On October 27, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, NPM, and Apple products.
See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
29 Oct	246,306,623	4,997,139

Deaths this week: 49,611

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
29 October 2021

In The News This Week

Microsoft: Russian SVR hacked at least 14 IT supply chain firms since May

Microsoft says the Russian-backed Nobelium threat group behind last year's SolarWinds hack is still targeting the global IT supply chain, with 140 managed service providers (MSPs) and cloud service providers attacked and at least 14 breached since May 2021. This campaign shares all the signs of Nobelium's approach to compromising a significant list of targets by breaching their service provider. Just as in previous attacks, the Russian state hackers used a diverse and ever-changing toolkit, including a long list of tools and tactics ranging from malware, password sprays, and token theft to API abuse and spear phishing. The main targets of these new attacks are resellers and technology service providers that deploy and manage cloud services and similar tech for their customers. Microsoft notified impacted targets of the attacks after spotting them and also added detections to their threat protection products enabling those targeted in the future to spot intrusion attempts. "Since May, we have notified more than 140 resellers and technology service providers that have been targeted by Nobelium," said Tom Burt, Corporate Vice President at Microsoft. Read the full story by Sergiu Gatlan here: Bleeping Computer

BlackMatter ransomware victims quietly helped using secret decryptor

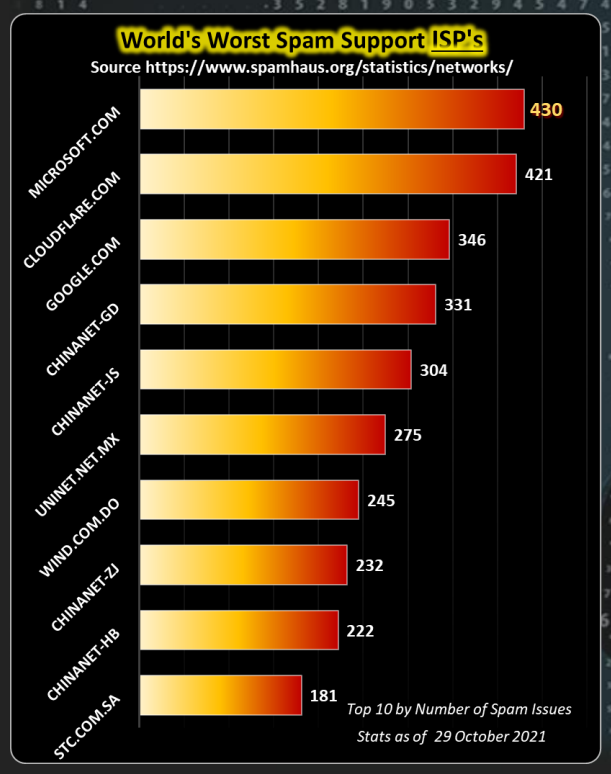
Cybersecurity firm Emsisoft has been secretly decrypting BlackMatter ransomware victims since this summer, saving victims millions of dollars. Emsisoft and its CTO Fabian Wosar have been helping ransomware victims recover their files since 2012, when an operation called ACCDFISA was launched as the first modern ransomware. Since then Wosar and others have been working tirelessly to find flaws in ransomware's encryption algorithms that allow decryptors to be made. However, to prevent ransomware gangs from fixing these flaws, Emsisoft quietly works with trusted partners in law enforcement and incident response to share the news of these decryptors rather than making them publicly available. Soon after the BlackMatter ransomware operation launched, Emsisoft discovered a flaw allowing them to create a decryptor recover victim's files without paying a ransom. Emsisoft immediately alerted law enforcement, ransomware negotiations firms, incident response firms, CERTS worldwide, and trusted partners with information about the decryptor. Read the story here: Bleeping Computer

Man who "scraped and sold 178 million users' data" is sued by Facebook

Facebook is suing a Ukrainian man for allegedly stealing the data of more than 178 million users, and then selling it on an underground cybercrime forum. In a lawsuit filed by the social networking giant on Friday, Facebook claims that between January 2018 and September 2019 Alexander Alexandrovich Solonchenko exploited a vulnerability in a feature which was supposed to help you connect with friends on the social network to scoop up users' personal data. According to Facebook, Solonchenko - who sometimes uses the online handles "Solomame" or "Barak_Obama" - took advantage of a "feature" in Facebook Messenger's Contact Importer that was supposed to tell users if contacts in their address book also had accounts on the site, and make it easier to connect. However, it is alleged that for over a year and a half Solonchenko managed to create a database of 178 million Facebook users' phone numbers and details, having fed Contact Importer many millions of random phone numbers.. Read the full story by Graham Cluley here: Bitdefender

FBI warns of Ranzy Locker ransomware threat, as over 30 companies hit

The FBI has warned that over 30 US-based companies had been hit by the Ranzy Locker ransomware by July this year, in a flash alert to other organisations who may be at risk. According to the alert, issued with the Cybersecurity and Infrastructure Security Agency (CISA), most of the victims were compromised after brute force credential attacks targeting Remote Desktop Protocol (RDP) to gain access to targets' networks. Recent victims, according to the FBI, have reported that the malicious hackers exploited known vulnerabilities in Microsoft Exchange Server and phishing attacks as a way of compromising systems. Once in place, those using the Ranzy Locker ransomware would exfiltrate files from the compromised network, often stealing personal information, customer details, and financial records, before deploying the ransomware to encrypt files across the system. Victims would find a ransom note in affected folders, demanding a cryptocurrency payment be made for the key to unlock the encrypted files, and to prevent the exfiltrated files being leaked online via the computer underground.. Read the full story by Graham Cluley here: Tripwire



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

DIY Home Surveillance over the Internet, what you need to know

The rapid expansion of IoT (Internet of Things) technology over the last few years, has paved the way for quite sophisticated Home Security and Surveillance systems at a fairly affordable price tag. Installation and implementation also became much simpler, and you don't need to be a technical guru to do it all yourself. Basically, on the technical side, if you know how to set up a mobile phone, you will be able to set up your home surveillance system. The only real limitation you'll have is how much you want to spend, as you can go from very basic to highly sophisticated, high quality, and high-resolution systems. Since the outbreak of the Covid-19 pandemic, the world has shifted to a remote working environment and most people upgraded their home wi-fi systems to cope with the demand. Therefore, most people already have the means to check in on their cameras and home security system from anywhere in the world, all you need is an internet connection. If you really want to go basic, you can even re-purpose an old smartphone or tablet as a surveillance camera. All you need is an old unused phone or tablet and an app like Manything. (I just tested this myself and it actually works). With that being said, if you let your mouse do the walking or clicking through the internet, you will find a myriad of sites giving advice on how to set up a surveillance system for your home. Unfortunately on many of these sites they will also try and sell you the biggest load of gunk. So, I thought I'll put together a short surveillance camera 101 composition of what I thought is important.

What you need to consider…

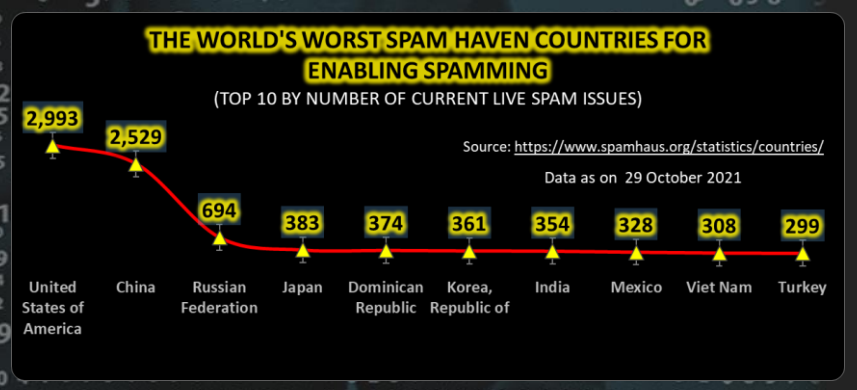
When you want to embark on this journey, you will have to do a bit of planning :

1. Obviously, you'll have to have wi-fi with an Internet connection. In general, a 10 Mbps connection will be more than adequate but if you want to stream uninterrupted high-resolution video, you will need to pump it up a bit.
2. Do you want to go with a wireless or wired solution? - Invariably, the latter will be the cheaper option from a camera perspective, but both options are viable. The main difference, apart from the budget, is on the wired solution, you will need a DVR (Digital Video Recorder) unit that can connect to your home or wi-fi network. With a wireless solution, you don't necessarily need a DVR, as the camera connects to the wi-fi directly and normally has some limited storage capacity. Depending on the DVR you want to purchase this can offset the price tag of the wired solution, which brings us to the next question.
3. Do you need a DVR, and if so, what capacity are you looking at? - Most wireless solutions nowadays don't really need a DVR as the mobile apps offered can be configured to record directly on your phone or to cloud storage if there is a movement or other alert. But, this is really a preference thing, if you want a system that records activity in a certain area all the time, like a baby room or something like that, then go for it as cloud storage can be expensive. You will need to decide how much and at what rate you want to record, as the DVR price will increase as the capacity increases. From a security perspective though, keep in mind that if intruders get past your perimeter defenses and enter your home, they can also find and trash the DVR. As already mentioned, many solutions also include a service to record to cloud storage, however, this is a premium service that comes at a price. For me, if you have the budget, this is the better option as evidence is kept off-site. If you opt for the wired solution, then in most cases you don't really have a choice as you need the DVR or some other alternative device to connect to the Internet.
4. Where do you want to place the cameras, and what areas do you want to cover? - Since most of the solutions out there are scalable, you don't need to cover everything from the word go. Depending on your budget, you can start with a basic outlay of 1 – 3 cameras, that cover strategic areas, then you can add on as you go. First, you want to cover the entry points of your home. Depending on the size or the layout of your home, you will typically have 3 to 4 entry points, front door, back door, and side entrances. You will want to make sure your camera placement is optimized to trigger at the smallest of movements and pick up if the door is slightly ajar.
5. Think cabling and power - Unless you opt for the more expensive options of battery-powered cameras, most cameras require a wired power source like a wall socket or existing power trunks in the ceiling. The challenge is to avoid a spaghetti scenario where unsightly cables are hanging about everywhere. So plan the trunking and cable layout to have the least visual impact. For wired cameras, keep in mind that you might need to drill a few holes through the wall for the coaxial cables to connect to the DVR. Keep the DVR close to your router unless you want to run a long network cable. If this is a challenge, you can use a wireless bridge or if supported on your particular DVR, a wireless dongle. Not many DVRs offer a build-in wi-fi radio. Lastly, invest in a hot glue gun to neatly glue the cables in corners rather than using unsightly cable saddles or trunking.
6. What type of cameras do you want to deploy? - There is a wide range of cameras available in the market ranging from an established brand named camera to a myriad of cheaper Far Eastern alternatives. The cameras however are divided into several categories, each to address a specific requirement or function. The main categories are:
   a) Dome Cameras – The dome-shaped camera is relatively discreet in appearance, but difficult for someone to see in which direction the camera is pointing due to the dark tint of the dome.
   b) Bullet Cameras - Bullet cameras have an iconic design that is highly visible. They are mostly cylindrical and are capable of observing long distances. These are most suitable for outdoor use as their casings are resistant to water, dust, and dirt.
   c) PTZ (Pan Tilt & Zoom) Cameras - With a PTZ camera, you can have complete control of the camera through your app. At the touch of a button, the camera lens can pan left and right, tilt up and down, or zoom in and out.
   d) Day/Night Cameras - These cameras have been built to operate effectively, regardless of how well lit the environment is.
   e) Infrared/night vision Cameras - These cameras are designed to operate optimally in pitch black conditions. They achieve this by using infrared technology but are generally more expensive than Day/Night cameras.
   f) Wireless Cameras - Wireless cameras were created to minimize installation time with a discreet and tidy appearance and a less obtrusive fitting. But, as I said earlier, these come with a higher price tag.

I hope this gave you some insight in the matter but tick here for more guidance: ZDNet, techradar, Reviews, Handyman, Sec.org

Other Interesting News and Cyber Security bits:

- Alarming Cybersecurity Stats For 2021
- NATO releases first-ever strategy for Artificial Intelligence
- Ransomware gang outraged at "bandit-mugging behavior of the United States" after REvil group pushed offline



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