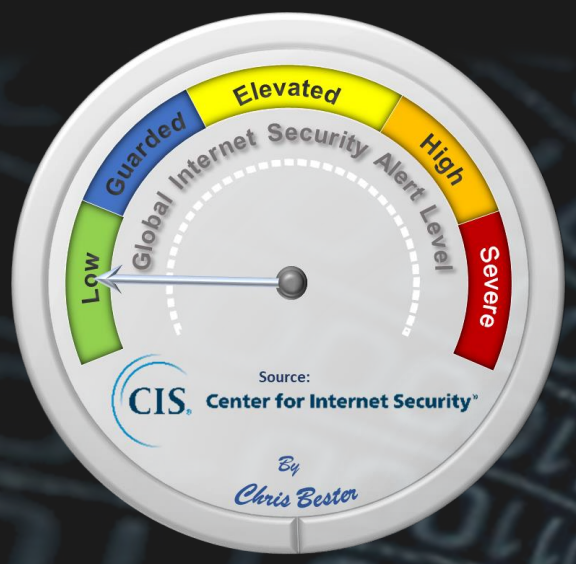


On January 2, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Green (Low).

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

03 January 2020

In The News This Week

U.S. Coast Guard Says Ryuk Ransomware Took Down Maritime Facility

The U.S. Coast Guard (USCG) published a marine safety alert to inform of a Ryuk Ransomware attack that took down the entire corporate IT network of a Maritime Transportation Security Act (MTSA) regulated facility. While the incident is still currently being investigated, the USCG says that **a phishing email is most likely the point of entry** within the MTSA facility's network. "Once the embedded malicious link in the email was clicked by an employee, the ransomware allowed for a threat actor to access significant enterprise Information Technology (IT) network files, and encrypt them, preventing the facility's access to critical files," says the USCG. . Read the full story by Sergiu Gatlan here: BleepingComputer

Non-profit organization Special Olympics New York hacked and its server used to send phishing emails

Special Olympics New York provides inclusive opportunities for people with intellectual disabilities to compete in Olympic-style, coached sports. Unfortunately, the non-profit organization was hacked during the Christmas holiday and the attackers later used its email server to launch a phishing campaign against its donors. "Friends, Boo! As you may have noticed, our email server was temporarily hacked. We have fixed the problem and send our sincerest apologies. While donating to Special Olympics NY is always a good idea, we would never ask in such a grinchy way." wrote Stacey Leinsterman, President & CEO of Special Olympics NY, in a post published on Instagram. The organization disclosed the hack and announced to have locked out the attackers, it also sent a data breach notification to affected people, recommending them to disregard the last received message from the organization. Read the full story by Pierluigi Paganini here: Security affairs

Ransomware Hits Maastricht University, All Systems Taken Down

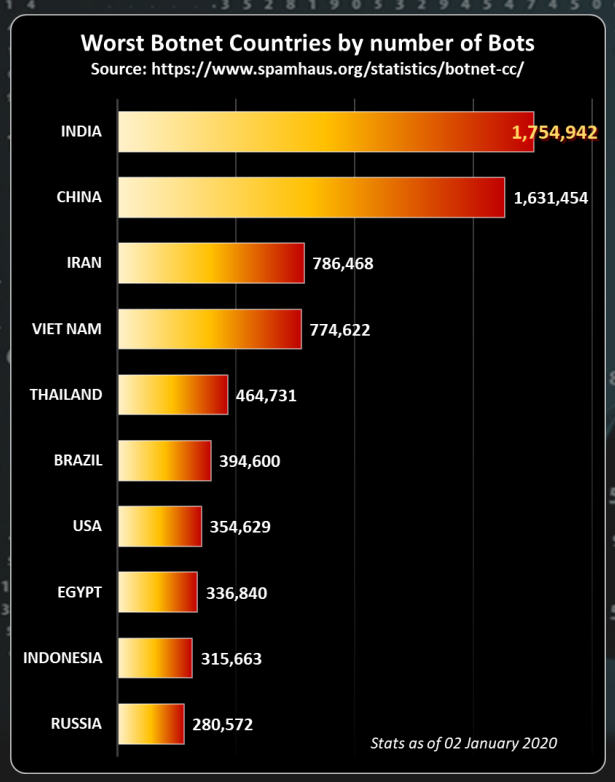
Maastricht University (UM) announced that almost all of its Windows systems have been encrypted by ransomware following a cyber-attack that took place on Monday, December 23. UM is a university from the Netherlands with over 18,000 students, 4,400 employees, and 70,000 alumni, UM being placed in the top 500 universities in the world by five ranking tables in the last two years. "Maastricht University (UM) has been hit by a serious cyber attack," the university announced on Christmas Eve, December 24. Read the full story by Sergiu Gatlan here: BleepingComputer

Chivalric Disorder as Knight and Dame Data Goes Errant

British Government Apologizes for New Year's Honours List Recipient Data Breach. Human error looks to be the obvious culprit in a data breach involving personal details for a who's who of British society. On Friday, Britain's Cabinet Office released a spreadsheet listing the recipients of the 2020 "New Year's Honours" list, which "recognizes the achievements and service of extraordinary people across the United Kingdom." Unfortunately, the original version of the CSV-formatted spreadsheet, posted online Friday night, also listed the home addresses for many recipients, who include members of the police, prison service, military, counter terrorism and celebrities like Elton John and Olivia Newton-John. Read the full story by Mathew J. Schwartz here: BankInfoSecurity

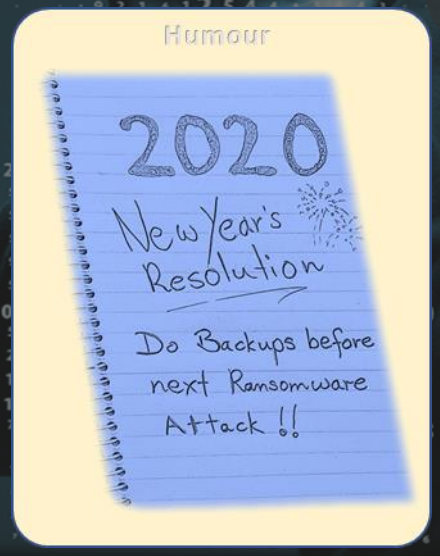
Funniest Hacks - The Spanish PM Was Replaced With Mr. Bean On An Official Site

Anyone visiting the official European Union website for the Spanish Prime Minister in 2010 came face-to-face with a strange surprise. Rather than a picture of Spanish Prime Minister Jose Luis Rodriguez Zapatero, visitors instead saw a picture of the British sitcom character Mr. Bean. Newspapers previously likened Zapatero to the character, possibly prompting the anonymous hacker to carry out the attack. According to the authorities who ran the site, the hack took advantage of a vulnerability known as cross-site scripting.
Read more funny hacks by Nathan Gibson here: Ranker



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

Humour



A decade of hacking: The most notable cyber-security events of the 2010s (Part 4)

Over the past decade, we've seen it all. We've had monstrous data breaches, years of prolific hacktivism, plenty of nation-state cyber-espionage operations, almost non-stop financially-motivated cybercrime, and destructive malware that has rendered systems unusable. This is the fourth and final instalment of an adapted article from ZDNet & CNBC make iT

~~~ 2018 Cont. ~~~

Meltdown, Spectre, and the CPU side-channel attacks - Details about the Meltdown and Spectre vulnerabilities were first made public on January 2, 2018, and they exposed an issue baked into the hardware of most CPUs that could allow hackers to steal data that was currently being processed inside CPUs. While the two aren't the easiest bugs to exploit, and **nor has any attack ever been reported**, Meltdown & Spectre exposed the fact that many CPU makers were cutting corners in terms of data security in their quest for speed and performance. Even if some people still describe the two bugs as "stunt hacks," they fundamentally changed how CPUs are designed and manufactured today.

Magecart goes mainstream - While Magecart attacks (also known as web skimming, or e-skimming) have been taking place since 2016, it was 2018 when attacks grew to a level where they were just impossible to miss -- with high-profile hacks being reported by British Airways, Newegg, Inbenta, and others. The scheme behind these attacks is simple, and it's a mystery why they took so many years to become popular. The idea is that hackers compromise an online store, and leave behind malicious code that logs payment card information, which they later send back to an attacker's server. Several variations on the original Magecart attacks have appeared, but since early 2018, Magecart attacks are, without a doubt, one of today's top cyber threats, and have been driving online shoppers mad, with many not being able to tell if an online shop is safe to use or not. Next to ATM skimming and POS malware, Magecart attacks are the primary method through which cybercriminal groups are getting their hands on people's financial data these days.

Marriott hack - Not as big as Yahoo's three-billion figure, but the Marriott data breach also gets a nod due to its sheer size. The breach was disclosed in November 2018, and impacted more than 500 million guests, a number which the company brought down to 383 million a few months later, after it finished its investigation. Just like in most cases, a post-mortem revealed the company was breached using mundane tactics and tools that could have been easily detected and prevented.

~~~ 2019 ~~~

Uighur surveillance - 2019 will be remembered as the year when China's holocaustic tendencies came to light, with the revelations surrounding the way it treats its Uyghur Muslim minority in the Xinjiang region. While news of organ harvesting and forced labour camps came to light in mainstream media, security researchers also played their part, revealing the widespread use of facial recognition software to track Muslims in Xinjiang cities, but also iOS, Android, and Windows exploits specifically targeted at infecting and tracking the local Uyghur population..

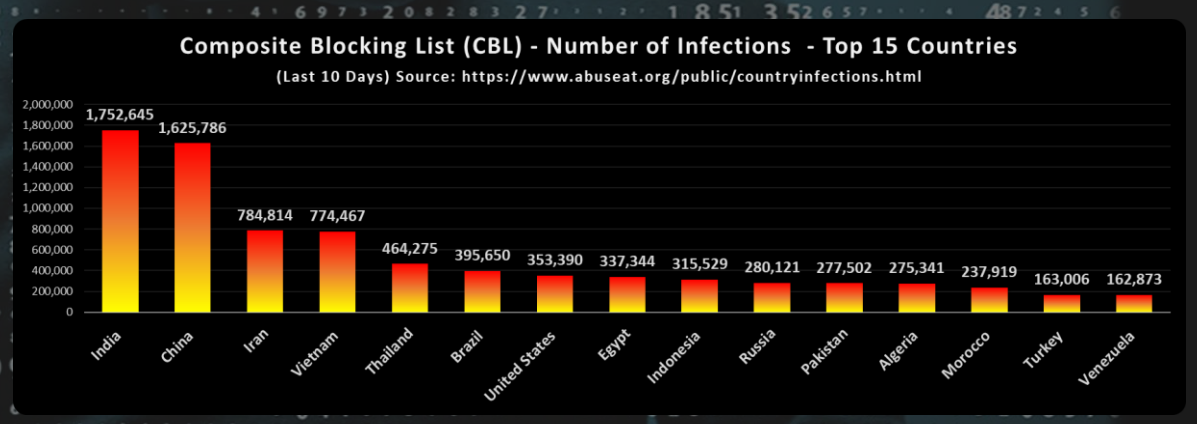
"Big game hunting" ransomware - While ransomware has been a problem all the 2010s, a particularly nasty form known as "big game hunting" has been extremely active in 2019. Big game hunting refers to ransomware gangs who go only after big targets, such as corporate networks, rather than going after the little guy, like home users. This allows hackers to demand more money from victim companies, who have much more to lose than just personal photo albums. The term big game hunting was coined by CrowdStrike in 2018 to describe the tactics of several ransomware gangs, and the number of groups currently engaging in this tactic has easily gone over ten. Big game hunting ransomware attacks ramped up in 2019, with most hitting managed service providers, US schools, US local governments, and, more recently, moving to Europe's bigger companies..

Gnosticplayers - The hacker who made a name for himself in 2019 is Gnosticplayers. Following the modus operandi of Peace_of_Mind and Tessa88 from 2016, Gnosticplayers hacked companies and began selling their data on dark web marketplaces. Companies that had their data stolen by Gnosticplayers and later put up for sale online include Canva, Gfycat, 500px, Evite, and many others. In total, the hacker claimed responsibility for over 45 hacks and breaches impacting more than one billion users.

CapitalOne - Number of records hacked: 100 million. The Capital One hack that was disclosed in July 2019 impacted more than 100 million Americans and six million Canadians. Data from the breach is not believed to have been publicly shared en-masse, so most users who had their data stolen are most likely safe. Yet, the breach stands out because of the way it happened. An investigation revealed that the suspect behind the hack was a former Amazon Web Services employee, who stands accused of illegally accessing Capital One's AWS servers to retrieve the data, along with the data from 30 other companies. The investigation is still ongoing, but if this turns out to be true, this introduces a new threat class for organizations -- namely, malicious insiders working for your supply-chain providers.al.

Dubsmash - Number of records hacked: 161.5 million. In February, video messaging app Dubsmash announced that hackers nabbed nearly 162 million users' account holder names, email addresses and hashed passwords. Hashed passwords are encrypted, so they must be cracked before they can be used. The breach actually occurred in December 2018, but cyber thieves posted that the data was for sale on the dark web in February. It was part of a data dump that included over 600 million accounts from 16 hacked websites.

Zynga - Number of records hacked: 218 million. Mobile game producer Zynga announced in October that a hacker had accessed account log-in information on Sept. 12 for customers who play the popular "Draw Something" and "Words with Friends" games.
In addition to the log-in credentials, the hacker accessed usernames, email addresses, log-in IDs, some Facebook IDs, some phone numbers and Zynga account IDs of about 218 million customers who installed iOS and Android versions of the games before Sept. 2, 2019.



Author: Chris Bester
chris.bester@yahoo.com