On April 27, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in WS02 and Google products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
29 Apr 22	512,268,198	6,256,576

Deaths this week: 19,932

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
29 April 2022

In The News This Week

Russia plumbs new depths in cyber war on Ukraine

Russian threat actors are sinking to new lows in support of Moscow's illegal and unprovoked war on Ukraine, according to new intelligence from Microsoft, which has catalogued more than 230 distinct cyber operations from at least six threat groups since the war began in February. Alongside more broad-brush espionage and intelligence-gathering activities that might be expected during a cyber war, Russia has been conducting destructive cyber attacks that are clearly designed to threaten the welfare of Ukrainian civilians by degrading the systems of Ukrainian institutions, disrupting access to reliable information and critical services, and attempting to damage citizen confidence in the Ukrainian government. "We believe it's important to share this information so that policymakers and the public around the world know what's occurring, so others in the security community can continue to identify and defend against this activity," said Tom Burt, corporate vice-president of security and trust at Microsoft. Read the full story by Alex Scroxton here: ComputerWeekly

China launches 'raging cyber-espionage battle' on Russia with new malware campaign

A CHINESE affiliated hacker group is targeting Russians using malware disguised as legitimate documents and downloads, cyber security experts have claimed. China's alleged actions against Russia is another twist in the complex relationship between the two countries. Presently, China has not condemned Russia for its military actions in Ukraine - but they are reportedly altering their cyber position in response to the matter, The Register reports... The Chinese threat groups have infiltrated servers with a decoy document written in English, the security researchers claim. If clicked, the decoy document allegedly installs three additional malicious files. Part of the scheme is a malware initiative called PlugX that gives the hackers "access to the compromised host to extract sensitive system information, upload and download files, and execute a remote command shell," according to the cybersecurity company. Read the article by Tyler Baum here: The Sun

NATO Plays Cyberwar to Prep for a Real Russian Attack

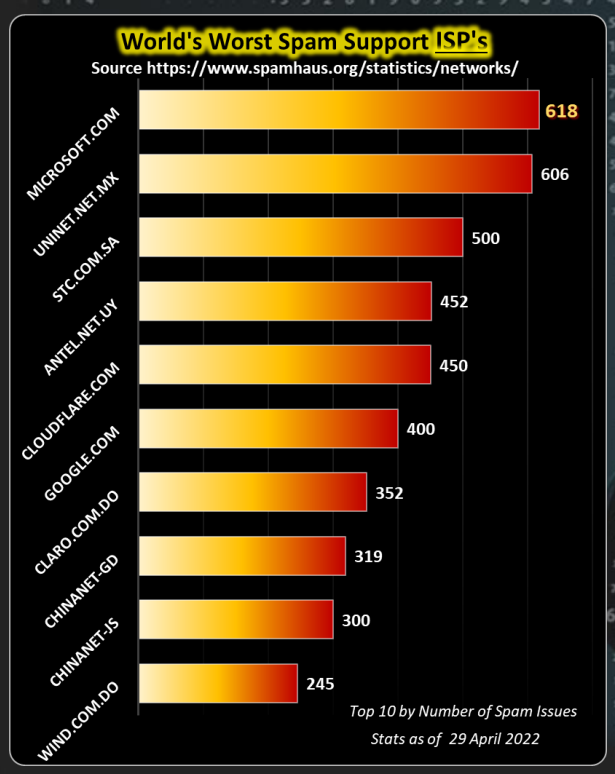
Cybersecurity experts representing 30 NATO members are fighting a digital war this week to defend a fictional island country in the northern Atlantic Ocean. Though "Berylia" is fake, experts involved hope the lessons learned from the staged attack will better prepare them for the possibility of a Russian attack as war ravages Ukraine. The war games, dubbed the "Locked Shields" exercises by The North Atlantic Treaty Organization's Cooperative Cyber Defense Centre of Excellence's, (or NATO CCDCOE, for short) are heralded by the organization as the "World's Largest International Live-Fire Cyber Exercise." Though participants engaged in the war games will role play an attack on Berylia, they'll actually be sitting in front of desks in Estonia, itself the site of a major 2007 cyberattack.. Read the rest of the story by Mack DeGeurin here: Gizmodo

Coca-Cola Investigates Data Breach Claim

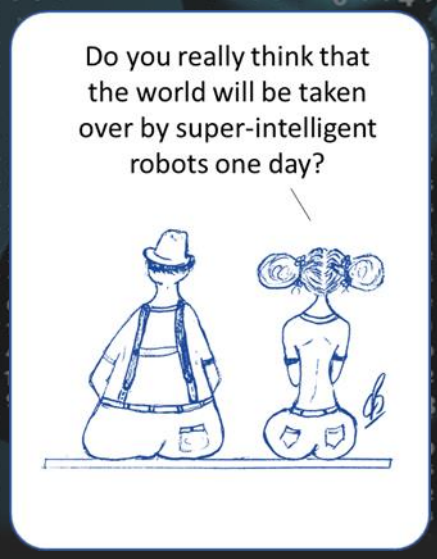
Coca-Cola is investigating claims of a large-scale data breach by **Russian-linked** cybercrime gang **Stormous**. The ransomware group posted on its website this week that it had successfully hacked the servers of the soft drinks giant and stolen 161GB of data. It also offered the data for sale for more than $64,000, or 1.6467 bitcoin. Stormous did not specify the type of data it stole. Stormous' statement read: "We hacked some of the company's servers and passed a large amount of data inside them without their knowledge and we want to sell it to someone else. You will win and we will win. You will also contact us! We will explain more Good deal, we'll give you the right to pay the amount you want depending on the amount of data you want! Click on the picture to contact us or via our email."... Read the rest by James Coker here: InfoSecurity

How to lock down your Twitter data, or leave, before Musk takes over

By now, most of Twitter's 217 million daily active users have probably heard the news: Elon Musk, the world's richest person, CEO of Tesla and SpaceX and a prolific Internet poster, has reached an agreement to buy the social network for about $44 billion. Twitter employees reacted with shock and dismay Monday as a new reality sank in: Musk, self-proclaimed free speech defender and strong critic of the social network would be the company's new owner. Twitter regulars are wondering what a Musk-owned platform will look like and what it will mean for online harassment, misinformation, democracy and — most of all — their data privacy on the service..
Read the full article by Heather Kelly and Pranshu Verma here: The Washington Post



For Reporting Cyber Crime in the USA go to the Internet Crime Complaint Center (IC3)



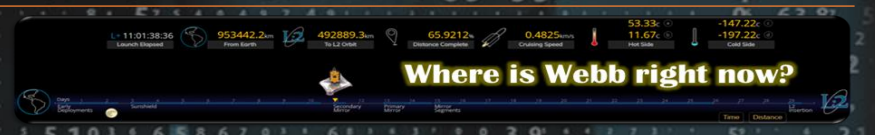
The dangers of Artificial Intelligence (AI) going rogue

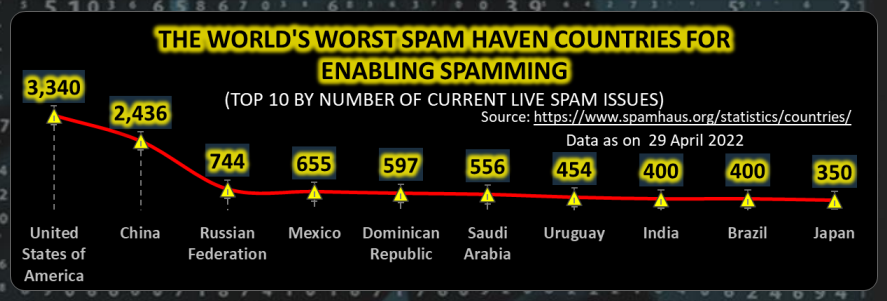
You may think that our planet being taken over by robots and machines in the future is a bit far-fetched or a good subject for an over-imaginative sci-fi movie script. The truth is though, with the rapid advancement of AI and machine learning, AI going rogue is seen by many as a clear and present danger. As we read in the media, even Governments are getting worried as they are speaking of setting up ground rules or treaties to curb the dangers of AI mistakes. They do have reason to be worried though, as AI is well embedded nowadays in military defense systems, autonomous cars, commercial flight controllers, and the list go on endlessly. Below is an extract of a recent article by Eray Eliaçik of Dataconomy that gives us some perspective on the subject..

Brief history and the risks vs. benefits of AI – In **1950**, John McCarthy coined the term "Artificial Intelligence." He added, "Every aspect of learning or any other feature of intelligence may in principle be so precisely described that a machine can be made to mimic it. It will be attempted to discover how to program machines to use language; create abstractions and concepts; solve problems that humans now only solve, and develop themselves."
Artificial Intelligence has developed swiftly since its inception. In recent years, the idea behind AI has been linked to just human-like personalities and robots, even though the concept encompasses everything from autonomous weapons to smartwatches and Google's search engine.
Today's AI is designed to complete more limited functions such as driving a car, performing internet searches, facial recognition, etc. On the other hand, the concept's primary purpose has been to develop a strong AI (or general AI) that can outperform humans in various activities, including everyday ones like solving equations or chess. AI can range from Google's search algorithms to IBM's Watson to automated weapons. Artificial intellect is the most advanced yet of humans' drive to use computers to solve or improve human life. What exactly are these computer systems, and where did they come from? One must inquire about their origins and whether they address the issues that they claim to fix. Are they ethical?
SOME BENEFITS OF AI – (1) Reduction in human error - Because humans make errors from time to time, "human error" was coined. However, if computers are programmed correctly, they do not make these mistakes. Artificial intelligence uses a particular set of algorithms to evaluate previously collected information and decide on an action. As a result, mistakes are reduced, and the possibility of achieving precision with greater accuracy is increased. **(2) Work with high accuracy** - Scientists are attempting to teach AI-powered computers to solve complex calculations and execute crucial operations on their own for the findings obtained to be more precise than those produced by humans. Automatons have become a standard tool for medical professionals across the world. These devices' high accuracy has made them essential in many fields, especially healthcare, due to their importance. Robots are getting better at diagnosing acute diseases in people and performing delicate operations to minimize the risk of human life or going to Mars, defusing a bomb, and more. **(3) Available 24×7** - We've created AI-powered machines capable of carrying out particular repetitive activities at a high rate. Unlike humans, these machines can execute their work with 100% accuracy and 24 hours a day, seven days a week. It eliminates the necessity for two sets of humans working day and night shifts to do other essential chores. The list of benefits is almost endless, but I'll stop at these three for now.
SOME RISKS OF AI - As previously said, the topic has always attracted arguments and debate. Various tech commentators, scientists, and typical individuals are concerned with artificial intelligence. In actuality, the lousy aspect has been represented and addressed in the form of science fiction movies depicting dystopian futures, in which these machines take control of the world and create only havoc. How real could this be, then? Let's look at these negative aspects of artificial intelligence. **(1) Misuse leading to threats** - One problem on the rise as AI is increasingly adopted is AI misuse. With autonomous vehicles and weapons being developed by militaries, this raises the prospect of weapons falling into the hands of the wrong people. **(2) Data discrimination** - AI-powered devices can readily gather, process, and store massive user data. These devices can also gain access to a person's sensitive information without consent. Once the data is stored on the cloud, anyone may view it lawfully or illegally. **(3) A future threat to humanity** - Elon Musk is regarded as one of the sharpest people working on AI. He also stated that AI is the greatest danger to human civilization in future generations. This implies that the dystopian future depicted in science fiction films isn't out of reach. Stephen Hawking has voiced his opposition to AI development on numerous occasions before. The most serious danger of AI is that machines would achieve sentience and rebel against people if they go rogue.
HOW CAN AI BE DANGEROUS? - Many experts believe that a superhuman AI would not be capable of human emotions such as love or hate, and that AI will not become purposefully good or evil. Instead, when considering how AI might endanger humanity, experts favor **two possibilities**: **(1) The AI is programmed to do something devastating** - Autonomous weapons are programmed to kill humans. These weapons could easily result in large fatalities in the hands of the wrong person. Furthermore, an AI arms race might inadvertently lead to an AI war that causes massive deaths. To avoid being outsmarted by the opponent, these weapons would be complicated to simply "turn off," thus giving humans a chance of losing control of such a scenario. This danger is already there with little AI but grows as AI intelligence, and autonomy levels grow. **(2) The AI is programmed to do something beneficial, but it develops a destructive method for achieving its goal** - When we don't fully align the AI's objectives with our own, it becomes complicated. It might bring you to the airport pursued by helicopters and covered in puke, doing not what you wanted but what you instructed it to do. If a super-intelligent system is put in charge of a large geoengineering project, it may wreak havoc on our ecosystem, seeing human attempts to prevent it as a danger to be overcome.
CONCLUSION - Artificial Intelligence has two sides, just like everything else in the world. There are risks and benefits of artificial intelligence. The development of AI-powered automation has undoubtedly improved our lives in many settings today. However, there is a need to strongly advocate for the formation of ethical rules and regulations to reduce risks associated with AI as much as possible.
That is all I have space for in this post; please visit the Dataconomy site to read the full article that hails much more information.

Other Interesting News and Cyber Security bits:

- China aiming to alter 'potentially hazardous' asteroid path by 2025
- Inside China's plot to find 'Earth 2.0' within Milky Way with planet-hunting probe
- The U.S. and China Need Ground Rules for AI Dangers?
- SANS Daily Network Security Podcast (Storm cast)





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