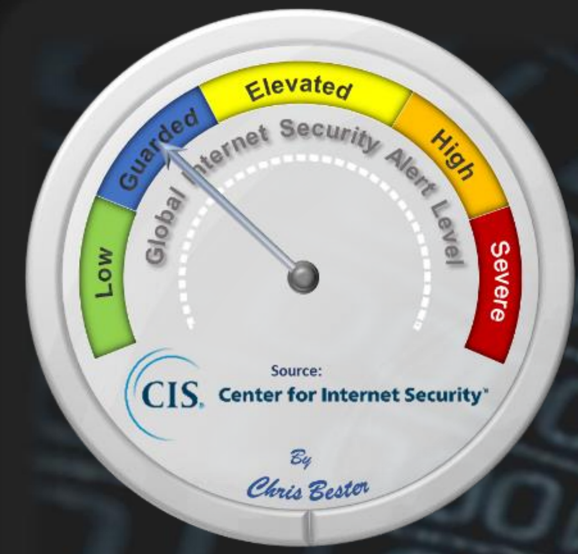

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On May 25, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in VMware, Firefox, and Google products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
27 May 22	530,367,523	6,307,895

Deaths this week: 10,561

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

27 May 2022

In The News This Week

Data protection concerns spike as states get ready to outlaw abortion

The use of personal data from brokers, apps, smartphones, and browsers to identify those seeking an abortion raises new data protection and privacy risks. The U.S. Supreme Court will almost certainly stick to its leaked draft decision to overturn the landmark Roe v. Wade decision that legalized abortion 50 years ago. According to some tallies, abortion may be banned or tightly restricted in as many as 28 states in the weeks after the Court formally hands down its decision next month. As the American Civil Liberties Union (ACLU) has noted, "The lack of strong digital privacy protections has profound implications in the face of expanded criminalization of reproductive health care."
Read the rest of the story by Cynthia Brumfield here: CSO

Snake Keylogger Spreads Through Malicious PDFs

While most malicious e-mail campaigns use Word documents to hide and spread malware, a recently discovered campaign uses a malicious PDF file and a 22-year-old Office bug to propagate the Snake Keylogger malware, researchers have found. The campaign—discovered by researchers at HP Wolf Security—aims to dupe victims with an attached PDF file purporting to have information about a remittance payment, according to a blog post published Friday. Instead, it loads the info-stealing malware, using some tricky evasion tactics to avoid detection.
"While Office formats remain popular, this campaign shows how attackers are also using weaponized PDF documents to infect systems,". Read the full post by Elizabeth Montalbano here: ThreatPost

Anonymous Declares Cyber War Against Pro-Russia Hacker Gang Killnet

Hacktivist group Anonymous has announced on social media that it's launching a cyber-war against the pro-Russian group Killnet, which recently attacked European institutions. The news comes after anonymous hackers recently declared "cyber war" against Vladimir Putin's government following the Russian invasion of Ukraine, including leaking over 360,000 Russian federal agency files in the process. On Twitter, the @YourAnonOne account announced that: "The #Anonymous collective is officially in cyber war against the pro-Russian hacker group #Killnet." Last week, Killnet attacked the websites of various Italian institutions and government ministries, including the superior council of the judiciary, its customs agency and its foreign affairs, education and cultural heritage ministries. On May 16, it was reported that Killnet also launched attacks in early May targeting Italy's upper house of parliament, the National Health Institute (ISS) and the Automobile Club d'Italia. Shortly after taking to Twitter and declaring cyber-war, Anonymous published a new message announcing that the official Killnet site was taken offline.... Read the rest by Benjamin David here: infosecurity magazine

South Africa - Load-shedding threatens digital security

As load-shedding forces remote workers to seek power from a multitude of sources, new vulnerabilities emerge, writes DOROS HADJISENONOS, Fortinet regional director for Southern Africa. Work-from-anywhere (WFA) model has greatly expanded in South Africa in recent weeks, as load-shedding forces remote workers to seek power from a multitude of sources, in malls and coffee shops, meaning they may be alternating between mobile phones, tablets and laptops across any number of potentially unsecured public Wi-Fi hotspots. This mobility increases the cyber security risks presented by all these devices that are often poorly secured, to begin with. Smartphones, in particular, have become a critical part of the remote workforce toolkit. They are such an integral part of each person's daily routine, people may regard them as trusted and safe. As a channel to your personal data, banking and accounts, and a link to your work and business data, smartphones drive cybercriminals directly to your pocket. As such, they may become the next big vector to hijack and weaponize in distributing attacks.. Read the rest of the article here: Gadget

Hackers steal 29 Moonbirds valued at $1.5 million in NFT phishing attack

The crypto Twitter community is encouraging everyone to check links and stay vigilant following a hack targeting the popular Moonbirds non-fungible token (NFT) project. Late Tuesday, 29 Moonbirds valued at about 750 ETH ($1.5 million) were taken from their owner, DigitalOrnithologist, according to on-chain data. Despite having only launched a month ago, Moonbirds are quickly joining the Bored Ape Yacht Club as a popular target for hackers. The collection, a product of venture capitalist Kevin Rose's Proof Collective, has skyrocketed in popularity and was at the center of a phishing scam shortly after its launch. Twitter sleuth 0xLosingMoney has linked this new attack to an account on Twitter named @DVincent_, which now, along with its corresponding OpenSea page, has disappeared. He also noted that, prior to the attack, other NFT holders reported being approached by @DVincent_ for private sales. Among them, Bored Ape holder @just1n_eth described how the account approached him on May 10. "We came to an agreement on price. Then this individual insisted we use a platform called 'p2peers.io'. I have been in the space [for] over a year and hadn't heard of it. I instantly knew something didn't seem right.".... Read the rest of the story by Callan Quinn here: The Block

Instagram Account Hack

This week I want to share a story by ZDNet's Steven Vaughan-Nichols who had his Instagram account hacked and his experience dealing with it. It just goes to show that even seasoned IT gurus can be fooled.

My Instagram account was hacked and two-factor authentication didn't help

After almost 40 years in technology, it finally happened. I had one of my accounts hacked. Blast it. The target was my Instagram account. While I'm very active on social networks, Instagram was the one I used the least. Here's what happened.

It all started when I got a plausible Instagram message from a friend. His message asked for my help and included a reset link for their account. Rather than asking me to click the link, which I'd never do in a million years, it simply asked me to send him back a screenshot of the message including the link. I thought, "How can I be hacked by sending a PNG image?" After all, it wasn't a reset link for my account. So I replied with the image. Oh foolish, foolish me.

It turns out the combination of the URL on the image and my reply gave them enough information to take over my account. Now, even when I saw trouble brewing -- an Instagram e-mail came asking me if I wanted to change my phone number to one in Nigeria -- I wasn't too worried. I'd protected my account with two-factor authentication (2FA). While 2FA isn't perfect, it's better than anything else out there for basic security.

But, here's where things went awry. Instagram should have sent me an e-mail with a link asking me to "revert this change." Instagram didn't send such a message. Instead, I received e-mails from security@mail.instagram.com that provided a link about how to "secure your account." This dropped me into Instagram's pages for a hacked account, which wasn't any help.

In the meantime, I got another Instagram message telling me that my account was now associated with a new e-mail account--a garbage Gmail account. Once more Instagram didn't give me a chance to refuse this change and the message sent me back to the Instagram hacked account page. Argh!

I followed up with Instagram's suggestions on how to bring my account back. I asked for a login link from my Android Instagram app. I got one, which didn't work. Next, I requested a security code. I got one. That didn't work either, no doubt because -- by that time -- the account was now responding to its "new" e-mail address and phone number. Next up, I verified my identity by providing the email address and phone number I signed up with and the type of device I used when I signed up. I had hoped for this message since I doubt very much there are that many people who sign up for Instagram do so from a Linux desktop! Well, it was a good idea, but nothing happened.

Then since my account had photos of me, I took a video selfie of myself to confirm that I'm a real person to confirm my identity. Nada.

I would have called the Instagram tech support number, except -- surprise! -- there's no such thing. After some digging, I was able to send a message directly to Instagram tech support. Instagram doesn't make it easy to find this. In fact, the Instagram support link is actually a Facebook page (*Which has since been removed*). Good going, Meta! But even after that, it didn't do me any good. I didn't hear a peep out of them.

So, I decided it was time to bring out the big guns. I sent a message as Steven J. Vaughan-Nichols, top technology journalist, to Instagram public relations asking for help and/or an explanation. That didn't work. I guess I'm not that special after all.

So, while I made the first mistake by opening the door to the hack, Instagram gets a lot of the blame for its 2FA system, indeed its entire security support system. But, hey at least I'm not alone.

The Bored Ape Yacht Club, a leading non-fungible tokens (NFT) collective, lost $3 million of NFTs to a hacker using a phishing attack. Like yours truly, the Bored Ape Yacht Club said, "At the time of the hack, two-factor authentication was enabled and security surrounding the IG account followed best practices." They also said they were working with Instagram security and they'd report on what happened. That was almost a month ago.

There appears to be a spat of these attacks going on. I've seen many reports of small businesses having their Instagram accounts hijacked. Several of my friends have reported the same. They also tell me that Instagram has been useless. One of them who works in security public relations reports he reached out to some white hats for advice, but they couldn't help. Instagram appears to be a security black hole, Users' complaints go in and nothing comes out.

Personally, this has been really annoying, but it hasn't really bothered me that much. I had less than 100 Instagram followers. My hacker appears to be using my former account to send cryptocurrency spam. Anyone who knows me knows I think cryptocurrency is a scam. I've spread the word that my account has been hacked, and people should report, unfriend, and block it.

You'd think all those reports, well over two dozen people have told me they've reported it, Instagram might have put two and two together and realized my account had been hacked. Three weeks into this and Instagram still hasn't bought a clue.

But, it could be worse. Hackers are taking over corporate and influencer Instagram accounts and demanding ransomware payments of up to $40,000.

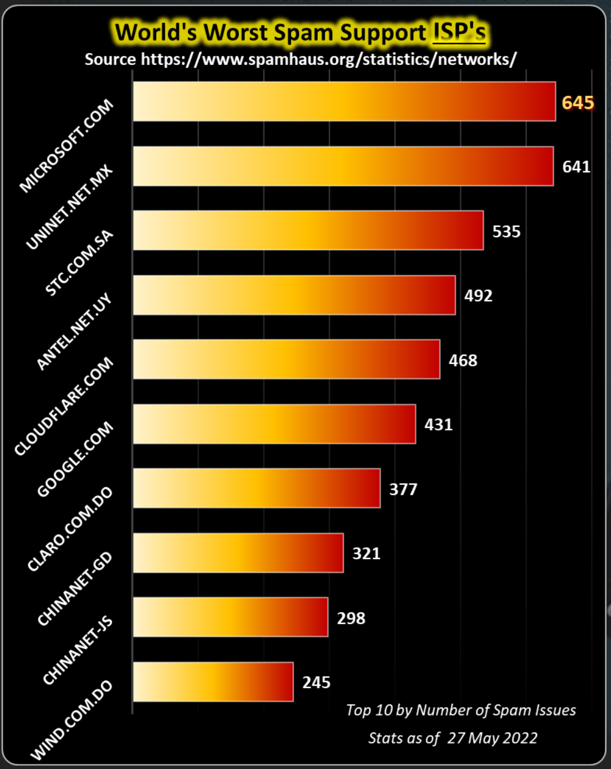
But what's irritating to me is a business killer for others. I'll shed no tears for the Bored Ape Yacht Club. NFTs are scams too and if you think otherwise I'll happily sell you an NFT of the Brooklyn Bridge. However, many design shops, videographers, photographers, and marketing people depend on it for their livelihood.

If Instagram doesn't step up its security game, it's time to find another platform for your business. I made, at most, one minor mistake, and lost my account. Instagram, with its pathetic security defenses, could lose your far more valuable account and you'd have no way to restore your account or your followers.

Read this and other stories here: ZDNet

World's Worst Spam Support ISP's

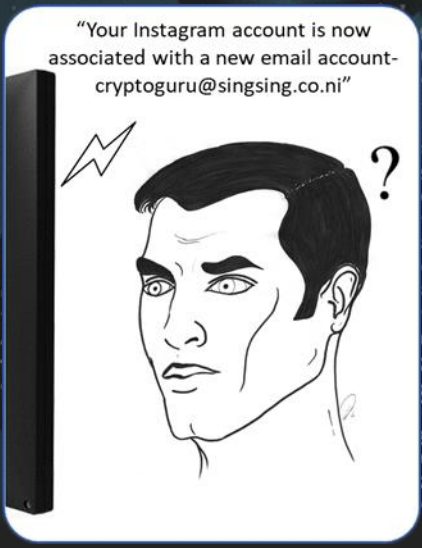
Source https://www.spamhaus.org/statistics/networks/



Top 10 by Number of Spam Issues

Stats as of 27 May 2022

For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud


"Your Instagram account is now associated with a new email account- cryptoguru@singsing.co.ni"
?

Other Interesting News and Cyber Security bits:

- Paying the ransom is not a good recovery strategy
- Military-made cyberweapons could soon become available on the dark web, Interpol warns
- Is Nanotechnology Ready to Enter the IoT Security War?
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

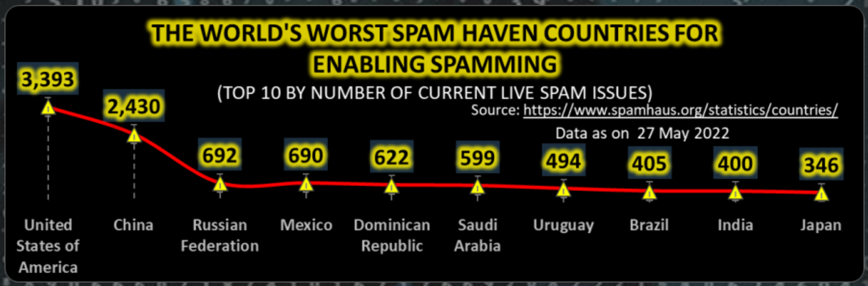
Marine Traffic
Track any Sailing Vessel globally

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 27 May 2022



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