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**

## 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

24 January 2020

## In The News This Week

### Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices

On Sunday ZDNet reported that a hacker has published a massive list of Telnet credentials for more than 515,000 servers, home routers, and IoT (Internet of Things) "smart" devices. The list, which was published on a popular hacking forum, includes each device's IP address, along with a username and password for the Telnet service, a remote access protocol that can be used to control devices over the internet. According to experts to who ZDNet spoke, and a statement from the leaker himself, the list was compiled by scanning the entire internet for devices that were exposing their Telnet port. The hacker then tried using (1) factory-set default usernames and passwords, or (2) custom, but easy-to-guess password combinations. These types of lists -- called "bot lists" -- are a common component of an IoT botnet operation. Hackers scan the internet to build bot lists and then use them to connect to the devices and install malware. ZDNet said, "To our knowledge, this marks the biggest leak of Telnet passwords known to date". Read the full story by Catalin Cimpanu here: ZDNet Article

### Beware, Snake has arrived - New ransomware can lock you out of your PC

Researchers and white-hat hackers associated with MalwareHunterTeam have discovered a new type of ransomware attack they've dubbed SNAKE. This ransomware stealthily infects systems and encrypts files without the user's knowledge. Then, once the user logs on again, it demands a ransom in exchange for access. But unlike other ransomware attacks, SNAKE slithers a bit deeper int o your system than you'd expect and disables remote management. Remote management, which allows users to log into their computer as the admin from another system, is one of the backbones of ransomware recovery in the cybersecurity field. With remote management disabled, there are no longer any backdoor methods to access a compromised system. Read the full story by James Gelinas here: KIMKOMANDO

### UN calls for investigation after Saudi crown prince implicated in hack of Jeff Bezos' phone

Davos, Switzerland (CNN Business)UN experts said they are "gravely concerned" by information they have received suggesting that a WhatsApp account belonging to Saudi Crown Prince Mohammed bin Salman was used to deliver spyware to the mobile phone of Amazon CEO Jeff Bezos. "The information we have received suggests the possible involvement of the Crown Prince in surveillance of Mr. Bezos, in an effort to influence, if not silence, The Washington Post's reporting on Saudi Arabia," the experts said in a statement Wednesday. The statement was released by UN special rapporteur Agnes Callamard, who specializes in extrajudicial killings and conducted an investigation into the murder of Washington Post journalist Jamal Khashoggi, and David Kaye, a UN special rapporteur focused on freedom of expression. The pair called for an investigation into the allegations. The UN experts released their statement after media outlets including CNN Business reported that a forensics team hired by Bezos had concluded that the CEO's mobile phone had been compromised and that the hack originated from an account controlled by bin Salman. A source told CNN that the forensics team had reached its conclusion with "medium to high" confidence. The story was first reported by The Guardian. Saudi Arabia denied on Tuesday that it was responsible for any such hack. The Saudi embassy in Washington wrote on Twitter that "recent media reports that suggest the Kingdom is behind a hacking of Mr. Jeff Bezos' phone are absurd."
"We call for an investigation on these claims so that we can have all the facts out," the embassy added.
The UN experts said in their statement that they "recently became aware" of a forensic analysis of Bezos' phone which assessed that it was infiltrated on May 1, 2018, with a video file sent from a WhatsApp account utilized personally by bin Salman.
Read the full CNN article by Charles Riley and Shimon Prokupecz here: CNN

### Craziest IoT Device Hacks – Becoming a Backseat Driver

Automotive cyber-security experts Charlie Miller and Chris Valasek have made waves (or speedbumps) in recent years by hacking into Chrysler Jeep Cherokees. What started as sending remote commands via the system that queries the GPS system has turned straight into a plot from an action movie such as Fast and Furious. They've now proven that a hacker can remotely turn the steering wheel or activate the parking brake, all at highway speeds. The long feared concept that somebody could turn you and your automobile into a crash test dummy is quickly becoming a reality. Find more crazy IoT hacks by Mike O'Malley here: RadwareBlog

## Most notable ransomware of the last decade – Part 1

By now, if you haven't heard of ransomware you are probably a recluse living in a grotto on a very, very remote island. The first notable ransomware incident took place in **1989** when an anthropologist mailed and distributed 20,000 floppy disks to subscribers and delegates of an Aids conference according to Becker's Hospital Review. From thereon, it just got worse and the last decade has been marred by an unprecedented rise in Ransomware attacks and there is no end in sight as the attackers gets increasingly sophisticated and are steadily raising the value of ransom demands. In a recent report by Julianna De Groot of DigitalGuardian there were an estimated 184 million ransomware attacks last year alone. The modern-day ransomware attacks however became more prevalent from 2012 onward and today I want to explore and highlight some of the most notable ransomware strains that surfaced over 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)

### Reveton (aka: Zeus) 2012

Reveton is a trojan infection that, once installed, will prevent the user from accessing the desktop and will display a message saying that the system was locked by a local law enforcement authority for illegal activities on the machine; the specific authority mentioned varies depending on the affected user's location. The message informs the user that to unlock their system, they would have to pay a fine using a voucher from an anonymous prepaid cash service such as paysafecard, Greendot, etc. The Reveton malware strain embedded itself as an executable in the start-up folder. This malware strain however, did not encrypt any files on the infected computer and was fairly easy to remove by IT technicians. Zain Qaiser, a distributer of the virus was sentenced to 6 years in prison in April 2019.

### CryptoLocker 2013

The CryptoLocker Ransomware attack surfaced in September 2013 and wreaked havoc until May 2014. CryptoLocker is a trojan that targeted Microsoft Windows PC's and was primarily deliver via infected email attachments and the Gameover ZeuS botnet. When activated, CryptoLocker encrypted certain types of files stored on local and mounted network drives after which a message was displayed on the PC which offered to decrypt the data if a payment through either bitcoin or a pre-paid cash voucher (Similar to Reveton), was made by a certain time else the decryption key would be deleted, and it threatened to delete the private key if the deadline passes. If the deadline was not met, the perpetrators offered to decrypt data via an online service for a significantly higher price in bitcoin. There was no guarantee that payment would release the encrypted content. The CryptoLocker itself could be removed easily but as per Wikipedia, the affected files remained encrypted in a way which researchers considered unfeasible to break. Many victims payed the ransom. It mainly ceased to spread after the "Operation Tovar" clampdown on the Gameover ZeuS Botnet gang in 2014.

### CryptoWall (aka. Cryptobit or CryptoDefence) 2014

At the time of the Operation Tovar clampdown on CryptoLocker, CryptoWall made it's appearance in early 2014. This ransomware infected Windows machines and was most noted for it's destructive nature and strong encryption. Later versions used an AES key for encryption and further encrypted the AES key using a unique public key generated on a remote server making it almost impossible to get the actual decryption key. At first it was mainly distributed through exploit kits on compromised websites or add campaigns but later also through widespread SPAM campaigns. Once the system is infected, it runs new registry with Windows start-up. From then on, it connects to distant locations and starts interacting with the Command and Control server. After infecting the system, the ransomware encrypts predetermined files and blocks the user so that they don't access them. CryptoWall is very popular under fraudsters as they could get it for cheap on the dark web and there is still variants running even today.

### Fusob (aka. Small) 2015

Fusob made the headlines in 2015 as it was one of the first notable ransomware that targeted mobile devices and till today accounts for more than half of all mobile ransomware attacks. Similar to Reveton, once a device was infected, Fusob first encrypted all the data on the device and then ordered victims to pay a ransom by displaying a warning message accusing the user of some random illegal or embarrassing act. The only form of payment accepted was in the form of iTunes gift cards. Fusob masqueraded as a pornographic video player, deceiving users into installing a seemingly safe app that downloaded Fusob's payload onto the device. Once installed, the device would be locked, and a ransom payment demanded. Germany, the U.S. and the UK were the primary targets.

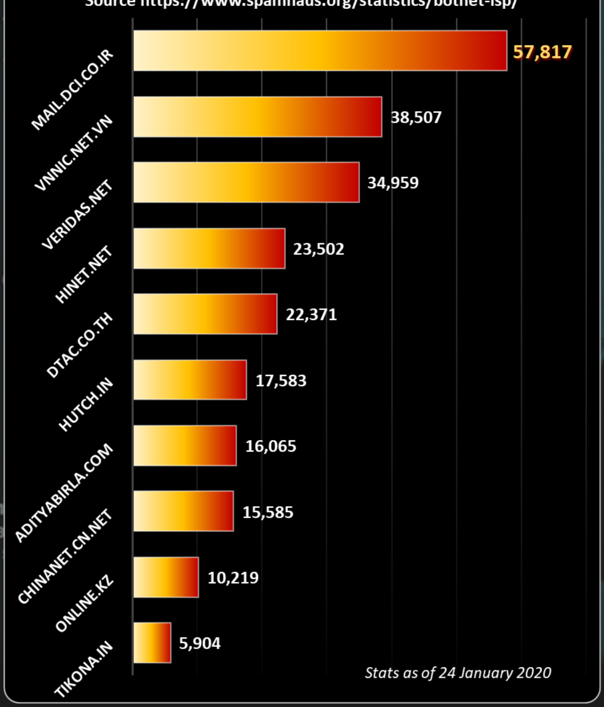
### WannaCry 2017

The famous WannaCry popped up in 2017 and was probably the ransomware with the widest spread of attack so far as hundreds of thousands of machines were infected over roughly 150 countries. Networks were infiltrated through a common vulnerability identified on most machines known as EternalBlue. EternalBlue is a cyberattack exploit developed by the U.S. National Security Agency. It was leaked by the Shadow Brokers hacker group in April 2017 (See last week's bulletin on notorious hacker groups). Although a patch was available, most organisations deemed it insignificant and many large conglomerates fell victim after leaving their systems unpatched for a couple of months after the patch were communicated and released. The scary thing is, you still get unpatched machines in smaller organisations even today.

Next week we'll continue and explore other famous and notable ransomware strains like Petya, Bad Rabbit, SamSam, etc. So stay tuned ☺

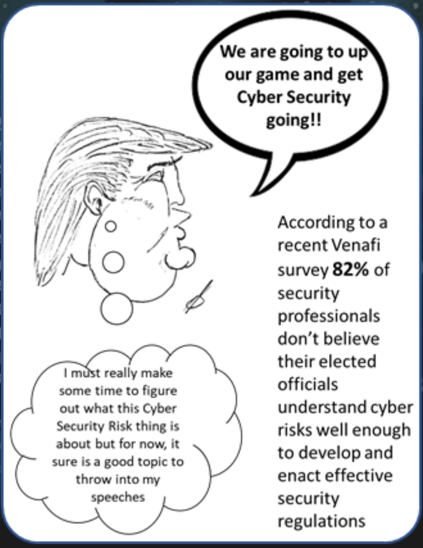
Worst Botnet ISP's by number of Bots

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



Stats as of 24 January 2020

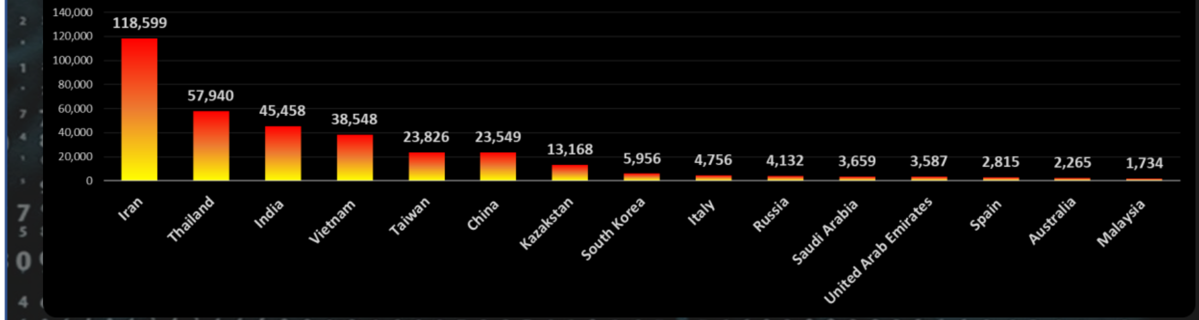
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov


We are going to up our game and get Cyber Security going!!
I must really make some time to figure out what this Cyber Security Risk thing is about but for now, it sure is a good topic to throw into my speeches

According to a recent Venafi survey **82%** of security professionals don't believe their elected officials understand cyber risks well enough to develop and enact effective security regulations

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