On April 8, 2020, the Cyber Threat Alert Level was evaluated and is remaining at 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

10 April 2020 – GOOD FRIDAY EDITION

In The News This Week

The COVID-19 pandemic is still the talk of the town and will probably be for quite some time to come. Therefore, the news clips of the week will focus on other cyber security events that needs to be highlighted.

How Just Visiting A Site Could Have Hacked Your iPhone or MacBook Camera

If you use Apple iPhone or MacBook, here we have a piece of alarming news for you. Turns out merely visiting a website, not just malicious but also legitimate sites unknowingly loading malicious ads as well, using Safari browser could have let remote attackers secretly access your device's camera, microphone, or location, and in some cases, saved passwords as well. Apple recently paid a $75,000 bounty reward to an ethical hacker, Ryan Pickren, who practically demonstrated the hack and helped the company patch a total of seven new vulnerabilities before any real attacker could take advantage of them. The fixes were issued in a series of updates to Safari spanning versions 13.0.5 (released January 28, 2020) and Safari 13.1 (published March 24, 2020). "If the malicious website wanted camera access, all it had to do was masquerade as a trusted video-conferencing website such as Skype or Zoom," Pickren said. When chained together, three of the reported Safari flaws could have allowed malicious sites to impersonate any legit site a victim trusts and access camera or microphone by abusing the permissions that were otherwise explicitly granted by the victim to the trusted domain only. Safari browser grants access to certain permissions such as camera, microphone, location, and more on a per-website basis.

Read the full article by Ravie Lakshmanan here: TheHackerNews

New York City bans Zoom in schools, citing security concerns

As schools lie empty, students still have to learn. But officials in New York City say schools are not permitted to use Zoom for remote teaching, citing security concerns with the video conferencing service. "Providing a safe and secure remote learning experience for our students is essential, and upon further review of security concerns, schools should move away from using Zoom as soon as possible," said Danielle Filson, a spokesperson for the New York City Dept. of Education. "There are many new components to remote learning, and we are making real-time decisions in the best interest of our staff and students." Instead, the city's Dept. of Education is transitioning schools to Microsoft Teams, which the spokesperson said has the "same capabilities with appropriate security measures in place." The ban will cover some 1.1 million students in more than 1,800 schools across the city's five boroughs. The decision to ban Zoom from schools was made in part by New York City's Cyber Command, which launched in 2018 to help keep the city's residents safe. Zoom did not comment by the time of publication, but Zoom's chief marketing officer Janine Pelosi later said that the company was in "continued dialogue" with the city "about how Zoom can be of service during this time." Read the full story by Zack Whittaker here: TechCrunch

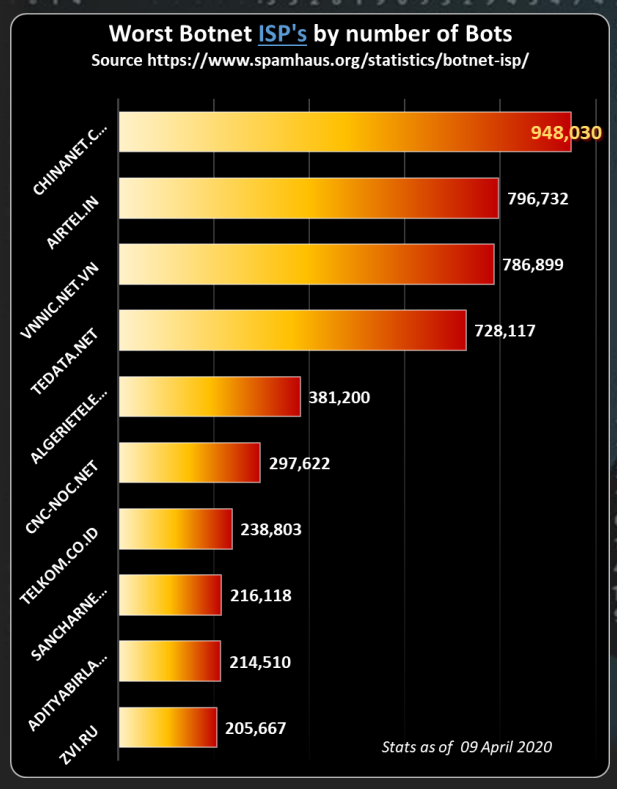
News snippets from the past - Computers & crime

No One Knows Police Beat Better Than The Computer - 1978

The following news snippet in The Hour – Norwalk, Ct. Aug. 23, 1978

New York (UPI).. For years, the police chief's plea at budget time has been, "give me more cars and more men and we'll get there faster and fight crime," but now, according to Police magazine, the validity of the argument is under sharp attack. The Magazine says in its September issue that increased reliance on computer technology is making law enforcement experts dubious of the random police patrol as a deterrent to crime – a view generally not shared by the line officers. "The officer can say, 'Nobody knows my beat better than I do'. New Haven, Conn., Police Chief Edward Morone is quoted as saying "But the truth is, nobody knows the beat better than the computer does."

Read the full story and more here: GoogleArchives



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

Why Do Hackers Hack?

We have touched on this topic a few times in previous editions but the answer to the question has many different answers depending on the type of hacker, the motive and the incentive. Many blogs, security experts and even the odd Psychoanalyst has traversed the path of speculation and assumption on this question and sometimes, in the midst of all this information you stand back and say to yourself "I still don't know". Well I'm not going to try lead you to a definitive answer but I came across a dated article that still holds true today, that explore the question and came up with a pretty good answer and explanation. Below is then an adapted version of the article by appknox published in 2018 and written by Prateek Panda.

Before deep-diving into the reasons which motivate hackers to hack, let us know more about the 3 common categories of hackers and some of the common hacking techniques they use. Generally, hackers are classified into three categories based on their motives behind hacking.

1. Black Hat Hackers: Black hat hackers are notoriously known to infiltrate into networks and systems by creating and spreading malware. Basically, they are the 'bad hackers'. They are generally motivated by monetary gains .
2. White Hat Hackers: Not all hackers are bad, some are white hat hackers also. Commonly known as 'ethical hackers', white hat hackers are often contracted by businesses and government agencies to check for security vulnerabilities.
3. Grey Hat Hackers: These hackers have characteristics from both black and white hat hackers, but they generally carry out their hacking missions without seeking permissions from anyone. Mostly they do report the vulnerabilities found to the concerned parties, but they also demand compensations in return.

Why do Hackers Hack

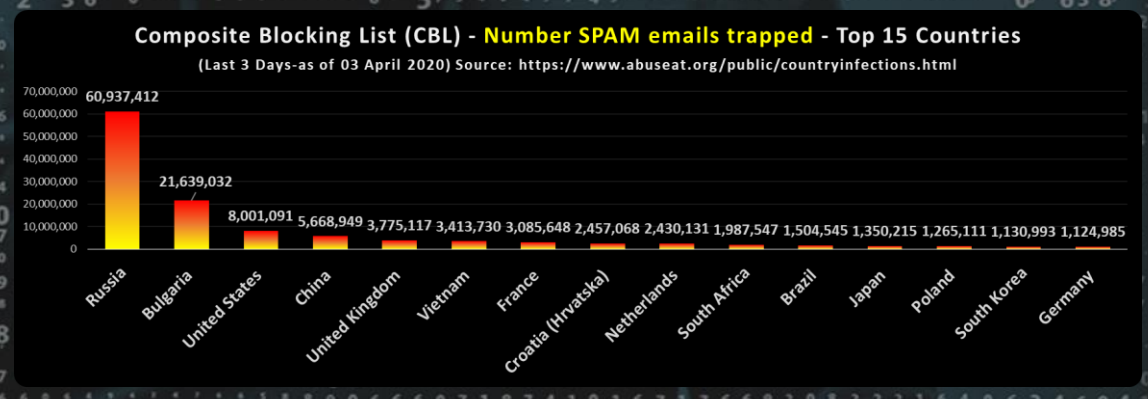
Steal/Leak Information: I am sure you guessed this. One of the most common reasons for hackers to hack is to steal or leak information. This could be data and information about your customers, your internal employees or even private data specific to your business. These are cases where hackers typically go after big targets in order to get the most attention. Some of the biggest examples are the Ashley Madison hack or the Starbucks app hack. In the Ashley Madison hack, hackers were able to break into the customer database and get access to all the information including many private pictures of popular celebrities. This incident was a big shakeup in the Internet world which also affected private lives of many people. A lot of times, hackers also steal information in order to assume your personal identity and then use it for something else like transferring money, taking a loan, etc. Such incidents have increased after Internet banking and mobile banking have started to become more popular. With the growth of smartphones and mobile devices, the potential for monetary gain through hacking has also increased. Many big businesses have fallen prey to this - Sony, Target, Yahoo, Equifax, eBay, HomeDepot, Adobe, to just name a few. Even though there has been a lot of media attention about all the above companies being hacked, most businesses still believe this won't happen to them. By not being proactive about security, you are only putting your data at risk.

Disrupt Services: Hackers just love to take something down. And then also leave a statement on the website - more on that later. But hackers have successfully taken down many services by creating bots that overwhelm a server with traffic, thus, leading to a crash. It is known as a DoS (Denial of Service) attack and can put a company's website out of service for a while. These days, there's also DDoS or Distributed Denial of Service attacks which use multiple infected systems to take down a single major system leading to a denial of service. There are other ways also, like infecting a large network with malicious software inserted onto one computer either through email or otherwise which leads to a chain reaction affecting the whole network. Server disruption attacks usually have their own personal motive. Mainly, it is to render a service or website useless. Sometimes it can also be to make a point.

Make a Point: The hackers who fall into this category are very interesting. They don't care about money or data. They seem to feel that they have a higher purpose in life. They want to steal information or disrupt your network in order to make a point. Again, going back to the Ashley Madison hack, the hackers had access to account details of 32 million users but before they made this public, the hackers left a message on the website to inform everyone on what they are done. They also mentioned what they thought about the website and why they thought a service like this was immoral.

Money: This is what everyone usually fears about. We've seen many businesses reach out to us at the stage when they have already been hacked and a hacker is demanding money. Hackers not only hack businesses and ask for ransom but they also try hacking into regular user accounts and try to take advantage of things like online banking, online retail, etc. where financial transactions are involved. Last year also saw the biggest ransomware attack called WannaCry where millions of computers around the world were hacked and users had to pay a ransom to get back access to their computers.

Driven by Purpose - Hacktivism, Idealism, Political Motives: Many hackers are also drive by a specific purpose. Sometimes, this comes out only when they get caught. Some of them aim to be idealists and take it upon themselves to expose injustice, some have political motives, some simple target the government, and so on. A major example is a hacktivist group called Anonymous who have been popular around the world for challenging and taking down many governments. These hackers can target religious groups, governments, movements, to promote a particular agenda. Another example of a politically driven agenda was when France was having an election last year. In fact, at the beginning of May, we all got to know that Emmanuel Macron, President-elect for France, had his presidential campaign emails leaked following a hack. Giving the timing of the hack, many speculate that it was done with a purpose – to sway the votes. And so are the speculations about the US presidential elections when Donald Trump became President.



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