On March 9, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla, Linux, Google, and Microsoft products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
11 Mar 22	453,833,910	6,052,190

Deaths this week: 49,159

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 March 2022

In The News This Week

89% of global cyberattacks are aimed at Russia or Ukraine

Following Russia's invasion of Ukraine, both countries became lucrative targets for state-sponsored and individual hackers. As such, Anonymous declared war on Russia while the Conti ransomware group sided with Putin. "The battles in the digital world can have a significant impact on communications and propaganda distribution on both sides," the report by Atlas VPN suggests. 70% of cyberattacks targeted Russia, with 5 billion incidents registered since March 5. Ukraine was targeted only in 19% of the cases, followed by the US (5%.) Although the US is usually the top target for threat actors, its popularity among cybercriminals has seemingly been overshadowed by recent events. Based on the data from Imperva Daily Cyber Threat Attack Map statistics, Distributed Denial-of-Service (DDoS) attacks accounted for 90% of all incidents, causing severe disruption with a wave of bots. Automated threats came second, accounting for 7% of cyberattacks, followed by the Open Web Application Security Project (OWASP) attacks (3%.) Not all industries were targeted equally. As such, the financial services sector was most of interest to malicious hackers. Banks and financial institutions were targeted in 72% of the cases globally. These attacks took place both in Ukraine and Russia in hopes of disrupting routine operations or blocking access to funds.
Read the rest of the story by Anna Zhadan here: Cybernews

Russian Pushing New State-run TLS Certificate Authority to Deal With Sanctions

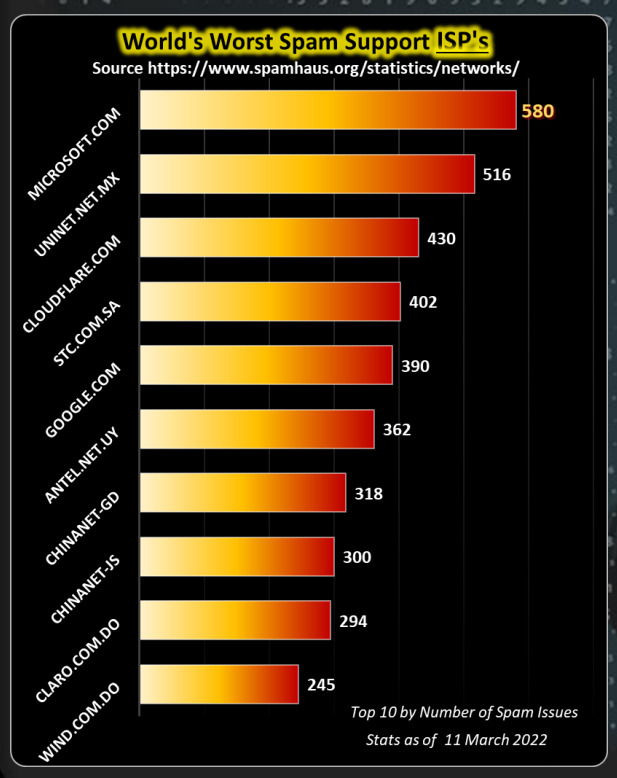
The Russian government has established its own TLS certificate authority (CA) to address issues with accessing websites that have arisen in the wake of sanctions imposed by the west following the country's unprovoked military invasion of Ukraine. According to a message posted on the Gosuslugi public services portal, the Ministry of Digital Development is expected to provide a domestic replacement to handle the issuance and renewal of TLS certificates should they get revoked or expired. The service is offered to all legal entities operating in Russia, with the certificates delivered to site owners upon request within 5 working days. TLS certificates are used to digitally bind a cryptographic key to an organization's details, enabling web browsers to confirm the domain's authenticity and ensure that the communication between a client computer and the target website is secure…
Read the rest of the story by Ravie Lakshmanan here: The Hacker News

Insurers checking their war exclusions for cyberattacks

While cyberattacks have increased since Russia invaded Ukraine and numerous countries responded with tighter sanctions, most of those attacks have been more basic distributed denial-of service attacks on both sides of the conflict, said a DBRS Morningstar commentary on cyber warfare's potential impact on North American and European insurers. "Although acts of war (declared or not) are typically excluded from cyber insurance policies," said Marcos Alvarez, senior vice president and head of insurance at DBRS Morningstar, "the current conflict could potentially increase cyber-related insurance and reinsurance claims in Europe and North America, as attribution can be very difficult to determine in cyber incidents." He added it's expected "that insurers and reinsurers will continue to clarify their cyber war exclusions to face the new realities of state-sponsored cyberattacks.".
Read the rest of the article here: Canadian Underwriter

Ukrainian Hacker Linked to REvil Ransomware Group in US Court after Extradition

Yaroslav Vasinskyi, a Ukrainian national tied to the Russian REvil ransomware group, has been extradited to the US to face charges over his role in file-encrypting cyberattacks against multiple companies. The alleged hacker was arrested in Poland in October 2021 when authorities cracked down on REvil affiliates and recovered $6 million extorted from ransomware victims. Vasinskyi appeared before a US court yesterday after being extradited on March 3. The US Department of Justice (DoJ) pressed multiple charges, including damage to protected computers, conspiracy to commit computer fraud, and money laundering. Vasinskyi had his charges formally read in the Northern District of Texas after being moved to Dallas on March 3. If found guilty of all charges, he could face a total of 115 years in prison.. Read more here: Bitdefender



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

Nuclear, autonomous and cyber weapons: how technology contributes to warfare

With the Russian invasion of Ukraine still in the forefront of the news, everybody and their cousins are writing about it and sharing their opinions. The newsrooms are flooded with stories and articles and in many cases duplications, which makes it difficult to know where to pause and read and what to skip. But, working through the masses of articles, I came across an interesting article by Sara Ibrahim of SWI giving us a rundown and comparison of Nuclear and Cyber weapons from a Swiss perspective. Below then is an extract of her article, but please visit the article site at SWI to get the full story and other related information.

Nuclear, autonomous and cyber weapons – A Swiss perspective

Warfare in 2022 means arsenals far more sophisticated than they used to be, made up of powerful nuclear weapons, lethal autonomous weapons guided by artificial intelligence, and digital weapons to be dropped on the internet – where not even Switzerland is safe. Russian President Vladimir Putin has reminded the world that nuclear weapons exist and that they could still be used. In the long period of peace and prosperity in Europe after the end of the Second World War, the risk of nuclear conflict remained in the recesses of our minds, and was revived only for a moment during the Cold War before sinking again into oblivion. However, throughout all these years of "nuclear silence", technology has been evolving, and nuclear weapons are now even more lethal and dangerous than before. Today, in fact, they are more compact, precise and powerful than those dropped on Hiroshima and Nagasaki. Some of the warheads in Putin's hands are 50 times more destructive than those used in 1945. And while the force of the bomb dropped on Hiroshima was 14-15 kilotonnes (between fourteen and fifteen thousand tonnes of TNT), China now has bombs in the order of megatonnes (millions of tonnes of TNT).

In a recent article, I analysed the state of nuclear weapons and what a nuclear war would look like with the help of Stephen Herzog and Alexander Bollfrass, two researchers from the Centre for Security Studies at ETH Zurich, which specialises in Swiss and international security policy. Alarm bells always ring too late - Herzog and Bollfrass also made me think about another point. The nuclear threat is a bit like the pandemic: everyone knows that it might come, but nobody does anything about it until it does. That's what happened with the Covid-19 pandemic, and it's happening with the danger of nuclear war.
"I think people should not only worry about nuclear weapons when there is a crisis," Herzog told me. "What would happen to the world if Russia used nuclear weapons? We are literally talking about the potential destruction of entire cities in Europe and the effects of radioactive fallout…" After all, who among us has ever really thought – until now – about the real repercussions of a nuclear war and the fact that cities could be razed to the ground in a matter of minutes? Why aren't there more protests against nuclear weapons like in the 1980s.

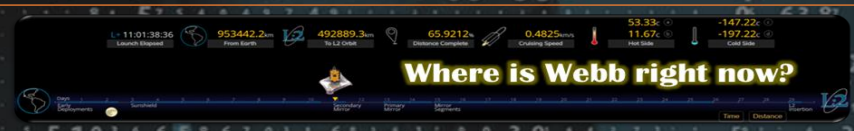
Lethal weapons, enhanced by AI - It would be wrong, however, to think of nuclear weapons as the only threat to humanity and world order: we also shouldn't forget the advances in military innovation made possible by artificial intelligence (AI).
We used to think of hyper-technological weapons in science fiction terms, imagining killer robots like Arnold Schwarzenegger in Terminator, only possible on the big screen. But we were wrong. Stuart Russell, a well-known British computer scientist and a professor at the University of California, Berkeley, explained why in a recent podcast: these weapons are not science fiction, they really exist and they are available for use in warfare.
Moreover, they are not robots that fire bullets randomly, but rather autonomous systems that can find, choose and eliminate – without human supervision. In future, Russell believes, we will see "smart" lethal weapons which are smaller, cheaper and more agile than a tank, an attack helicopter or an armed soldier.
Of course, using AI allows for more precise attacks and the reduction of collateral damage and civilian casualties, claim those who support this technology, especially the US and Russia. But on the other hand we have to ask to what extent these algorithms, which decide in a cold and calculated way who to kill and who to spare, can lead to the escalation of armed conflicts – and at what cost to humanity.

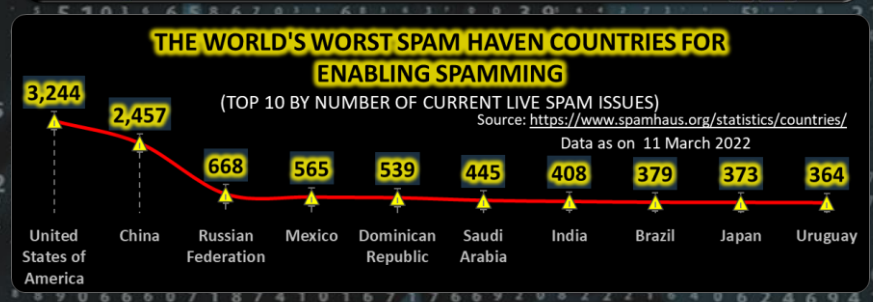
The other question concerns the intelligence of the AI models which drive these autonomous systems: are they capable of discernment? Where does responsibility lie? A research team at the Idiap research institute in Switzerland, which specialises in artificial and cognitive intelligence, made me think of a key point: there is no intelligence behind artificial intelligence, because no AI system can properly mirror human thought, nor demonstrate a capacity for reasoning and common sense equal to that of humans. Is it therefore moral that algorithms hold such lethal power over us?

Geneva fears cyberwarfare - If Switzerland has less to fear from a direct military offensive, because of its neutrality, the same cannot be said of cyber-attacks. We already discussed this in a previous newsletter, but as the war in Ukraine goes on, the issue remains open – not least because cyber-attacks in Switzerland have been increasing significantly. In 2021, 65% more attacks were recorded than in 2020, and this year an all-time peak was reached in the second week of January.
Because of Geneva's decisive role on the international geopolitical scene, many important NGOs based there are considering how to increase the level of digital security and protect themselves against a potential cyber war. The UN refugee agency for example, the UNHCR, is particularly wary due to the support it is currently providing to those fleeing Ukraine.
However, what is really lacking to strengthen the "digital shield" of International Geneva is first and foremost a qualified workforce: even in Switzerland, there is a shortage of cyber security experts. Globally, this deficit amounts to some three million cyber professionals, according to a report by the World Economic Forum.
Read the article here: SWI

Other Interesting News and Cyber Security bits:

- Global Risks Report 2022 – World Economic Forum
- For those who missed the war declaration of Anonymous, see the video here
- Good book to read – HACKING THE BOMB, by Andrew Futter
- SANS Daily Network Security Podcast (Storm cast)





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