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

On January 22, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google and Microsoft products. No change since 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

31 January 2020

In The News This Week

Wawa's massive card breach: 30 million customers' details for sale online

The Wawa breach may rank as one of the biggest of all time, comparable to earlier Home Depot and Target breaches. On Monday, hackers put up for sale the payment card details of more than 30 million Americans and over one million foreigners on Joker's Stash, the internet's largest carding fraud forum. This new "card dump" was advertised under the name of BIGBADABOOM-III; however, according to experts at threat intelligence firm Gemini Advisory, the card data was traced back to Wawa, a US East Coast convenience store chain. A month before, in December 2019, Wawa disclosed a major security breach during which the company admitted that hackers planted malware on its point-of-sale systems. Wawa said the malware collected card details for all customers who used credit or debit cards to buy goods at their convenience stores and gas stations. The company said the breach impacted all its 860 convenience retail stores, of which 600 also doubled as gas stations. According to Wawa, the malware operated for months without being detected, from March 4 until Dec. 12, when it was removed from the company's systems. This prolonged infection period, along with a massive compromise of hundreds of different locations, appears to have allowed the criminal group behind this hack to amass a huge trove of payment card details. Read the full story by Catalin Cimpanu here: ZDNet Article

Avast and AVG collect and sell your personal info via their free antivirus programs

Avast and its subsidiary AVG, caught selling customer data to corporate clients last year, are at it again—this time using its free antivirus programs if you opt in to data collection, a new report said Monday. The joint report by Vice's Motherboard and PCMag build upon reports by Adblock Plus creator Wladimir Palant, who reported in October, 2019 that the Avast Online Security Extension as well as the AVG Secure Browser spy on users, harvesting their information. Read the full story by Mark Hachman here: PCworld

Russian Brothers Sentenced to 12 Years for Fraud and Identity Theft

The pair, based in Fort Lauderdale, Fla., were running a sophisticated credit card fraud factory.
Igor and Denis Grushko, brothers previously convicted in federal court of aggravated identity theft, conspiracy to possess and use stolen credit cards, production of fraudulent credit cards, and production of counterfeit identification documents, have been sentenced to 145 months in prison. The sentences were handed down in the District Court for the Southern District of Florida. The brothers, Russian nationals living in Fort Lauderdale, Fla., were accused of conspiring with Ukrainian national Vadym Vozniuk to run a sophisticated and successful credit card fraud and identity theft ring based in South Florida. Vozniuk was convicted separately and sentenced to 27 months in prison. Read the full story here: DarkReading

Security risk for e-scooters and riders

New research finds e-scooters have risks beyond the perils of potential collisions. Computer science experts have published the first review of the security and privacy risks posed by e-scooters and their related software services and applications. Micromobility vehicles, such as e-scooters, zip in and out of traffic. In San Antonio alone, over 12,000 scooters are on the road. For this reason, micromobility is seen as an alleviating trend to help tackle traffic congestion. However, new research out of UTSA finds e-scooters have risks beyond the perils of potential collisions. Computer science experts at UTSA said "We've identified and outlined a variety of weak points or attack surfaces in the current ride-sharing, or micromobility, ecosystem that could potentially be exploited by malicious adversaries". Hackers can cause a series of attacks, including eavesdropping on users and even spoof GPS systems to direct riders to unintended locations. Some e-scooter models communicate with the rider's smartphone over a Bluetooth channel and someone with malicious intent could eavesdrop on these wireless channels and listen to data exchanges between the scooter and riders' smartphone app by means of easily and cheaply accessible tools such as Ubertooth and WireShark. Read the full story here: ScienceDaily

Most notable ransomware of the last decade – Part 2

As discussed last week, since the first notable ransomware in **1989** the ransomware landscape has evolved dramatically and money spent globally to recover from and protect against ransomware attacks are running into the billions. The number of attacks are not really going up but the sophistication levels are, in fact more and more variants of malware are introduced weekly, as we saw three new strains hit the headlines last week alone. With this bit of background and carrying on from last week , we are looking at the most notable ransomware variants that made headlines over the last decade and last week I covered Reveton, CryptoLocker, CryptoWall, Fusob and WannaCry. We carry on this week and look at the next most notable ransomware that mainstreamed in the last decade. (Note: If you are a victim, scan the net for remediation steps and/or decryptors, free decryptors or paid decrypting services are available for most historic and some current Ransomware strains, see this site as an example: Decryptors)

Petya (aka: GoldenEye, NotPetya) 2016

The malware is believed to be named after the satellite in the James Bond movie, GoldenEye. Although identified in 2016, Petya really made headlines in 2017 when a global cyber attack was launched with the biggest concentration in the Ukraine. The attack, believed to be state sponsored, targeted mostly organisations in the Ukraine and experts strongly speculated that it was a politically motivated attack to destabilise the Ukrainian government. Evidence investigated by major security companies like ESET and F-Secure suggested that a compromised software update mechanism of "M.E.Doc", a Ukrainian tax preparation program, were used to spread the malware. Petya's payload infects the computer's master boot record, overwrites the Windows bootloader, and then triggers a restart without an option to postpone or stop the restart. When the system starts up again, the virus encrypts the Master File Table and then a ransom message pops up demanding payment in Bitcoin to decrypt the system and render it usable again. What made this one stand out even more is that one variant actually carried a second virus, "Mischa" that kicked of if the original Petya infection failed to install. Mischa was more conventional and encrypted files on the hard drive but the effect were the same. The NotPetya variant also used the NSA's EternalBlue exploit used in the WannaCry attacks. Some believe that the threat group Black Energy might have been responsible for he attack.

Bad Rabbit 2017

Bad Rabbit first appeared in October of 2017 mainly targeting news and media organizations in Russia and a few in the Ukraine. Security experts strongly believe that Black Energy (Same group believed to be responsible for NotPetya) were responsible for the attack and that the group operates under the direction of the Russian government. Bad Rabbit spread through "drive-by attacks" where insecure websites were compromised. While the user is visiting a legitimate website, a malware dropper is being downloaded from the perpetrator's infrastructure. Bad Rabbit differs from Petya and WannaCry in the sense that the malware did not install itself, it was rather disguised as a "legitimate" software update file, in this case it was disguised as an Adobe Flash installer file. When the file is opened it starts locking the infected computer and pops up the ransom note. Bad Rabbit first encrypts files on the user's computer and then replaces the MBR (Master Boot Record). This means you need to buy two keys, one for the bootloader and one for the files themselves. While it doesn't appear to include the Eternal Blue Windows exploit that was stolen from the NSA and used in NotPetya and WannaCry, it does use one of the NSA's security exploits called EternalRomance. The attack didn't last long, suggesting that the instigators shut it down themselves.

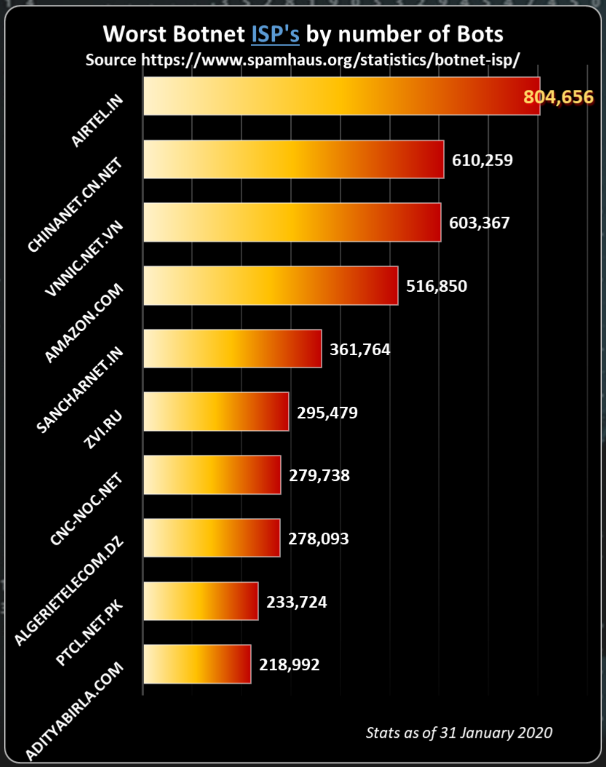
SamSam 2018

SamSam ransomware is a custom made infection used in targeted attacks that does not act like most other ransomware but rather perpetrate as ransomware-as-a-service whose controllers or threat actors carefully probe pre-selected targets for weaknesses. Although around since 2015, it really got mainstream attention in 2018 when the City of Atlanta and several healthcare institutions was targeted. The malware are using various tactics from exploiting vulnerabilities in remote desktop protocols (RDP), Java-based web servers, file transfer protocol (FTP) servers or brute force password attacks to gain access to the targets network. Once in, the real attack takes place and 2048 bit encryption of the target's files takes place. Malwarebytes report that hospitals, city municipalities, and many more from Indiana to New Mexico were all struck down by SamSam in varying degrees of severity. A hospital in Indiana, in particular, was reduced to working with pen and paper in stormy weather. They decided to pay the ransom and get systems back up and running, given the cost of the fix was more than the ransom.

Ryuk 2018-2020

Like SamSam, Ryuk is another targeted ransomware variant that had a huge impact in the last two years, with its targets being chosen specifically as organizations that cannot afford to have any downtime other than planned maintenance slots. Some of the victims included The North Carolina Water utility and some of the larger newspapers. Some experts believe it is somehow connected to the HERMES ransomware strain attributed to the infamous North Korean Lazarus Group. Each attack seems to be exclusively tailored for the targeted organisation which makes it extremely difficult defend against. It is also know as the ransomware with the highest ransom demands, up to 50 Bitcoins per infection. Security Boulevard named it Ransomware of the month this week as they said "the state of Florida had to cough up $1 million worth of ransom to pay off Ryuk attackers. The situation was so bad that cities like Riveria beach were completely shut down: cops started giving paper tickets, 911 line was in a fix, the city's water supply grid went offline, it bought the city to a grinding halt". They also said that many countries like the UK issued a Ryuk ransomware alert.

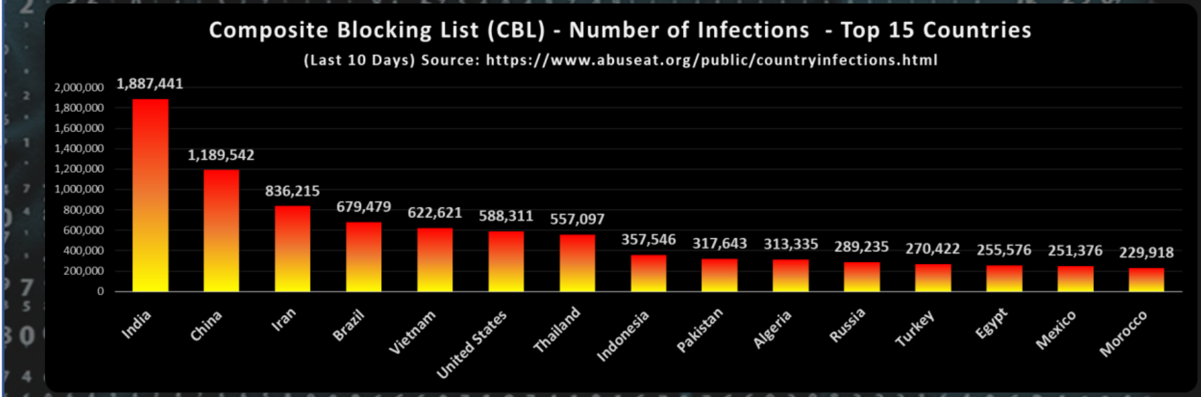
Although the number of ransomware attacks are steadily declining, the sophistication and the size of the targets are going up at an alarming rate. To stay ahead of the game, we have to use all the resources in our arsenal to prevent, detect and respond to these increasing menaces of the Cyber world


Worst Botnet ISP's by number of Bots
Source https://www.spamhaus.org/statistics/botnet-isp/

Stats as of 31 January 2020

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

Hey Frank, just hacked the GPS on my son's e-scooter, he's on his way to you at the barber shop … hie hie hie..!!!
The power of a tech-savvy parent ☺


Composite Blocking List (CBL) - Number of Infections - Top 15 Countries
(Last 10 Days) Source: https://www.abuseat.org/public/countryinfections.html

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