On November 6, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google and Microsoft products. (Unchanged from last week)

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
15 November 2019

In The News This Week

Brave browser reaches v1.0, its first stable version.

On the 14 of November, the team behind Brave, a privacy-first browser, announced the release and roll-out out its first stable release v1.0, complete with innovative features such as its own private ad platform and a user's and websites rewards initiative.

Developed from the ground up to be a **privacy-first alternative to modern-day browsers**, Brave 1.0 comes with many features not present in any other competitor's software. This includes:

BRAVE ADS

Brave blocks all ads by default, and instead uses its own private ad platform, designed to work right inside the browser, and with a focus on preserving users' privacy.

The Brave team says this ad network was designed with privacy in mind, and that no user data is sent back to any remote server. All the ad matching operations happen directly on the users' devices.

Furthermore, this new ad platform also uses a new blockchain-based advertising model that rewards users with Basic Attention Tokens (BAT) for every ad they view.

Users can keep the BAT they earn in a wallet app built into the browser, convert it to other cryptocurrency or fiat currency, or they can donate it to the websites they like, via the Brave Rewards program (see below).

Brave says that 70% of this ad network's revenue goes back to its users, while the company keeps 30%.

BRAVE REWARDS

Brave Rewards is probably the most interesting feature added to any of web browser today. The Rewards program allows users to donate some of the BAT tokens they make by viewing Brave ads to the websites they like the most.

They can choose to sent BAT to any website they like, or the websites they frequent the most -- based on stats provided by Brave itself, based on the user's browsing history.

Brave says that more than 300,000 websites have verified profiles through which they collect BAT donations, including some of today's biggest names, such as The Washington Post, The Guardian, Wikipedia, creators on YouTube, Twitch, Twitter, GitHub and more.

More on the Brave Rewards program can be found in this documentation page, here.

BRAVE SHIELDS

Brave 1.0 also comes with a built-in ad blocker, anti-tracking, and anti-fingerprinting features that block online advertisers, analytics, and social media companies from bombarding users with ads and tracking users as they move across websites.

This feature is getting constant improvements, with the latest update arriving last week.

The Brave team says that since it rolled out Brave Shields, the biggest benefit has been an improved performance. For example, the Brave team says websites load to up to three to six times faster than other browsers, resulting in significant memory and battery savings.

"Brave saves an average of 27 seconds per page load against Chrome on macOS and 22 seconds per page against Firefox, and Brave uses 58% less data than Chrome to load those same pages," the Brave team said in a pre-launch press release. "Brave also uses less memory than other browsers, with an improvement of 40% over Chrome and 47% over Firefox."

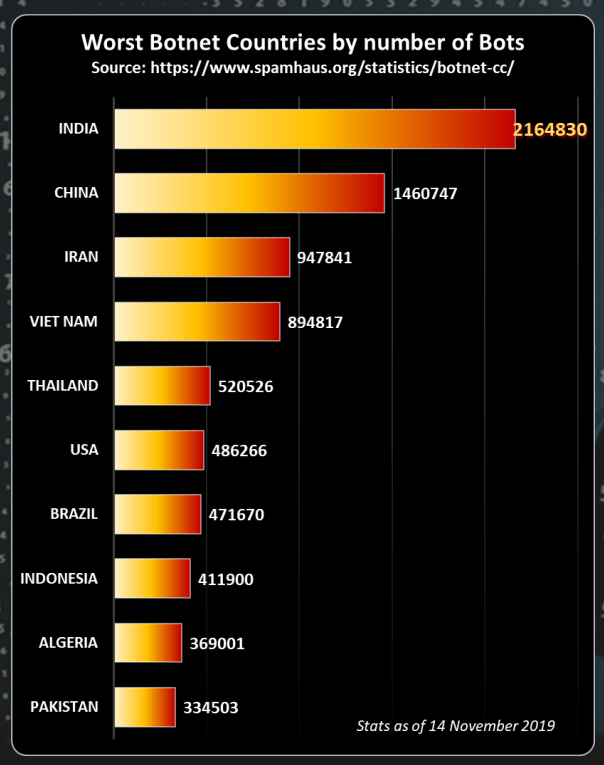
Brave 1.0 should roll out to active installations starting 14 November. New users can also download and test it.

The browser is available for Windows, macOS, Linux, Android, and iOS.

The company said the browser had around 8.7 million monthly active users (MAU) during its beta testing phase, which, in perspective is around a tenth of Firefox' 100 million MAU, and a fraction of Chrome's 1+ billion MAU.

Under the hood, Brave 1.0 is built on the Chromium open-source browser engine, the same browser engine at the heart of Chrome, Opera, and Vivaldi.

Read the full story here: ZDNet Article Check Brave out here



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

Cyber Security Tips for Black Friday up to Cyber Monday

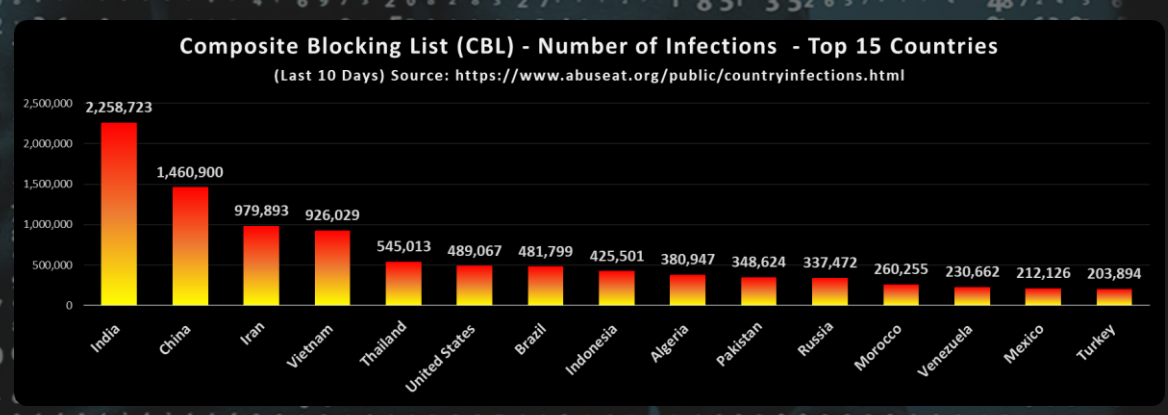
Black Friday happens the day after the US holiday of Thanksgiving, always celebrated on the 4th Thursday of November and is regarded as the first day of the Christmas shopping season, on which retailers offers massive discounts. Black Friday dates back the 1950's and has since then became a worldwide phenomenon. The name "Black Friday" coined by the police to describe the mayhem surrounding the event and came about due to the overwhelming pedestrian congregations outside big retail stores causing massive congestion issues and was often linked to elevated numbers of accidents and injuries and sometimes violence. This year it will happen on the 29th of November and in most countries are extended over the weekend.

In the modern era though, the biggest portion of Black Friday sales are offered online and are extended up to Cyber Monday and cybercriminals are preparing huge campaigns to exploit this retail "feeding frenzy" as sales are estimated to top 7.5 Billion US dollars this year according to Forbes. There are over 4350 Black Friday themed apps available to online consumers on the various app stores and an estimated 4% of these are Malicious.

Following is some Cyber Security Tips for Black Friday written by Hardeep Singh form appknox

1) Be careful while downloading new apps for shopping, coupons, deals etc.
   Ensure that you download mobile apps, be it Android or iOS, from the official app stores of the E-commerce retailer. Before you click on the download button, do check the app permissions and other information that is being asked by the application. Avoid downloading apps from third-party app stores as threat actors make use of the festive season to create fraudulent apps that look as if they are associated with the real brand.
2) Shop online only through trusted sites with a valid SSL certificate
   While you search for your favourite product online or check out on a fantastic deal, ensure that you click on those websites whose site addresses begin with 'https' instead of 'http'.
   In the case of a regular HTTP connection the data that is sent between your browser & the E-commerce website you are connected to, will be in plain text and therefore can be read by any hacker looking to trick and exploit you. Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, where all communications are securely encrypted.
   For the implementation of an HTTPS connection, you will need a valid SSL certificate.
3) Enable security alerts for all your financial transactions
   There's no such thing as being 100% secure but we can surely give our 100% while being aware and proactive. Like they say, 'Prevention is better than cure'. So before you start shopping online, ensure you log on to your net banking and update your profile details while setting up text alerts as well as email alerts for every transaction that you make online.
   In doing so you will be alerted in case of fraudulent transactions made through your debit or credit card without your consent.
4) Avoid online shopping using public WiFi networks
   Restrict conducting sensitive activities such as making an online payment at ecommerce websites using a public wireless network as they pose a major security threat. These free networks are often a hacker's paradise due to lack of proactive security.
5) Set up 2-step verification for your online account
   In case someone catches hold of your password, a 2-step verification would ensure that they are still unable to log on to your account as an additional code is needed that can only be sent through your mobile phone.
   A lot of Ecommerce websites provide the option of setting up an additional 2-step verification. So ensure that you make use of this added security layer.
6) Create unique passwords for your accounts online
   Restrict the use of using similar passwords for several accounts instead create unique passwords for multiples websites and ensure that you use a combination of symbols, numbers, and letters while choosing a password. Throw in a mixture of upper- and lower-case alphabets to make it stronger and more unique.
7) Be proactive about protecting your identity and social accounts
   Make it a regular affair to keep track of your financial records and activities of your social accounts for the coming weeks to ensure that there is no unauthorized activity. Also remember to alert your banking officials and even the police if you have any reason to believe that your identity has been compromised.
   It's imperative to alert the law enforcement about the threats as soon as they occur as even the banks or insurance companies would require a police report while they conduct their own investigation on those fraudulent transactions.

We hope these 7 cyber security tips for Black Friday and Cyber Monday would help you to have a better shopping experience while keeping you ahead of the security curve. Do let us know in comments if you come across any suspicious or fraudulent activity while browsing through the various holiday deals online.



Author: Chris Bester
chris.bester@yahoo.com