
**On January 27, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco, Mozilla and Apple products.**

Covid-19 Global Stats

| Date | Confirmed Cases | Deaths |
|---|---|---|
| 29-Jan | 102,003,005 | 2,199,099 |

## 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

29 January 2021

## In The News This Week

### Apple May Be Forced To Remove Telegram From The App Store

According to The Washington Post, the American non-profit organization Coalition for a Safer Web is demanding the removal of the Telegram messenger from the Apple App Store. On 17 January, the organization Coalition for a Safer Web filed a lawsuit, in which the Telegram leadership is accused of the fact that the messenger does not in any way fight against calls for violence and messages with extremist content. In particular, the situation with the breaking in of the US Capitol in early January is mentioned. The lawsuit says it violates Apple's App Store Terms of Service. In this regard, the plaintiffs demand to remove Telegram from the App Store. It is also reported that Coalition for a Safer Web plans to ask the court to remove Telegram from the Google Play store. Recall that in the latter case, Android users always have the opportunity to download applications from other sources. iOS users don't have this option. Pavel Durov said that in the first week of January, Telegram's active user base exceeded 500 million people a month. As of January 12, 25 million new users joined Telegram within 72 hours.
Read the full story here: GizChina, Washington Post

### TikTok Flaw Lay Bare Phone Numbers, User IDs For Phishing Attacks

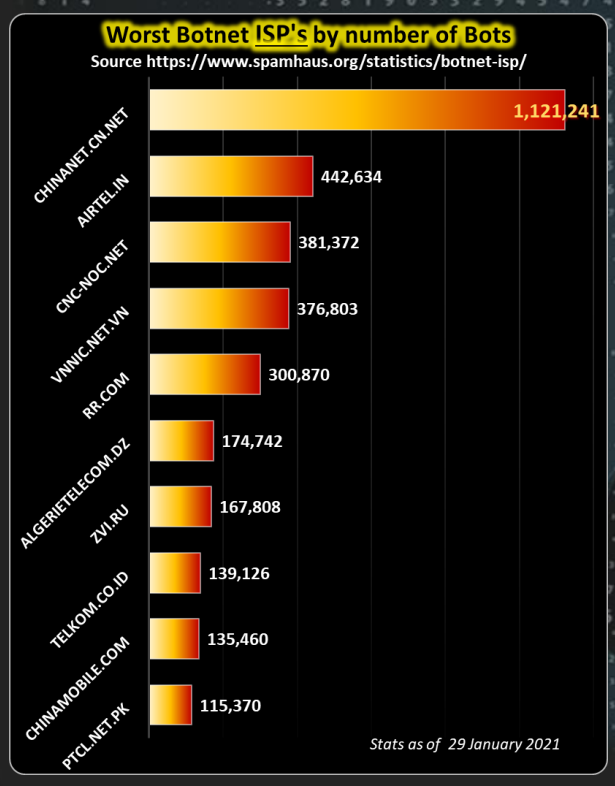
A security flaw in TikTok could have allowed attackers to query the platform's database – potentially opening up for privacy violations. A vulnerability in the popular TikTok short-form video-sharing platform could have allowed attackers to easily compile users' phone numbers, unique user IDs and other data ripe for phishing attacks. TikTok, owned by ByteDance, has more than 800 million active users worldwide. The vulnerability, which was reported and patched before its disclosure on Tuesday, existed in the "Find Friends" feature of the TikTok mobile app. This feature allows users to find their friends, either via their contacts, via Facebook or by inviting friends. In order to help users find friends through their contacts, TikTok contained a sync feature for contacts who had TikTok accounts. That means that it is possible to connect profile details with phone numbers. Researchers said an attacker could leverage this feature in order to query TikTok's entire database – potentially opening up for privacy violations. Read the full story by Lindsey O'Donnell here: ThreatPost

### Biden's $10 Billion Cybersecurity Proposal: Is It Enough?

President-elect Joe Biden's $1.9 trillion proposal for COVID-19 relief includes nearly $10 billion in cybersecurity and IT spending. Tucked away near the end of the "American Rescue Plan" is a proposal to spend $9 billion to help the U.S. Cybersecurity and Infrastructure Security Agency and the General Services Administration complete cybersecurity and IT modernization projects. The Biden administration also proposes spending $1 billion for several other cybersecurity and IT initiatives, including: $200 million for the rapid hiring of security experts to work for the Office of the U.S. Chief Information Security Officer as well as the Digital Service unit in the White House; $300 million to fund additional IT projects within the GSA; $690 million for a CISA project designed to improve monitoring and incident response across federal agencies. The proposed new spending on security and IT improvements is in direct response to the SolarWinds supply chain hack.
Read the full story by Scott Ferguson here: BankInfoSecurity

### Apple's new privacy tool lets you choose which apps can see and share your data

Apple's long-awaited "app tracking transparency" tool, which lets users decide whether they agree to their data being tracked across various different apps and websites, will be rolling out in a matter of months. Coming in early spring as part of a new release of iOS 14, iPadOS14 and tvOS14, the feature will require apps to get users' permission before tracking their data across other companies' apps or websites for advertising purposes. When asked by users not to track their data, apps will also have to refrain from sharing information with data brokers. Data brokers collect information or buy it from other companies, including social media platforms, and aggregate thousands of pieces of data to create consumer profiles that can be used for targeted advertising. A new privacy report published by Apple mentions one broker that is currently collecting data on 700 million consumers worldwide, building up profiles that include as many as 5,000 characteristics... Read the story here: ZDNet Article




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


## Privacy: Why does it matter?

We are past the days of saying "I don't have anything to hide", which was a standard response from many people when you start talking about privacy. The world has changed dramatically from the days of the first social "chat rooms" to the massive digital and social platforms of today. Everything there is to know about you is recorded in digital format somewhere, from your birth certificate to your bank account and everything in-between. This is called Personal Identifiable Information (PII), and is basically proof of who you are in this world. And, as we traverse the online platforms to socialise or to do business and what not, more and more of who you are is recorded. Unfortunately, as we have seen in the last couple of weeks, big data companies and criminals alike have figured out that the more of this data they can get their hands on, the more money they can make. Big data companies will gather as much information as they can and do something called behavioural analytics. This is to figure out what makes you tick, and what particular stimulus will make you respond to a particular advertising campaign or what will sway your political viewpoint. That is just some of the reasons why it becomes increasingly important to keep your personal data private and secure.

The big blow-up a few weeks ago on the "personal identifiable" and "personal behavioral" data that companies like Facebook, Google and the likes are gathering and recording, brought home the fact for many people across the globe that their private data is not really private anymore. Week on week I report in this bulletin of hackers that breached the digital defences of large companies and stole this very data I am talking about.

So why does privacy matter really – In December Charlie Osborne and Zack Whittaker wrote a piece in ZDNet, which I quite like, and it brings home some of the real issues why data privacy matters. Following is an excerpt of the article, but please visit the site to read the full story.

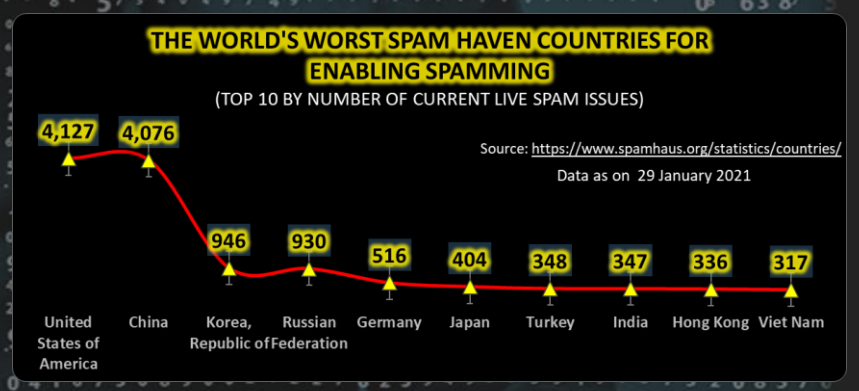
### Why does it matter?

**Data management is at the heart of privacy** - Data is a vague concept and can encompass such a wide range of information that it is worth briefly breaking down different collections before examining how each area is relevant to your privacy and security.
**PERSONALLY IDENTIFIABLE INFORMATION (PII)** - Known as PII, this can include your name, physical home address, email address, telephone numbers, date of birth, marital status, Social Security numbers (US)/National Insurance numbers (UK), and other information relating to your medical status, family members, employment, and education.
Why does it matter? All this data, whether lost in different data breaches or stolen piecemeal through phishing campaigns, can provide attackers with enough information to conduct identity theft, take out loans using your name, and potentially compromise online accounts that rely on security questions being answered correctly. In the wrong hands, this information can also prove to be a gold mine for advertisers lacking a moral backbone.
**BROWSING HABITS AND WEBSITE VISITS** - Internet activity is monitored by an Internet Service Provider (ISP) and can be hijacked. While there is little consumers can do about attacks at the ISP level, the web pages you visit can also be tracked by cookies, which are small bits of text that are downloaded and stored by your browser. Browser plugins may also track your activity across multiple websites.
Why does it matter? Cookies are used to personalize internet experiences and this can include tailored advertising. However, such tracking can go too far, as shown when the unique identifiers added to a cookie are then used across different services and on various marketing platforms. Such practices are often considered intrusive.
**MESSAGE AND EMAIL CONTENT** - Our email accounts are often the pathway that can provide a link to all our other valuable accounts, as well as a record of our communication with friends, families, and colleagues. As central hubs to other online services, hackers may try to obtain our passwords through credential stuffing, social engineering, or phishing scams in order to jump to other services.
Why does it matter? If an email account acts as a singular hub for other services, a single compromise can snowball into the hijack of many accounts and services.
**ONLINE PURCHASES, FINANCIAL INFORMATION** - When you conduct a transaction online, this information may include credentials for financial services such as PayPal, or credit card information including card numbers, expiry dates, and security codes. New attacks known as Magecart campaigns are not possible to avoid by the average consumer as they take place on vulnerable e-commerce websites, with code injected into payment portals to skim and steal card data input by customers. Past victims of Magecart groups include Ticketmaster, Boom! Mobile, and British Airways.
Why does it matter? Cybercriminals who steal financial services credentials through phishing and fraudulent websites, who eavesdrop on your transactions through Man-in-The-Middle (MiTM) attacks, or who utilize card-skimming malware, can steal these details when they are not secured. Once this information has been obtained, unauthorized transactions can be made, clone cards may be created, or this data may also be sold on to others in the Dark Web.
**MEDICAL RECORDS AND DNA PROFILES** - Another entrant to the mix, hospitals are now transitioning to electronic records and home DNA services store genetic information belonging to their users, submitted in the quest for health-related queries or tracing family histories.
Why does it matter? The loss of medical information, which is deeply personal, can be upsetting and result in disastrous consequences for everyone involved. When it comes to DNA, however, the choice is ours whether to release this information -- outside of law enforcement demands -- and it is often the use of ancestry services that release this data in the first place. Privacy concerns relating to DNA searches have been cited for sales downturns with some popular home ancestry kits.

Please ZDNet to read to full article.

## More News

- Apple CEO sounds warning of algorithms pushing society towards catastrophe
- 'Carpet-bombing' DDoS attack takes down South African ISP for an entire day
- Facebook's foolish attack on Apple
- Lazarus Affiliate 'ZINC' Blamed for Campaign Against Security Researcher




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