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

On May 12, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). No further update this week.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
21-May	165,857,655	3,444,901

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 May 2021

In The News This Week

CNA Financial Paid $40 Million in Ransom After March Cyberattack

CNA Financial Corp., among the largest insurance companies in the U.S., paid $40 million in late March to regain control of its network after a ransomware attack, according to people with knowledge of the attack. The Chicago-based company paid the hackers about two weeks after a trove of company data was stolen, and CNA officials were locked out of their network, according to two people familiar with the attack who asked not to be named because they weren't authorized to discuss the matter publicly. In a statement, a CNA spokesperson said the company followed the law. She said the company consulted and shared intelligence about the attack and the hacker's identity with the FBI and the Treasury Department's Office of Foreign Assets Control, which said last year that facilitating ransom payments to hackers could pose sanctions risks.
Read the full story here: Bloomberg

Qbit becomes Eurofins Cyber Security The Netherlands

HAARLEM and GRONINGEN, Netherlands, May 18, 2021 /PRNewswire/ -- Eurofins Cyber Security, a global leader in end-to-end cyber security and testing services, announced today that its operation in the Netherlands 'Qbit' will be known as Eurofins Cyber Security the Netherlands. Qbit has been a part of Eurofins Cyber Security (itself a division of Eurofins Digital Testing) since early 2018, but continued to trade under the Qbit name, particularly in its home territory. Over the past three years it has built an enviable reputation in delivering a broad portfolio of cyber security services both within the Netherlands and internationally. The name change brings the operation in line with Eurofins Cyber Security operations in Europe, Asia and the US and puts it in an excellent position to expand its operations globally. Read the rest of the story here: Yahoo

New Zealand Health Board hit by cyber security incident

Waikato District Health Board confirmed on 18 May that it was addressing "a cyber security incident" and was "experiencing a full outage" of its information systems. The district board said the incident has affected five hospitals (Waikato, Thames, Tokoroa, Te Kite and Taumarunui) "to varying degrees". An update, posted on May 19, said "good progress" had been made overnight to get systems back online. "Our staff are working to restore the infected systems and on the remediation process. We are working with the relevant government departments to ensure a secure environment is successfully re-established," the statement said.
Read the article by Hannah Crouch here: digitalhealth

U.S. has almost 500,000 job openings in cybersecurity

Help wanted: thousands and thousands of people interested in a career in cybersecurity. - There are about 465,000 open positions in cybersecurity nationwide as of May 2021, according to Cyber Seek — a tech job-tracking database from the U.S. Commerce Department — and the trade group CompTIA. The need for more web watchmen spans from private businesses to government agencies, experts say, and most of the job openings are in California, Florida, Texas and Virginia. That means for anyone looking to switch careers and considering a job in cybersecurity, there's no greater time than now to find work, the job trackers said. "You don't have to be a graduate of MIT to work in cybersecurity," said Tim Herbert, executive vice president for research at CompTIA. "It just requires someone who has the proper training, proper certification and is certainly committed to the work." Switching careers to cybersecurity could be as easy as grabbing a Network+ or Security+ certification, said Michelle Moore, who teaches cybersecurity operations at the University of San Diego. An eight-week online course could help someone land an entry-level job as a "pen tester," a network security engineer or an incident response analyst, Moore said. Those jobs pay between $60,000 to $90,000 a year, she added.
Read the full story by Khristopher J. Brooks: CBS News

"Anonymous", friend or foe?

A couple of weeks ago I covered the topic of hacktivism and the name 'Anonymous' popped up numerous times and I was asked who exactly is this hacking group who calls themselves 'Anonymous'? Are they good or bad?
The original hacking or hacktivist group reared its head in 2006 and was founded by a motley character called Aubrey Cottle whose aim was to establish a digital protest platform. A protest platform that could disrupt organizations, state departments, or any other group that were party to or sympathetic to perceived corrupt entities. It was further said to seek mass awareness and revolution against such perceived corrupt entities and to expose child molesters and anyone involved with child pornography and trafficking.

Last year MarketWatch published a short piece on a Reddit talk by Cottle discussing his current activities and his quest to take down *QAnon*, a discredited American far-right conspiracy theory cult that surfaced in October 2017. Supporters of the *QAnon* movement were among the crowd that stormed the US Capitol building earlier this year. There is plenty to say about *QAnon* but I'll save that for another time.

Anonymous is a decentralized virtual community with disparate goals depending on the current affairs both local or international. It can operate as a collective or sometimes more independent as many jumped on the bandwagon of anonymity to fulfill their quest for what they believe is just. I know, it sounds like no one can actually put a handle on it and say, "this is what Anonymous is", and is it actually an organization or rather independent groups that follow their own goals? Who knows?

Traversing the Internet jungle to get a clear picture of Anonymous just gets you more confused than ever. In my travels, I came across a blog on Blueshoon I want to share to give some insight into Anonymous. Following is an extract of the blog.

ANONYMOUS: THE PROS AND CONS OF HACKTIVISM

When you picture a modern-day activist, who do you imagine?
Is it a long-haired hippie with love beads and tribal tattoos? A social justice warrior holding an "Occupy Wall Street" sign, eager to pick a fight with any modern ideology that strikes their fancy? How about your geeky, yet computer-savvy next-door neighbour?

Yes, in the digital age, nearly anybody with the right set of tech skills can be a hero to the weak and downtrodden. And plenty of hungry hackers do just that—leveraging their exceptional technological abilities to manipulate, harass, and intimidate any party that they see fit. The lack of transparency of online activity makes these "hacktivists" notoriously difficult to track, yet one group has gained considerable fame for its coordination, effectiveness, and unforgiving nature: the grassroots group of Internet militants known as "Anonymous."

WE ARE ANONYMOUS

Starting as a disparate group of activists and bored hackers on the popular online imageboard 4chan, the users who would eventually form the group Anonymous would often unite under the banner of a common cause and create mayhem around their target. In 2008, the group gained notoriety for the hacktivism initiative known as "Project Chanology;" a coordinated series of hacking attempts and protests against the Church of Scientology.
More recently, Anonymous targeted the Twitter accounts of the international terrorist group ISIS by releasing a "how-to" guide for hacking Twitter profiles and a pledge to "wipe ISIS from the face of the Internet." Within a day, the Internet group claimed that 20,000 Twitter accounts tied to ISIS had been taken down. Other targets have included everyone from the Westboro Baptist Church to credit card companies and even military organizations.

FRIEND OR FOE?

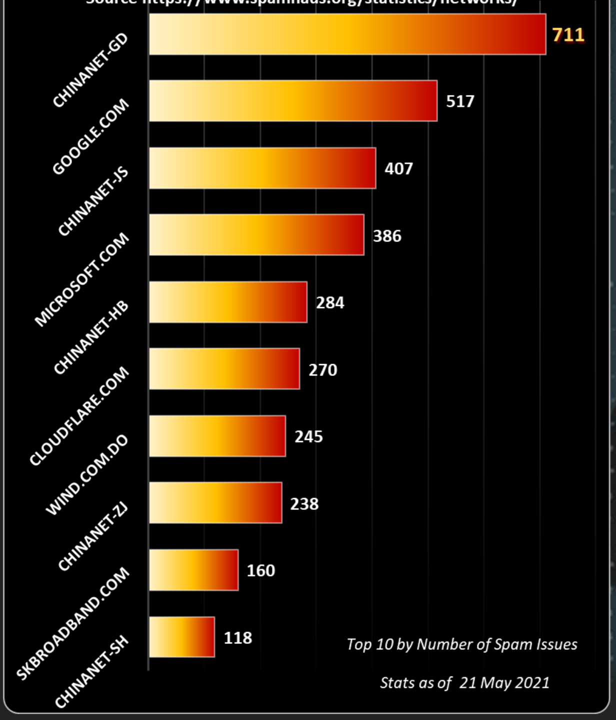
The subject of Internet hacktivism creates debate on the legal boundaries of online crime, the morality of cyber justice, and the nature of online privacy.
The idea of a cyber crusader, admittedly, has some dramatic flair—individuals striking back against terrorist groups and greedy corporations by any means available. It brings to mind iconic comic book crusaders like Batman; individuals willing to take a stand against injustice.

However, not everybody sees these hackers as heroes to be admired. Though it's hard to argue against hacktivism ideologies when they strike against known terror groups and those who seem to genuinely deserve a kick in the pants, many governmental bodies and police organizations are quick to point out that cybercrime is still crime.
Many innocent people get caught in the crossfire when tech-savvy vigilantes have free reign over the Internet, and Anonymous is known to choose its targets on a whim.

While the presence of these Internet vigilantes may provide peace of mind to those wanting to strike digital blows against corruption, there is no outside regulation on the actions of anonymous users. Most members of hacktivist groups operate with proxies to ensure their anonymity, even in the face of legal scrutiny. This creates a lack of accountability to any civilized body—and raises serious questions when large-scale operations reveal valuable and sensitive information.
At the end of the day, it's hard to say whether Internet activist groups like Anonymous are truly friend or foe. **They give a voice to the unheard and fight against evil…but as they're the ones who decide what's evil, their actions must not be romanticized and should be assessed for what they are**. We're all activists, one way or another. Some of us just take it a little further than others.

References: MarketWatch, Blueshoon, Mirror, BBC News, Wikipedia, The Atlantic, The Wall Street Journal

World's Worst Spam Support ISP's
Source https://www.spamhaus.org/statistics/networks/



Top 10 by Number of Spam Issues

Stats as of 21 May 2021

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

Anonymous, friend or foe?

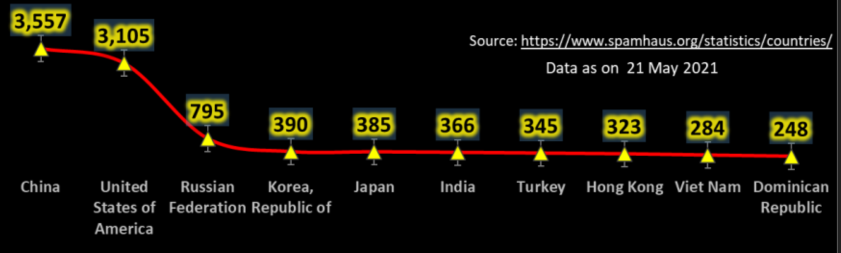
You decide

Other Interesting News and Cyber Security bits:

- CYBER SECURITY AS COUNTER-TERRORISM: SEEKING A BETTER DEBATE
- Center for Internet Security Releases CIS Controls Version 8
- Integrated cyber attack analysis platform "NIRVANA Kai" supports IPv6

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 May 2021



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