On April 20, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Apache and Oracle products. CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
22 Apr 22	507,912,150	6,236,644

Deaths this week: 22,150

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 April 2022

In The News This Week

Five Eyes Nations Warn of Russian Cyber Attacks Against Critical Infrastructure

The Five Eyes nations (Australia, Canada, New Zealand, the United Kingdom, and the United States) have released a joint cybersecurity advisory warning of increased malicious attacks from Russian state-sponsored actors and criminal groups targeting critical infrastructure organizations amidst the ongoing military siege on Ukraine. "Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks," authorities from Australia, Canada, New Zealand, the U.K., and the U.S. said. "Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as material support provided by the United States and U.S. allies and partners." Read the full story by Ravi Lakshmanan here: The Hacker News

Pwn2Own Miami hacking contest awarded $400,000 for 26 unique ICS exploits

The Pwn2Own Miami 2022 is a hacking contest organized by Trend Micro's Zero Day Initiative (ZDI) that focuses on demonstrating exploits for ICS systems belonging to the following categories: the OPC UA Server, Control Server, Human Machine Interface, and Data Gateway. During the three days of competition, 11 participants made 32 attempts of demonstrating their ICS exploits against products from Unified Automation, Iconics, Inductive Automation, Prosys, Aveva, Triangle MicroWorks, OPC Foundation, Kepware, and Softing. Participants demonstrated a total of 26 unique zero-day exploits, only two attempts failed and the other eight were classified as BUG COLLISION, which means that the white hat hackers successfully demonstrated the ICS exploits but they were using already known issues. Each "bug collision" attempt was awarded a pay-out of $5,000, while remote code execution were awarded $20,000 on average. The pay-out for DoS ICS exploits was $5,000..
Read the article by Pierluigi Paganini here: SecurityAffairs

Critical security flaws put millions of Android users' privacy at risk

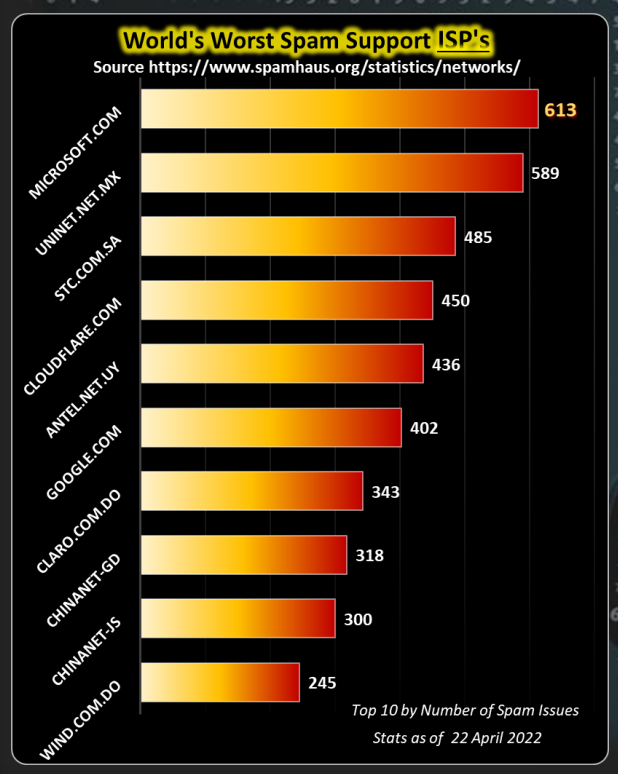
Security firm Check Point has announced that it discovered a security vulnerability in millions of Android devices powered by Qualcomm and MediaTek chipsets. The firm found the bug residing in an open-source version of the Apple Lossless Audio Codec (ALAC). Apple introduced ALAC in 2004 to allow lossless audio compression via iTunes and released it as open-source software in 2011. Apple continued development on the proprietary version of its codec, including security updates, but it had not implemented these patches in the open-source version since 2011. These vulnerabilities could allow attackers to launch remote code execution attacks (RCE) on affected devices. Read the rest of the story here: My Broadband

The Anonymous collective and affiliate groups intensify their attacks and claimed to have breached multiple organizations

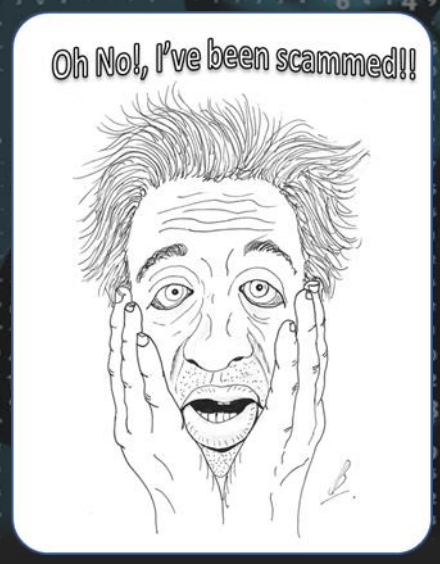
- Anonymous and groups linked to the famous collective continues to target Russian organizations, the hacktivist are breaching their systems and leak stolen data online. Below are some of the organizations breached in the last week:
(1) Tendertech is a firm specializing in processing financial and banking documents on behalf of businesses and entrepreneurs. The list of the partner banks of the firms includes Transcapitalbank, Bank Uralsib, Bank Soyuz, RGS Bank, Bank ZENIT and Otkritie Bank. Anonymous claims to have stolen 426,000 emails and leaked an archive of 160 GB in size. **(2)** GUOV i GS – General Dept. of Troops and Civil Construction is a construction company that works on projects in the interests of the Russian Ministry of Defense. "GUOV i GS" is wholly owned by the Russian Ministry of Defense through JSC Garnizon (formerly Oboronservis) and JSC GUOV / ГУОВ, the Main Directorate for the Arrangement of Troops with 49% and 51% shares, respectively. Anonymous claims to have stolen 15,600 emails and leaked an archive of 9.5 GB in size. **(3)** Neocom Geoservice is an engineering firm specializing in exploring oil and gas fields and providing drilling support. Their primary clients include Gazprom, Orenburgneft, Samotlorneftegaz, Tyumenneftegaz, and Rospan International. Anonymous claims to have stolen 87,500 emails and leaked an archive of 107 GB in size. See the rest of the breaches here: SecurityAffairs

Russia Blames Hackers for Imminent Warning of NATO Nuclear Attack

Russian officials blamed hackers for a Tuesday message posted on the press website for the country's emergency services agency that warned about a possible "threat of a retaliatory nuclear strike from NATO countries."
The message appeared on a media site for the Ministry of Emergency Situations of the Russian Federation, and it included recommendations for citizens to be prepared for such an event. Read the story here: NewsWeek



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



Online Scams – Don't become a victim

Although some scams are as old as the internet, online scams have a seasonal or event-driven nature as perpetrators exploit local and world events to lure their prey in for the proverbial kill. In the first few months of the Covid pandemic, for instance, Google reported that they were blocking as many as 18 Million Covid email scams per day! It seems like whatever is making the news, scammers jump at the opportunity to exploit it. More so if the issue has emotional undertones like the current Russian invasion of the Ukraine.
Cryptocurrency schemes are gaining popularity amongst scammers as many desperados who perhaps lost their jobs during Covid or are just desperate in an uncertain economic climate, are lured to the "easy money" bait that smooth-talking scammers are throwing out there.
Pensioners, in particular, has been a target for years now as the older generation are still grasping to understand modern technology and online commerce. As they see the value of their pension dwindle and inflation takes its toll, the worry sets in on just how they are going to make it. And then, when they get this promising email that could perhaps stretch their pension a bit further, they fall for it. It is always heart wrenching to read or hear about people that got scammed out of their entire live savings.
With that being said, be vigilant, be sceptical, do your homework, and as I have said many times, if it sounds to good to be true, it generally is. Check the fraud and scam sites listed below. - Fraud!Org has put together a list of the top 10 scam topics observed in 2021 which will give you an indication of what to look out for in our cyber dominated world.

Top Ten Scams

Each year, the National Consumers League analyses the thousands of complaints received at Fraud.org from consumers and releases it to the public, in order to track trends in scams and to use as an educational tool for fraud prevention.

The year 2021 have been especially trying for consumers, but scammers have continued to use the pandemic to make their crimes ever more lucrative. More than one in four consumers (41.49 percent) who filed complaints at Fraud.org reported a loss. While that number was a slight dip from the 43.19 percent who reported losses in 2020, the median fraud loss was $800, which is the highest since 2012. The percentage of complaints that included a reported loss peaked in 2019, with nearly half (47.48 percent) of all complainants reporting a loss that year. This increase could be attributed to scammers' tactics becoming more effective, consumers becoming less resistant to fraudulent schemes, or some combination of the two.

2021's top scam: Bogus prizes and sweepstakes fraud - Complaints about scams involving fake prizes, bogus sweepstakes, and "free" gifts were the top complaint consumers reported to Fraud.org in 2021. In 2020, such complaints made up nearly a quarter (23.78 percent) of the reports we received. In 2021, these complaints made up more than one in three (35.23 percent) of complaints, an increase of more than 48 percent year-over-year. Investment scams, many tied to cryptocurrency, were the fastest growing type of complaint in 2021, with complaints more than doubling (168 percent increase year-over-year). This increase correlates with data released last spring by the Federal Trade Commission, showing a dramatic increase in cryptocurrency investment scams, often fuelled by social media.

Phone & the web continue to be scammers' contact methods of choice - With email spam filters getting progressively better, phone and the Web continued to be the most frequent ways that consumers reported being contacted by scammers. Combined, they were the first method of contact in more than 81 percent of complaints (44.48 percent phone; 35.94 percent Web).

Credit cards remain top target, but scammers are looking to other payment methods - Getting access to consumers' credit card information continued to be the top way that scammers sought to obtain funds in 2021, with 44 percent of complaints with a loss reporting funds were sent via credit card. However, other payment methods such as gift cards, cryptocurrency, and peer-to-peer apps continue to gain popularity for fraudsters, increasing by nearly half (45.28 percent) year-over-year. One reason for this popularity, we believe, is that funds sent via one of these methods is available to the scammers quickly and, often, anonymously. Fraud.org continues to press federal regulators to do more to plug loopholes in federal consumer protection laws like the Electronic Funds Transfer Act that allow these new payment platforms to be abused.

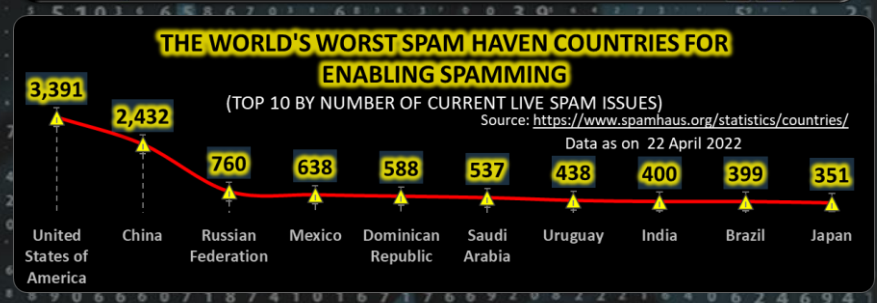
Meet the scams: The worst of 2021

(1) Prizes/Sweepstakes/Free Gifts - Requests for payment to claim fictitious prizes, lottery winnings, or gifts (2) Internet: General Merchandise Sales (not auctions) - Goods purchased are either never delivered or misrepresented (3) Phishing/Spoofing - Emails pretending to be from a well-known source ask consumers to enter or confirm personal information (4) Fake Check Scams - Consumers paid with phony checks for work or for items they're trying to sell, instructed to wire money back to buyer (5) Friendship & Sweetheart Swindles - Con artist nurtures an online relationship, builds trust, and convinces victim to send money (6) Investments - Investment opportunities in: day trading; gold and gems; art; rare coins; other investment products; reports about companies that offer advice or seminars on investments; etc. (7) Advance Fee Loans, Credit Arrangers - False promises of business or personal loans, even if credit is bad, for a fee upfront (8) Family / Friend Imposters - A scammer calls or emails, claiming that a friend or family member is in distress (in jail, in the hospital, etc.) and urgently needs funds to help (9) Computers - Equipment and Software Scammers claim to offer "technical support" for computer problems and charge a fee to fix a non-existent problem
(10) Scholarships /Grants - Offers of fictitious "guaranteed" scholarship or grant funds in exchange for up-front payment or personal information.

Fact Check or Reporting Fraud Scams (Google for sites in your own country): ReportFraud, ScamAdvisor, AARP, Fact Check Website List, Finder(Business Loan Scams), CISA, ScamWatch (AU), Citizens Advice(UK), ScamBuster(ZA), ScamAlert (ZA)

Other Interesting News and Cyber Security bits:

- Warrior Trading forced to pay $3 million for 'misleading' day trading scheme
- The 6 best ethical hacking certifications: Hone your skills
- Who has the right to be anonymous?
- SANS Daily Network Security Podcast (Storm cast)



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