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

On August 31, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Atlassian and Google 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

02 September 2022

In The News This Week

Sembcorp Marine hit by cyber-security incident

Sembcorp Marine has recently discovered a cybersecurity incident where an unauthorised party accessed part of its IT network via third-party software products. Sembcorp Marine took immediate actions to manage and mitigate any potential risks. Cybersecurity experts have been appointed to conduct detailed analytics to flush out all breaches and related root causes, assist with impact assessment, review and enhance security measures to further strengthen the Company's core IT infrastructure and systems. Based on investigations and impact assessment to-date, the incident and related risks have been effectively addressed. Sembcorp Marine's business operations remain unaffected throughout.
Read the report here: Safety4Sea

Chinese Hackers Used ScanBox Framework in Recent Cyber Espionage Attacks

A months-long cyber espionage campaign undertaken by a Chinese nation-state group targeted several entities with reconnaissance malware so as to glean information about its victims and meet its strategic goals. "The targets of this recent campaign spanned Australia, Malaysia, and Europe, as well as entities that operate in the South China Sea," enterprise security firm Proofpoint said in a published in partnership with PwC. Targets encompass local and federal Australian Governmental agencies, Australian news media companies, and global heavy industry manufacturers which conduct maintenance of fleets of wind turbines in the South China Sea. Proofpoint and PwC attributed the intrusions with moderate confidence to a threat actor tracked by the two companies under the names TA423 and Red Ladon respectively, which is also known as APT40 and Leviathan.... Read the full story by Ravie Lakshmana here : The Hacker News

UK mobile and broadband carriers face heavy fines if they fail to follow new cybersecurity rules

More than three years in the making, the U.K. government today announced a new, sweeping set of rules it will be imposing on broadband and mobile carriers to tighten up their network security against cyberattacks — aimed at being "among the strongest in the world" when they are rolled out, said the Department for Digital, Culture, Media and Sport. The new requirements cover areas such as how (and from whom) providers can procure infrastructure and services; how providers police activity and access; the investments they make into their security and data protection and the monitoring of that; how providers inform stakeholders of resulting data breaches or network outages; and more. The rules will start to get introduced in October, with carriers expected to fully implement new procedures by March 2024. Critically, those who fail to comply with the new regulations will face big fines: non-compliance can result in up to 10% of annual revenues; continuing contraventions will see fines of £100,000 ($117,000) per day. Communications regulator Ofcom, which worked with the National Cyber Security Centre to formulate the new regulations and code of practice, will enforce compliance and fines.." ... Read the rest by Ingrid Lunden here: TechCrunch

Montenegro blames Cuba ransomware for attacking the country

The cyberattack that crippled the Montenegro government's digital infrastructure was likely carried out by a **Russia-linked Cuba ransomware gang**, authorities claim. Montenegro's Public Administration Minister Maras Dukaj told state television hackers had created a special virus for the attack called Zerodate, Reuters reports. Dukaj claims that 150 workstations in 10 state institutions were infected due to a cyberattack against the NATO member. Government internet sites have been closed since the attack, which Montenegro's National Security Agency (ANB) has linked to Russia, although the extent of any data theft is unclear. Local authorities attributed the attack to the Cuba ransomware group. "We have already got an official confirmation, it can also be found on the dark web where the documents that were hacked from our system's computers will be published," Dukaj said. .. Read the full article by Vilius Petkauskas here: Cybernews, more here: Balkan insight

Google tackles open source security with vulnerability rewards program

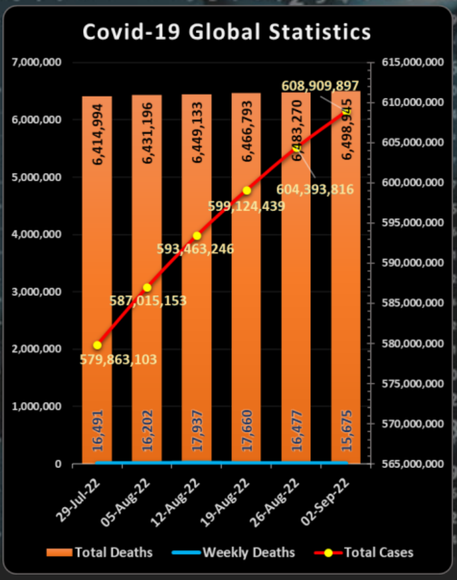
The program follows a surge in supply chain attacks impacting the open source software ecosystem. - Google calls itself one of the largest contributors to open source in the world, citing its role as the maintainer of projects including Golang, Angular and Fuchsia. Google's original bug bounty program, which began more than a decade ago, has expanded to include issues surrounding Chrome, Android and other areas. Since the program began, Google has paid more than $38 million on more than 13,000 submissions. The new OSS VRP follows a year when supply chain attacks aimed at open source skyrocketed by 650%, including incidents like Codecov and Log4Shell, according to the blog. "Opening this new VRP scope furthers the importance of security research being rewarded in the open source ecosystem," Francis Perron, open source security technical program manager at Google, said via email. "It also emphasizes the importance and value of vulnerability disclosure in open source."...
Read the full story by David Jones here: Cybersecuritydive

Inside the IT Army of Ukraine, 'A Hub for Digital Resistance'

Ukrainian cyber officials claim hundreds of thousands of people from around the world have volunteered to be part of a pick-up cyber force they call the IT Army of Ukraine. Click Here spoke to one of their key administrators at the start of the war and now we check back in with him six months later. In the intervening months, the IT Army has been part of what the head of the UK's signals intelligence branch, GCHQ, has called "the most effective defensive cyber activity in history." Working with other hacker groups around the world – from Anonymous to Squad 303 out of Poland – the IT Army of Ukraine hacked Russia's Davos meeting – delaying President Vladimir Putin's opening address for more than an hour – released military plans, and interrupted Russia's central television news with their own dispatches from the war. The latest episode of the Click Here podcast includes an extended sitdown with a high ranking member of the force — Click Here agreed to withhold his identity for safety reasons. The interview has been edited and condensed for clarity... Read the transcript of interview here: The Record , (The voice interview can be heard at about 12 minutes into the podcast found on the site)

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

Cyber Security
Training
CYBER SECURITY
A Basic Guide On Cyber Security For Beginners [2022 Edition]
1:13:56
simplilearn



Russia vs. Ukraine Cyber War Timeline

For those who are following the ongoing Russian invasion of the Ukraine, below is an extract of the Cyberwar timeline posted by MSSP Alert. An interesting read but due to limited space in this post, please visit the MSSP Alert site to see events before 1 April.

Russia Invades Ukraine: Kinetic Warfare and Cyberattack Timeline

August 29, 2022: Ericsson, Nokia, Logitech Exiting Russia: Ericsson said it will gradually wind down business activities in Russia over the coming months as the Swedish telecoms equipment maker completes its obligations to customers. Nokia and Logitech made similar statements. (Reuters)
August 27, 2022: Dell Exits Russia: Dell Technologies said it had ceased all Russian operations after closing its offices in mid-August, the latest in a growing list of Western firms to exit Russia. (Reuters)
July 22, 2022: Google Search Blocked: Russian-backed separatists in a breakaway region of eastern Ukraine have blocked access to Google's search engine, citing alleged disinformation. (Reuters)
July 12, 2022: Five months after Russia's invasion, Ukraine continues to see significant increases in cyberattacks targeting state systems and infrastructure as a result of the war, according to the country's top cyber defense agency. (SC Media)
July 6, 2022: Breakup: Russian cybersecurity outfit Group-IB will split its domestic and international business into two separate companies in a bid to maintain a presence in both the Russian and overseas markets. (Reuters)
June 30, 2022: Norway, NATO Members Targeted: Russian hacker group Killnet targeted a string of Norwegian public service websites in the latest digital salvo against NATO member countries. (Bloomberg)
June 23, 2022: Cisco Systems Exiting Russia: Cisco plans to wind down its business in Russia and Belarus. (Reuters)
June 9, 2022: Russia warned the West that cyberattacks against its infrastructure risked leading to direct military confrontation, and that attempts to challenge Moscow in the cyber sphere would be met with targeted countermeasures. (Reuters)
June 8, 2022: (1) Ukraine Internet Access: In areas of Ukraine under Russian occupation, Internet access has often been shut down or disrupted, leaving the local population isolated from the rest of the world. Now, a new trend is emerging: The internet is coming back online, but the traffic is no longer managed by Ukraine. It's been re-routed to networks owned by the Russian government. (Bloomberg) - (2) Banning Russia Cloud Services?: The European Union is working on a possible ban on the provision of cloud services to Russia as part of new sanctions against the Kremlin for the invasion of Ukraine. (Reuters)
June 6, 2022: Ukraine Phones Allegedly Targeted: The phones of Ukrainian officials have been targeted by hackers as Russia pursues its invasion of Ukraine, Reuters reported. Victor Zhora, the deputy head of Ukraine's State Special Communications Service, said that phones being used by the country's public servants had come under sustained targeting, the report indicated. (Reuters)
May 31, 2022: DDoS Attacks Against German Banks?: The German financial regulator BaFin issued a fresh cyber security warning to the nation's financial sector due to the war in Ukraine following a recent increase in cyber attacks. BaFin has repeatedly warned about cyber attacks but this security notice marks an escalation of its concerns. "In recent days there have been repeated attacks on IT infrastructure," BaFin said — many of which involved DDoS attacks, the organization said. (Reuters)
May 19, 2022: Russia Disinformation Campaign: Mandiant research has detailed several Russian-aligned disinformation and propaganda campaigns, including bogus online claims that Ukrainian President Vladimir Zelenskyy had committed suicide or fled Ukraine. (Associated Press)
May 10, 2022: More Kaspersky Concerns?: The National Security Agency is investigating the extent that software made by the Russian cybersecurity company Kaspersky is embedded in U.S. businesses and organizations amid rising security concerns arising from Russia's invasion of Ukraine. (Bloomberg)
May 3, 2022: Germany Warning: Germany's financial regulator BaFin warned of a "very big and very present" risk of cyberattacks in the wake of Russia's invasion of Ukraine. (Reuters)
April 27, 2022: (1) Microsoft Research: Microsoft alleges that Russia has launched nearly 40 cyberattacks vs. Ukraine. (Microsoft)
(2) Atos Exits Russia: The IT services company has moved its Russia services to such countries as India and Turkey. (Reuters)
April 14, 2022: More than 600 Western companies have said they would exit or cut back operations in Russia, according to researchers at Yale University. (The Wall Street Journal)
April 12, 2022: (1) Nokia Exits Russia: Telecoms equipment maker Nokia is pulling out of the Russian market. (Reuters)
(2) Russia's Sandworm hackers attempted a third blackout in Ukraine. The attack was the first in five years to use Sandworm's Industroyer malware, which is designed to automatically trigger power disruptions. (Wired) and (SC Media)
April 11, 2022: Ericsson Exits Russia: Swedish telecom equipment maker Ericsson is suspending its business in Russia indefinitely. Ericsson will record a US$95 million provision in the first quarter for costs related to the move. (Reuters)
April 8, 2022: Cyberattacks Target Finland: The cyberattacks on Finland government websites and a suspected airspace violation by Russian aircraft just as speculation mounts that the Nordic nation will opt to apply for membership in the NATO alliance. (Bloomberg)
April 7, 2022: Microsoft Disrupts Hackers: Details about the alleged Strontium threat actor are here. (Microsoft)
April 6, 2022: FBI vs. Russia: The FBI has wrested control of thousands of routers and firewall appliances away from Russian military hackers by hijacking the same infrastructure Moscow's spies were using to communicate with the devices. (Reuters)
April 4, 2022: Nordex Cyberattack: Nordex is the second German wind turbine maker to suffer a cyberattack since Russia's invasion of Ukraine began. Nordex rival Enercon's remote service links had been cut at start of the war. (ReCharge)
April 1, 2022: AcidRain Cyberattack: Satellite communications company Viasat said its own research is consistent with a new report from a cybersecurity firm that said a February attack on their infrastructure in Ukraine involved the use of a new malware named AcidRain. (The Record)

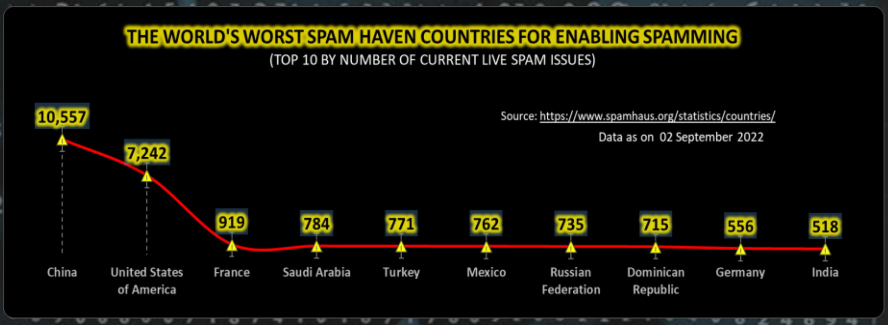
Other Interesting News and Cyber Security bits:

- What is Artemis? Everything you need to know about NASA's new Moon mission
- Royal Caribbean will equip all its cruise ships with Starlink internet
- NASA has solved the mystery of Voyager 1's strange data transmissions
- 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



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