
**On May 27, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to a vulnerability in Cisco 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

29 May 2020

## In The News This Week

### 26 Million logins believed to be stolen from LiveJournal in 2017 pop up on hacker forum

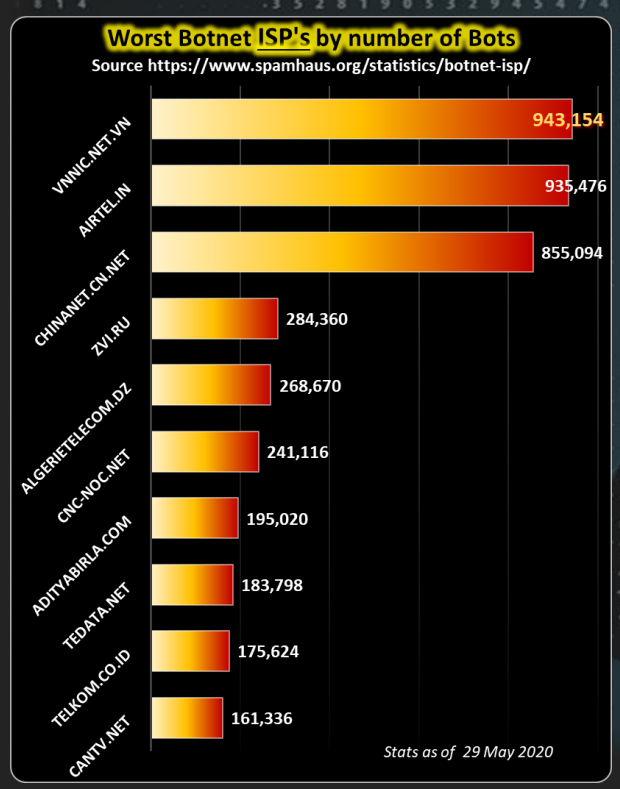
Russian-owned blogging service LiveJournal has reportedly suffered a hack affecting 26 million user accounts. According to the reliable Troy Hunt's Have I Been Pwned? service, the incident occurred at some point in 2017. One year later a forked spinoff of LiveJournal called Dreamwidth began noticing credential-stuffing attacks. Around 26 million "unique" usernames, email addresses and passwords are said to have been stolen from LiveJournal and ended up circulating cybercrime forums. A lengthy statement from Dreamwidth itself, published on the 27th , alleged that stolen data was being used in a fresh round of seemingly successful account compromise attempts. "We have no way to tell for sure whether LiveJournal has actually had a data breach," the forked platform added, advising: "It's best if you treat any password you've ever used on LiveJournal in the past as compromised, since we can't tell for certain when the alleged breach happened."
Read the full story here: The Register

### Popular App Mathway Leaks 25 Million User Records

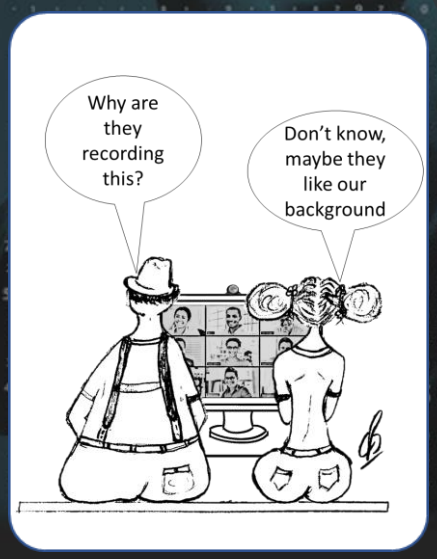
More than 25 million user records, belonging to popular math app Mathway, are being sold on the dark web. According to ZDNet, the hack is the latest in a long line of security breaches carried out by a hacker going by the name of ShinyHunters, the threat actor also responsible for intrusions at Tokopedia, Wishbone, Zoosk, and others. For the past few months, says ZDNet, the hacker has been breaching companies and putting their data on sale on a dark web marketplace and internet hacking forums. In total, it is believed that the hacker has sold access to more than 200 million user details. In an interview with ZDNet, the hacker said he had breached Mathway in January 2020 by accessing the company's backend, dumping the database, and then removing access to avoid getting detected. But, since the start of May, the hacker has been selling the records on the dark web and on a popular hacking forum. The Mathway data has been up for sale for the equivalent of $4,000 in Bitcoin or Monero, reports ZDNet. According to samples reviewed by ZDNet, the data includes user emails and hashed passwords. Since the password hashing algorithm is unknown, says ZDNet, it's unclear if these passwords can be cracked and reverted back to their cleartext forms, which would make the entire data dump a lot more valuable for other cybercrime gangs. Read the full article here: SecurityMagazine

### New York Teen Masterminds $23.8m Crypto Heist

An American cryptocurrency investor is suing a New York high school senior over the theft of $23.8m in digital currencies. Michael Terpin has filed a civil complaint against 18-year-old Ellis Pinsky alleging that in 2018, at the tender age of 15, Pinsky masterminded a plot to defraud Terpin out of millions. Pinsky was allegedly the leader of what Terpin described as a "gang of digital bandits" who stole from multiple victims after using SIM swapping to gain control of their smartphones. None of the teen's alleged co-conspirators were named in the complaint, in which Terpin accuses them and Pinsky of racketeering and computer fraud. Terpin claims that, after hijacking the native wallet on his BlackBerry, Pinsky cockily bragged to his peers that he would get away with his cybercrime. "On the surface, Pinsky is an 'All American Boy,'" Terpin said in a complaint filed May 7 in a federal court in White Plains, New York. "The tables are now turned." In May last year, Terpin won a $75.8m civil judgement in a California state court in a related case against an alleged associate of Pinsky, Nicholas Truglia, who has faced criminal hacking charges. Now Terpin is gunning for Pinsky, seeking triple damages of $71.4m.
According to Reuters, court records show that Terpin is also suing his carrier AT&T Mobility in Los Angeles for $240m. To his classmates at Irvington High School, Pinsky was an unremarkable individual who achieved decent grades and liked playing soccer.
Read the full story by Sarah Coble here: Infosecurity-Magazine




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




## Lockdown Video Meetings – Security Do's and Don'ts

The COVID-19 pandemic brought people home, yes home from the controlled corporate environment, home from formal and add-hoc face to face business meetings, even the casual family gatherings or virtual pub meets. Probably more than 80% of people around the globe are in some form of lockdown, quarantine or self-isolation and meetings went almost entirely online. It is human nature to want to see the person or people they are conversing with. For that, we all say 'Thank Goodness' for modern-day technology like Zoom, Facetime, Skype or any of the plethora of apps out there that allows us to do online collaboration or video-teleconferencing like never before. This extends to online classrooms and other media offerings where there is a need to address one or more people. Even popular television competitions like American Idol was done via iPhones this year. But, with this unprecedented move to online video collaboration and conferencing , we also get exposed to security threats that are growing by the day as threat actors jumped to exploit this mostly uncharted field of inexperienced users and a vast array of insecure home networks. In March the FBI in Boston even warned of Teleconferencing and Online Classroom Hijacking (also called "ZOOM-Bombing") during the COVID-19 Pandemic, as they received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language. What to do to stay secure and avoid being "bombed"?

Although most corporates, schools or mid size businesses already took steps to ensure secure collaboration through VPN's and other means, most of our everyday home users and smaller informal business setups do not have the knowhow or financial means to add those necessary controls to stay secure. Whether using your phone or computer, below then is a few basic tips, steps to take and things to think about when it comes to video collaboration or even one-to-one video chats.

(1) Choose the App that will work for you - If you are the meeting organiser or chat instigator, have a look at the different offerings out there and in particular, look at the security controls of the app. Sometimes less popular offerings means less threat actors for that app and ask the intended participants to use the same if possible. It all depends on how much you want to reduce your exposure. Although some of the most popular offerings have stepped up their controls lately, this is something to keep in mind.

(2) Know who is in your meeting – Although "Zoom-Bombing" is disruptive, a bigger threat is the unwanted intruders who join or lurk in meetings without revealing their presence for whatever sinister reason. Avoid open meetings where anyone can join in. If you are anything like me, It is difficult to keep track of all your invitees if there are more than 20 or 30 people, so make sure the app you are using supports invites with unique meeting ID's.

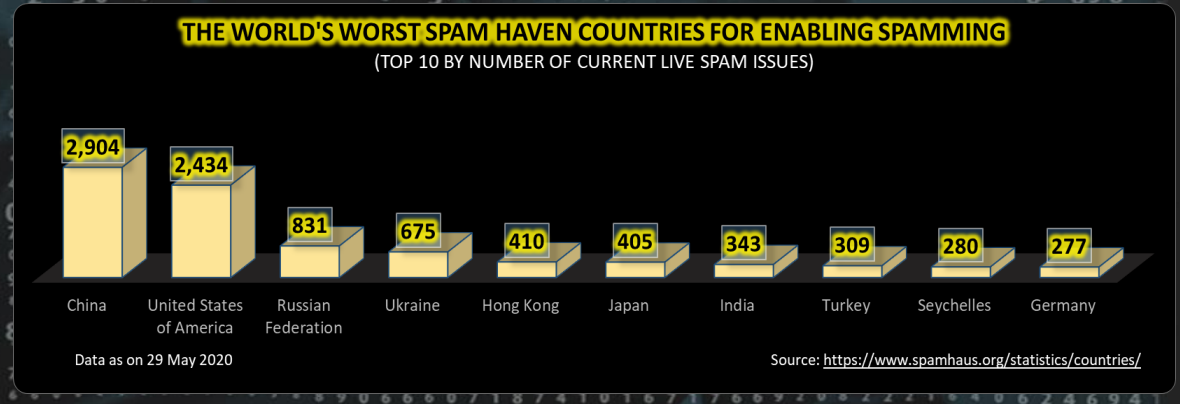
(3) Enable the waiting room facility – Most apps support a "Waiting Room" facility where you can screen anyone who wants to connect and choose whether you want them in or not, specially if you do not recognise the name. This is easier said than done in larger meetings though, specially if you are the host and cannot be disrupted to constantly look for latecomers and allow them in. In this case you can delegate authority to someone else you trust. Be careful though and look at the default settings, many apps delegate authority to anyone who is already in. If possible, keep a list of the invitees handy and tick them off as they join, crooks are constantly devising new ways to sneak in.

(4) Recordings – Recently news reports revealed that many thousands of zoom meeting recordings were leaked by hackers and other recordings found in the open on the Internet. Most video collaboration apps allow participants to record meeting sessions by default, which means that an uncontrolled copy of your meeting can be stored on any participant's end-user device which in turn can be shared or stored on cloud based file sharing or storage facilities which might be or might not be protected. As the meeting organiser, make sure you are in control of who can enable recording. As a participant, make sure you are comfortable with the fact that the meeting is recorded and what the purpose of the recording is.

(5) Audio transcripts – Hand-in-hand with recordings, many of the video collaboration apps offer a facility where audio transcripts of the meeting is emailed to the participants afterward. If there are only two or three of you it might be okay, but if there are many participants, this becomes a huge security concern. Decide whether you want this or not and change your settings accordingly. Also, if it is turned on, convey this to your participants beforehand.

(6) Backgrounds – It is all good and well that we can do these meetings from the comfort of our own homes, but be mindful of what the other participants can see in the background. Some meeting stalkers, invited or not, are more interested in what they can see in the background than the content of the meeting. A few months ago I wrote about the Japanese popstar who was assaulted after a fan analysed her profile pictures and figured out where she stayed. Well, the same goes for video backgrounds. Those nice family pictures on the wall behind you might just give those ominous prowlers more information than what they need. Does your background include a hallway or mirrors or anything else that can give an idea of the layout of your house? Where possible pick a spot in your house with a background as neutral as possible or better yet, make use of the virtual background facility that most of these apps offer.

**News Snippet for the Raspberry Pi fans out there** .....
The Raspberry Pi Foundation has released an 8GB Raspberry Pi 4 along with a beta of an official 64-bit operating system it's calling 'Raspberry Pi OS' instead of Raspbian.




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