On December 23, the Cyber Threat Alert Level was evaluated and is being set to Blue (Guarded) due to vulnerabilities in Firefox, Hewlett Packard, SolarWinds and Treck 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
24 December 2020

In The News This Week

Lazarus Group Hits COVID-19 Vaccine-Maker in Espionage Attack

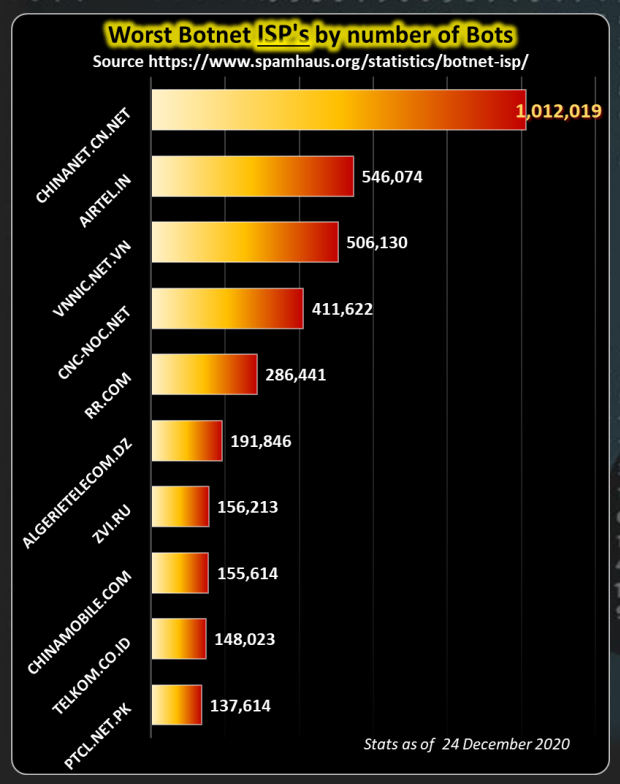
The advanced persistent threat (APT) known as Lazarus Group and other sophisticated nation-state actors are actively trying to steal COVID-19 research to speed up their countries' vaccine-development efforts. That's the finding from Kaspersky researchers, who found that Lazarus Group — widely believed to be linked to North Korea — recently attacked a pharmaceutical company, as well as a government health ministry related to the COVID-19 response. The goal was intellectual-property theft, researchers said. "On Oct. 27, 2020, two Windows servers were compromised at the ministry," according to a blog posting issued Wednesday. Researchers added, "According to our telemetry, [the pharmaceutical] company was breached on Sept. 25, 2020….[it] is developing a COVID-19 vaccine and is authorized to produce and distribute COVID-19 vaccines." They added, "These two incidents reveal the Lazarus Group's interest in intelligence related to COVID-19. While the group is mostly known for its financial activities, it is a good reminder that it can go after strategic research as well.". Read the full story by Tara Seals here: Threatpost

Fashion marketplace giant 21 Buttons exposes millions of users' data

An alarming aspect of the entire incident is that vpnMentor contacted both 21 Buttons and Amazon but no one responded nor cared to secure the data. There are different platforms that have carved out a niche for themselves on the internet. 21 Buttons with over 5 million downloads on Android happens to be one such social network that is primarily geared towards the fashion industry. It allows users to share their content and also features e-commerce capabilities to sell clothes. In the latest though, there isn't good news about them. As discovered by vpnMentor on 2 November 2020 in a research report led by Noam Rotem, it has been found that its app has exposed the data of hundreds of influencers due to an AWS bucket being misconfigured. Overall, the data stored was of over 50 million files which exposed sensitive info including full names, addresses, financial information such as bank account numbers, PayPal email addresses, photos, and videos. Many of these though were already published on the app for everyone to see even before the breach.. Read the full story here: HackRead

Emotet Campaign Restarts After Seven-Week Hiatus

Multiple security researchers note the return of an email campaign attempting to spread the malware, which is often used to drop the Ryuk ransomware and Trickbot banking Trojan.
In October, three surges of spam laden with the Emotet downloader worked to spread the malware to vulnerable users' systems, starting a sequence that often results in a Ryuk ransomware infection or attempts to steal bank account credentials via the Trickbot banking Trojan. On Oct. 30, with the completion of the third campaign, the group's spamming died down and almost no subsequent traffic appeared. Until now.
Seven weeks after the last major Emotet campaign, the cybercriminals behind the downloader have started up their attempts to compromise more systems, according to multiple cybersecurity organizations. Anti-spam crusader Abuse.ch noted on Dec. 22 that the cybercrime group had ramped up activity right before Christmas. The day before, messaging security provider Proofpoint noted that its systems were seeing more than 100,000 messages in various languages and with a variety of attachments or links.
The latest campaign could lead to compromised systems and threats to business networks, as most employees continue to work from home.
"What makes Emotet particularly dangerous for organizations is that it has been the primary foothold for the future deployment of other banking Trojans," says Sherrod DeGrippo, senior director of threat research and detection at Proofpoint. "At this point, any mainstream banking Trojan may lead to devastating ransomware attacks.". Read the full story by Robert Lemos here: DarkReading



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

Dealing with Cyberbullies

Today I want to revisit an article I posted in November 2018 on Cyber Bullying. The Covid-19 pandemic forced the world to be more online than ever before. Staying home during lockdown periods, our kids inevitably have more screen time than parents are comfortable with. Unfortunately, this is the new norm as schools are forced to go online and parents are not necessarily equipped to fulfil the policing role of the teacher if it comes to bullying. Knowing what your kids are exposed to on the internet and knowing if they are being victimised by a cyber bully is important, now more than ever. The following article is posted on the Cybersecurity & Infrastructure Security Agency (CISA) tips page and provides good insight on what cyberbullying is and how to deal with it. Please visit the CISA site for more information on various cybersecurity topics.

What is cyberbullying?

Cyberbullying is using technology to harass, or bully, someone else. Bullies used to be restricted to methods such as physical intimidation, postal mail, or the telephone, but computers, cell phones, tablets, and other mobile devices offers bullies forums such as email, instant messaging, web pages, and digital photos.

Forms of cyberbullying can range in severity from cruel or embarrassing rumours to threats, harassment, or stalking. It can affect any age group; however, teenagers and young adults are common victims, and cyberbullying is a growing problem in schools.

Why has cyberbullying become such a problem?

The relative anonymity of the internet is appealing for bullies because it enhances the intimidation and makes tracing the activity more difficult. Some bullies also find it easier to be more vicious because there is no personal contact. The internet and email can also increase the visibility of the activity. Information or pictures posted online or forwarded in mass emails can reach a larger audience faster than more traditional methods, causing more damage to the victims. A large amount of personal information is available online, so bullies may be able to arbitrarily choose their victims.

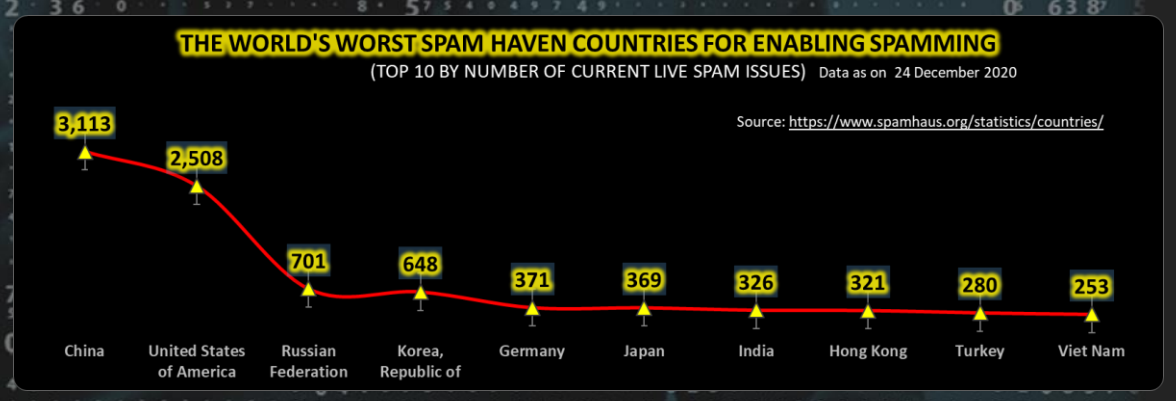
Cyberbullying may also indicate a tendency toward more serious behavior. While bullying has always been an unfortunate reality, most bullies grow out of it. Cyberbullying has not existed long enough to have solid research, but there is evidence that it may be an early warning for violent behavior.

How can you protect yourself or your children?

- Teach your children good online habits. Explain the risks of technology and teach children how to be responsible online. (See Keeping Children Safe Online for more information.) Reduce their risk of becoming cyberbullies themselves by setting guidelines for and monitoring their use of the internet and other electronic media (cell phones, tablets, etc.).
- Keep lines of communication open. Regularly talk to your children about their online activities so that they feel comfortable telling you if they are being victimized.
- Watch for warning signs. If you notice changes in your child's behavior, try to identify the cause as soon as possible. If cyberbullying is involved, acting early can limit the damage.
- Limit availability of personal information. Limiting the number of people who have access to contact information or details about interests, habits, or employment reduces exposure to bullies that you or your child do not know. This may limit the risk of becoming a victim and may make it easier to identify the bully if you or your child are victimized.
- Avoid escalating the situation. Responding with hostility is likely to provoke a bully and escalate the situation. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. Other options include subtle actions. For example, you may be able to block the messages on social networking sites or stop unwanted emails by changing the email address. If you continue to get messages at the new email address, you may have a stronger case for legal action.
- Document the activity. Keep a record of any online activity (emails, web pages, instant messages, etc.), including relevant dates and times. In addition to archiving an electronic version, consider printing a copy.
- Report cyberbullying to the appropriate authorities. If you or your child are being harassed or threatened, report the activity. Many schools have instituted anti-bullying programs, so school officials may have established policies for dealing with activity that involves students. If necessary, contact your local law enforcement. Law enforcement agencies have different policies, but your local police department or Federal Bureau of Investigation (FBI) branch are good starting points.

The following organizations offer additional information about this topic:

Federal Trade Commission, StopBullying.gov, Teacher.org, Talking with Kids About Being Online



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