
**On September 30, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Microsoft and Apple products.**

## 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

## 02 October 2020

## In The News This Week

### Flightradar24 hit by third cyber-attack in two days

Popular real-time flight-tracking website Flightradar24 was hit by a cyber-attack that knocked out access to its services for hours. The attack is the third the company has suffered in two days, it said. Early attempts to restore the site failed, with "significant instability due to the sustained attacks", it said. It said the Distributed Denial of Service (DDoS) attack had hit "the availability of our services" but not compromised user data. The site appeared to be improving on Tuesday, with intermittent loading errors. The website allows users to track planes - both commercial passenger flights and private ones - in mid-air, following flight paths live. Flightradar24 says it has about two million users and tracks 180,000 flights every day. It includes aircraft manufacturers - such as Airbus and Boeing - among its customers. Read the full story here: BBC News

### Nevada school district refuses to submit to ransomware blackmail, hacker publishes student data -

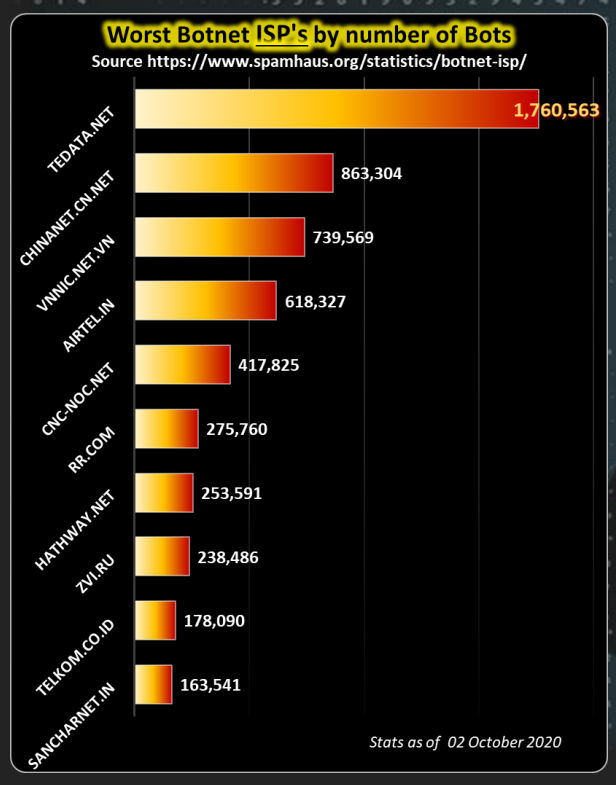
A cybercriminal has published private data belonging to thousands of students following a failed attempt to extort a ransomware payment from a Nevada school district. In the case of the Clark County School District in Nevada, officials reportedly refused to pay the ransom, leading to the potential exposure of student data. First reported on September 8 by the Associated Press, the Clark County School District said its computer systems had been infected with malware on August 27, locking up access to files. At the time, it was thought that some employee personally identifiable information (PII) may have been exposed, including names and Social Security numbers, but students were not mentioned. The district pulled in law enforcement and cyberforensic investigators to manage the incident. However, this doesn't appear to have been enough to prevent a leak.
The ransomware's operator was holding data hostage in the hopes of forcing the distinct to pay up but was left disappointed, as reported by Business Insider. In retaliation, student information has been published on an underground forum. Read the full story here: ZDNet Article

### Judge blocks TikTok ban in second ruling against Trump's efforts to curb popular Chinese services -

The ruling comes hours before TikTok was to be removed from mobile app stores. TikTok received a reprieve of its ban from U.S. app stores on Sunday after a federal judge in Washington granted a preliminary injunction blocking an order from President Trump. It was the second setback for the Trump administration in its effort to curb U.S. residents' access to popular Chinese mobile apps. Last weekend, a federal magistrate in San Francisco cited First Amendment issues in blocking a proposed ban of the WeChat app. U.S. District Judge Carl J. Nichols, who was appointed to the bench by Trump in 2019, was not expected to make public his full ruling until Monday. He filed his decision publicly, but his full reasoning was filed separately as a sealed document. Nichols granted the injunction for the piece of the ban that was set to go into effect Sunday night, but denied a motion to halt a second aspect of the ban that doesn't go into effect until Nov. 12. During a rare Sunday hearing, he questioned whether TikTok had been given enough opportunity to defend itself before Trump issued an executive order last month barring the app from online stores. It seemed, the judge said, that "this was a largely a unilateral decision with very little opportunity for plaintiffs to be heard." Read the story here: Washington Post

### Russian Hacker Sentenced for 2012 Data Theft of LinkedIn & Dropbox Users

SAN FRANCISCO (CN) — A federal judge on Tuesday sentenced convicted Russian hacker Yevgeniy Nikulin to 88 months in prison for stealing more than 100 million user credentials from LinkedIn, Dropbox and Formspring databases in 2012. "I think you're a brilliant guy. Very smart. I urge you to apply that brilliance to a lawful profession and do something good with your life other than hacking into computers," U.S. District Judge William Alsup said he took into account the nearly four years Nikulin has spent behind bars awaiting trial when handing down the sentence. - Read the full story here: Courthousenews




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

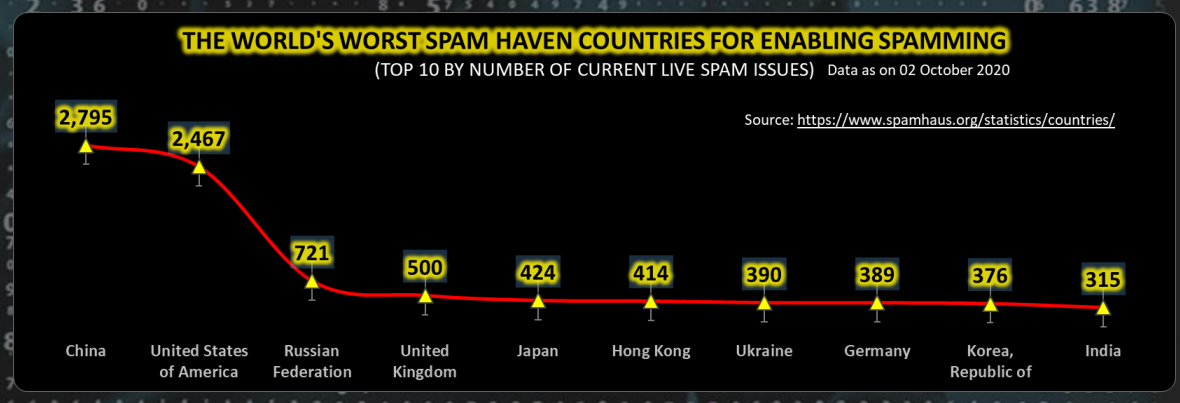
No matter how sexy or convincing the voice on the other side, never share your password over the phone!!

## More on How to Tell if Your Phone Has Been Hacked or Cloned

The article on phone cloning last week elicited a huge response and tons of questions on the topic. It seems that a number of readers either had/have this happened to them or they know of someone who fell victim to it. For that reason I decided to revisit the phone hacking article in the June 5th edition and expand on it and the points sited last week with some more things to look out for. Are you experiencing any of the signs listed below? Sources: Techlicious; Techlicious2; YouTube;

**Signs your phone may have been hacked or cloned**

1. You notice some new apps on your phone that you didn't install yourself – Sometimes the major operating system service providers (Apple, Android, etc.) will introduce a new feature app which will load automatically but these you can verify easily if you visit the respective sites. Other apps however can be a sign of malware apps loaded when you visit certain malicious websites, or if your phone has been cloned and the crook operating the cloned device are loading new apps. (See last week's bulletin -25 Sep 2020)
2. Noticeable decrease in battery life - While a phone's battery life inevitably decreases over time, a smartphone that has been compromised by malware may start to display a significantly decreased lifespan. This is because the malware – or spy app – may be using up phone resources to scan the device and transmit the information back to a criminal server. (That said, simple everyday use can equally deplete a phone's lifespan. Check if that's the case by running through these steps for improving your Android or iPhone)
3. Some of your apps are giving problems and stop working properly – this can be an indicator that the last app you installed may contain malware and are doing stuff in the background that are trying to harvest credentials from your regular apps or hogging other resources. And most of the time, the newly loaded app will work without a glitch. Get rid of the app and your problems will most likely be over with.
4. Sluggish performance - Do you find your phone frequently freezing, or certain applications crashing? This could be down to malware that is overloading the phone's resources or clashing with other applications (See point 3 above). You may also experience continued running of applications despite efforts to close them, or even have the phone itself crash and/or restart repeatedly. Some malware apps will also run in "stealth mode", not showing up even if you close all your apps. (As with reduced battery life, many factors could contribute to a slower phone – essentially, its everyday use, so first try deep cleaning your Android or iPhone.)
5. Your phone is getting warm even if you are not using it – This is another indicator that something is running on your phone in the background, working so hard that the CPU get hot.
6. High data usage - Another sign of a compromised phone is an unusually high data bill at the end of the month, which can come from malware or spy apps running in the background, sending information back to its server or a cloned phone making calls or browsing the net as if it is your phone.
7. Outgoing calls or texts you didn't send - If you're seeing lists of calls or texts to numbers you don't know, be wary – these could be premium-rate numbers that malware is forcing your phone to contact; the proceeds of which land in the cyber-criminal's wallet. Your phone could be cloned, and you are footing the bill for the criminal's activities. In this case, check your phone bill for any costs you don't recognize.
8. Unknown numbers appear in your contact list – This is a clear sign that someone else has access to your phone, either through malware on your phone or a cloned device.
9. Strange noises or an echo during calls – This means that someone else might have access to your phone and are listening in on your calls or are tracking your whereabouts.
10. All of a sudden you can't make calls, or your calls are dropped - Although this can sometimes be attributed to a technical fault, in general it is an indicator of a compromised phone.
11. Missed call notifications but your phone didn't ring – When a compromised or cloned phone is used to make call, often the call recipient will call the number back and either the malware instance or the clone phone operator will drop the call immediately.
12. Your phone reboots for no reason or switch off, dial numbers or start apps – This is normally a sign that your phone has been cloned or a hacker is using your device for illicit activities.
13. Mystery pop-ups - While not all pop-ups mean your phone has been hacked, constant pop-up alerts could indicate that your phone has been infected with adware, a form of malware that forces devices to view certain pages that drive revenue through clicks. Even if a pop-up isn't the result of a compromised phone, many may be phishing links that attempt to get users to type in sensitive info – or download more malware.
14. You notice that your emails are blocked by spam filters – Spam registers could have blocked your email account as a result of a perpetrator using your account from your compromised phone to send tons of unsolicited or phishing mails.
15. Unusual activity on any accounts linked to the device - If a hacker (or clone user) has access to your phone, they also have access to its accounts – from social media to email to various lifestyle or productivity apps. This could reveal itself in activity on your accounts, such as resetting a password, sending emails, marking unread emails that you don't remember reading, or signing up for new accounts whose verification emails land in your inbox. In this case, you could be at risk for identity fraud, where criminals open new accounts or lines of credit in your name, using information taken from your breached accounts. It's a good idea to change your passwords – without updating them on your phone – before running a security sweep on your phone itself.
16. You cannot switch off your device – If your phone is hacked, the attacker can load software on your phone to manipulate its configuration like setting to prevent you from switching off the device. Most phone has a "hard boot" feature though which will enable you to switch it off, check the manufacturers website to find out how to hard boot your device.




**Author: Chris Bester** (CISA,CISM)
chris.bester@yahoo.com