On December 1, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
03 Dec	264,474,902	5,250,070

Deaths this week: 50,590

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

03 December 2021

In The News This Week

Russian Man Gets 60 Months Jail for Providing Bulletproof Hosting to Cyber Criminals

A Russian national charged with providing bulletproof hosting services for cybercriminals, who used the platform to spread malware and attack U.S. organizations and financial institutions between 2009 to 2015, has received a 60-month prison sentence. 34-year-old Aleksandr Grichishkin, along with Andrei Skvortsov, founded the bulletproof hosting service and rented its infrastructure to other criminal clientele for distributing a wide range of malware and attempted to cause millions of dollars in losses to U.S. victims. Skvortsov is pending sentencing and faces a maximum penalty of 20 years in prison. Read the full story by Ravie Lakshmanan here: TheHackerNews

Twitter removes another 3,000 state-backed accounts linked to six countries

Twitter has removed another 3,465 state-backed accounts as part of efforts to limit the influence of information manipulation campaigns on the web. The social media platform explained in a blog post that the account sets that have been removed include eight "distinct operations" that can be attributed to China, Mexico, Russia, Tanzania, Uganda, and Venezuela. "Every account and piece of content associated with these operations has been permanently removed from the service," Twitter said.

Listing out the operations, the majority of accounts removed in this round of purges were linked to China, with over 2,000 of them amplifying Chinese Communist Party narratives related to the treatment of the Uyghur population in Xinjiang. Another network of around 100 accounts were connected to "Changyu Culture", a private company backed by the Xinjiang regional government. Read the complete article by Campbell Kwan here: ZDNet

Colorado energy company loses 25 years of data after cyberattack

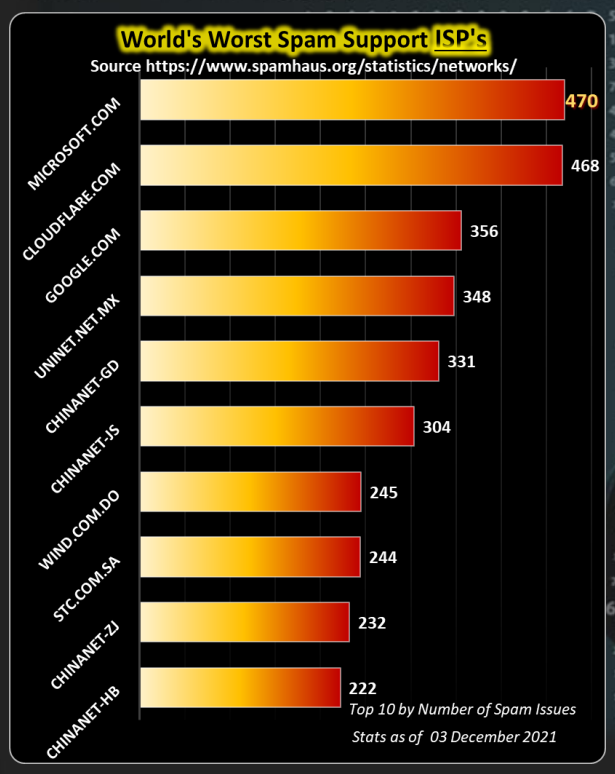
Colorado's Delta-Montrose Electric Association (DMEA) is still struggling to recover from a devastating cyberattack last month that took down 90% of its internal systems and caused 25 years of historic data to be lost. In an update sent to customers this week, the company said it expects to be able to begin accepting payments through its SmartHub platform and other payment kiosks during the week of December 6. "We also tentatively estimate we will be able to resume member billing the week of December 6 - 10. We recognize this will result in members receiving multiple energy bills close together. As a reminder, we will not disconnect services for non-payment or assess any penalties through January 31, 2022," the company said on a page that has been updated repeatedly over the last month. Read the article by Jonathan Greig here: ZDNet

Malicious Android app steals Malaysian bank credentials, MFA codes

A fake Android app is masquerading as a housekeeping service to steal online banking credentials from the customers of eight Malaysian banks. The app is promoted through multiple fake or cloned websites and social media accounts to promote the malicious APK, 'Cleaning Service Malaysia.' This app was first spotted by MalwareHunterTeam last week and was subsequently analyzed by researchers at Cyble, who provide detailed information on the app's malicious behavior. Upon installing the app, users are requested to approve no less than 24 permissions, including the risky 'RECEIVE_SMS,' which allows the app to monitor and read all SMS texts received on the phone. This permission is abused for monitoring SMS texts to steal one-time passwords and MFA codes used in e-banking services, which are then sent to the attacker's server. Read more here: Bleeping Computer

A Software Bug Let Hackers Drain $31M From a Crypto Service

An attacker exploited a vulnerability in MonoX Finance's smart contract to inflate the price of its digital token and then cash out. - BLOCKCHAIN STARTUP MONOX Finance said on Wednesday that a hacker stole $31 million by exploiting a bug in software the service uses to draft smart contracts. The company uses a decentralized finance protocol known as MonoX that lets users trade digital currency tokens without some of the requirements of traditional exchanges. "Project owners can list their tokens without the burden of capital requirements and focus on using funds for building the project instead of providing liquidity," MonoX company representatives wrote in November. "It works by grouping deposited tokens into a virtual pair with vCASH, to offer a single token pool design." An accounting error built into the company's software let an attacker inflate the price of the MONO token and then use it to cash out all the other deposited tokens, MonoX Finance revealed in a post. Read more here



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

Shared from an anonymous source on WhatsApp

ADD COMMAS TO YOUR PASSWORDS TO MESS WITH THE CSV FILE THEY WILL BE DUMPED INTO AFTER BEING BREACHED

Here's what data the FBI can get from your messaging app

In the wake of the WhatsApp privacy debacle I reported on in January, Malwarebytes reported on Tuesday that a recently revealed FBI training infographic shows the type of information the FBI can obtain from the most commonly used messaging apps like WhatsApp, Signal, Telegram, and so on. The infographic, dated 7 January 2021 (can be seen "here"), talks about what the FBI could see at the time. Who knows what the picture looks like now? Following is an outline of the most commonly used apps. (Extracted from the Malwarebytes blog)

SIGNAL

Signal is a cross-platform centralized encrypted instant messaging service. Users can send one-to-one and group messages, which can include files, voice notes, images and videos. Signal uses standard cellular telephone numbers as identifiers and secures all communications to other Signal users with end-to-end encryption. The apps include mechanisms by which users can independently verify the identity of their contacts and the integrity of the data channel. The document notes about Signal:

- No message content.
- Date and time a user registered.
- Last date of a user's connectivity to the service.

This seems to be consistent with Signal's claims.

TELEGRAM

Telegram is a freeware, cross-platform, cloud-based instant messaging (IM) system. The service also provides end-to-end encrypted video calling, VoIP, file sharing and several other features. There are also two official Telegram web twin apps—WebK and WebZ—and numerous unofficial clients that make use of Telegram's protocol. The FBI document says about Telegram:

- No message content.
- No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram may disclose IP and phone number to relevant authorities.

WhatsApp

WhatsApp, is an American, freeware, cross-platform centralized instant messaging and VoIP service owned by Meta Platforms. It allows users to send text messages and voice messages, make voice and video calls, and share images, documents, user locations, and other content. WhatsApp's end-to-end encryption is used when you message another person using WhatsApp Messenger. The FBI notes:

- Message content limited.
- Subpoena: Can render basic subscriber records.
- Court order: Subpoena return as well as information like blocked users.
- Search warrant: Provides address book contacts and WhatsApp users who have the target in their address book contacts.
- Pen register: Sent every 15 minutes, provides source and destination for each message.*
- If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content.

iMessage

iMessage is Apple's instant messaging service. It works across Macs, iPhones, and iPads. Using it on Android is hard because Apple uses a special end-to-end encryption system in iMessage that secures the messages from the device they're sent on, through Apple's servers, to the device receiving them. Because the messages are encrypted, the iMessage network is only usable by devices that know how to decrypt the messages. Here's what the document says it can access for iMessage:

- Message content limited.
- Subpoena: Can render basic subscriber information.
- 18 USC §2703(d): Can render 25 days of iMessage lookups and from a target number.
- Pen Register: No capability.*
- Search Warrant: Can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return. Can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud.

WeChat

WeChat is a Chinese multi-purpose instant messaging, social media and mobile payment app. User activity on WeChat has been known to be analyzed, tracked and shared with Chinese authorities upon request as part of the mass surveillance network in China. WeChat uses symmetric AES encryption but does not use end-to-end encryption to encrypt users messages. The FBI has less access than the Chinese authorities and can access:

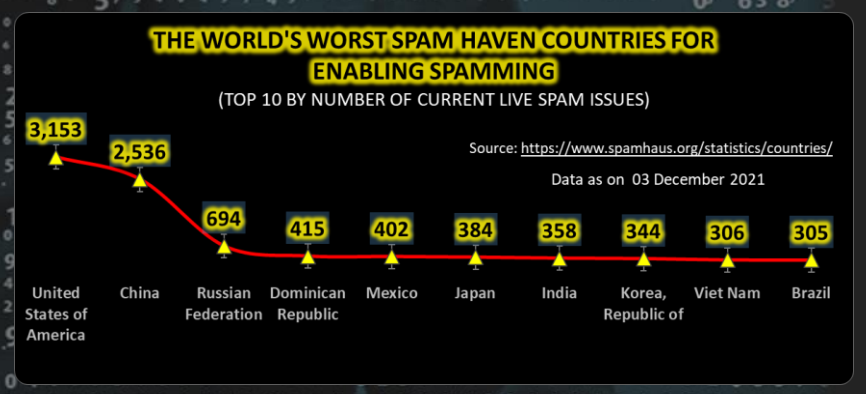
- No message content.
- Accepts account preservation letters and subpoenas, but cannot provide records for accounts created in China.
- For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active.

In conclusion: Most, if not all, of your messages are more or less safe from prying eyes in these apps unless you're using WeChat in China.

*Note: A pen register is an electronic tool used by the FBI to capture phone numbers that are dialled from a specific phone line.

Other Interesting News and Cyber Security bits:

- Researches Detail 17 Malicious Frameworks Used to Attack Air-Gapped Networks
- The future of security in space: A thirty-year US strategy
- The Hidden Cyber Risks Of Electric Vehicles



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