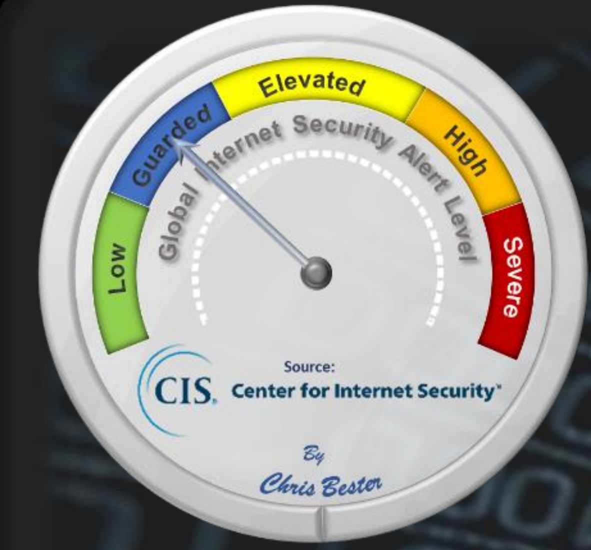

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On June 22, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe, Cisco, Splunk and Google products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
24 JUN 22	547,496,387	6,347,883

Deaths this week: 9,585

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 June 2022

In The News This Week

Defending Ukraine: Early Lessons from the Cyber War

Editor's note: Wednesday Microsoft published a new intelligence report, **Defending Ukraine: Early Lessons from the Cyber War**. This report represents research conducted by Microsoft's threat intelligence and data science teams with the goal of sharpening our understanding of the threat landscape in the ongoing war in Ukraine. The report also offers a series of lessons and conclusions resulting from the data gathered and analyzed. Notably, the report reveals new information about Russian efforts including an increase in network penetration and espionage activities amongst allied governments, non-profits and other organizations outside Ukraine. This report also unveils detail about sophisticated and widespread Russian foreign influence operations being used among other things, to undermine Western unity and bolster their war efforts. We are seeing these foreign influence operations enacted in force in a coordinated fashion along with the full range of cyber destructive and espionage campaigns. Finally, the report calls for a coordinated and comprehensive strategy to strengthen collective defenses....
Read the report by Brad Smith - President & Vice Chair of Microsoft here: Microsoft Blog, or Published PDF Report

Slovenia Hosts Cyber Security Exercise to Test Nuclear Security Capabilities

Unusual and suspicious behaviour of a disgruntled employee captured in a 10 second surveillance video of a hypothetical nuclear facility opened a large-scale cybersecurity exercise in Slovenia. Following the employee footage, a series of simulated events unfolded and culminated in a malware attack at the hypothetical nuclear facility operational technology systems. Conducted by the Slovenian Nuclear Safety Administration (SNSA), this highly interactive exercise — included hands-on examples and involved key Slovenian nuclear sector stakeholders. The scenario involved real operational technology systems with insider threats, external cyber-attacks, and physical intrusions to a hypothetical nuclear facility exhibiting the impacts of a computer security compromise of critical operational control systems leading to a nuclear security event... Read the rest of the article by Vasiliki Tafili here: IAEA – International Atomic Energy Agency

This phone-wiping Android banking trojan is getting nastier

A nasty Android banking trojan that is best known for wiping smartphones to cover its tracks has gained several new features to improve its ability at phishing online-banking credentials, intercepting SMS two-factor authentication codes, and more. The BRATA or the 'Brazilian Remote Access Tool, Android' has been circulating since at least 2019, initially as spyware although it later became a banking trojan. Researchers at Cleafy, an Italian cybersecurity firm, last year discovered BRATA's makers had started abusing Android's factory reset to prevent victims from discovering, reporting and preventing unauthorized wire transfers. The factory reset was executed after a successful illicit wire transfer or when the malware detected analysis by installed security software. BRATA originally targeted customers from Brazilian banks only, but Cleafy reported that it started targeting customers of UK, Spanish and British banking brands more recently.
Read the rest of the post by Liam Tung here: ZDNet

Space-based assets aren't immune to cyberattacks

One of the most significant cybersecurity incidents related to Russia's war on Ukraine was a "multi-faceted" attack against satellite provider Viasat's KA-SAT network on February 24, one hour before Russia's invasion began. The assault, which both Ukraine and Western intelligence authorities attribute to Russia, was intended to degrade the Ukrainian national command and control. However, the attack, which was localized to a single consumer KA-SAT network operated on Viasat's behalf by another satellite company, a Eutelsat subsidiary called Skylogic, disrupted broadband service to several thousand Ukrainian customers and tens of thousands of other fixed broadband customers across Europe. It also highlighted how space-based assets, such as satellites are as vulnerable to malicious exploitation as any other piece of critical infrastructure. Against this backdrop, the timing was perfect for the Space Cybersecurity Symposium III hosted by the U.S. National Institute of Standards and Technology (NIST) last week... Read the post by Cynthia Brumfield here: CSO

Harmony's Horizon Bridge hacked for $100M

The layer-1 blockchain's main bridge between Ethereum, Binance Chain, and Bitcoin has been exploited for nine figures, but says its BTC bridge has not been affected. - The Horizon Bridge facilitates token transfers between Harmony and the Ethereum network, Binance Chain and Bitcoin. Harmony, the operator of the bridge, announced late on June 23 that the bridge has been halted. It said the BTC bridge and its assets have not been affected by the attack. The Harmony team also said it was working with "national authorities and forensic specialists" to determine who is responsible. A post-mortem is sure to follow. The developers and the co-founder of Harmony Nick White did not respond to requests for comment. Harmony is a layer-1 blockchain using proof-of-stake consensus. Its native token is ONE....
Read the story by Brian Newar here: COINTELEGRAPH

Five active ransomware gangs and their tactics

We hear about ransomware attacks almost on a daily basis and it became such a common phenomenon that the major news agencies don't even report on it anymore unless it involves one of the tech giants or Five Eye Governments. Experts recons that it is not a matter of "if" your company gets hit by ransomware anymore, it is a matter of "when". So most organisations are spending more and more resources planning for recovery in parallel with their prevention efforts.
There are many threat actors on the ransomware scene but a few are more prominent than others. Crystel Saraie of the Cyber Security Hub posted an article on the top five gangs that were active in recent months. So let's meet them.

Crystel's Post: As ransomware gangs continue to threaten organization's cyber security, it is important to make note of the most prominent groups at the moment and their techniques. Today's ransomware gangs continue to evolve and Ransomware-as-a-Service (RaaS), double extortion and cross-platform functionality are now common traits. In this article we review just five of the top ransomware gangs active today, some of their recent attacks and the tactics they are deploying.

Hive

Hive, who first emerged in June 2021, has become renown as an incredibly aggressive group targeting the healthcare sector.
On 31 May, Hive attacked the Costa Rican Social Security Fund, Costa Rica's public health service. Other notable cases include the attack on the Missouri Delta Medical Center, where patient data was leaked, and the Memorial Health System in Ohio, where urgent surgeries and radiology exams had to be cancelled.
Healthcare organizations have been warned against the gang, and advised to apply strong cybersecurity systems and defenses by the US Department of Health and Human Services. Hive operates as RaaS and uses the double extortion method, where data is stolen as well as encrypted. Their malware design uses the Golang programming language.

AlphV (BlackCat)

AlphV, also known as BlackCat, was first observed by Microsoft in November 2021. It also works as a RaaS and uses the double extortion method. This organisation is unique for being the first ransomware gang using the RUST programming language.
The gang has attacked many high-profile organizations, such as fashion brand Moncler and the Swissport airline cargo handling service provider. In May 2022 the Austrian federal state Carinthia was targeted and BlackCat demanded US$5mn for the decryption of stollen data.
BlackCat continues to gain attention and on 14 June they debuted a dedicated website for victims to search for their stolen data, taking ransomware operations to the next level. The site exposes the personal information of organization employees and clients, such as names, US Social Security Numbers, addresses, emails, and more.

Lapsus$

Lapsus$ first became active in December 2021. The cybercriminals their private Telegram channel to communicate with the public, rather than traditional data leak websites. They also conduct polls, giving members a choice in who should be targeted next.
According to Microsoft the hacking group is known for using a pure extortion and destruction model without deploying ransomware payloads. The gang typically focuses on compromising user identities but using compromised credentials.
In late March 2022, seven people aged 16 to 21 were arrested in the UK in relation to the gang's activities, despite the gang initially believed to be based in Brazil as one of its first victims was the nation's Ministry of Health.
The UK arrests have not brought the group down as days later Lapsus$ released a 73GB archive from software services company Globant, whose clients include Disney and Google. The group, therefore, is seemingly still active.

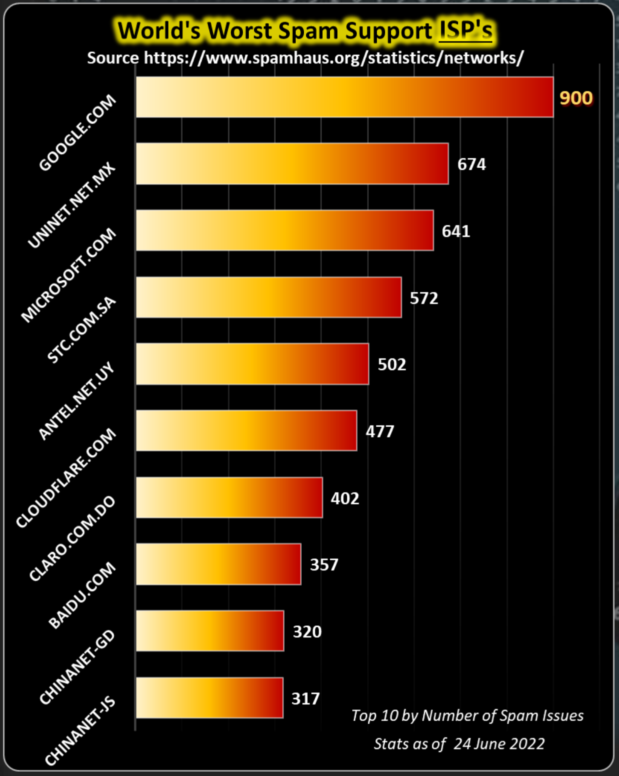
Conti

Conti, thought to led by cybercriminal Wizard Spider, accounted for 20% of attacks in the first three months of 2022, according to Digital Shadows.
Operating on a double extortion system, they use a multithreading method, which allows a fast spread of malware.
The group is believed to have ties to Russia as it released a statement in solid support of the Kremlin's decision to invade Ukraine. They are responsible for a number of high-profile ransomware attacks, including the City of Tulsa and Japanese multinational electronics company JVC Kenwood.
In May 2022, Costa Rica declared a national emergency after their government systems were attacked by Conti.
However, in the midst of this, the group disbanded.
The Conti cybercrime syndicate will, however, continue to live on, with reports of partnerships with smaller ransomware gangs, such as Hive, BlackCat, BlackByte, and more.
Members will spread to these gangs and work as part of those organizations but will still be a part of the larger Conti syndicate. The Costa Rica attack has been theorized to be a publicity stunt as Conti members slowly migrated to other gangs.

LockBit

A RaaS organization using double extortion methods, LockBit was responsible for 38% of ransomware attacks between January and March 2022 according to Digital Shadows. They have been present since 2019.
Their malware tool Stealbit automates data exfiltration.
It was released allongside LockBit 2.0, which has been coined as the fastest and most efficient encryption system by its creators.
They have attacked large cooperations including tyre manufacturer Bridgestone Americas and the French electronics multinational Thales Group. Lockbit has also hit the French Ministry of Justice, threatening to release sensitive data.

Resources: Cyber Security Hub



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

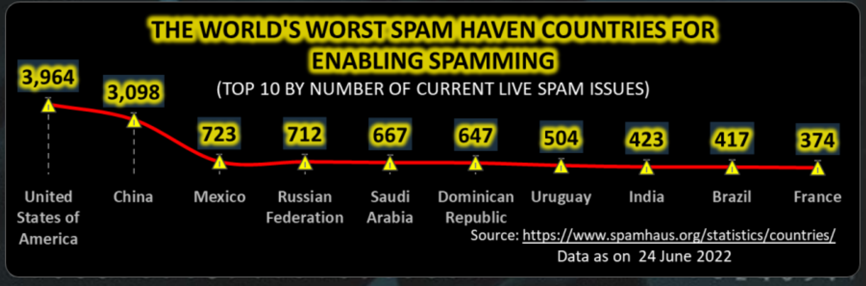
It didn't take a Genius to see this one coming!
Space - Cyber Target Frontier?

Other Interesting News and Cyber Security bits:

- Inside North Korea's global cyber war: The intersection of hacking and organized crime
- Flame: The Most Sophisticated Cyber Espionage Tool Ever Made
- Car dealer loses court appeal over buyer's claim £140k Bentley couldn't tow caravan
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally



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