the internet has quietly and dramatically increased in recent years — and there's a lot at stake when major providers go down. Like landline providers, companies that manage digital phone calls, also known as Voice over Internet Protocol (VoIP) services, are required to transmit audio in real time, facilitating personal, business and even emergency calls. It's probably a bigger part of our lives than many people realize. It's much cheaper and often more accessible and scalable, a staple of working from home during the coronavirus pandemic... Read the rest of the article by Jenna Mclaughlin here: NPR

Ransomware hits Spar supermarkets and petrol stations

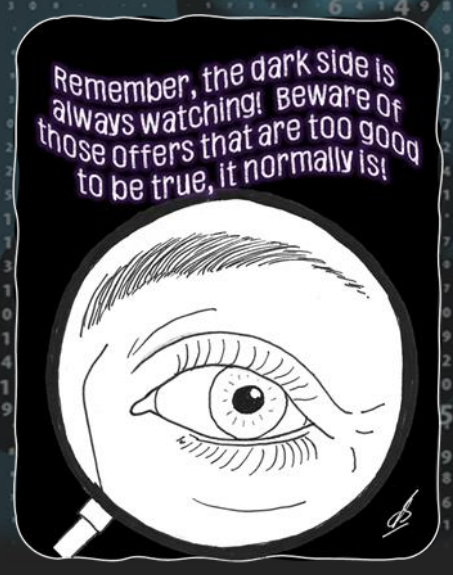
Supermarket chain Spar has had more than 300 of its convenience stores in the UK affected by a ransomware attack, which has forced some to close their doors or only accept cash payments. The cyber attack, which first struck at the weekend and was confirmed to involve ransomware on Tuesday afternoon, not only shut convenience stores but also prevented the public from fuelling at petrol stations. It appears that the ransomware attack hit Lancashire-based James Hall & Co, which operates Spar's tills and IT systems. Visitors to James Hall's website are currently greeted by an ominous signal that things have not yet returned to normal..
Read the story by Graham Cluley here

Swiss Firm Executive Operates Secret Surveillance Operation, Sources Say

The co-founder of a company that has been trusted by technology giants including Google and Twitter to deliver sensitive passwords to millions of their customers also operated a service that ultimately helped governments secretly surveil and track mobile phones, according to former employees and clients. Since it started in 2013, Mitto AG has established itself as a provider of automated text messages for such things as sales promotions, appointment reminders and security codes needed to log in to online accounts...But a Bloomberg News investigation, carried out in collaboration with the London-based Bureau of Investigative Journalism, indicates that the company's co-founder and chief operating officer, Ilja Gorelik, was also providing another service: selling access to Mitto's networks to secretly locate people via their mobile phones. Read more here: Bloomberg



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



Security Tips for the Holidays

As we are entering the holiday season and opening up our wallets for those perfect gifts for our loved ones, now, more than ever, we need to be vigilant and look at the world around us with a focus on possible criminal intent. Online shopping has more than quadrupled since the advent of the Covid pandemic, and more families find it rather convenient to walk through the virtual hallways of the Internet mall rather than a physical visit. The problem is that it's not only the marketing companies that are excited about this growth, the criminal element in our world welcomed this shift too. It is not to say that old-fashioned scams are dwindling, no, it is still out there in force, it is just that more opportunities are presenting themselves to the criminal element to exploit the online world.
So, if you are out and about this holiday season, whether online or not, be mindful that the dark side is always on the lookout for easy prey. It may sound cynical but make sure the pick-pocket racketeer go for the easier target in the crowd rather than you. For example, I personally have a "holiday" wallet with a nice-looking, but strong chain attached, which I hook onto my belt.
That doesn't mean they can't steal my wallet, it only means it will be easier to take the wallet of the guy next to me who doesn't have a chain on his wallet. The same goes for your online habits, make sure you have enough controls in place so the hacker goes elsewhere to look for easier prey.

In a bulletin like this, we can only make you aware or point you in the right direction, but your safety is still your responsibility. There are many resources available online to get yourself skilled up and knowledgeable to protect yourself against the supervillains of the dark side. Do some reading in those lazy days leading up to Christmas and make sure you and your loved ones practice safe online habits, and look out for those classic scams like the gift card and other scams mentioned below.

Online Gift Scams

If you've ever received an email asking you to help someone with an emergency, and that email asked for a gift card as payment, it was most likely a scam. Thieves have come up with creative ways to manipulate gift cards sold in stores, like scratching off the protective coating to steal the PINs and then replacing the layer with a sticker so it looks brand new. Scammers will add those PINs into software that alerts them when someone has purchased and activated that gift card, then drain all its funds.
The easiest way to avoid becoming the target of a gift card scam is to be vigilant and follow these best practices:

- You've probably heard it a million times, but the first thing you should do is set strong passwords for all your online accounts and use a different password for each site. Password management apps are great for keeping track of your various accounts. As I mentioned in the cartoon last week, consider using commas in your password. Generally, when hackers break into an establishment and get hold of a bunch of passwords, the easiest way to distribute it is via a CSV (Comma Separated Value) text file. The file is then typically pulled into a spreadsheet application which converts the comma-separated values into columns and thus a workable format. Imagine using two commas in your password, it messes up the column formulation, and chances are good that they'll never have your full password.
- Update your login credentials and check your payment accounts regularly for signs of any unusual activity. Most banks and credit unions will give you a quick call if something looks awry.
- If you buy a gift card in a store, check it out for tampering signs before loading funds. And only buy them from retailers that keep them secured behind the checkout counter.
- Never agree to pay for online purchases in gift cards from an email. In these cases, the thing you're trying to "purchase" probably doesn't even exist. Shop with retailers you know and trust, and always ensure the site's checkout system is secure.

Be extra vigilant for phishing attacks during the holidays

Phishing attacks are more sophisticated than ever, and phishers are ramping up attacks more than ever during this holiday season. A few common phishing attacks you'll see during the 2021 Holiday Season are:

- Brand impersonation. Phishers craft emails to look exactly like they are coming from a trusted brand.
- Fake order receipts. Phishers send a receipt to you for something you didn't buy. They are counting on you clicking on the link to notify the store, or open the attached "bill".
- Fake shipping and delivery notices. Buried with all your legitimate shipping and delivery email notices are ones crafted to look like just like the legitimate ones, but if you click, you're phished. Phishers are also inundating mobile phone users with smishing attacks, or SMS phishing attacks, where they send fake shipping and delivery notices. This method is extremely effective because **82% of people open every text message**.
- Compromised account. An email warns you that your email account or security software is compromised. Be on alert for web page notices or pop-up messages alerting you to security problems.

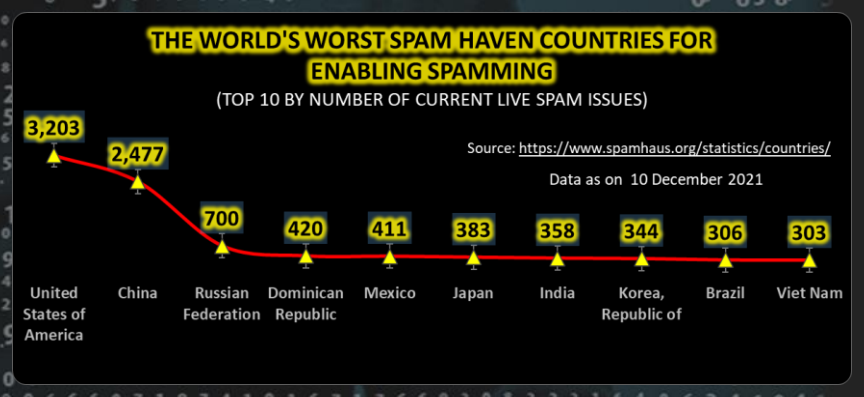
Practice social media restraint

Social media is rampant with scams year-round, but especially during the holidays. Two common holiday scans to avoid. 1) Fake social media ads which mimic legitimate ads but take you to fraudulent copycat sites. 2) In social media gift exchanges (e.g., "Secret Santa", "Secret Sister", "Secret Santa Dog", and wine exchanges), you sign up and buy a gift for an unknown stranger in the hopes you will receive multiple gifts in return. These gift exchanges are not only designed to steal your money and information; they are also illegal. Finally, protect your own information during the holidays. Don't post your vacation plans online, where thieves can't find them, and use them to plan burglaries.

References: IBTimes, Security Mentor, CISA, NCSNT

Other Interesting News and Cyber Security bits:

- Remote-working job surveillance is on the rise. For some, the impact could be devastating
- Quantinuum's new cybersecurity project signals that the future of quantum computing is—maybe, finally—here
- Number of journalists behind bars reaches global high



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