On May 5, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded).

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
07-May	156,669,821	3,268,949

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

07 May 2021

In The News This Week

South Africa - Virgin Active hit by 'sophisticated' cyberattack

Gyms group Virgin Active has fallen victim to a cyberattack. The company posted a notice on its website late on Friday warning clients that its systems have been compromised. "Virgin Active South Africa became aware of a cyberattack yesterday and our security teams immediately started working with cybersecurity experts to carefully contain, manage and investigate the cyber event," the company said in a notice posted on its website.
"While we take the necessary steps to protect data, we have been targeted by sophisticated cybercriminals. As a precautionary measure, we have taken all systems offline while we resolve this. Our clubs are operating as normal and we sincerely apologise for any inconvenience while we address this event.". Read the story here: TechCentral

Deepfake Attacks Are About to Surge, Experts Warn

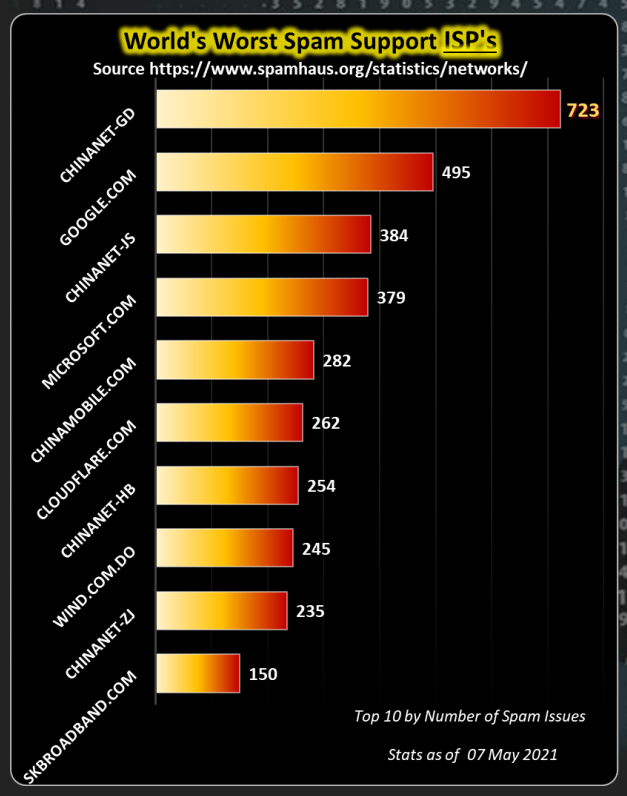
New deepfake products and services are cropping up across the Dark Web. - Artificial intelligence and the rise of deepfake technology is something cybersecurity researchers have cautioned about for years and now it's officially arrived. Cybercriminals are increasingly sharing, developing and deploying deepfake technologies to bypass biometric security protections, and in crimes including blackmail, identity theft, social engineering-based attacks and more, experts warn. Time to get those cybersecurity defences ready. A drastic uptick in deepfake technology and service offerings across the Dark Web is the first sign a new wave of fraud is just about to crash in, according to a new report from Recorded Future, which ominously predicted that deepfakes are on the rise among threat actors with an enormous range of goals and interests. Read the rest of the story by Becky Bracken: ThreatPost

Cymulate nabs $45M to test and improve cybersecurity defenses via attack simulations

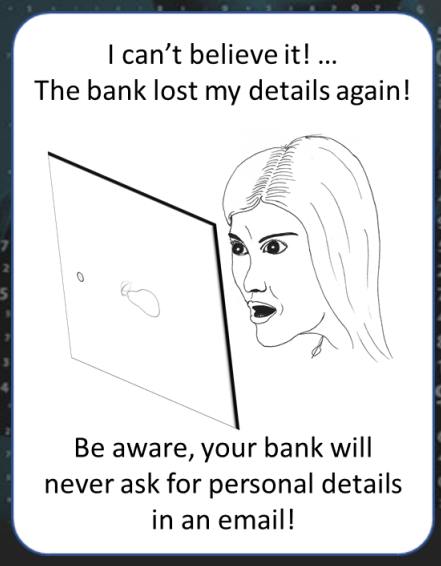
With cybercrime on course to be a $6 trillion problem this year, organizations are throwing ever more resources at the issue to avoid being a target. Now, a start-up that's built a platform to help them stress-test the investments that they have made into their security IT is announcing some funding on the back of strong demand from the market for its tools. Cymulate, which lets organizations and their partners run machine-based attack simulations on their networks to determine vulnerabilities and then automatically receive guidance around how to fix what is not working well enough, has picked up $45 million, funding that the start-up — co-headquartered in Israel and New York — will be using to continue investing in its platform and to ramp up its operations after doubling its revenues last year on the back of a customer list that now numbers 300 large enterprises and mid-market companies, including the Euronext stock exchange network as well as service providers such as NTT and Telit.
Read the full story here: TechCruch

Cyber-Attack on Belgian Parliament

A coordinated cyber-attack has been carried out against Belgium's parliament, scientific institutions, police services, and universities. Internet service provider Belnet, which serves the country's government agencies, fell victim to what it described as a "large-scale attack" on Tuesday. At around 11:00am CEST, the company was hit by a distributed denial of service (DDoS) attack that overloaded its servers, preventing the availability of online services. Websites with .be domains were impacted. As a result of the hack, around 200 Belnet customers lost internet access, either partially or totally. News outlet VRT was among the organizations affected. "The attack is still in progress and takes place in successive waves," Belnet said in an update on Wednesday morning. "Our teams are working hard to mitigate them. We are constantly monitoring our network to counter any new attempts."
Belnet said that no data had been stolen or exfiltrated during the attack and that no personal information had been compromised. Some websites, including the official site of the City of Brussels, remain down, while others, including the site for the Brussels Police, are back online. The attack disrupted the workings of the Belgian parliament, causing several meetings to be postponed. Distance learning at some universities and colleges was impacted by unstable connections. Read the full story by Sarah Coble here: InfoSecurity Magazine



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



What is the difference between IT, OT, ICS, and IoT

I attended the Cyber Security for Critical Assets World event this week and listening to or reading the comments throughout the day, I realised that there is still some ignorance around the differences between IT, OT, ICS, and IoT and where it all fits in. (Thanks to the organisers of the event, by the way, it was a well-presented event and I thoroughly enjoyed it). So I thought it will be a good idea to bring the topic up in the bulletin today.

What is Information Technology?

Most of us are familiar with Information Technology (IT), which refers to anything related to computer technology, including hardware, software, and communications technologies. Your email, the Internet, and applications (Apps) that you run relies on IT. IT is less common in industrial settings, but often constitutes the technological backbone of most organizations and companies. IT devices and programs have little autonomy, have a limited lifespan (Normally between 1 and 3 years), and are updated frequently. Access to IT programs and connected devices are typically less restricted than to OT devices, and many, if not all, employees at a given organization may be granted access. In a broader sense, IT is defined by its programmable capacity. That is, while certain technologies are designed to perform a static set of functions (like a water pump or a piston), IT can be adjusted, augmented, and re-programmed in countless ways to fit the evolving networks, applications, and user needs.

What is Operational Technology?

Operational technology (OT) refers to the hardware and software used to change, monitor, or control physical devices, processes, and events within a company or organization that typically operates in the industrial space. This form of technology is most commonly used in industrial settings, and the devices in an OT setup typically have more autonomy than information technology devices or programs.
Examples of OT include **SCADA** (Supervisory Control and Data Acquisition), which is used to gather and analyze data in real-time and is often used to monitor or control plant equipment. Industries such as telecommunications, waste control, water control, mining, and oil and gas refining rely heavily on SCADA systems.
Many types of OT rely on devices such as **PLC**s (Programmable Logic Controllers), which receive information from input devices or sensors, process the data, and perform specific tasks or output specific information based on pre-programmed parameters. PLCs are often used to do things like monitor machine productivity, track operating temperatures, and automatically stop or start processes. They are also often used to trigger alarms if a machine malfunctions.
Access to OT devices is typically restricted to a small pool of highly trained individuals within an organization, and these types of devices may not be updated or changed for months or even years. Since these devices are highly specialized, they rarely run on standardized operating systems (like iOS or Windows), and instead, generally, require custom software to function.

The main difference between OT and IT devices is that OT devices control the physical world, while IT systems manage data.

What are Industrial Control Systems?

Industrial control systems (ICS) are a type of OT and consist of any systems that are used to monitor or control industrial processes. This could include a mining site's conveyor belt or an alarm that lets employees know if a piece of equipment is getting dangerously close to overheating.
ICSs are often managed by SCADA systems, which may provide users with a graphical user interface. This interface allows the user to observe the system's current status, enter system adjustments to manage the process, and observe any alarms that indicate something is wrong.

What is "The Internet of Things"?

The Internet of Things (IoT) refers to a system of interrelated, internet-connected physical objects that are able to collect and transfer data over a wireless network without human intervention. Other than OT systems that also refer to physical objects that are connected and interact in an industrial environment, IoT is more focused on a consumer/commercial environment. IoT technology is typically used in automated systems to make life easier for individuals or to protect their stuff, making use of the already present wireless Internet network. IoT gives people the ability to monitor or control physical objects through the Internet where distance is eliminated as a factor.
We do see however, a convergence in IoT and OT technology in certain areas as the convenience of managing physical industrial devices from an off-site location anywhere in the world, become more appealing. This however comes with a greater cyber risk factor and typically means tighter cybersecurity controls which come at a cost.

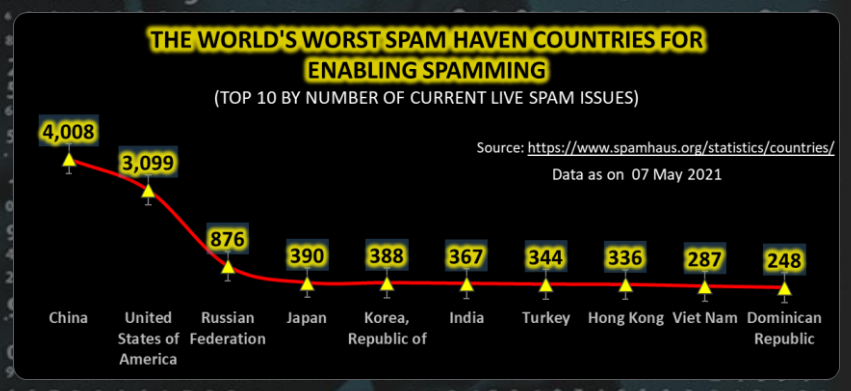
Can you Intermix Operational & Information Technology with Industrial Control Systems?

At first glance, IT and OT may not seem compatible. OT systems are isolated and self-contained, designed to run autonomously, and rely on proprietary software. On the other hand, IT systems are connected by nature, have little autonomy, and generally run using readily available operating systems. However, incorporating IT into your OT operations can have many benefits. In the past, most OT devices were utterly cut off from not only the internet but even most internal networks, and could only physically be accessed by a select few authorized employees. However, it's becoming increasingly common (as mentioned for IoT) for OT systems (including ICSs) to be monitored and controlled using IT systems. While inputs on many OT devices may have traditionally been limited to a physical panel or keypad that required workers to input commands or data physically, more and more OT systems and devices are now being controlled and monitored remotely via the internet.

References: VirtualArmour, Coolfire Solutions, ISA, Tripwire

Other Interesting News and Cyber Security bits:

- Cybersecurity 101: The Difference Between IT and OT Attacks
- Spy bosses warn of cyber-attacks on smart cities
- Apple introduces AirTag - AirTag is a small device that enables iPhone users to securely locate and keep track of their valuables using the Find My app.



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