On January 18, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Juniper, Oracle, and Mozilla products.
CIS Security Advisories

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
20 January 2023

In The News This Week

Microsoft Defender ASR rules strip icons, app shortcuts from Taskbar, Start Menu

Microsoft script recreates shortcuts deleted by bad Defender ASR rule. - Microsoft released advanced hunting queries (AHQs) and a PowerShell script to find and recover some of the Windows application shortcuts deleted Friday morning by a buggy Microsoft Defender ASR rule. Early morning on January 13th, Microsoft released a new Microsoft Defender signature update that included a change to the Attack Surface Reduction (ASR) rule known as "Block Win32 API calls from Office macro" in Configuration Manager and "Win32 imports from Office macro code" in Intune. This rule detects and blocks malware from using VBA macros to call Win32 APIs. However, a bug in the updated rules caused Microsoft Defender to exhibit false positives, deleting application shortcuts from the desktop, the Start menu, and the Windows Taskbar. This faulty rule caused widespread disruption in corporate environments, with users unable to quickly launch their applications and Windows administrators scrambling to restore shortcuts. Microsoft later reverted the change in the new signature update 1.381.2164.0 but warned admins that it could take a few hours for the latest signatures to propagate to all environments.
On Saturday morning, Microsoft released advanced hunting queries to find affected shortcuts and a PowerShell script to recreate shortcuts for some of the more commonly deleted applications.
Read the articles here: Bleeping Computer & The Register

Ukraine calls for 'Cyber United Nations' amid Russian attacks

A top cyber official proposed the idea as Moscow targets Ukraine's infrastructure. - Ukraine's top cybersecurity leader is calling for the establishment of a single global organization to help share threat information and prepare for future attacks as Russia pounds Ukraine's infrastructure and seeks to inflict maximum chaos on the ground. The proposed "Cyber United Nations" is one of a number of efforts Ukrainian officials hope the global community will pursue as Russia pairs cyberattacks with missile strikes to create misery for citizens during the winter months. "We need the Cyber United Nations, nations united in cyberspace in order to protect ourselves, effectively protect our world for the future, the cyber world, and our real, conventional world," Yurii Shchyhol, the head of Ukraine's State Service of Special Communications and Information Protection, said in an interview with POLITICO through an interpreter. "What we really need in this situation is a hub or a venue where we can exchange information, support each other and interact." Read the story by Maggie Miller here: Politico

New Backdoor Created Using Leaked CIA's Hive Malware Discovered in the Wild

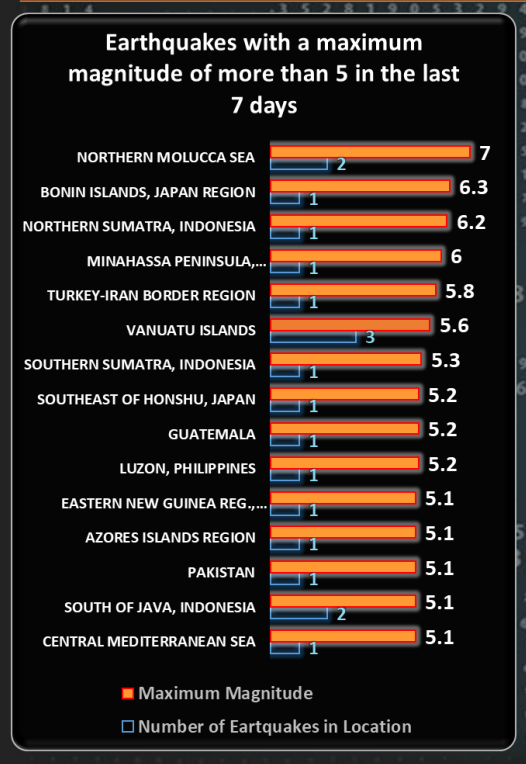
Unidentified threat actors have deployed a new backdoor that borrows its features from the U.S. Central Intelligence Agency (CIA)'s Hive multi-platform malware suite, the source code of which was released by WikiLeaks in November 2017. "This is the first time we caught a variant of the CIA Hive attack kit in the wild, and we named it xdr33 based on its embedded Bot-side certificate CN=xdr33," Qihoo Netlab 360's Alex Turing and Hui Wang said in a technical write-up published last week. xdr33 is said to be propagated by exploiting an unspecified N-day security vulnerability in F5 appliances. It communicates with a command-and-control (C2) server using SSL with forged Kaspersky certificates. The intent of the backdoor, per the Chinese cybersecurity firm, is to harvest sensitive information and act as a launchpad for subsequent intrusions. It improves upon Hive by adding new C2 instructions and functionalities, among other implementation changes.
Read the full article by Ravie Lakshmanan here: The Hacker News

KFC, Pizza Hut parent shuts UK restaurants after cyber attack

A ransomware attack on Yum! Brands, the parent organisation of restaurants including KFC and Pizza Hut, was forced to shut approximately 300 outlets in the UK following a ransomware attack by an unspecified group. - Yum! Brands, the organisation behind iconic restaurant and fast food franchises including KFC, Pizza Hut and Taco Bell, was forced to close approximately 300 outlets across the UK on Wednesday 18 January following a ransomware attack by an as-yet unspecified group. The US-based restaurant operator said that on detecting the incident, it implemented planned response protocols, deployed containment measures to prevent the malware spreading – including taking certain systems offline – and implemented enhanced monitoring for further activity. In a statement, it said it had also begun an investigation, engaged cyber security forensics and notified law enforcement in the US. Read the full story by Alex Scroxton here: ComputerWeekly

Small business owners warned not to rely on Gen Z to handle cyber security

Small business owners could be putting their businesses at risk by relying on younger family members or employees to manage their cybersecurity. A new survey has found two-thirds of Australia's small business owners believe tech-savviness equates to cyber-safety skills. But our first generation of digital natives, Gen Z (born between 1997 and 2010), are among the least cyber safe in the country. The survey found members of Gen Z were most likely to rate cyber security as a low or medium threat. According to the survey, the safest pair of hands in the small appear to be those Gen Xers and upper Millennials in their 30s, who are the most likely group to take cyber security seriously. Read the full article by Gareth Hutchens here: ABC News



For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

IRIS Interactive Earthquake Map

"Camfecting" - Camera and microphone hacking

Wikipedia describes it as follows: Camfecting, in the field of computer security, is the process of attempting to hack into a person's webcam and activate it without the webcam owner's permission. The remotely activated webcam can be used to watch or record anything within the webcam's field of vision. Historically, individuals have been viewed as the main victims of webcam hacks, however, businesses are also at significant risk of camera and microphone hacking. Smartphones, laptops, PCs, and CCTV systems are all vulnerable, and a successful breach can be devastating. Through camera and microphone access, hackers can record meetings, learn information about your business and clients, or even gain deeper access to your devices and probe for sensitive data to use in a ransomware attack.
From an individual perspective, once a camera has been hacked, one can become the victim of a sextortion campaign. The FBI recently warned of an explosion in sextortion cases targeting teenagers. Teens are generally tricked into sending explicit photos of themselves to someone but in many cases, webcams, phone cameras and cameras on gaming consoles are hacked to record private spaces. These private spaces, like a bedroom, are typically where someone feels safe to express themselves or do ordinary things like changing clothes etc., not knowing they are being watched. Once a device has been hacked, the perpetrator can get access to Personally Identifiable Information (PII). This information is then used to contact the victim and threaten to splash the recorded images over social media unless they exchange sexual favors or pay a ransom fee.

How big can the problem potentially be? To put things in perspective, a recent survey indicated that there are approximately 6.8 billion smartphones in use currently, and Statista says that about 47.1% of the global population had a home computer at the end of 2019, a ripe picking field for hackers. Another survey shows that around 95% of teens in the US has their own smartphone or has access to one, the prime target for sextortionists. No matter where you are in the world, or even if you have access to unlimited protection resources, no one is exempted from this threat. Our best defense is knowledge and vigilance. The more people are made aware, the easier they will spot the proverbial snake in the grass and act accordingly.

How to tell if your webcam or laptop camera has been hacked.
Following is an article extract from NordVPN giving you a good idea what to look for and some counter measures you can take:

1) Check if the camera indicator light is on - If your webcam indicator light is on or it's acting abnormally (you see a blinking LED) even though you haven't turned the webcam on, it's a sign that something might not be right. But don't freak out just yet – it may only be another program or browser extension running in the background and using your webcam. Let's double-check it.
2) Check browser extensions - Reboot your computer and launch your browser. If the webcam light turns on the moment you open the browser, the problem is likely to be in a browser extension. But which one exactly? Deactivate your extensions one at a time to identify the culprit and take back control.
3) Check known and unknown applications - Another potential reason why your light is flashing might be applications. To test them, do this: launch an application and see if the webcam indicator lights up, if yes – bingo, if not – continue to open apps one by one until you spot the one secretly using it. Since you may have a lot of them on your computer, the process might be time-consuming. If your webcam light turns on a few seconds after you reboot your computer, without launching any applications – you might've been hacked. If this is what's happening, move on to the next step.
4) What apps are using my camera on Windows? - Windows provides users with an easy way to check which apps are using your camera. It works both for external and built-in cameras. Here's how to access this feature and view your webcam history on Windows: (a) Go to Settings > Privacy > Camera. (b) Scroll through the app list and see which ones can access your camera. (c) Disable the camera in apps where you feel it is not needed.
5) What apps are using my camera on Mac? – (a) Open Terminal. (b) Type this command: lsof | grep "AppleCamera". It will allow you to see your webcam history on Mac. If you don't get any information, you can alternatively try these commands as well: lsof | grep "iSight" and lsof | grep "VDC". (c) Type the following command and the process ID (the 4 digits next to the program's name) to terminate the app that uses your camera: sudo kill -9 XXXX.
6) See if your webcam process is running - Go to the Task Manager and look for all currently running programs under the Processes tab. Check for webcam utility. Again, don't panic yet if you do find it. It may simply be a default setting to launch once you reboot your device. You can test it by restarting your computer and checking if the webcam utility has started automatically.
7) Try running the webcam - Close all the programs and apps and activate your webcam. If you get an error message stating that your camera is already in use, it might be that your laptop's camera has been hacked… or there's an app running in the background (you can check this by following the instructions in Step 1).

The above are basic steps that will give you a good indication if your camera is hacked but bear in mind that some sophisticated firmware hacks can even control the indicator light on your camera. The best countermeasure, however, is to cover your webcam… tape it. Yes, that's right. Even Mark Zuckerberg does it. It's the easiest and 100% reliable way to prevent someone from watching you through your computer camera if you are not actively using it. There are some commercial solutions available to cover your camera should the tape thing not work for you.

Now, what about your phone camera?
In general, same as above, check if your camera indicator light is on at times when it should not be. Check the settings on your apps, for instance, on an iPhone, for Safari change the camera setting to either "deny" or "ask" and turn the camera function off on Google. On Facetime, turn off "FaceTime Live Photos". And so, you can go through all your apps and wherever there is a camera option, decide whether it is a good idea to have it on or not. Apply the same measures for Android and other devices. You can always switch the function back on when you need it.

In many cases, it will be difficult to know whether your phone is hacked but look out for warning signs, if your battery is suddenly running down quicker than normal, it could be an indication that something sinister is going on. Check your apps, are there some apps that you do not recognize? For more indicators of compromise, please follow these links - PixelPrivacy, or Top10VPN, and check out the resources below.

Resources: Daily Mail, bbpMedia, NordVPN, WizCase, BBC, Identity Theft Scout, CNBC, ZDNet

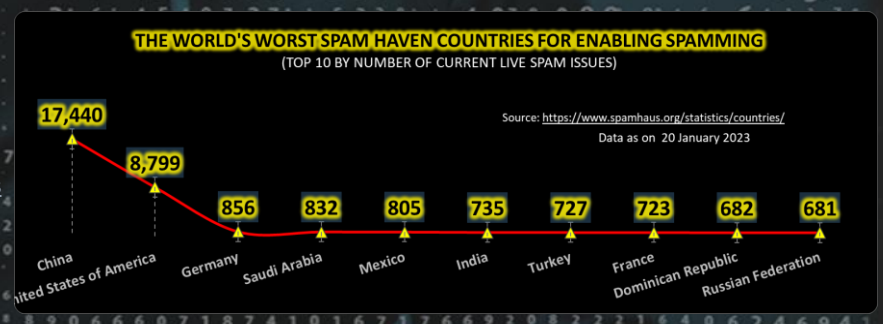
Other Interesting News and Cyber Security bits:

- Cybersecurity predictions for 2023, according to experts
- Flying cars are here and available to preorder
- Flipper Zero: Geeky toy or serious security tool?
- Blockchain start-up allows customers to buy, resell solar power
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally

Marine Traffic

SatelliteXplorer Track satellites in orbit



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