On March 6, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apache, RedHat, WordPress, Google and 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
13 March 2020

In The News This Week

Kentucky university system network reboots after month-long cyberattack

The University of Kentucky and UK HealthCare conducted a major reboot of their computer systems early Sunday morning in an effort to end a month-long cyber-attack that university officials say is the most substantial cyber intrusion in university history. The unidentified "threat actors" infiltrated Kentucky's largest university system in early February from somewhere outside the United States and installed malware that utilized UK HealthCare's vast processing capabilities to mine cryptocurrency, such as Bitcoin, said Eric Monday, university executive vice president for finance and administration. The protracted intrusion, which the university believes it resolved early Sunday morning during a campus-wide network outage, has repeatedly caused a slowing or temporary failure of computer systems used by students and employees, an effect that was likely "most acute" on the health care side, said university spokesman Jay Blanton. Blanton said patient safety and access to care "was never compromised" and there is no evidence personal information or other sensitive data was accessed or downloaded. UK HealthCare has nearly 2 million registered patients. Read the full story here: WHAS11 Article

How poor IoT security is allowing this 12-year-old malware to make a comeback

Conficker peaked in 2009, but unsupported connected devices are allowing it to spread in 2020 - and the **healthcare sector** is where it's infecting the most targets. The proliferation of Internet of Things devices and unsupported operating systems is leaving networks open to simple cyberattacks. Conficker first emerged in 2008, exploiting flaws in Windows XP and older Microsoft operating systems to mostly form botnets to launch attacks. One of the ways Conficker continues to spread is through infecting connected medical devices thanks to their use of outdated or unsupported versions of Windows; the problem has grown to such an extent that researchers note that nearly one in five Palo Alto Networks customers have detected Conficker at some point over the past two years. Read the full story by Danny Palmer here: ZDNet Article(1)

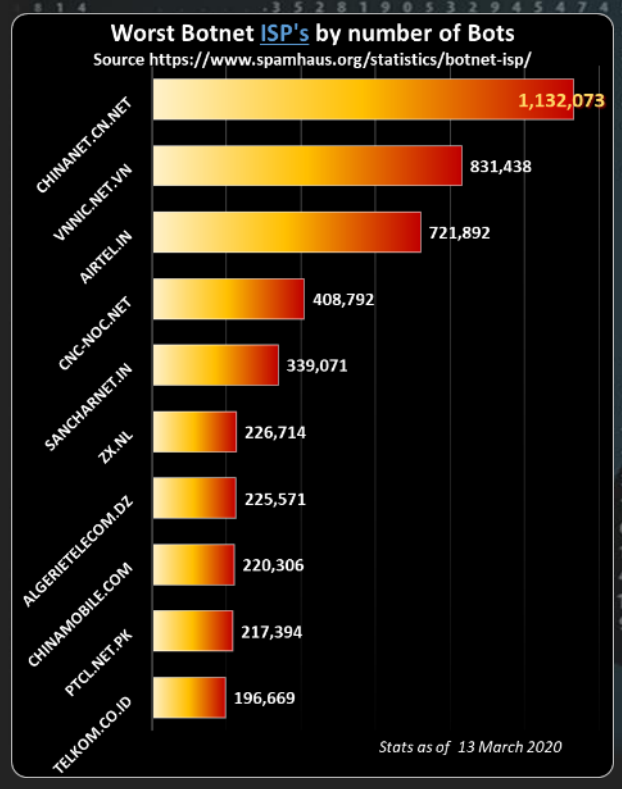
Microsoft shares nightmare tale: 6 sets of hackers on a customer's network

Microsoft reveals its first report on incident response work carried out by its Detection and Response Team (DART) - Microsoft's first report from its recently formed Detection and Response Team (DART), which helps customers in deep cyber trouble, details the case of a large customer with six threat actors simultaneously on its network, including one state-sponsored hacker group that had been stealing data and email for 243 days.
Read the full story here: ZDNet, and the actual report here: DART report

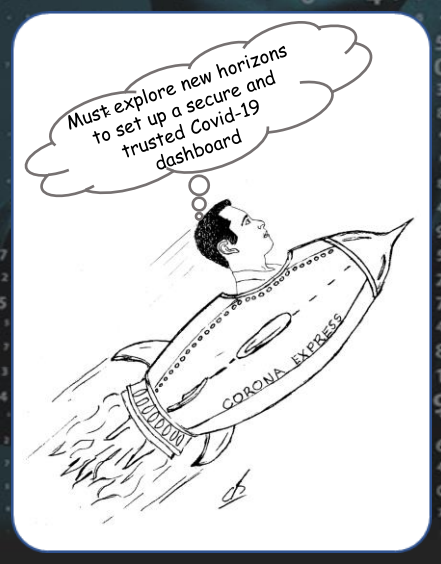
News snippets from the past - Computer crime

Five Men Sentenced for Altering Clients Records at TRW Credit - 1976

The following news snippet was published in the Computerworld publication on November 29, 1976 – *"LOS ANGELES - Five men convicted of conspiring to alter hundreds of credit records at TRW Credit Data and making false statements were sentenced last week in federal court here. The five men were charged with working with an employee of TRW to alter computerized credit records of poor-risk clients [CW, Sept. 13]. Some of the companies victimized by this plot included Diner's Club, American Express, Master Charge, the Bank of America, Sears Roebuck and several leasing firms, the Los Angeles Times reported. Philip Kostoff, the ringleader, was sentenced to 60 days in jail to be served on consecutive weekends, placed on five **years'** probation and fined $3,000. The other four defendants Paul Kostoff, Ronald Rossi, John R. Dubos and Kenneth L. Stevenson were each sentenced to 40 days in jail, placed on five with years' probation and fined $1,000. A sixth man initially indicted in September, Sean Shanahan, was found guilty by the jury of conspiracy but acquitted of a false statement charge. Judge Manuel Real then acquitted him of both charges".* Read more here: GoogleArchives



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



Impact of Corona (COVID-19) on the Cyber Security World

As the World Health Organization (WHO) officially declared the outbreak and spread of the COVID-19 virus (commonly known as the Corona virus) as a worldwide pandemic, we saw a significant impact to the world at large as stock markets plummet to an all time low and travel restrictions are implemented but also specific to the cyber security world.

The first is an increasing number of threat actors that reared their heads exploiting the extensive media coverage of the disease to spread malware and scams. The threats are ranging from corona virus-themed malware, credential stuffing scams, booby trapped websites, look-alike malicious online dashboards, etc. Check Point reported, "Since January 2020, based on Check Point Threat Intelligence, there have been over 4,000 coronavirus-related domains registered globally. Out of these websites, 3 percent were found to be malicious and an additional 5 percent are suspicious. Coronavirus- related domains are 50 percent more likely to be malicious than other domains registered at the same period.

Also, due to widespread travel bans and mass gathering restrictions, most major Cyber Security conferences, summits and other events, are either cancelled or delayed indefinitely. The RSA conference in February was the last one to escape the impact of Corona. Los Angeles Times reported in Europe alone, at least 260 conferences have been cancelled due to the coronavirus. This has enormous financial implications for the organisers, caterers, airlines, hotels and so forth. The announcement by President Trump this week, restricting travel of foreigners between Europe and the USA for at least 30 days starting Friday 13th at midnight, drove home the seriousness of the situation.

Some Malware and Scams to look out for:

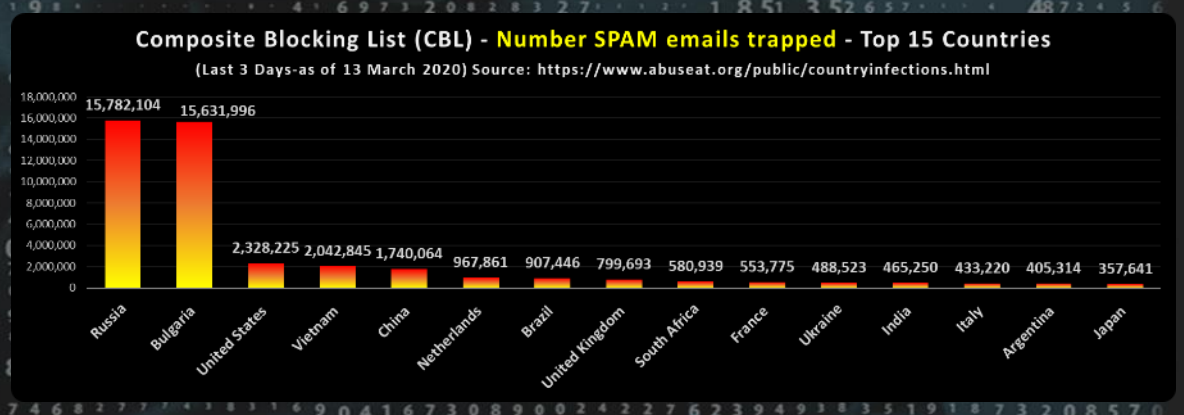
- **Remcos RAT** - This campaign is in the form of a phishing email with a PDF offering coronavirus safety measures. Instead, the PDF–named "CoronaVirusSafetyMeasures_pdf"–includes executables for a Remcos RAT dropper that runs together with a VBS file executing the malware, researchers said.
- **MS Word** – In this email campaign a three-page coronavirus-themed Microsoft Office document is included, purported to be from the Center for Public Health of the Ministry of Health of Ukraine.
- **Fake Messages from CDC** - Another phishing campaign pushes fake messages out purportedly from The Centers for Disease Control (CDC) that the coronavirus has "officially become airborne" and there "have been confirmed cases of the disease in your location."
- **Fake Map** – The Johns Hopkins popular COVID-19 dashboard has been a go-to source for people who want to stay up to date on the virus, but researchers at Malwarebytes discovered a malicious program, "**Corona-Virus-Map.com**", that produces a map that looks exactly like the university's graphic. This site however has embedded malware called corona.exe that's a variant of AzorUlt, a type of spyware that steals usernames, passwords, credit card numbers and other data stored in the user's browser. You can find the official map here: Johns Hopkins University

(*Sources: ThreatPost, InfoSec, Check Point, American Banker, Trend Micro*)

Conferences, seminars and summits cancelled or postponed: (*Statements from organisers*)

- Dell Technologies World 2020, scheduled for May 4-7, has been cancelled amid coronavirus outbreak concerns. Some portions of the conference will be available online. Details are pending.
- Due to the recent outbreak of COVID-19, we've decided not to move forward with O'Reilly Strata Data & AI in San Jose, and London. Strata Data & AI 2020 in San Jose (March 15–18), will be merged with Strata NY in September.
- Due to ongoing concerns about the coronavirus (COVID-19), Gartner has decided to postpone the Digital Workplace Summit, scheduled to take place in Phoenix, March 16 - 17, 2020. We will be communicating new dates shortly.
- IBM cancels its biggest event of the year over coronavirus fears, as it makes a new rule that employees can't go to a conference with over 1,000 attendees. IBM Think was scheduled for May 5-7 and had 30,000 attendees last year.
- Due to the growing concern around the coronavirus (COVID-19), and in alignment with the best practices laid out by the CDC, WHO and other relevant entities, Google Cloud has decided to reimagine Google Cloud Next '20, which will still take place from April 6-8. We are transforming the event into Google Cloud Next '20: Digital Connect, a free, global, digital-first, multi-day event connecting our attendees to Next '20 content and each other through streamed keynotes, breakout sessions, interactive learning and digital "ask an expert" sessions with Google teams.
- The Dublin Tech Summit has become the latest event to be impacted by the Covid-19 outbreak. The event, which attracts over 10,000 global attendees and scheduled for April 22-23 is now been postponed until September 9 and 10.

Listed here are just a few examples to give an indication of the magnitude of the Corona virus impact on the Cyber community worldwide and we didn't even touch on the supply chain impact on computer components from China. No one knows how long it will take to eradicate the virus and things to normalise, so lets settle in for a rocky year ahead.



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