On May 12, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). Last Advisory 09 Jun 2021 Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution .

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
11 June	175,594,378	3,787,969

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

11 June 2021

In The News This Week

Evil Corp Impersonates PayloadBin Group to Avoid Federal Sanctions

The cybercriminals try to pin new ransomware on Babuk Locker in an effort to fly under the radar of an ongoing FBI investigation. - The criminal group Evil Corp is trying to mask its latest activity by using previously unknown ransomware called PayloadBin, according to researchers. The move is believed to be an attempt to confuse law enforcement and avoid sanctions imposed by the U.S. federal government against entities it believes are linked to Evil Corp, according to published reports. Evil Corp, widely associated with the info-stealing Dridex malware, has been the target of a crackdown by U.S. authorities since 2019. As part of that effort, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) imposed sanctions against anyone or organization it believes has ties with the criminal enterprise. This action effectively prevents ransomware negotiation firms from facilitating ransom payments with Evil Corp, which limits its ability to profit from criminal activity.
Read the full story here: ThreatPost

Hong Kong to censor movies for national security breaches

New rules to determine the suitability of movies planned for public exhibition - Hong Kong is instructing censors to ban any movie that could be seen as endorsing activities that would contravene the national security law imposed by China last year, the latest curb on freedom of expression in the Asian financial hub. On Friday, Hong Kong said it was amending guidelines under the Film Censorship Ordinance to consider the security law, which bars subversion, terrorism, secession and collusion with foreign forces. The rules will determine the suitability of movies planned for public exhibition in the city. Read the rest of the story here: BusinessDay

JBS Foods cyber attack highlights need for more local processing capacity

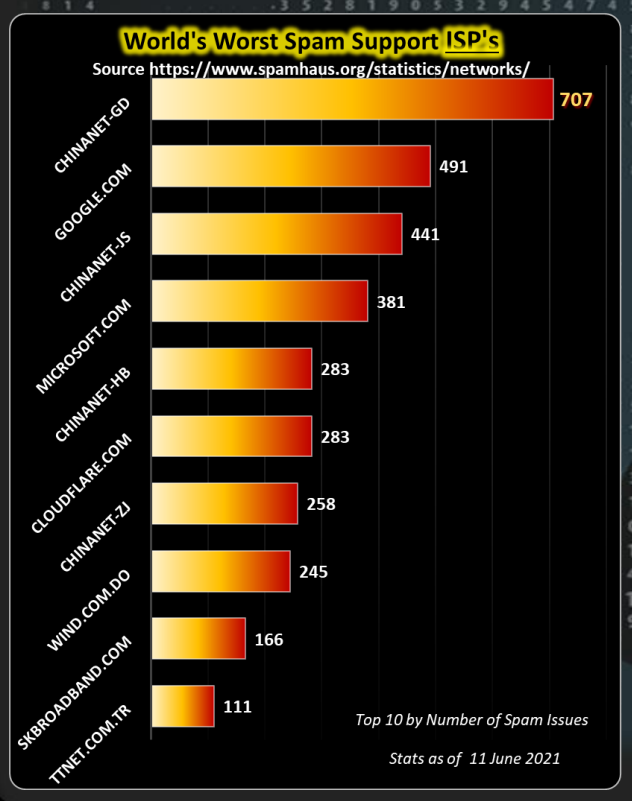
Brazilian-owned JBS Foods was hit with a ransomware attack recently that shuttered a number of the international conglomerates' processing facilities. Fortunately the company was able to resume operations within a few days. JBS controls 25% of the meat processing in the U.S. so a prolonged shutdown can have far-reaching impacts on producers. Since the disruption was brief, it won't likely impact Wyoming producers, said Jim Magagna, executive vice president for the Wyoming Stockgrowers Association. "I don't want to say it can't have an impact, but it doesn't look likely," Magagna said. However, Magagna said the issue highlights the problem of having 80% of America's processing capacity controlled by four large conglomerates, of which JBS is one. During last year's COVID-19 pandemic, a number of meat processing facilities were shut down, creating problems for meat producers who couldn't get their livestock to market. Read the article by Kevin Killough here: Powell Tribune

Cost of Redcar Council cyber-attack over-estimated

A council left without online services for weeks following a cyber-attack over-estimated the cost of the incident, it has been revealed. Redcar and Cleveland Council initially put the figure at £10.4m after its computers and website were targeted in February last year. However, following a financial impact assessment it has been reduced to £8.7m. Staffing and IT costs were lower than expected, the council said. A briefing note to council members said the task of quantifying the financial impact had been difficult, according to the Local Democracy Reporting Service. It added early estimates were "predicted on worst-case scenarios". The hack left about 135,000 people without online access to public services and frontline council staff resorted to using pens and paper.
Read the story here: BBC News

Coronavirus: Germany fights trade in fake Covid vaccine certificates

German police force has set up a special team to combat a growing black market in forged vaccine certificates. Police in Cologne told the broadcaster ARD that fraudsters were communicating via an encrypted messenger service which makes investigations difficult. They are still trying to determine the scale of the problem nationally. Some people are duped into paying about €100 (£86; $122), then get nothing. Read story here: BBC News



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

Lets talk about Fuzzy Logic and AI

In the media, we read about the constant and ever-going battle between the Cyber Security fraternity and hacker groups, the one to build the best defences and the other to break those defences down as fast as they can. The defences that the security fraternity put out there are ever-evolving as the threats are ramping up in the cyber world. On the technology side, the changes are rapid as knowledge is gained exponentially and demands are growing at a stupid rate due to technology innovations that bring about endless possibilities. But, endless possibilities bring about enormous challenges to keep our cyber world safe and secure. Now, this is where Artificial Intelligence (AI) comes into play. The challenge Security firms are facing when developing AI solutions is the uncertainty factor that goes with all these possibilities. Nothing is just a simple yes or no when possible threat avenues and actors are analysed. As humans, making a decision is sometimes based on what we call a "gut feel", as the information presented to us is vague and not clear. An Artificial Intelligence machine or system does not have a "gut feel" and scientists had to figure out how to compensate for that and they came up with something called "Fuzzy Logic". The term fuzzy logic was first used by Berkeley professor Lotfi Zadeh in 1965 when he observed that conventional computer logic was not capable of manipulating data representing subjective or unclear (fuzzy) human ideas.

What is Fuzzy Logic?

Zadeh, observed that, unlike computers, human decision making includes a range of possibilities between YES and NO, such as:

(1) CERTAINLY YES **(2)** POSSIBLY YES **(3)** CANNOT SAY **(4)** POSSIBLY NO **(5)** CERTAINLY NO

Wikipedia describes it as follows: In logic, fuzzy logic is a form of many-valued logic in which the truth value of variables may be any real number between 0 and 1 both inclusive. It is employed to handle the concept of partial truth, where the truth value may range between completely true and completely false.[1] By contrast, in Boolean logic, the truth values of variables may only be the integer values 0 or 1.

Kechit Goyal gave this example in the upGrad Blog:

Problem – Is it hot outside?

Boolean Logic - Solution -
- Yes (1.0)
- No (0)

According to conventional Boolean Logic, the algorithm will take a definite input and produce a precise result Yes or No. This is represented by 0 and 1, respectively.

Fuzzy Logic - Solution
- Very hot (0.9)
- Little hot (0.20)
- Moderately hot (0.35)
- Not hot (1.0)

As per the above example, Fuzzy Logic has a wider range of outputs, such as very hot, moderately hot and not hot. These values between 0 and 1 display the range of possibilities.

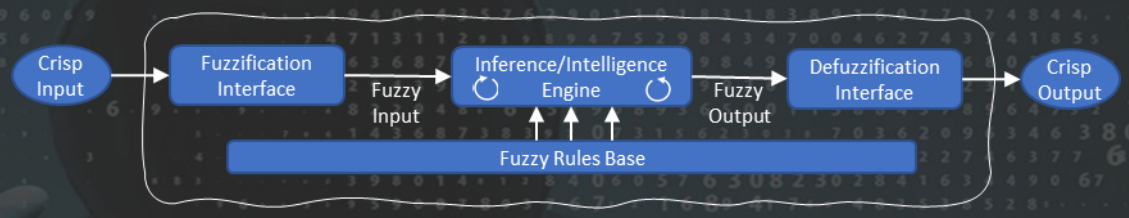
Why Fuzzy Logic for Cyber Security?

Fuzzy logic helps to deal with the uncertainty of how a threat will culminate in a given landscape with many variables.

How it works (High-Level description)

The Fuzzy Logic Systems Architecture has four main parts:

- Fuzzification Interface – It transforms the system inputs, which are crisp numbers (Crisp Input), into fuzzy sets. It splits the input signal into five steps such as –
  LP x is Large Positive MP x is Medium Positive S x is Small MN x is Medium Negative LN x is Large Negative
- Knowledge/Rule Base – It stores IF-THEN rules provided by experts.
- Inference/Intelligence Engine – It simulates the human reasoning process by making fuzzy inference on the inputs and IF-THEN rules.
- Defuzzification Interface – It transforms the fuzzy set obtained by the inference engine into a crisp value. (Crisp Output)

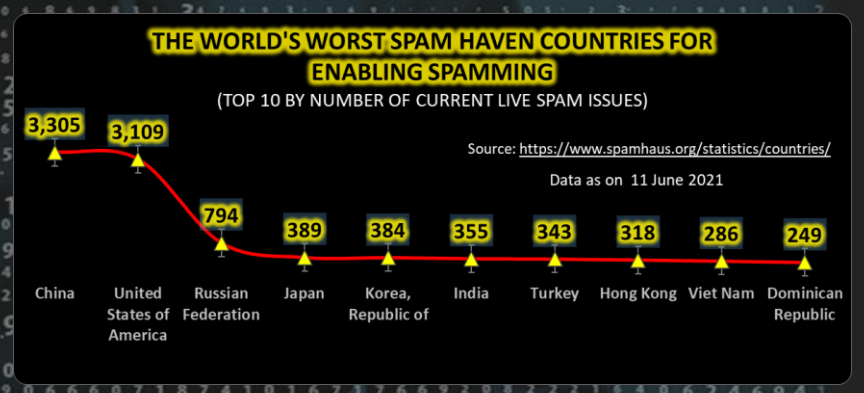


There is much more to say about fuzzy logic systems and AI and how the concepts are used in the Cybersecurity space but space is limited in this bulletin, so please, if this is of interest to you, click on the reference links below and delve deeper.

References: Tutorialspoint, Guru99, upGrad, Nanonets, Security Boulevard, Brighterion

Other Interesting News and Cyber Security bits:

- 2021: The Evolution of Ransomware – Free eBook
- This is how fast a password leaked on the web will be tested out by hackers
- The rise of cybersecurity debt



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