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

**On January 6, 2020, the MS-ISAC Cyber Threat Alert Level was evaluated and is being raised to Blue (Guarded). US Department of Homeland Security released a National Terrorism Advisory describing that several members from Iranian leadership and affiliated violent extremist organizations have publicly stated that they intend to retaliate against the United States following the death of Iranian General Qasem Soleimani.**

### 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

10 January 2020

## In The News This Week

### US Government Agency Website Breached By 'Iranian' Hackers

An Iranian hacker group, probably members of AP33, defaced the website of an U.S. government agency and posted messages vowing revenge for the death of top military commander Qassem Suleimani who was killed in a US drone-strike in Iraq on the 2nd of January. According to news reports, the website of the Federal Depository Library Program was replaced on Saturday with a page titled "Iranian Hackers!" that displayed images of Iran's supreme leader Ayatollah Ali Khamenei and the Iranian flag. "Martyrdom was (Suleimani's)... reward for years of implacable efforts," read the graphic, which also depicted U.S. president Donald Trump being punched in the face.
Several resources carry the story: Security Magazine, Daily Mail, GBHackers

### The Y2K bug is back, causing headaches for developers again

Twenty years ago, as the world celebrated the start of a new millennium, IT professionals across the globe were getting cold sweats at the prospect of the Y2K bug kicking in: the fear that important systems relying on two-digit date logs would come to a standstill if computers interpreted the 1 January 2000, registered as 01/01/00, as the first day of the year 1900. No major incident happened, because developers had seen Y2K coming and prepared well. But two decades later, it has become apparent that some resorted to a quicker fix than others, and simply postponed the problem to 2020. Parking meters across New York, for example, declined credit card payments after an outdated software took the payment option offline in the New Year. The Department of Transportation is still going through the city to manually update the 14,000 parking meters one by one and dubbed the problem a "Y2K2X software glitch". Many other issues related to the date bug were reported world wide. So why are computer systems suddenly struggling with a 20-year-old bug? In some cases it may come down to a technique informally called "the pivot year" and which many a developer used back in 2000 to tackle the Y2K bug.
Read the full story here: ZDNet Article

### City of Las Vegas said it successfully avoided devastating cyber-attack

Officials from the city of Las Vegas said they narrowly avoided a major security incident that took place on Tuesday, January 7. According to a statement published by the city on Wednesday, the compromise took place on Tuesday, at 4:30 am, in the morning. The city said IT staff immediately detected the intrusion and took steps to protect impacted systems. The city responded by taking several services offline, including its public website, which is still down at the time of writing. City officials have not disclosed any details about the nature of the incident, but local press reported that it might have involved an email delivery vector. In a subsequent statement published on Twitter on Wednesday, the city confirmed it "resumed full operations with all data systems functioning as normal." "Thanks to our software security systems and fast action by our IT staff, we were fortunate to avoid what had the potential to be a devastating situation," it said. "We do not believe any data was lost from our systems and no personal data was taken. We are unclear as to who was responsible for the compromise, but we will continue to look for potential indications," the city also added. Read the full story here: MaritimeCyberSecurity

### Craziest IoT Device Hacks – Cayla, the Illegal Espionage Apparatus

With waist-length golden hair and a voice designed to warm a child's heart, the doll named Cayla has brought delight to millions of children throughout Germany. In reality, she's an "illegal espionage apparatus" that must be destroyed immediately, according to Germany's Federal Network Agency. Once hackers are in control of this Wi-Fi-enabled interactive doll, they can use its cameras and microphones to see and hear whatever Cayla does, allowing hackers to track their location or potentially heist profits from the local street-side lemonade stand.
Find more crazy IoT hacks by Mike O'Malley here: RadwareBlog

## Notorious Hacker Groups and the Impact they had

Hacker Groups are really "street" gangs with a common launchpad for their activities, computers and telecommunication networks. Hackers and hacking groups can be categorised by their motivation and interests. Some are in it purely for financial gain, others are motivated by the hacking subculture that promotes the challenge of breaking in and leaving their mark. There is also a rise in sophisticated crime syndicates with varied objectives that sometimes offer their services to anyone who is willing to pay to disrupt or spy on rivals or businesses. Then the latest and scariest trend is State Sponsored hacking groups with unlimited resources and very focused political and/or terror objectives and agendas. Today we will look at only a few historical and currently active groups and the impact they had or have on society. The list of active groups and their activities are quite staggering and if this article sparked your interest I encourage you to dig a little on the net, you'll be surprised of the sophistication and creativity of some of these groups.

**The scrap between Legion of Doom (LOD) & Masters of Deception (MOD)** - The scrap between LOD and MOD that caused the AT&T phone outage in 1990 was probably the ignition point for many hacker groups that followed. Although the interest in breaking in to computer systems through the telecommunications network was already sparked by the movie **Wargames** that was released in 1984, the feud between these two groups really spawned an unprecedented number of underground computer enthusiasts.
The feud culminated in a showdown between the groups that resulted in the following: On January 15, 1990, millions of Americans picked up their phones to make perfectly routine long-distance phone calls only to hear a slightly hollow, ghostly recorded voice on the other end. "All circuits are busy now," it said. "Please try later." But they were still busy 9 hours later. Almost half of all long-distance calls attempted on the AT&T network failed. The Secret Service and FBI were already investigating the groups after a young hacker by the name of Fry Guy spilled the beans about the group's activities and subsequently to the outage, made several arrests and over time the two groups fizzled out. A number of the members of these groups made a positive turnaround and is today big players in the cyber security and white hat hacking space.
There are several resources that details the full story of the groups but here is one that sums it up nicely: CyberSecurityMastersDegree

**The Shadow Brokers Group** - No one really knows for sure how the Shadow Brokers group came about, but some suggest that their name is possibly a reference to a character in the video game series Mass Effect. Shadow Brokers first appeared on the scene in August 2016 when the group placed a twitter post announcing a GitHub repository with instructions on how to participate in an auction where the successful bidder would receive various tools used by the infamous "Equation Group" owned by the NSA. These tools included EternalBlue, EternalRomance, and other known exploits that spawned some of the most famous malware attacks in 2017 like WannaCry and NotPetya. After failing to sell the tools, the group released a password on a blog to grant access to the tools. Subsequent to these attacks, the group started to offer "data dumps" on the darknet with quite affordable prices to anyone interested. What the Shadow Brokers also did was to expose the covert actions and capabilities of the state sponsored "Equation Group" which in effect is the "Tailored Access Operations" or TAO unit of the US's National Security Agency. The group's apparent knowledge of the inner working of TAO and the NSA also raised suspicions on collaboration or a possible mole in the agency. There was also some speculations that the group had some links with the Russian government.

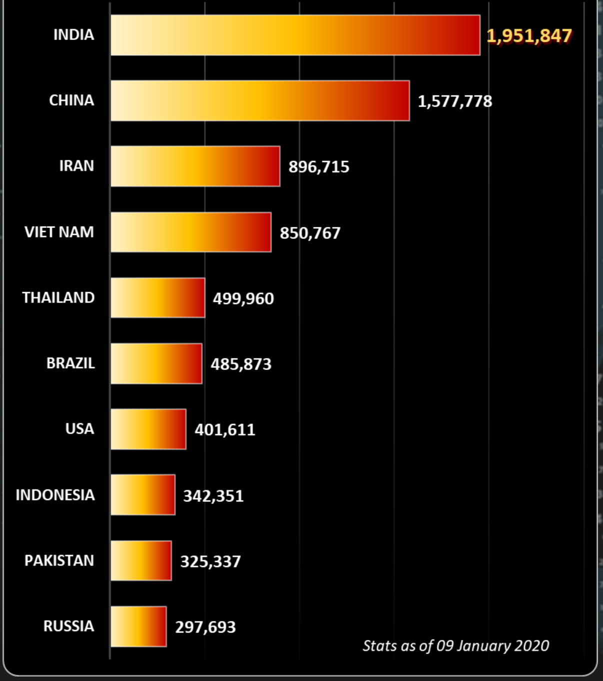
**Bureau 121** - Little is known about the North Korean state sponsored "Bureau 121" hacking group. A North Korean defector, Prof Kim Heung-Kwang, said in 2015 that the agency has around 1,800 members which probably grew significantly since. Although the FBI first claimed that North Korea's cyber capabilities are unsophisticated, cyber security experts says that it is Kim Jong-un's elite cyber-attack unit and that "Bureau 12" is staffed by the best and brightest the country has to offer. North Korea's Military is investing heavily in their cyber-attack capabilities and training of this elite unit. The group is linked to the massive cyberattacks on DNS provider Dyn that knocked down websites like Twitter, Reddit and The New York Times in 2016 but what really put them on the radar was the famous Sony hack prior to the release of the movie "The Interview" in 2014. Today they are considered by AVG as one of the most dangerous hacker groups around.

**Elfin (aka APT33, Holmium, Refined Kitten, etc.)** – (to be continued) The Iranian based Elfin espionage group (aka APT33) is currently an highly active hacking group, believed to be state sponsored. They are mainly targeting organizations in Saudi Arabia, the United States, South Korea and some other countries in the Middle East. The group, which first became active in late 2015 or early 2016, specializes in scanning for vulnerable websites and using this to identify potential targets, either for attacks or creation of command and control (C&C) infrastructure. It has compromised a wide range of targets, including governments along with organizations in the research, chemical, engineering, manufacturing, consulting, finance, telecoms, and several other sectors. Elfin is one of several active Iranian hacking groups who's activity tripled since the assassination of Iranian General Qasem Soleimani last week according to news resources. It was also reported by "USA Today" that a federal website was breached and taken offline on Sunday night after a hacker uploaded photos to the site that included an Iranian flag and an image depicting a bloodied President Donald Trump being punched in the face. The Center for Internet Security (CIS) subsequently raised the Cyber Security Alert level to "Guarded" and cautioned against possible attacks after Iranian leadership and several affiliated violent extremist organizations have publicly stated that they intend to retaliate against the USA.

**Unit 8200** – Unit 8200 is the Cyber Intelligence unit of the Israeli Defence Force and believed to be jointly responsible (collaborating with the US NSA) for developing the famous Stuxnet Malware that was deployed in Iran in 2010 to sabotage and destabilise the Iranian nuclear program. Stuxnet is widely seen as the worlds first digital weapon. Stuxnet was unlike any other virus or worm as it escaped the digital realm to wreak physical destruction on computer controlled equipment. Unit 8200 is said to be the largest unit in the Israeli Defence Force and one of the most sophisticated and dangerous state sponsored hacking groups around.

### Worst Botnet Countries by number of Bots

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



*Stats as of 09 January 2020*

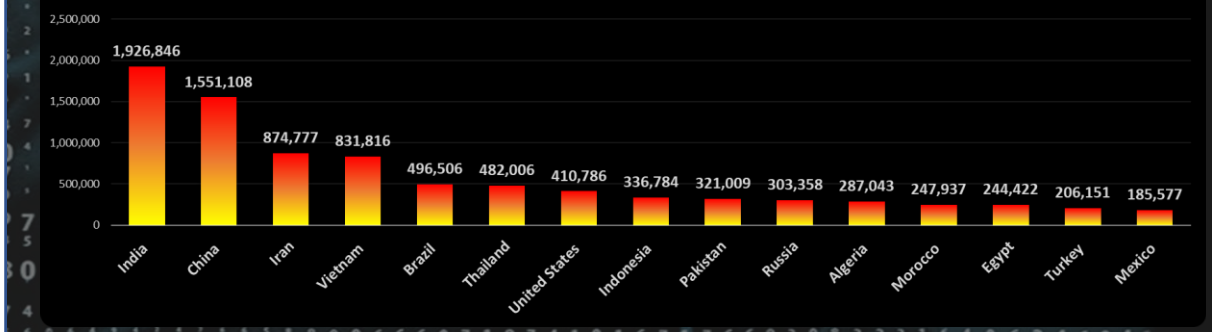
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

### Humour

Oh dear! an email from the IRS? It must be a phishing attempt, lets ignore it..

### Composite Blocking List (CBL) - Number of Infections - Top 15 Countries

(Last 10 Days) Source: https://www.abuseat.org/public/countryinfections.html



**Author: Chris Bester**
chris.bester@yahoo.com