Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On June 24, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Treck, Google and BitDefender products.

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

26 June 2020

In The News This Week

BlueLeaks: Data from 200 US police departments & fusion centers published online

An activist group has published on Friday the 19th, 296 GB of data they claim have been stolen from US law enforcement agencies and fusion centers. The files, dubbed BlueLeaks, have been published by Distributed Denial of Secrets (DDoSecrets), a group that describes itself as a "transparency collective." The data has been made available online on a searchable portal. According to the BlueLeaks portal, the leaked data contains more than one million files, such as scanned documents, videos, emails, audio files, and more. DDoSecrets claims it received the BlueLeaks data "courtesy of Anonymous," the infamous hacktivist group. Most of the files listed on the BlueLeaks portal are labelled "Netsential.com Inc," a web hosting company based in Houston Texas. KrebsOnSecurity reported earlier that the National Fusion Center Association (NFCA), the central association representing all fusion centers across the US, confirmed the leak's authenticity in an internal security alert it sent to its members. The NFCA said that after a preliminary analysis the data appears to have originated from the servers of Netsential, a web hosting provider for many US law enforcement agencies and fusion centers.

Read the full story by Catalin Cimpanu here: ZDNet Article

Chinese bank forced western companies to install malware-laced tax software

GoldenSpy backdoor trojan found in a Chinese bank's official tax software, which the bank has been forcing western companies to install - A Chinese bank has forced at least two western companies to install malware-laced tax software on their systems, cyber-security firm Trustwave said in a report published today. The two companies are a UK-based technology/software vendor and a major financial institution, both of which had recently opened offices in China. "Discussions with our client revealed that [the malware] was part of their bank's required tax software," Trustwave said on Thursday. "They informed us that upon opening operations in China, their local Chinese bank required that they install a software package called Intelligent Tax produced by the Golden Tax Department of Aisino Corporation, for paying local taxes.".. Read the full article here: ZDNet Article

New Ransomware Attacks Android Devices Encrypts Photos and Videos Posing as COVID-19 Tracing App - A new ransomware strain dubbed CryCryptor targeting Android users, particularly users in Canada posing as an official COVID-19 tracing app from Health Canada. The CryCryptor is a new ransomware based on the open-source ransomware CryDroid published on Jun 11, 2020. The malicious campaign started after the Canadian government announced the official tracing app, according to sources the app is still in the testing phase and to be live possibly next month. Security researchers from ESET observed that malicious COVID-19 tracing app distributed using two third-party websites and not through Google Play. Once the malicious app launched in the device it seeks permission to access files on the device, once permission provided it encrypts files with certain extensions. The extensions include txt, jpg, BMP, png, pdf, doc, Docx, ppt, pptx, avi, Xls, vcf, pdf, and db files. .

Read the full article here: GBHackers

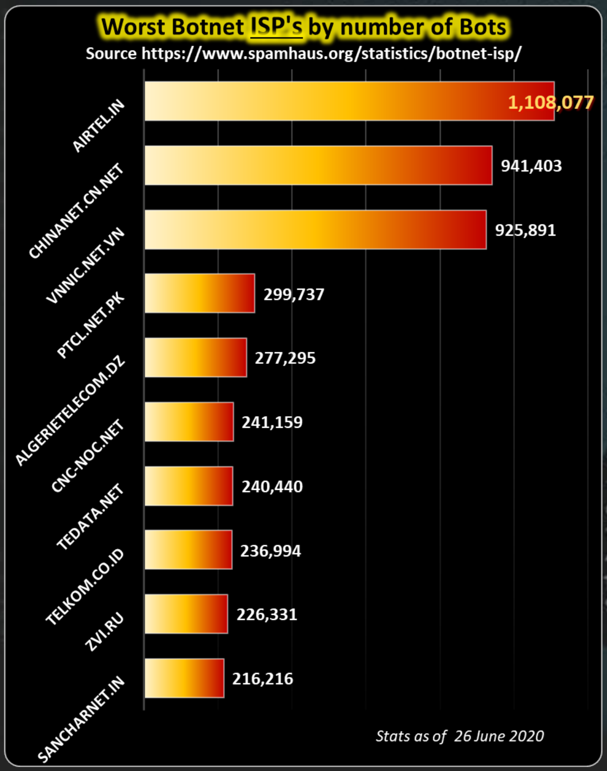
70 malicious Chrome extensions found spying on 32 million+ users

The massive spying campaign targeting Chrome users was exposed by researchers at Awake Security. Over the past few months, we've uncovered various instances how threat actors have been targeting Google Chrome users through malicious extensions. Turns out, the game continues with another similar incident just recently reported. Discovered by Awake Security, 70 new malicious Chrome extensions have been found boasting over 32 million downloads in totality. To put the number of downloads into perspective, according to the co-founder & chief scientist of Awake – Gary Golomb – to date, this happens to be the largest malicious campaign targeting Chrome. According to the firm, these extensions were posing as tools meant to convert files between different formats. However, in actuality, they were stealing the browsing history of users and trying to gain access to any sensitive credentials they could get their hands on.

Read the full story here: HackRead

Worst Botnet ISP's by number of Bots

Source https://www.spamhaus.org/statistics/botnet-isp/



Stats as of 26 June 2020

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

Social Networking Safety and Security Tips

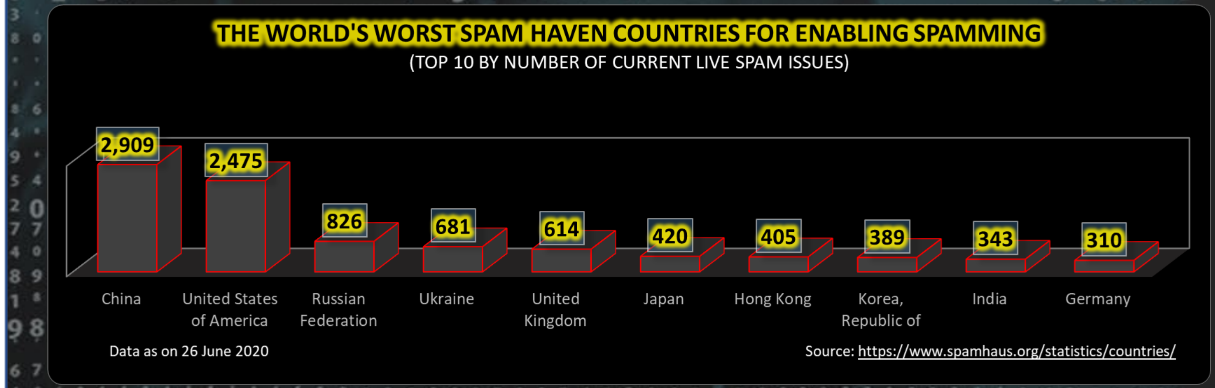
Social networking through Facebook, twitter, LinkedIn, Telegram, to name just a few, has become an indispensable and intrinsic part of our lives. So much so that if we lose connection or can't find a telecom or wi-fi signal, it transcends into this huge crisis in our lives as we become more and more dependent on this technology and the social interaction it provides. Being so utterly dependent on it, also brings with it some safety and security challenges that we have to constantly bear in mind. Norton Security has put together 15 basic safety and security tips to help us with exactly that. Below I have included 10 of the essential ones but please check it out online.

1. Be Cautious of Sharing Too Much - When utilizing a social networking website, people have the option of sharing personal details with friends and followers. While sharing some information is okay, other facts can reveal too much about who a person is. For the sake of personal safety, one should never reveal their date and place of birth, home address or phone number, as this could put them at serious risk for identity theft and fraud. In addition, it is extremely important that a person never reveal their credit card numbers, banking information, passwords, or social security number on any networking site. If such information is shared it would be very easy to fall victim to crimes ranging from stalking to identity theft.
2. Adjust Privacy Settings - Nearly all social networking sites have pre-set or default privacy settings. People often feel that these setting are sufficient enough and never put forth the effort to make changes. Altering one's privacy settings can allow the account holder to block strangers and people who are not friends with them from viewing his or her private information. These settings also limit what information is available in search results; for example, Facebook allows the account holder to modify their settings so only their friends, friends and networks, specific groups, or no one can see their status, photos, videos, likes, etc. Privacy settings can be adjusted at any time; however, the account holder must log in to make adjustments.
3. Limit Details About Work History - On some social networking sites, such as LinkedIn, people are able to post resumes and other information that pertains to their work history. Work related information can reveal too much about a person's personal life and can give criminals such as hackers personal information which may help them to hack into one's account. The information that is found on resumes can also be used in identity theft.
4. Verify Who You're Connecting With - There are a number of reasons why a person may put up a false account. If there is ever uncertainty about the authenticity of an account that claims to belong to a friend, is important to check with the individual for verification. These accounts may be setup in efforts to misrepresent themselves as another person in order to make false statements. This may be done to embarrass someone or to create problems that either of a legal or personal nature. False accounts may also be set up to for the purpose of sending people to malicious sites or with the intent of committing fraud.
5. Keep Control of Comments (Be Aware of Impersonators) - Impersonation can be a problem when it comes to comments on networking websites. Typically, people who are misrepresented online only need to ask that the impersonator be removed. This can be a hassle, however, networking sites are beginning to require commenters to go through an authentication process in which they are identified as registered users or not.
6. Don't Share Personal Details - Microblogging websites encourage people to share in the moment activities and slices of life. For people who enjoy this sort of social interaction, they may find that they are revealing too much about what is happening and as a result making themselves the ideal victim for thieves and other criminals. Because these networks are visible to practically everyone, a person should not reveal information that alerts criminals to their whereabouts or other actions. For example, a person should never reveal where they are vacationing, shopping, or traveling. It should also never be revealed when they expect to leave or return home.
7. Check Out Your Own Account - In order to ensure the security of one's account, it is wise to search for their profile from the prospective of someone who is conducting a search. This step will let the account holder know what others are able to view. When using a search engine to look for one's profile they will also be able to see if there are any false accounts set up in his or her name.
8. Control What Information is Shared with Outside Sources - When a person joins a social networking site, they should understand how that site uses their private information. A user's personal details may be shared with partners, advertisers, or other outside companies. Reading the privacy policy of the social networking platform will explain exactly how private information is used. Unfortunately, people do not fully read these policies before agreeing to them. The privacy terms should be rechecked in the event that a company is sold as these policies may change.
9. Be Careful of Over-Friending - As a member of a social networking group, it can be exciting to gain new "friends" or followers. Looking through the network it is easy to find members with high numbers of friends, which can inspire a competitive streak in some. A high number of friends, however, is not always positive. Some "friends" can be problematic by introducing spam into one's timeline or some may even have criminal intentions. When accepting friends, choose people who are actual friends.
10. What Goes Online Stays Online - When sharing information online it is important for people to realize the permanence of what they type or download. Once information goes on the Internet, through social networking, microblogging, etc., it is difficult, if not impossible to remove. In some instances, the information may even be captured via screen shot and used on blogs or news sites. Depending on what was originally submitted, the information can prove detrimental for future job prospects, relationships, and may even leave a person vulnerable to crimes.

(Thank you to Sergio Stefani who highlighted the need for safety and security awareness in social networking)

THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING

(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)



Data as on 26 June 2020

Source: https://www.spamhaus.org/statistics/countries/

Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com