On March 10, the Cyber Threat Alert Level was evaluated and is being raised to Yellow (Elevated) due to Emergency Directive (ED) 21-02, addressing critical vulnerabilities in versions of Microsoft Exchange servers.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
12-Mar	119,109,199	2,641,683

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

12 March 2021

In The News This Week

New critical vulnerabilities found in F5 devices

Can be used to remotely commandeer BIG-IP and BIG-IQ systems. - Enterprise security and network appliance vendor F5 has issued an advisory covering four critical vulnerabilities that attackers can exploit to remotely take over unpatched systems. Unauthenticated attackers can exploit the Common Vulnerabilities and Exposures (CVE) 2021-22986 flaw in the F5 iControl representational state transfer (REST) application programming interface to remotely run arbitrary system commands on several F5 products. Given a Common Vulnerabilities Scoring System version 3 rating of 9.8 out of 10 possible, the critical bug allows attackers to create and delete files as well as execute commands, and disable system services. Read the full story by Juha Saarinen here: ITNews and here F5

Millions in Covid relief funding to be used for federal cybersecurity efforts

Millions of dollars in funding from the Covid-19 relief bill passed Wednesday will be used to help the federal government improve its cybersecurity efforts in the wake of high-profile breaches that have caused alarm for officials and lawmakers.
"[I]t reflects a recognition by this administration of the urgency of improving cybersecurity," said cyber chief Eric Goldstein of the Cybersecurity and Infrastructure Security Agency, adding that it will provide funding ahead of the next budget cycle, given the current threats facing federal networks. The funding comes as CISA, a Department of Homeland Security agency that was founded during the Trump administration, is dealing with the fallout from two recent cyber breaches. Congress, Goldstein said, included $650 million in the $1.9 trillion Covid relief bill for CISA's cybersecurity risk management programs.
Read the full story by Geneva Sands here: CNN

Collaboration key to Sierra Leone's first national cyber security strategy

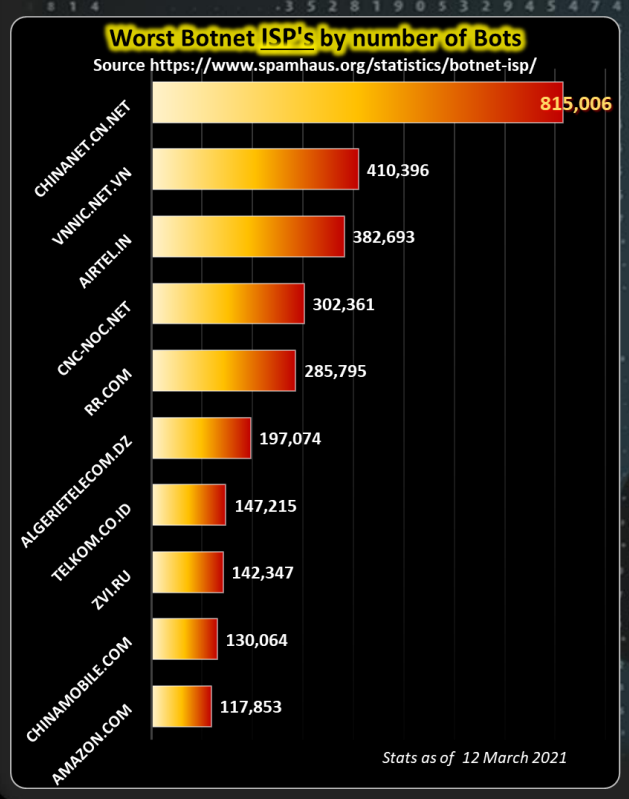
Sierra Leone's Ministry of Information and Communication has produced a first draft of its cyber security strategy, in collaboration with the private sector. As cyber threats grow in scale and complexity, most Commonwealth countries find themselves ranked low on global indices of cyber security. This means they are unable to safeguard their own interests or cooperate internationally. Francis Sesay, the Information, Communications and Technology Manager for Sierra Leone Cable, who works closely with the Ministry of Information and Communication, explained that three dimensions of society are at risk, "The government, the country's businesses and connected citizens." The Foreign and Commonwealth Office's (FCO) Commonwealth Cyber Security Programme has benefited every Commonwealth country in some way, helping many to put in place national Cyber strategies, legislation and Critical Information Infrastructure Protection (CIIP) plans. "It was a shock to us when we attended the [regional Commonwealth National Cyber Security Incident Response conference in Accra, Ghana in 2019 and saw a lot of African countries were way ahead of us," said Francis. Read the full article here: Gov.UK

Veracode Tackles Cybersecurity Skills Gap with Launch of The Hacker Games

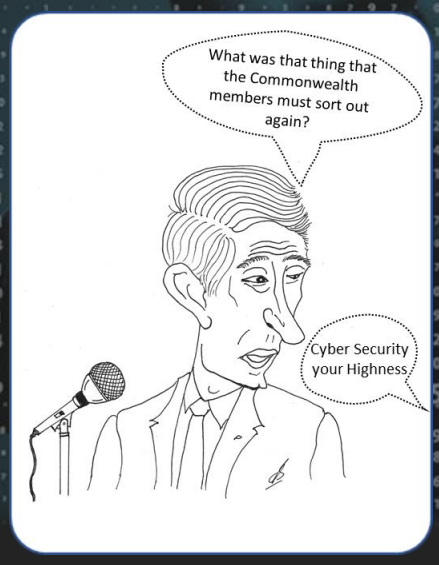
Secure coding competition challenges university students to hack and patch real-life apps online - Veracode, the largest global provider of application security testing (AST) solutions, announced today the launch of the Veracode Hacker Games. The two-week collegiate competition will challenge computer science and cybersecurity student teams from eight leading universities across the U.S. and the U.K., including University of Virginia, Tufts and University of Warwick, to test their secure coding skills and give them the opportunity to win individual prizes, plus $15,000 in charitable donations for the top universities.
"With mounting pressure on developers to deliver software that is secure and keeps society safe from harmful cyberattacks, gaining foundational security knowledge translates to fewer exploitable problems during production and after deployment," said Chris Wysopal, Founder and Chief Technology Officer at Veracode. "Yet, training around secure coding is almost absent at the university level. We've launched The Veracode Hacker Games to help universities make secure coding a core part of their computer science and cybersecurity curriculum, while giving students an edge when it comes to putting their skills to the test in a real-world environment."
Read the full story and get the details here: Yahoo Finance

Australia's answer to thwarting ransomware is good cyber hygiene

The federal government has provided advice on how to counter ransomware in Australia, encouraging the use of multifactor authentication and urging businesses to keep software up to date, archive data and back-up, build in security features to systems, and train employees on good cyber hygiene. The advice was provided in Locked Out: Tackling Australia's ransomware threat, which is a 14-page document [PDF] prepared by the Cyber Security Industry Advisory Committee. It's touted by the Department of Home Affairs as "[building] awareness for all Australians and their businesses on the current ransomware threat landscape". Read the article here: ZDNet



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



Stalkerware?

The recent release of the "State of Stalkerware in 2020" report by Kaspersky highlighted once again the dangers of the lesser talked about malware variant called "Stalkerware". You my ask, "What is Stalkerware? "

What is Stalkerware?

The term Stalkerware reared its head in 2018 and Wikipedia describes it as follows: "The term was coined when people started to widely use commercial spyware to spy on their spouses or intimate partners".
Stalkerware is a hidden app that enables a user to monitor the activities on another user's device without that user's consent. It can facilitate activities like intimate partner surveillance, harassment, abuse, stalking, etc. In certain cases, it can be classified as an aid to domestic violence. It became such a problem that an organization called "Coalition Against Stalkerware" even was formed to combat the issue. The main difference between the more talked about Spyware and Stalkerware for me is that Stalkerware is freely and commercially available online for anyone to buy. You don't have to traverse the ominous world of the Darknet to get your hands on it. Although Google and other App Stores have banned many variants of the software, new variants are popping up almost daily. Originally designed for People to "spy" on their spouses or intimate partners, but the advent of the Covid-19 pandemic forced people to stay at home which lessened this specific need. The trend during the height of the pandemic however revealed that the focus has shifted to other targets like co-workers, remote workers, company CEOs, politicians, community leaders, and so forth. The people hawking Stalkerware realized the market has changed a bit and therefore their marketing targets had to be adjusted to include anyone where there is a physical trust relationship between people or parties. In saying that though, as the Covid-19 restrictions are starting to ease around the world, the original intent on spying on a loved one is slowly rising again.
According to the Kaspersky report, 53,870 mobile users within its telemetry (meaning, their customer base) were affected by Stalkerware during the year. That's a drop from the year before when 67,500 mobile users were affected, but still up from the 40,386 instances detected amongst Kaspersky's client base in 2018. To put the Kaspersky report numbers in perspective, according to Enlyft, Kaspersky Endpoint Protection software has an approximate 2% market share. This means that the actual number of Stalkerware victims is much higher.

How is it distributed?

Stalkerware isn't delivered in the same way as other malware; it can't be sent via a sneaky email or installed in some other remote way, Kaspersky said. This means that the abuser will need to have physical access to a device to install it. Once past any lock-screen, it only takes a few minutes to load an app, researchers have said. "The main barrier that exists is that Stalkerware has to be configured on an affected device," according to the report. "Due to the distribution vector of such applications, which are very different from common malware distribution schemes, it is impossible to get infected with Stalkerware through a spam message including a link to Stalkerware or a trap via normal web surfing."
Stalkerware is usually downloaded from third-party sources. This is easy for Android users, but iPhone Stalkerware tools are less frequent because iOS is traditionally a closed system with apps from third-party stores barred from running on it.
However, "an abuser can offer their victim an iPhone – or any other device – with pre-installed Stalkerware as a gift," according to Kaspersky. So be wary if all of a sudden your company, or anyone for that matter, offers you a phone as a gift. Kaspersky said, "There are many companies who make their services available online to install such tools on a new phone and deliver it to an unwitting addressee in factory packaging to celebrate a special occasion."

Is it legal?

Globally it appears that in most countries there is no law prohibiting the marketing and vending of Stalkerware. Also in the majority of the cases, Stalkerware only becomes illegal if it is being installed and used on the device without the victim's knowledge or consent.

How to recognize if you have it on your device – Things to look out for

Coalition Against Stalkerware Lists 10 things that you should look out for, please visit the site to get a full description - (1) Mobile phone, device or laptop goes missing and then reappears. (2) Lending your device for an extended period to someone and noticing changes in settings or unknown apps you do not recognize. (3) 'Unknown sources' setting 'Enabled' on an Android device. (4) Unexpected battery drain (Android and iOS devices). (5) Strange behavior from the device operating system or applications (Android and iOS devices). (6) An unfamiliar app or process is on your device. (7) Presence of an app called Cydia (iOS devices). This is an issue for jailbroken iOS devices and allows the culprit to install software packages. (8) Active sessions on devices you did not authorize. If you use Google services, it allows you to check on active sessions. (9) Using easy passwords that someone close to you can guess. (10) Webcam permissions are on for applications you did not permit to.

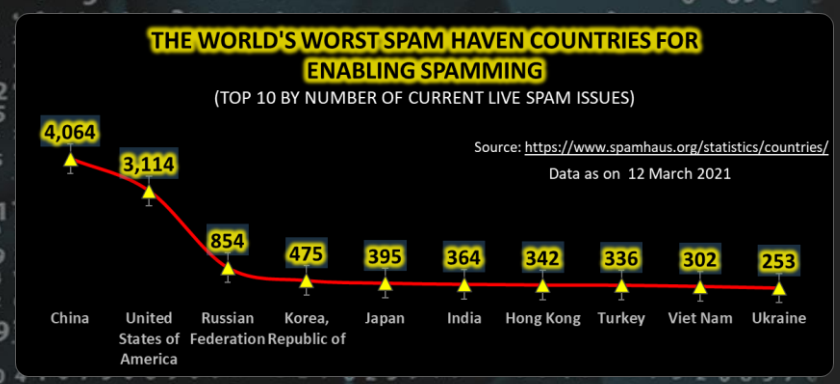
Steps to remove or disable Stalkerware

Important to Note. If you delete Stalkerware, whoever installed it would know that it's been disabled. So it's important to understand that before taking any action that you have a safety plan ready. Contact organizations working with victims of domestic violence. Consider going to law enforcement before taking any action.
(1) Change all your passwords and security reset questions for all online accounts. (2) Protect your device physically to prevent any future tampering. Make sure mobile devices are locked via PIN code, biometrics, or patterns. (3) Enable two-factor authentication. (4) Make sure the OS is up-to-date on your device. (5) Run a malware scan. It may be able to detect, but not proven to be effective in every case. (6) Consider creating a new email address known only to you and link your main accounts to it. (7) Turn off permissions for any application that does not need access to your webcam. (8) Factory Reset your device. Most Stalkerware can be removed this way, but some have been claimed to survive even past a factory reset. (9) If all else fails, consider getting a new device. It may be best to get a new device if all other attempts of removal do not work.

References: Coalition Against Stalkerware, ThreatPost, IT Web, Kaspersky, enlyft, wired
(Thanks to my colleague Christo Deysel who suggested this content for today)

Other Interesting News and Cyber Security bits:

- Cybersecurity Trends and Emerging Threats in 2021
- FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server
- FP Virtual Dialogue, 24 March: How Afghanistan Will Impact America's Role in the World



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