On February 15, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Mozilla, Microsoft, and Adobe products.
CIS Security Advisories

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

17 February 2023

In The News This Week

Massive HTTP DDoS Attack Hits Record High of 71 Million Requests/Second

Web infrastructure company Cloudflare on Monday disclosed that it thwarted a record-breaking distributed denial-of-service (DDoS) attack that peaked at over 71 million requests per second (RPS). "The majority of attacks peaked in the ballpark of 50-70 million requests per second (RPS) with the largest exceeding 71 million," the company said, calling it a "hyper-volumetric" DDoS attack. It's also the largest HTTP DDoS attack reported to date, more than 35% higher than the previous 46 million RPS DDoS attack that Google Cloud mitigated in June 2022. Cloudflare said the attacks singled out websites secured by its platform and that they emanated from a botnet comprising more than 30,000 IP addresses that belonged to "numerous" cloud providers. Targeted websites included a popular gaming provider, cryptocurrency companies, hosting providers, and cloud computing platforms... Read the full story by Ravie Lakshmanan here: The Hacker News

Russian Hackers Disrupt NATO Earthquake Relief Operations

NATO's Special Operations Headquarters and Strategic Airlift Capability — both working to deliver humanitarian aid to victims of the recent Turkish-Syrian earthquake — were among NATO organizations disrupted by a weekend cyberattack. Russian-based Killnet threat group has claimed responsibility for launching distributed denial-of-service (DDoS) attacks against NATO, according to reports. "We are carrying out strikes on NATO," Killnet wrote on its Telegram channel, according to The Telegraph. Reports added NATO's NR network, reportedly used to transmit sensitive and classified data, was also targeted. Besides knocking sites temporarily offline, the cyberattack disrupted communications between NATO and at least one of its airplanes transporting search and rescue equipment to Incirlik Air Base in Turkey, The Telegraph reported.....
Read the rest of the article here: Dark Reading

Scandinavian Airlines Hit by Cyber Attack

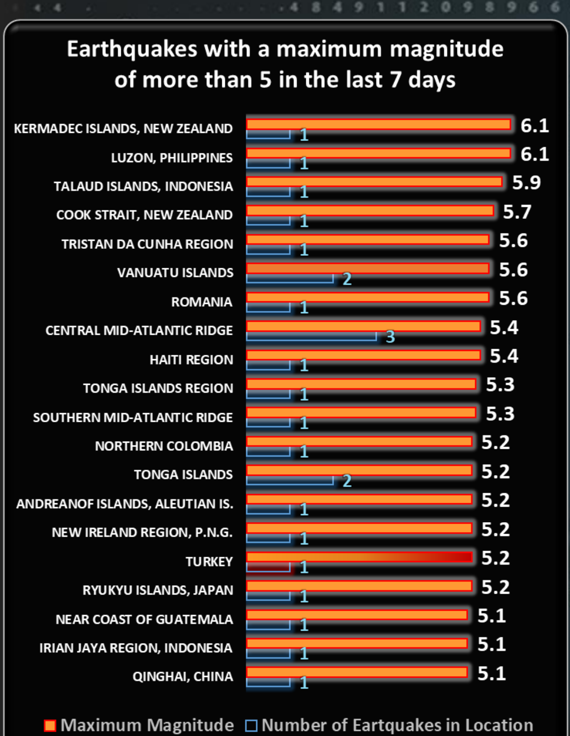
A bankruptcy filing, striking pilots and now this cyber attack, could things get any worse for SAS? - Scandinavian airline SAS said it was hit by a cyber attack Tuesday evening and urged customers to refrain from using its app but later said it had fixed the problem. News reports said the hack paralyzed the carrier's website and leaked customer information from its app. Karin Nyman, head of press at SAS, told Reuters at 20:35 GMT that the company was working to remedy the attack on its app and website. "We aren't able to say a lot more right now as we are right in the attack right now," she said, adding that the app was at that point working fine. Earlier, she told the national news agency TT that there was a risk of getting incorrect information by logging onto the app and urged customers to refrain from using it. The entire website was down for a while on Tuesday. According to TT, customers who tried to log into the SAS app were logged onto the wrong accounts and had access to personal details of other people. Norwegian newspaper Verdens Gang reported that this happened to Norwegian customers as well. Various Swedish companies and organizations have recently been hit by presumed cyber attacks...
Read the full article by Marie Mannes of Reuters here: Skift

Hackers target Bahrain airport, news sites to mark uprising

DUBAI, United Arab Emirates (AP) — Hackers said they had taken down the websites of Bahrain's international airport and state news agency on Tuesday to mark the 12-year anniversary of an Arab Spring uprising in the small Gulf country. A statement posted online by a group calling itself Al-Toufan, or "The Flood" in Arabic, claimed to have hacked the airport website, which was unavailable for at least a half hour in the middle of the day. It also claimed to have taken down the website of the state-run Bahrain News Agency, which was sporadically unavailable. . The group posted images showing 504 Gateway Timeout Errors, saying the hacking was "in support of the revolution of our oppressed people of Bahrain."
The same group appears to have hacked and changed articles on the website of Akhbar Al Khaleej, a pro-government newspaper in Bahrain, hours earlier. The newspaper's website was still down Tuesday...
Read the rest of the story here: The Hill

New Mirai Botnet Variant 'V3G4' Exploiting 13 Flaws to Target Linux and IoT Devices

A new variant of the notorious Mirai botnet has been found leveraging several security vulnerabilities to propagate itself to Linux and IoT devices. Observed during the second half of 2022, the new version has been dubbed V3G4 by Palo Alto Networks Unit 42, which identified three different campaigns likely conducted by the same threat actor. "Once the vulnerable devices are compromised, they will be fully controlled by attackers and become a part of the botnet," Unit 42 researchers said. "The threat actor has the capability to utilize those devices to conduct further attacks, such as distributed denial-of-service (DDoS) attacks." The attacks primarily single out exposed servers and networking devices running Linux, with the adversary weaponizing as many as 13 flaws that could lead to remote code execution (RCE).s.
Read the article by Ravie Lakshmanan here: The Hacker News



For Reporting Cyber Crime in the USA go to **(IC3)** , in SA go to **Cybercrime**, in the UK go to **ActionFraud**

To the people of Turkey and Syria, our thoughts and prayers are with you.

Exploiting the earthquake crisis in Turkey and Syria

As we follow the various newsfeeds on the tragic events in Turkey and Syria over the last week, our heartfelt sorrow and empathy go out to the people affected by the tragedy. Unfortunately, there is a sick element in our society who do not share the same sentiments and are exploiting the emotional response of millions of people across the globe. They prey on good-hearted people who just want to contribute something to help those affected and alleviate some of their immediate needs. This activity is not uncommon, and I have seen it many times in the past whenever there is a humanitarian crisis in the world. These are sick people and even organisations who wants to profit from other people's misery. In today's post, I want to highlight some of the scams going on as well as awareness messages going around. I'll start with a post from Stu Sjouwerman, Founder and CEO of KnowBe4.

"Just when you think they cannot sink any lower, criminal internet scum is now exploiting the recent earthquake in Turkey and Syria. Less than 24 hours after two massive earthquakes claimed the lives of tens of thousands of people, cybercrooks are already piggybacking on the horrible humanitarian crisis. You need to alert your employees, friends and family... again. Just one example are scammers that pose as representatives from a Ukrainian charity foundation that seeks money to help those affected by the natural disasters that struck in the early hours of Monday.
There are going to be a raft of scams varying from blood drives to pleas for charitable contributions for victims and their families. Unfortunately, this type of scam is the worst kind of phishbait, and it is a very good idea to inoculate people before they get suckered into falling for a scam like this. I suggest you send the following short alert to as many people as you can:

ALERT "Lowlife internet scum is trying to benefit from the Turkey-Syria earthquake. The first phishing campaigns have already been sent and more will be coming that try to trick you into clicking on a variety of links about blood drives, charitable donations, or "exclusive" videos. Don't let them shock you into clicking on anything, or open possibly dangerous attachments you did not ask for!
Anything you receive about this recent earthquake, be very suspicious. With this topic, think three times before you click. It is very possible that it is a scam, even though it might look legit or was forwarded to you by a friend -- be especially careful when it seems to come from someone you know through email, a text or social media postings because their account may be hacked.
In case you want to donate to charity, go to your usual charity by typing their name in the address bar of your browser and do not click on a link in any email. Remember, these precautions are just as important at the house as in the office, so and tell your friends and family.""

Bitdefender posted the following: **Cybercriminals exploit human misery in earthquake-hit Turkey and Syria with new online disaster scam**
"Less than 24 hours after two massive earthquakes claimed the lives of thousands of people in Turkey and Syria, cybercrooks are already piggybacking on the humanitarian crisis. - Cybercriminals never take a break from defrauding internet users, and the latest attempts spotted by Bitdefender Antispam Lab show, once again, just how unscrupulous they can be.
While thousands of people were killed and tens of thousands more are left scouring crumbled buildings in search of those caught under the rubble, fraudsters are targeting the generosity of people around the world who wish to make a small contribution to victims of this disaster.
The scammers pose as representatives from a Ukrainian charity foundation that seeks money to help those affected by the natural disasters that struck in the early hours of Monday.
"We are launching support the people of Turkey and Syria who have been hit badly with The Ongoing Earthquake, this has displaced many families and children, leaving them homeless. WLADIMIR FOUNDATION has taken it upon herself to render firsthand Aid on ground to help as many people as possible.. We are urging you to please donate to Victims""
"According to our research, these scammers are using a fictitious Ukrainian-based charity to lure victims. The domain hosting the so-called Wladimir Charity Foundation was created on Oct. 3, 2022, and is already blacklisted by our anti-spam and anti-fraud filters. The fake charity, initially set up to assist victims of war-torn Ukraine, seems to have shifted sides for the moment, opening its crypto wallets to donations for victims of the devastating earthquake..."

PetaPixel reported the following: **Scammers Using AI Images to Profit from Turkey-Syria Earthquake**
"Scammers are using images of the earthquakes in Turkey and Syria that have been generated with artificial intelligence (AI) to trick people into donating money. - According to the BBC, security experts have warned that fraudsters are using AI to create emotive images of the Turkey-Syria earthquake and then creating fake appeal pages for survivors. Online scammers have been sharing these AI-generated images of the disaster on Twitter alongside links to cryptocurrency wallets asking for charitable donations.
However, while claiming to be raising money for survivors of the disaster, the scammers are reportedly putting the donated funds into their own accounts.
The BBC reports that a Twitter account posted a fake appeal eight times in twelve hours, sharing the same "photo" of a firefighter holding a child surrounded by collapsed buildings.
However, the Greek newspaper OEMA later discovered that the image was generated by AI text-to-image generator, Midjourney. Midjourney creates similar pictures when given the prompt "Image of firefighter in aftermath of an earthquake rescuing young child and wearing helmet with Greek flag."
Social media users also spotted that the AI-generated firefighter had six fingers on his right hand!

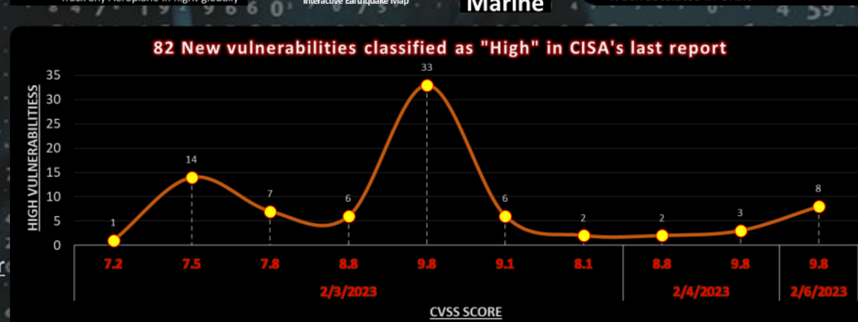
And so, you will find many more posts and reports on the appalling scams that goes around, not only for the Turkey/Syria crisis but any other humanitarian crisis on the globe. Keep your eyes open and be vigilant, if you receive any email or phone call asking for a donation, be very cautious. If you want to help, contact the United Nations in Turkey or any other registered and sanctioned charity organisation and ask for official ways of contributing.

Resources: France24, DailyMail, Chronicle Live, United Nations, KnowBe4, BBC News

Other Interesting News and Cyber Security bits:

- Ex Google CEO, Eric Schmidt Is Building the Perfect AI War-Fighting Machine
- More on ChatGPT and the State of AI
- Lessons All Industries Can Learn From Automotive Security
- SpaceX curbed Ukraine's use of Starlink internet for drones -company president
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
IRIS Interactive Earthquake Map
Marine Traffic
SatelliteXplorer Track satellites in orbit



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