On January 12, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in WordPress, Microsoft, Mozilla, Adobe, and Citrix products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
14 Jan	320,988,645	5,539,421

Deaths this week: 47,997

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
14 January 2022

In The News This Week

Hacking group accidentally infects itself with Remote Access Trojan horse

Patchwork, an Indian hacking group also known by such bizarre names as Hangover Group, Dropping Elephant, Chinastrats, and Monsoon, has proven the old adage that to err is human, but to really cock things up you need to be a cybercriminal. The hackers, who have become notorious for launching spear phishing attacks against Pakistani institutions, managed to infect themselves with their own Remote Access Trojan (RAT) in January, according to experts at Malwarebytes. In a blog post, security researchers at Malwarebytes describes how it found a new variant of the BADNEWS RAT (which it dubbed Ragnatela) being launched via spear phishing emails which pretended to come from the Pakistani authorities. Investigations by the researchers uncovered that a number of Pakistani institutions had been successfully compromised by the RAT. However, it was also discovered that the hacking group had managed to also infect its own development machine, and the RAT had captured the criminals' own keystrokes alongside screenshots of their own computers…
Read the rest of the story by Graham Cluley here: Cluley

Faking an iPhone Reboot

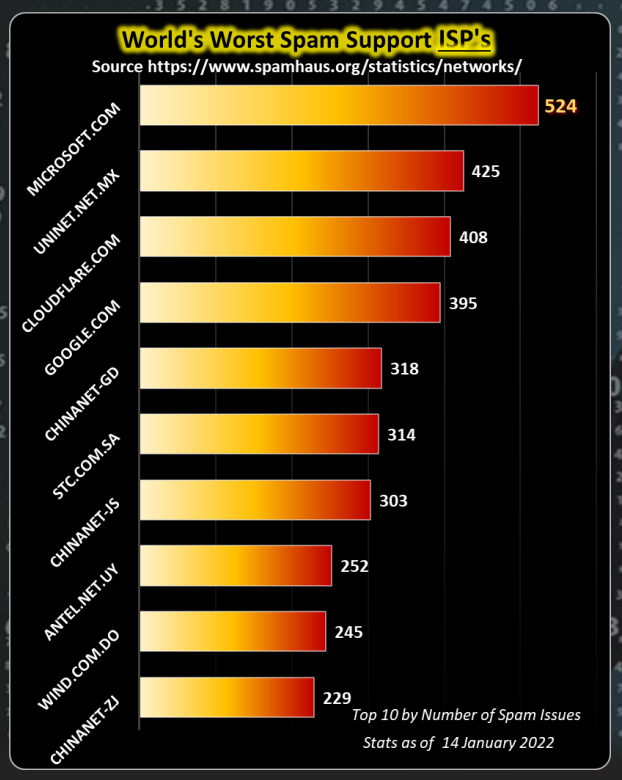
Researchers have figured how to intercept and fake an iPhone reboot: We'll dissect the iOS system and show how it's possible to alter a shutdown event, tricking a user that got infected into thinking that the phone has been powered off, but in fact, it's still running. The "NoReboot" approach simulates a real shutdown. The user cannot feel a difference between a real shutdown and a "fake shutdown." There is no user-interface or any button feedback until the user turns the phone back "on." It's a complicated hack, but it works.
Historically, when malware infects an iOS device, it can be removed simply by restarting the device, which clears the malware from memory. However, this technique hooks the shutdown and reboot routines to prevent them from ever happening, allowing malware to achieve persistence as the device is never actually turned off.
Read Bruce Schneier's blog here : Schneier .. See simulation

North Korea hackers stole $400m of cryptocurrency in 2021, report says

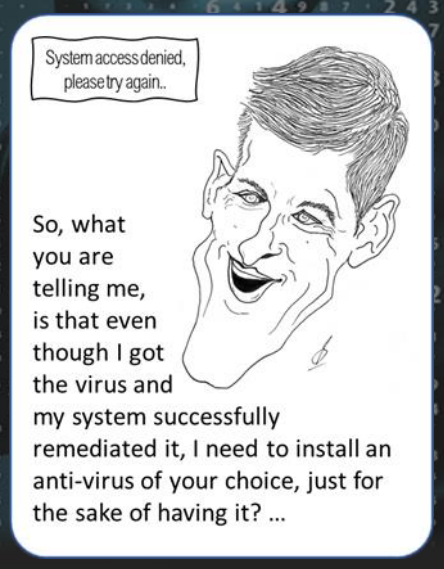
North Korean hackers stole almost $400m (£291m) worth of digital assets in at least seven attacks on cryptocurrency platforms last year, a report claims. Blockchain analysis company Chainalysis said it was one of most successful years on record for cyber-criminals in the closed east Asian state. The attacks mainly targeted investment firms and centralised exchanges. North Korea has routinely denied being involved in hack attacks attributed to them. "From 2020 to 2021, the number of North Korean-linked hacks jumped from four to seven, and the value extracted from these hacks grew by 40%," Chainalysis said in a report. The hackers used a number of techniques, including phishing lures, code exploits and malware to siphon funds from the organisations' "hot" wallets and then moved them into North Korea-controlled addresses, the company said..
Read the rest of the story here: Yahoo News

U.K. Hacker Jailed for Spying on Children and Downloading Indecent Images

A man from the U.K. city of Nottingham has been sentenced to more than two years in prison for illegally breaking into the phones and computers of a number of victims, including women and children, to spy on them and amass a collection of indecent images. Robert Davies, 32, is said to have purchased an arsenal of cyber crime tools in 2019, including crypters and remote administration tools (RATs), which can be used as a backdoor to steal personal information and conduct surveillance through microphones and cameras, catching the attention of the U.K. National Crime Agency (NCA). The cyber voyeur's modus operandi involved catfishing potential targets by using fake profiles on different messaging apps such as Skype, leveraging the online encounters to send rogue links hosting the malware through the chats. "Davies was infecting his victims' phones or computers with malicious software by disguising it with the crypters so their antivirus protection would not detect it," the NCA said in a statement. "He then used the RATs to gain remote access to their devices and steal any sexual images (mainly of females) they had stored on there." At least in one instance, Davies spied on a teenage girl via a hacked webcam. Officials said a total of 27 compromising images and videos of children were found on his computer, with over 30 victims identified over the course of the investigation.. Read the rest of the article here: The Hacker News



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



Cyber Security for OT Systems, what does the future hold?

OT systems generally refer to the "Operational Technology" systems used in the industrial world. It is typically used in manufacturing plants, mines, airports, and so on, to monitor and control machinery, robotic functions, building management, and security systems. Traditionally these were isolated and autonomous systems that can only be accessed if you have physical access to the isolated network. That is largely not the case anymore as technology and internet advances made it possible to access and manipulate these systems from anywhere in the world through the Internet, provided that you have the access credentials. As we look back over the last few years, we have seen how more and more OT systems became part of the larger IoT (Internet of Things) concept.
OT and IoT are generally mentioned separately, but there is an enormous overlap and the dividing line is getting more blurry as we go along. IoT Systems, on the other hand, are generally focused on domestic automation and monitoring systems which include home surveillance and security systems. Both of these systems however rely on Internet access to function as intended. And this is where Cybersecurity comes into play as the pessimistic or even cynical Cybersecurity practitioners believe that if you can see the Internet, those on the Internet can see you. Thus, if your system is accessible through the Internet, it is hackable.

The Challenges

As quoted in the CPO Magazine - "*Cybersecurity has quickly become a top challenge for manufacturers and industrial services around the world. According to a September 2021 survey of manufacturing executives, 61 percent identify cybersecurity as a "high/very high priority." These challenges are especially pronounced as manufacturers turn to remote and hybrid teams to attract and retain top talent while maintaining operational continuity. As a result, manufacturers are introducing remote operations capacity for OT systems, allowing employees, contractors, and trusted third parties to operate on-site infrastructure from anywhere in the world*".
To add to the complexity of securing OT systems, Its interface with Industrial Control Systems (ICS) in critical infrastructures makes it particularly sensitive to outside interference, and simply putting a firewall in place would not necessarily solve the problem. A real-life example of what can happen is the attack on the Florida Oldsmar water-treatment facility in February last year. A hacker gained remote access to the control systems and changed the level of sodium hydroxide in the water from 100 parts per million to 11,100 parts per million, effectively poisoning the area's drinking water. Luckily, in this case, the plant supervisor picked it up in time and changed it back immediately, but can you imagine the consequence if he didn't. This kind of attack has tangible life and limb consequences if launched successfully. Just think if this guy hacked a Nuclear Power Station and changed some settings… Chernobyl all over again! Other examples include the cyberattacks on Molson Coors Beverage Co. in March last year and the famous hack on meat supplier JBS in June that rendered plants to a standstill in several countries, including the USA, Canada and Australia.
The original design of OT systems did not pay much attention to the broader sense of cyber security as it was designed to be on an isolated network accessible only if you have physical access to the environment. To take advantage of modern remote control technology, however, in many cases, these systems were not redesigned to address Cybersecurity but rather modified or adapted with plugins or program interfaces to interact with the regular Information Technology (IT) infrastructure. These modified systems are often wide open for an attack as it does not generally fall in the scope of the IT network cyber defenses. Hackers look at IT, OT, and IoT devices as a single continuous system, and I believe that the Industrial Industry has to take the same approach. Hackers don't care where they get in, as long as they get in.

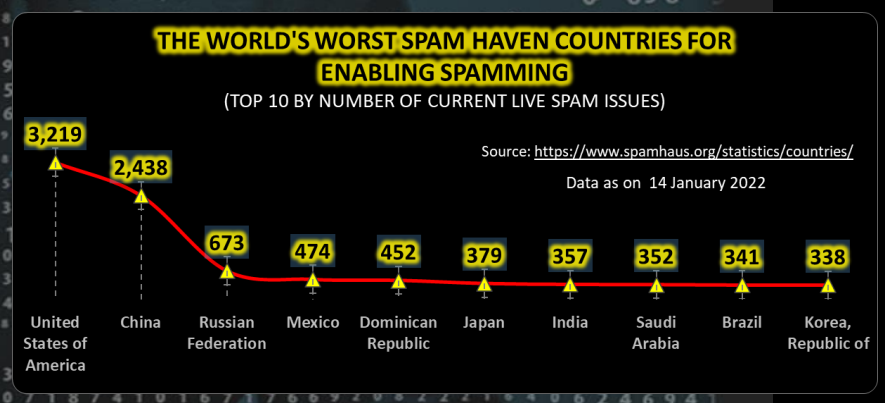
What needs to be done

As mentioned above, Cybersecurity for IT, OT, and IoT devices need to be addressed holistically as a single continuous system or network. Cyber security practitioners and vendors are heavily campaigning for changes and redesigns all over the place and even Governments are revisiting Critical Infrastructure Protection laws to include a much stronger emphasis on Cyber Security.
Most countries have had Critical Infrastructure Protection laws and regulations in place for more than a decade, but the picture has changed dramatically over the last 10 years and if they haven't revisited or amended it yet, they need to make it a top priority else they are in for a struggle.
In the midst of Vendors pushing out products that speak to most of the OT Cyber Security challenges out there, scholars are debating the best approaches. Should we rely on Firewalls alone or monodirectional gateways or both to manage access to OT networks? and so on…
The bottom line is, OT and the underlying controls systems (ICS) are not just seen as lucrative targets but also open the possible gateway to sabotage and cyber terrorism for those nation-state actors that have almost unlimited funding. Be aware, identify, mitigate and plan to respond. Don't be that guy that has to respond without a plan when the proverbial @#doodles%# hit the fan!

Resources: CPO, Darkreading, Waterfall, Nozomi, Nomios, Skybox, HelpNetSecurity, Purplesec, Dept of Homeland Security

Other Interesting News and Cyber Security bits:

- This AI Software Nearly Predicted Omicron's Tricky Structure
- Android users can now disable 2G to block Stingray attacks
- Critical Infrastructure Security and a Case for Optimism in 2022
- SANS Daily Network Security Podcast (Stormcast)



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