On February 13, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in PHP, Apple, Adobe, Microsoft, and Mozilla products. (Still no update from CIS at the time of publication, this means that the alert level will remain unchanged)

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

01 March 2019

In The News This Week

Thailand passes internet security law decried as 'cyber martial law'

Thailand's military-appointed parliament on Thursday passed a controversial cybersecurity law that gives sweeping powers to state cyber agencies, despite concerns from businesses and activists over judicial oversight and potential abuse of power. The Cybersecurity Act, approved unanimously, is the latest in a wave of new laws in Asian countries that assert government control over the internet. Civil liberties advocates, internet companies and business groups have protested the legislation, saying it would sacrifice privacy and the rule of law, and warning compliance burdens could drive foreign businesses out of Thailand. The military government has pushed for several laws it said would support the country's digital economy, including an amendment to the Computer Crime Act in 2017, which has been used to crack down on dissent. Internet freedom activists have called the legislation a "cyber martial law," as it encompasses all procedures from everyday encounters of slow internet connections to nationwide attacks on critical infrastructure. If a cybersecurity situation reached a critical level, the legislation allows the military-led National Security Council to override all procedures with its own law.
(Read the full Reuters Article here: https://www.reuters.com/)

Hackers Favorite CoinHive Cryptocurrency Mining Service Shutting Down

Coinhive, a notorious in-browser cryptocurrency mining service popular among cybercriminals, has announced that it will discontinue its services on March 8, 2019.
Regular readers of The Hacker News already know how Coinhive's service helped cyber criminals earn hundreds of thousands of dollars by using computers of millions of people visiting hacked websites. For a brief recap: In recent years, cybercriminals leveraged every possible web vulnerability [in Drupal, WordPress, and others] to hack thousands of websites and wireless routers, and then modified them to secretly inject Coinhive's JavaScript-based Monero (XMR) cryptocurrency mining script on web-pages to financially benefit themselves.
Millions of online users who visited those hacked websites immediately had their computers' processing power hijacked, also known as cryptojacking, to mine cryptocurrency without users' knowledge, potentially generating profits for cybercriminals in the background. Now, while explaining the reason to shut down in a note published on its website yesterday, the Coinhive team said mining Monero via internet browsers is no longer "economically viable." "The drop in hash rate (over 50%) after the last Monero hard fork hit us hard. So did the 'crash' of the cryptocurrency market with the value of XMR depreciating over 85% within a year," the service said. "This and the announced hard fork and algorithm update of the Monero network on March 9 has lead us to the conclusion that we need to discontinue Coinhive."
So users who have an account on Coinhive website with above the minimum payout threshold balance can withdraw funds from their accounts before April 30, 2019.
Though Coinhive was launched as a legitimate service for website administrators to alternative generate more revenue from their websites, its extreme abuse in cyber criminals activities forced tech companies and security tools to label it as "malware" or "malicious tool." To prevent cryptojacking by browser extensions that mine digital currencies without users' knowledge, last year Google also banned all cryptocurrency mining extensions from its Chrome Web Store. A few months after that Apple also banned all cryptocurrency mining apps from its official app store.
(Read the full story by Wang Wei here: https://thehackernews.com/)

TOP Vulnerabilities listed last week in the USA

#	KNOWN AS	(%)
1	Exploit.MSOffice.CVE-2017-11882.gen	52.90%
2	Exploit.Script.Generic	27.55%
3	Exploit.Win32.CVE-2017-11882.gen	4.38%
4	Exploit.MSOffice.CVE-2017-11882.b	4.26%
5	Exploit.Java.Generic	0.70%
6	Exploit.AndroidOS.Lotoor.a	0.66%
7	Exploit.MSOffice.CVE-2018-0802.gen	0.49%
8	Exploit.MSOffice.CVE-2017-8570.gen	0.44%
9	Exploit.Script.CVE-2018-8174.a	0.31%
10	Exploit.MSOffice.Oleink.a	0.30%

Source: Kaspersky Labs

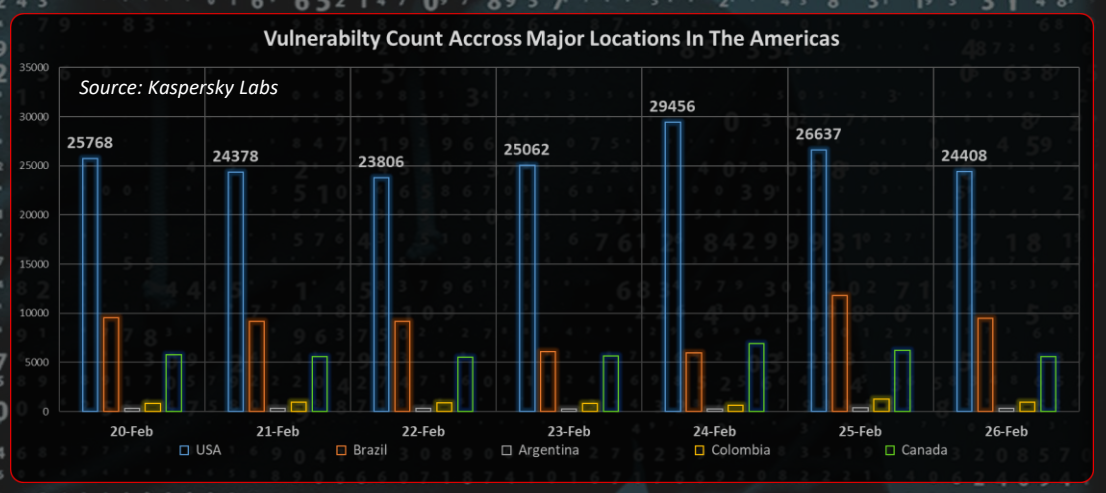
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Source on th Internet suggests
That approximately
90% of all websites is located in the Dark Net, and the "visible" internet comprises only around **10%**

What is the "Darknet" or "Deep Web"?

I recently posted a news article that spoke about a database of more that 2.2 billion stolen private credentials that were for sale on the darknet. So, what is this Darknet everyone is speaking about? - Wikipedia describes the Darknet as follows: *"Dark Net (or Darknet) is an umbrella term describing the portions of the Internet purposefully not open to public view or hidden networks whose architecture is superimposed on that of the Internet. "Darknet" is often associated with the encrypted part of the Internet called Tor network where illicit trading takes place such as the infamous online drug bazaar called Silk Road. It is also considered part of the Deep Web. Anonymous communication between whistle-blowers, journalists and news organisations is facilitated by the "Darknet" Tor network through use of applications including Secure Drop."*
The term "dark net" was originally coined in the starting days of the Internet and it described computers on ARPANET that were hidden from normal web browsing and was basically designed to listen and receive but never responded back. These machines were in the dark so to speak and only accessible by those few who knew the location and access credentials/methods to get to them.
The Internet, or "visible" public network consists of millions of websites distinguished by their unique web address names or URL's (Uniform Resource Locator) that is searchable through search engines like Google, Yahoo, Bing and many more. As we all know, the internet is a massive repository of information and databases in various formats and forms. This "visible" Internet however, represents only a small portion of all websites, the Deep Web lurking in the dark, represents approximately 90 percent of all websites and that is only a rough estimate. An article by ZDNet a while back stated that in fact, this hidden Web is so large that it's impossible to discover exactly how many pages or sites are active at any one time.
Following is an extract of an article from Kaspersky: **(1)** Defining the Deep/Dark Web - There are a number of terms surrounding the non-visible Web, but it's worth knowing how they differ if you're planning to browse off the beaten path. According to PC Advisor, the term "Deep Web" refers to all Web pages that that are unidentifiable by search engines. The "Dark Web," meanwhile, refers to sites with criminal intent or illegal content, and "trading" sites where users can purchase illicit goods or services. In other words, the Deep covers everything under the surface that's still accessible with the right software, including the Dark Web. **(2)** Use and Misuse - For some users, the Deep Web offers the opportunity to bypass local restrictions and access TV or movie services that may not be available in their local areas. Others go deep to download pirated music or grab movies that aren't yet in theatres. At the dark end of the Web, meanwhile, things can get scary, salacious and just plain...strange. As noted by The Guardian, for example, credit card data is available on the Dark Web for just a few dollars per record, while ZDNet notes that anything from fake citizenship documents to passports and even the services of professional hit men is available if you know where to look. Interested parties can also grab personal details and leverage them to blackmail ordinary Internet users. Vast amounts of stolen account data, including real names, addresses and phone numbers; ended up on the Dark Web for sale. Illegal drugs are also a popular draw on the Dark Web. As noted by Motherboard, drug marketplace the Silk Road; which has been shut down, replaced, shut down again and then rebranded. They offer any type of substance in any amount to interested parties. Hacking tools, custom made viruses and any cyber criminal resources can be found with minimal effort. Business Insider, meanwhile also details some of the strange things you can track down in the Deep, including a DIY vasectomy kit and a virtual scavenger hunts that culminated in the "hunter" answering a NYC payphone at 3 a.m. **(3)** Real Risks - Thanks to the use of encryption and anonymization tools by both users and websites, there's virtually no law enforcement presence down in the Dark. This means anything, even material well outside the bounds of good taste and common decency, can be found online. This includes offensive, illegal "adult" content that would likely scar the viewer for life. According to some articles, a large portion of Dark Web hits are connected to paedophilia and child pornography. Here, the notion of the Dark as a haven for privacy wears thin and shores up the notion that if you do choose to go Deep, always restrict access to your Tor-enabled device so children or other family members aren't at risk of stumbling across something no one should ever see. Visit the Deep Web if you're interested but do yourself a favour: don't let kids anywhere near it and tread carefully, it's a long way down.

You can read the full Kaspersky article here : **https://usa.kaspersky.com/resource-center/threats/deep-web**



Author: Chris Bester