Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On October 19, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Aruba 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

21 October 2022

In The News This Week

New Chinese attack framework Alchimist serves Windows, Linux, and macOS implants

Researchers have discovered a new attack framework of Chinese origin that they believe is being used in the wild. The framework is made up of a command-and-control (C2) backend dubbed Alchimist and an accompanying customizable remote access Trojan (RAT) for Windows and Linux machines. The framework can also be used to generate PowerShell-based attack shellcode or distribute malicious implants for other platforms such as macOS. "Our discovery of Alchimist is yet another indication that threat actors are rapidly adopting off-the-shelf C2 frameworks to carry out their operations," researchers from Cisco Talos said in a new report. "A similar ready-to-go C2 framework called 'Manjusaka' was recently disclosed by Talos." The Alchimist tool is written in GoLang and is deployed on servers as a single standalone file that contains both the implants as well as the user interface that attackers use to interact with their victims' systems. The fact that the backend is self-contained in a single cross-platform executable makes it easy for attackers to deploy. ...
Read the rest of the story by Lucian Constantin here: CSO

Germany fires cybersecurity chief 'over Russia ties'

Germany's cybersecurity chief has been fired after allegations of being excessively close to Russia through an association he helped set up. - Arne Schönbohm had led the Federal Cyber Security Authority (BSI) - charged with protecting government communications - since 2016. German media have accused him of having had links with people involved with Russian intelligence services. The interior ministry is investigating allegations made against him. But it confirmed he had been fired with immediate effect. Mr Schönbohm had come under scrutiny after his potential links to a Russian company through a previous role were highlighted by Jan Böhmermann, the host of one of Germany's most popular late-night TV shows.
Before leading the BSI, Mr Schönbohm had helped set up and run the Cyber Security Council Germany, a private association which advises business and policymakers on cybersecurity issues. He is said to have maintained close ties to the association and attended their 10th anniversary celebrations in September. One of the association's members was a cybersecurity company called Protelion, which was a subsidiary of a Russian firm reportedly established by a former member of the KGB honoured by President Vladimir Putin.. Read the full story by Matt Murphy here: BBC News

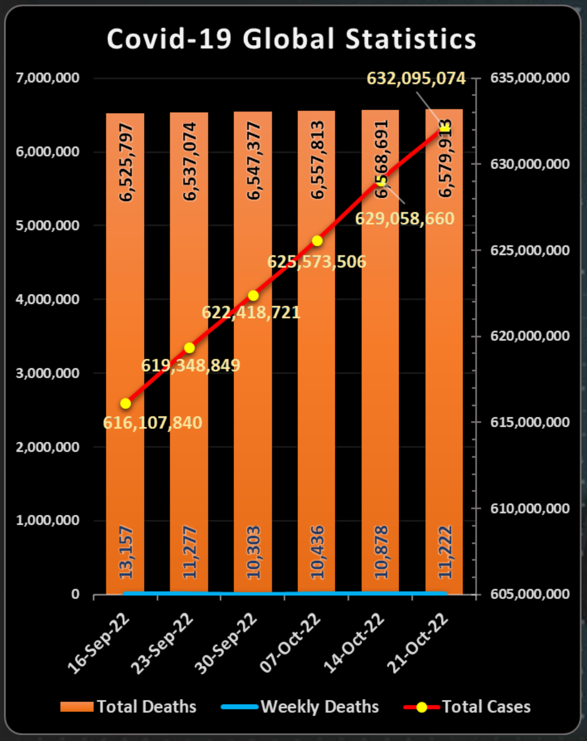
Health insurer Medibank Private halts trading after receiving message from company claiming to be behind cyber attack - Health insurer Medibank Private has confirmed it has received messages from a group wishing to negotiate with the company regarding their alleged removal of customer data. The update comes less than a week after the company was hit by a cyber attack. Medibank says it is working urgently to establish if the claim is true, but is treating the matter seriously. As a result of this, the health insurer has halted trading on the share market until further notice. Medibank CEO David Koczkar has apologised to customers and said he understood the latest update was distressing. "We have always said that we will prioritise responding to this matter as transparently as possible," Mr Koczkar said. "Our team has been working around the clock since we first discovered the unusual activity on our systems, and we will not stop doing that now. "We will continue to take decisive action to protect Medibank customers, our people and other stakeholders."...
Read the story here: ABC News

Government institutions in Bulgaria have been hit by a cyber attack believed to be from Russia

The infrastructure of government institutions in Bulgaria has been hit by a massive DDoS attack. The attack started on Saturday and experts believe that it was orchestrated by Russian threat actors. The attack hit multiple government offices, including the Internal Affairs Ministry, the Defence Ministry, the Justice Ministry, and the Constitutional Court. The Bulgarian government launched an investigation into the incident and warned that these attacks threaten the foundations of the state. Chief Prosecutor Ivan Geshev, during a special briefing on the subject, defined the attack as a criminal offense. ""Here, not only the website of the presidency is under attack, the object of the attack is the entire Bulgarian state as part of the European family," said Ivan Geshev, quoted by BTA. The object of the attack are numerous ministries, including the Ministry of Internal Affairs, Defense, and Justice." reported the Euractive website. Initial investigation revealed that the attack originated from Magnitogorsk, Russia, explained the deputy chief prosecutor and director of the national investigation Borislav Sarafov...
Read the full story by Pierluigi Paganini here: Security Affairs

NSA urges enterprises to watch China, Taiwan tensions

Tensions between the US, China, and Taiwan have far-reaching impacts beyond semiconductor saber-rattling and trade restrictions. There is an enterprise security angle that CISOs should be on guard to tackle, according to US intelligence. NSA Director of Cybersecurity Rob Joyce has some critical lessons on how companies can withstand an escalation in China-Taiwan tensions and what such conflicts matter in the first place. "We had advance warning of the Russia invasion" of Ukraine, said Joyce during a keynote at Mandiant's mWISE security conference. "What would you do if tomorrow you got advanced warning of a China-Taiwan conflict? What business decisions would you have to make?" Read the rest here: The Register


Covid-19 Global Statistics

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

I don't know anymore.
First, we had to worry about Deep Fakes, now they say we have to worry about Shallow Fakes too!

Cyber War: 5 Nations Conducting the Most Cyberattacks

Since the Russian invasion of Ukraine earlier this year, the Western world went into a frenzy about a cyber war brewing between the East and West. The truth of the matter is, the Cyber war has started already some time ago. For several years now, we saw Nation State attacks from both sides on critical infrastructure and other key-economic targets. Peter Suciu of ClearanceJobs posted an article this week putting some of it in perspective as he explores the 5 most notorious countries. Below then is an extract from the article.

The Not-So Secret Cyber War

CHINA – A HOTBED OF HACKERS
China has continued to wage large scale cyber attacks, and this includes stealing intellectual property. More than a third of all cyber attacks are instituted in China, where the People's Liberation Army (PLA) even employs military units that are specialized in network attack and defense.
A Foreign Policy magazine estimate from 2017 suggested that China's "hacker army" could be upwards of 100,000 personnel strong, larger than the size of many nations' actual military force. According to Venafi research, APT groups like APT41 use cyber espionage to support China's long-term economic, political and military goals, often targeting carefully selected victims.
"In China, there are myriad state-sponsored groups, and we see evidence of the nation's cyber offensive capabilities on a near-constant basis," said Blachman. "Recently, as the threat of war in Taiwan has escalated, we've witnessed attacks on Taiwan's infrastructure, which could be a precursor to invasion."
Given how it continues to train the next generation, the threat from China is likely only to increase.

NORTH KOREA – SMALL NATION WITH STRONG HACKER FORCE
2021 was seen as a banner year for North Korean hackers, who reportedly stole $400 million in cryptocurrency – and 2022 will certainly be even better, as cyber agents operating from the Hermit Kingdom allegedly lifted some $600 million from a cryptocurrency gaming start-up this past March. Hacking is increasingly important for North Korea, and it now seeks to increase its efforts. "It has been reported that North Korea, gives aptitude tests and starts training as young as 11 years old," said Tim Morris, technology strategist at cybersecurity firm Tanium.
"Then those skills are used for ransomware and/or cryptocurrency theft to finance other programs for the government or military," Morris told ClearanceJobs. North Korea is also notable in that it is now the only nation in the world whose government is known to conduct such open criminal hacking for monetary gain.
"Infamous North Korean cybercrime groups such as Lazarus and APT38 are renowned for their links to the state. Lazarus is particularly prolific and has made a name for itself with attacks on Sony, the Bangladesh Bank cyber heist, WannaCry and recently targeting US energy companies," Blachman continued. "Our research shows that North Korean state-employed hackers help to circumvent the international sanctions placed on DPRK, with the proceeds of cybercrime funnelled directly into the nation's nuclear weapons program."

IRAN – QUASI-GOVERNMENT GROUP
The Islamic Republic's Iranian Cyber Army has a known connection with Tehran, and it has even pledged its loyalty to the nation's Supreme Leader. It is also believed that the Islamic Revolutionary Guard initiated plans for the group as early as 2005, while it was possibly commanded by Mohammad Hussein Tajik until his death in early 2020.
The Islamic Revolutionary Guard has also stated that it had the fourth largest cyber power among the world's cyber armies. Hackers tied to the Iranian government have recently been targeting individuals specializing in Middle Eastern affairs, nuclear security, and genome research as part of a new social engineering campaign designed to hunt for sensitive information.
However, Iran's hacking efforts could now be used against the government – as the country's state broadcaster was recently hacked as protests for reform, and greater rights for women, grip the Middle Eastern nation. It seems that Iran could have a hard time controlling the beast it created.

RUSSIA – A HACKER SUPERPOWER
Even as the mighty Russian bear appears to be more of a paper tiger on the battlefield, its cyber capabilities shouldn't be underestimated. Moscow has been focused on STEM (science, technology, engineering, math) skills for longer than the United States, and it has paid off. "Russia has half of our population and churns out six times the number of engineering graduates, many of whom use their skills for state-sponsored cyber attacks on America," Gunn explained to ClearanceJobs. "If some of the battles of the future will be fought online, we could end up woefully outmanned and the gap is growing every year." This puts Russia among the greatest cyber threats – even as it faces setbacks in its so-called "Special Military Operation" against Ukraine.
"Russia will increase its use of cyber warfare to gain a better foothold in Ukraine," said Henry Collier, program director for Norwich University's online Master of Science in Cybersecurity program. "Russia has previously used cyber attacks against its adversaries, to include Ukraine, with some degree of success."

UNITED STATES – READY FOR THE CYBER DOMAIN
Cyberattacks aren't just something the "bad guys" conduct. The United States maintains its own wide-reaching cyber warriors. This includes the United States Cyber Command, which is one of the 11 unified combatant commands of the United States Department of Defense. While originally created with a defensive mission in mind, Cyber Command has increasingly been viewed as an offensive force. "The U.S. has its own programs that do the reconnaissance, defensive, and offensive operations," said Morris.
In just the past month, China alleged that U.S. cyber operatives have conducted cyberattacks against its interests. Beijing accused the National Security Agency of infiltrating China's telecommunication infrastructure to steal user data by intercepting digital communication between multiple parties. ...

Please visit the ClearanceJobs site to read the full article

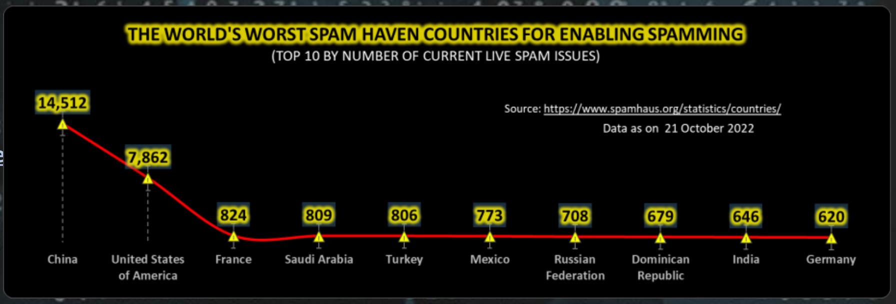
Other Interesting News and Cyber Security bits:

- The difference between shallow fakes vs. deep fakes.(Podcast)
- Apple has won a patent for the creation of Deepfakes that alter the facial expression and pose of a person in a photo or video
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally

SatelliteXplorer
Track satellites in orbit


THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)
Source: https://www.spamhaus.org/statistics/countries/
Data as on 21 October 2022

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