On March 17, the Cyber Threat Alert Level was evaluated and is remaining at Yellow (Elevated) due to the ongoing exploitation attempts observed by the MS-ISAC regarding critical vulnerabilities in versions of Microsoft Exchange servers..

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
19-Mar	122,352,443	2,702,269

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

19 March 2021

In The News This Week

TTP Table for Detecting APT Activity Related to SolarWinds and Active Directory/M365 Compromise - CISA has released a table of tactics, techniques, and procedures (TTPs) used by the advanced persistent threat (APT) actor involved with the recent SolarWinds and Active Directory/M365 compromise. The table uses the MITRE ATT&CK framework to identify APT TTPs and includes detection recommendations. This information will assist network defenders in detecting and responding to this activity. CISA encourages network defenders to review SolarWinds and AD/M365 Compromise: Detecting APT Activity from Known TTPs and implement the recommendations. CISA also recommends network defenders review the following resources regarding this incident:

- Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise web page
- CISA Emergency Directive 21-01 - Mitigate SolarWinds Orion Code Compromise & Supplemental Guidance v.1
- CISA Activity Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations.

Find the article and more information here: CISA

White House tees up cyber labeling policy

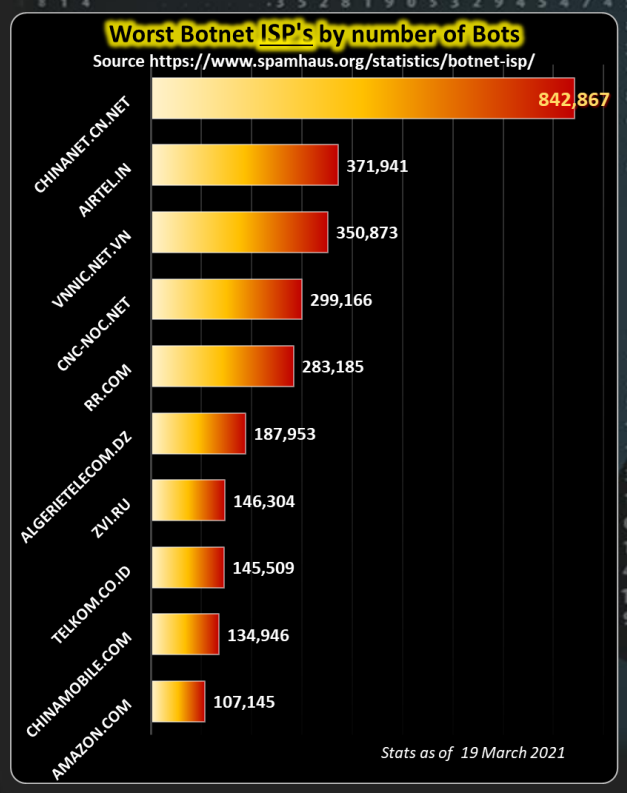
The Biden administration is considering two new policies to give government, corporate and individual tech consumers assurance that products are being designed with cybersecurity in mind. In the wake of two massive cybersecurity breaches, one involving the SolarWinds remote IT management software and the other exploiting four vulnerabilities in Microsoft Exchange Server software, the government is looking to move fast to elevate cybersecurity standards for products used by government, industry and consumers. During a background briefing on March 12, a senior administration official told reporters that executive actions are coming in the "next couple of weeks" to give security grades to software companies and to add security labels to internet-of-things devices.. Read the full story by Adam Mazmanian here: FCW

China Suspected Of Cyber Attack On Western Australia's Parliament

A large number of Australian organisations, including Western Australia's parliament, were hit by a cyberattack earlier this month, allegedly by the Chinese. The attacks came in the middle of election campaigning in Western Australia, which was conducted on March 13 to elect the new members of the parliament. According to ABC, Western Australia's parliamentary email server was hit during the attack, following which lawmakers received an alert message from the Department of Parliamentary Services. After Western Australia's Parliamentary Services Department detected the attack, they shut down the server until the next morning. The department later concluded that no data was stolen during the attack. Read the full article here: REPUBLICWORLD

New Privacy Complaint Against Apple Alleges iOS 14 Does Not Meet EU Privacy Requirements - France Digitale, a tech industry lobbying organization with a focus on start-up companies, has filed a complaint against Apple with the country's data privacy watchdog CNIL. The privacy complaint focuses on Apple's privacy changes to iOS 14, which created new consent and notification requirements for app publishers. France Digitale argues that Apple's refusal to apply the same standards to itself constitutes a breach of EU regulations as users of pre-installed iOS apps are subject to first-party targeted advertising without ever being asked for consent. The privacy complaint is significant as France Digitale is one of France's largest lobbying organizations, representing over 2,000 companies that include most of the country's venture capital firms and heavyweight entrepreneurs. Read the full story by Scott Ikeda here: CPO Magazine

Microsoft investigates potential ties between partner security firm, Exchange Server attack code leak - Microsoft is reportedly investigating a potential partner leak that could have exacerbated the current wave of attacks against Microsoft Exchange servers. The Redmond giant is examining whether potentially "sensitive information" required to conduct the attacks was obtained through "private disclosures it made with some of its security partners," according to the Wall Street Journal. On March 2, Microsoft issued emergency patches to tackle four zero-day vulnerabilities in Microsoft Exchange Server which were being actively exploited in the wild. The critical bugs were disclosed privately in January, and since then, exploit usage has gained traction to the point researchers estimate that tens of thousands of businesses worldwide have been impacted. Read the full article by Charlie Osborne here: ZDNet



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

Cryptojacking?

The topic of Cryptojacking came up as a subsection in one of the articles in this bulletin before, but I still get asked about it frequently. Malwarebytes is sporting a really good article on this topic and I thought it will be a good idea to share it with you. Below is an **adapted and shortened** version of the article as a taster but please visit the site to get the full picture.

All about cryptojacking

Cryptojacking (also called malicious cryptomining) is an emerging online threat that hides on a computer or mobile device and uses the machine's resources to "mine" forms of online money known as cryptocurrencies. It's a burgeoning menace that can take over web browsers, as well as compromise all kinds of devices, from desktops and laptops to smartphones and even network servers. Like most other malicious attacks on the computing public, the motive is profit, but unlike many threats, it's designed to stay completely hidden from the user. To understand the mechanics of the threat and how to protect yourself against it, let's begin with a bit of background.

What are cryptocurrencies?

Cryptocurrencies are forms of digital money (electronic money) that exist only in the online world, with no actual physical form. They were created as an alternative to traditional money and gained popularity due to growth potential and anonymity. One of the earliest, most successful forms of cryptocurrency, Bitcoin, came out in 2009. Units of cryptocurrency (called "coins") are nothing more than entries in a database. In order to perform a transaction that alters the database, one must meet certain conditions. Think of how you track your own money in a bank account. Whenever you authorize transfers, withdrawals, or deposits, the bank's database updates with your new transactions. Cryptocurrencies work in a similar way, but with a decentralized database.
The decentralized, anonymous nature of cryptocurrencies means there is no regulating body that decides how much of the currency to release into circulation. Instead, the way most cryptocurrencies enter circulation is through a process called "cryptocurrency mining." Without going too in-depth, the mining process essentially turns computing resources into cryptocurrency coins. At first, anyone with a computer could mine cryptocurrency, but it quickly turned into an arms race. Today, most miners use powerful, purpose-built computers that mine cryptocurrency around the clock. Before long, people started to look for new ways to mine cryptocurrency, and cryptojacking was born. Instead of paying for an expensive mining computer, hackers infect regular computers and use them as a network (with their combined processing power) to do their bidding. (Read more in the full online article)

How do people use cryptocurrencies?

Cryptocurrency owners keep their money in virtual "wallets," which are securely encrypted with private keys. In a transaction, the transfer of funds between the owners of two digital wallets requires that a record of this exchange be entered into the decentralized public digital ledger. Special computers collect data from the latest Bitcoin or other cryptocurrency transactions about every 10 minutes and turn them into a mathematical puzzle. There, the transaction-within-a-puzzle awaits confirmation. Confirmation only happens when members of another category of participants, called miners, independently solve the complex mathematical puzzles that prove the transaction's legitimacy, thereby completing the transaction from the owner of one wallet to another. Typically, an army of miners toils away on the puzzle simultaneously in a race to be the first with the puzzle proof that authenticates the transaction. The miner who first solves the encrypted problem receives a reward, some amount of cryptocoin.

What is cryptojacking?

Cryptojacking is a scheme to use people's devices (computers, smartphones, tablets, or even servers), without their consent or knowledge, to secretly mine cryptocurrency on the victim's dime. Instead of building a dedicated cryptomining computer, hackers use cryptojacking to steal computing resources from their victims' devices. When you add all these resources up, hackers are able to compete against sophisticated cryptomining operations without the costly overhead. If you're a victim of cryptojacking, you may not notice. Most cryptojacking software is designed to stay hidden from the user, but that doesn't mean it's not taking its toll. This theft of your computing resources slows down other processes, increases your electricity bills, and shortens the life of your device. Depending on how subtle the attack is, you may notice certain red flags. If your PC or Mac slows down or uses its cooling fan more than normal, you may have reason to suspect cryptojacking. The motivation behind cryptojacking is simple: money. Mining cryptocurrencies can be very lucrative, but turning a profit is now next to impossible without the means to cover large costs. To someone with limited resources and questionable morals, cryptojacking is an effective, inexpensive way to mine valuable coins.

How does cryptojacking work?

Cryptojackers have more than one way to enslave your computer. One method works like classic malware. You click on a malicious link in an email and it loads cryptomining code directly onto your computer. Once your computer is infected, the cryptojacker starts working around the clock to mine cryptocurrency while staying hidden in the background. An alternative cryptojacking approach is sometimes called drive-by cryptomining. Similar to malicious advertising exploits, the scheme involves embedding a piece of JavaScript code into a Web page. After that, it performs cryptocurrency mining on user machines that visit the page.

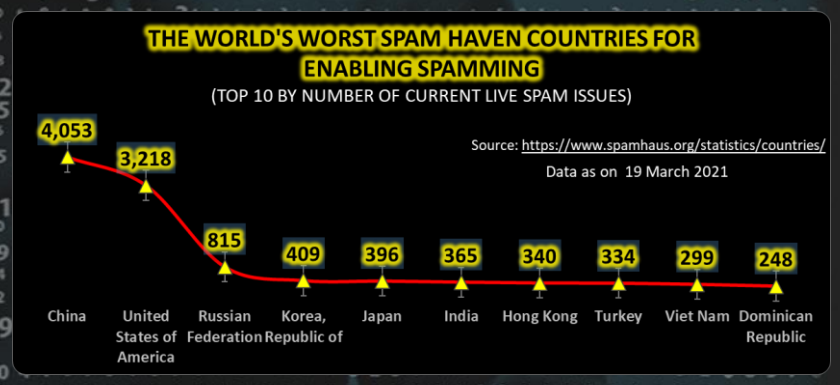
How do I protect myself from cryptojacking?

It can be difficult to manually detect the intrusion and finding the origin of the high CPU usage can be difficult. Processes might be hiding or masking as something legitimate to hinder you from stopping it. As a bonus to the cryptojackers, when your computer is running at maximum capacity, it will run ultra-slow, and therefore be harder to troubleshoot. As with all other malware precautions, it's much better to install security before you become a victim. One obvious option is to block JavaScript in the browser that you use to surf the web. Although that interrupts the drive-by cryptojacking, this could likewise block you from using functions that you like and need. There are also specialized programs, such as "No Coin" and "MinerBlock," which block mining activities in popular browsers. Both have extensions for Chrome, Firefox, and Opera. Opera's latest versions even have NoCoin built-in.

See the full article here and for some additional reading on how to protect yourself from Cryptojacking go here.

Other Interesting News and Cyber Security bits:

- Pioneering Experiment Turns IBM's Largest Quantum Computer Into a Quantum Material.
- Durban cyberbully who harassed neighbours convicted in landmark judgment (Thanks to Bill Graham who pointed me to this one)



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