Unchanged from last week - On December 4, 2019, the Cyber Threat Alert Level was evaluated and is being raised to Blue (Guarded) due to vulnerabilities in Google and Mozilla 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
13 December 2019

In The News This Week

Snatch Ransomware Reboots Windows in Safe Mode to Bypass Antivirus

Cybersecurity researchers have spotted a new variant of the Snatch ransomware that first reboots infected Windows computers into Safe Mode and only then encrypts victims' files to avoid antivirus detection.
Unlike traditional malware, the new Snatch ransomware chooses to run in Safe Mode because in the diagnostic mode Windows operating system starts with a minimal set of drivers and services without loading most of the third-party startup programs, including antivirus software. Snatch has been active since at least the summer of 2018, but SophosLabs researchers spotted the Safe Mode enhancement to this ransomware strain only in recent cyber attacks against various entities they investigated. "The ransomware, which calls itself Snatch, sets itself up as a service [called SuperBackupMan with the help of Windows registry] that will run during a Safe Mode boot." "When the computer comes back up after the reboot, this time in Safe Mode, the malware uses the Windows component net.exe to halt the SuperBackupMan service, and then uses the Windows component vssadmin.exe to delete all the Volume Shadow Copies on the system, which prevents forensic recovery of the files encrypted by the ransomware." Read the full story by Mohit Kumar here: The Hacker News

Zeppelin Ransomware Targets Healthcare and IT Companies

A new variant of the VegaLocker/Buran Ransomware called Zeppelin has been spotted infecting U.S. and European companies via targeted installs. This family first started out as VegaLocker and then was renamed to Buran Ransomware, where it was promoted as **Ransomware-as-a-Service (RaaS)** in May 2019 on Russian malware and hacker forums. Affiliates who joined the RaaS would earn 75% of the ransom payment, while the Buran operators would earn 25%. It is not known exactly how the Zeppelin ransomware is being distributed, but it is likely through Remote Desktop servers that are publicly exposed to the Internet.
Read the full story by Lawrence Abrams here: Bleeping Computer

Maze Ransomware Behind Pensacola Attack, Data Breach Looms

Maze exfiltrates data as well as locks down systems. Officials said they don't know yet whether any residents' personal information has been breached. The Maze ransomware is likely the culprit behind the recently reported cyberattack on Pensacola, Fla. that occurred earlier this week, which downed systems citywide. The Florida Department of Law Enforcement said that the Pensacola attack was indeed ransomware, and Maze operators quickly took responsibility for the incident, saying that they are demanding $1 million in ransom. It's unclear whether the city is paying the ransom, but officials did say they don't know yet whether any residents' personal information has been breached. The data breach fears are particularly relevant given that Maze has a quirk not found in most ransomwares: In addition to encrypting files and offering the decryption key in exchange for a ransom payment, it also automatically copies all affected files to the malicious operators' servers, according to researchers. The fact that the attackers have exfiltrated the data means the incident is a data breach as well as a malware infection," Read the full story by Tara Seals here: ThreatPost

Funnies Hacks - Operation Cupcake Changed Bomb Instructions To Cake Recipes

Security services do an important job of taking down propaganda and information from terrorist websites. MI6 from the UK achieved this in a rather unique way back in in 2011. Rather than just take down the instructions for making pipe bombs from an online al-Qaeda magazine, they simply replaced the instructions with recipes for cake. Anyone looking to create explosives would instead only get the recipes for cupcakes taken directly from Ellen DeGeneres's "Best Cupcakes in America."
Read more funny hacks by Nathan Gibson here: Ranker

A decade of hacking: The most notable cyber-security events of the 2010s (Part 1)

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. Adapted from an article by ZDNet

~~~ 2010 ~~~

Stuxnet - Stuxnet is a computer worm that was co-developed by the US and Israeli intelligence services as a means to sabotage Iran's nuclear weapons program, which was getting off the ground in the late 2000s. The worm was specifically designed to target SCADA equipment.
Operation Aurora, the Google hack - Not that many internet users know that even the mighty Google had its backend infrastructure hacked. It was part of a series of attacks that later become known as Operation Aurora -- a coordinated hacking campaign carried by the Chinese government's military hackers against some of the world's biggest companies at the time, like Adobe, Rackspace, Juniper, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and others. The actual attacks took place in the 2000s, however, they came to light in early 2010.

~~~ 2011 ~~~

LulzSec and the "50 days of luls" - Every time you see a hacker bragging on Twitter about their hacks, using a broad array of internet memes to make fun of their targets, or taking suggestions on who to DDoS or hack, you're seeing another LulzSec copycat. The group's impact on today's hacking scene cannot be ignored. The group liked to hack big-name companies and then showboat all over the internet. Their "50 days of lulz" campaign and all the other major hacks they carried out set the trend for what we ended up seeing for the rest of the decade from a slew of copycat attention-seeking hacking groups, such as Lizard Squad, New World Hackers, TeaMp0isoN, CWA, and others.
Diginotar hack changes the browser landscape - The hack of DigiNotar is a little-known incident from 2011 that ended up changing how browsers, Certificate Authorities (CAs), and the internet works -- and for the better. In 2011, it was discovered that Iranian government hackers breached DigiNotar and used its infrastructure to issue SSL certificates for mimicking popular websites, including Google and Gmail. Iranian hackers then used the certificates to intercept encrypted HTTPS traffic and spy on more than 300,000 Iranians.
Sony PlayStation hack and massive outage - In the spring of 2011, Sony announced that a hacker stole details for 77 million PlayStation Network users, including personally identifiable information and financial details. Nowadays, this might seem an insignificant number, but at the time, and for many years after, this was one of the biggest hack in the world.

~~~ 2012 ~~~

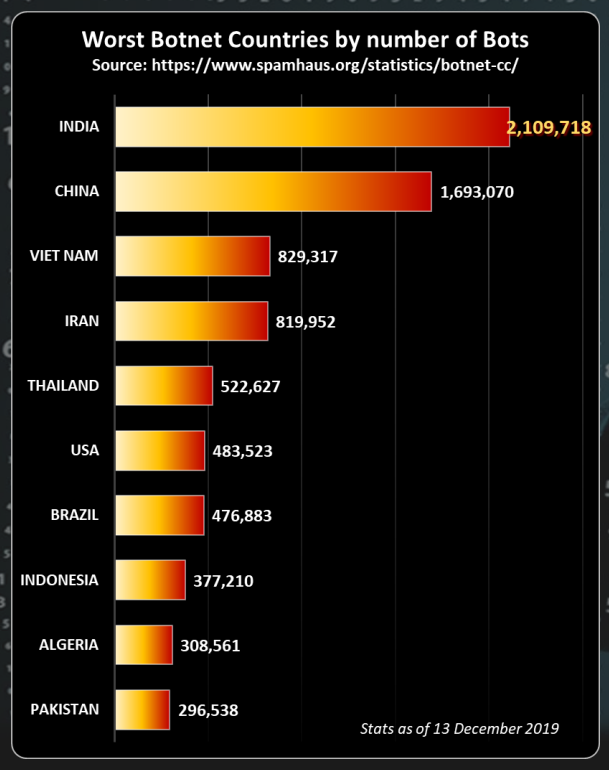
Shamoon and its destruction - Created in Iran, Shamoon (also known as DistTrack) is a piece of malware that can be considered the direct result of the Stuxnet attack from two years before. Having learned first-hand how destructive malware can be, the Iranian government created its own "cyber-weapon," one that it first deployed in 2012. Designed to wipe data, Shamoon destroyed more than 35,000 workstations on the network of Saudi Aramco, Saudi Arabia's national oil company, bringing the company to its knees for weeks.
Flame, the most sophisticated malware strain ever created - Discovered by Kaspersky and linked to the Equation Group (a codename for the US NSA), Flame was described as the most advanced and sophisticated malware strain ever created. It eventually lost this title when Kaspersky found Regin two years later in 2014, but Flame's discovery revealed the technical and capabilities gap between the cyber arsenal of the United States and all the other tools employed by other nation-state groups.

~~~ 2013 ~~~

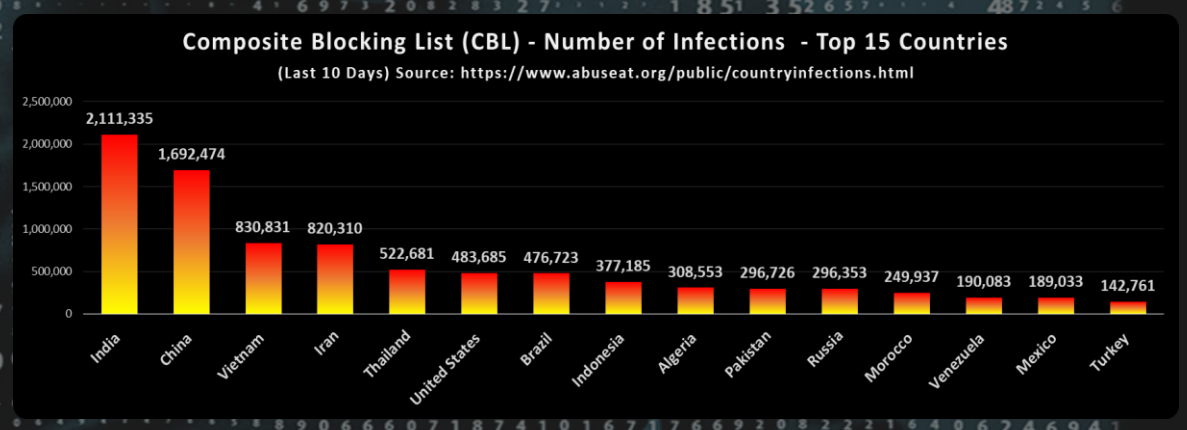
Snowden revelations - So much to say, so little space. We'll just get to the point. The Snowden leaks are probably the most important cyber-security event of the decade. They exposed a global surveillance network that the US and its Five Eyes partners had set up after the 9/11 attacks.
The Target hack - In December 2013, the world was introduced to the term of POS malware when retail giant Target admitted that malware planted on its stores' systems had helped hackers collected payment card details for roughly 40 million users.
The Adobe hack - In November 2013, Adobe admitted that hackers had stolen the data of more than 153 million users. The data was dumped online, and user passwords were almost immediately cracked and reversed back to their plaintext versions.
Silk Road takedown - Silk Road was the first major takedown of a Tor-hosted dark web marketplace for selling illegal products. Its takedown in 2013 showed the world for the first time that the dark web and Tor weren't perfect, and that the law's arm could reach even in this corner of the internet, thought to have been impenetrable up to that point.

~~~ 2014 ~~~

North Korea's brazen Sony hack - The hacks were carried out by a group calling themselves the Guardians of Peace (subsequently referred to as the Lazarus Squad) that were eventually linked to North Korea's intelligence apparatus. The purpose of the hack was to force the studio to abandon releasing a movie called The Interview, a comedy about an assassination plot against North Korea's leader Kim Jong-un. When Sony refused, hackers destroyed the company's internal network and leaked studio data and private emails online.
Celebgate - To this day, cyber-security companies use Celebgate (also known as The Fappening) as an example in training courses about spear-phishing, and what happens when users don't pay attention to the validity of password reset emails. This is because back in 2014, a small community of hackers used fake password reset emails aimed at celebrities to gain access to trick famous stars into entering their Gmail or iCloud passwords on phishing sites. The hackers used these credentials to access accounts, find sexual or nude images and videos, which they later dumped online.



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



Author: Chris Bester
chris.bester@yahoo.com