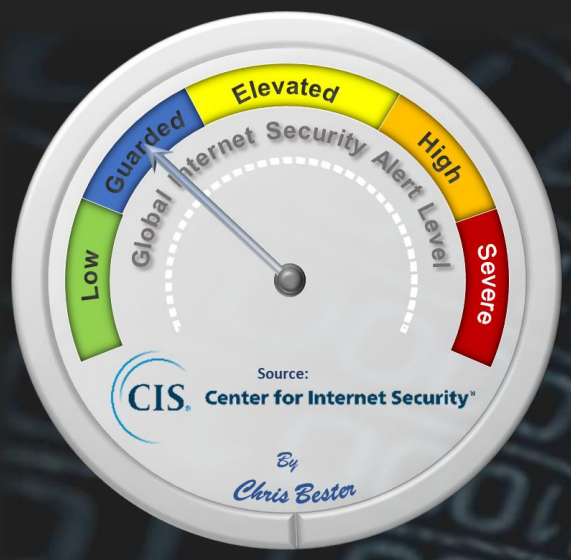


On November 18, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple and Google products.

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

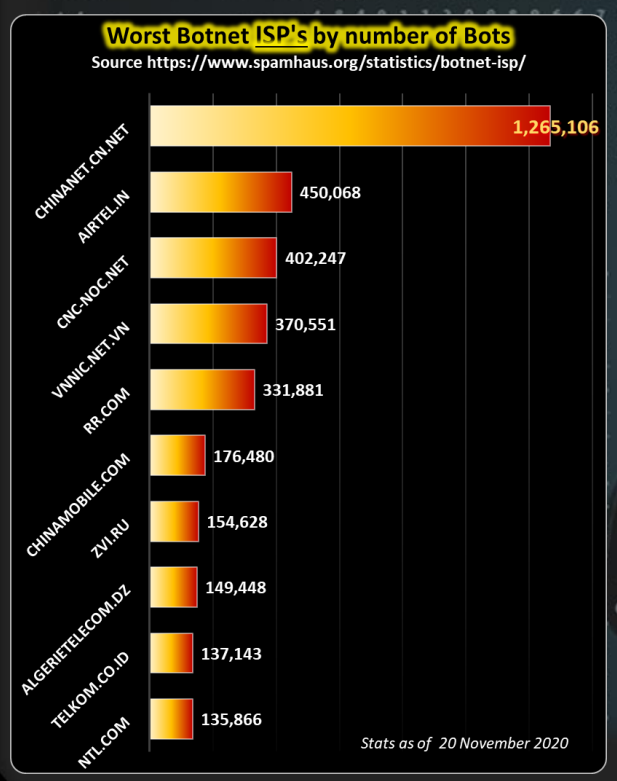
20 November 2020

In The News This Week

Microsoft reveals Pluton, a custom security chip built into Intel, AMD and Qualcomm processors - For the past two years, some of the world's biggest chip makers have battled a series of hardware flaws, like Meltdown and Spectre, which made it possible — though not easy — to pluck passwords and other sensitive secrets directly from their processors. The chip makers rolled out patches, but required the companies to rethink how they approach chip security. Now, Microsoft thinks it has the answer with its new security chip, which it calls Pluton. The chip, announced today, is the brainchild of a partnership between Microsoft and chip makers Intel, AMD and Qualcomm. Pluton acts as a hardware root-of-trust, which in simple terms protects a device's hardware from tampering, such as from hardware implants or by hackers exploiting flaws in the device's low-level firmware. By integrating the chip inside future Intel, AMD and Qualcomm central processor units, or CPUs, it makes it far more difficult for hackers with physical access to a computer to launch hardware attacks and extract sensitive data, the companies said. Microsoft said Pluton made its first appearance in the Xbox One back in 2013 to make it far more difficult to hack the console or allow gamers to run pirated games. The chip later graduated to Microsoft's cloud service Azure Sphere, used to secure low-cost Internet of Things devices.
Read the full story here by Zack Whittaker: TechCrunch

Trump fires top U.S. election cybersecurity official who defended security of vote
Trump has made debunked allegations that the election was "rigged" and refused to concede defeat to President-elect Joe Biden. His campaign has filed a flurry of lawsuits in battleground states, although election officials in both parties have said they see no evidence of serious irregularities. Reuters reported last week that Krebs, who worked on protecting the election from hackers but drew the ire of the Trump White House over efforts to debunk disinformation, had told associates he expected to be fired.. Trump said on Twitter on Tuesday that Krebs had assured people in a "highly inaccurate" statement that the election had been secure when there were "massive improprieties and fraud -including dead people voting, Poll Watchers not allowed into polling locations," and voting machine errors that flipped votes from Trump to Biden. Twitter slapped warning labels on Trump's tweets, noting: "This claim about election fraud is disputed." Krebs headed up the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency from its inception two years ago. He angered the White House over a website run by CISA dubbed "Rumor Control," which debunks misinformation about the election, according to the three people familiar with the matter. A CISA spokesperson did not respond to a request for comment. Krebs was not given notice of Trump's plan to fire him on Tuesday evening, according to a person familiar with the matter, and learned of the decision through Twitter. Read the full story here: dailymaverick

Egregor Ransomware Hijacks POS Printers to Spit Out Ransom Notes in Chile and Argentina - So, you're a ransomware gang and you want to ensure that you have caught the attention of your latest corporate victim. You could simply drop your ransom note onto the desktop of infected computers, informing the firm that their files have been encrypted. Too dull? Cencosud was infected by an Egregor ransomware attack which, in time honoured fashion, stole sensitive files that it found on the compromised network, and encrypted data on Cencosud's drives to lock workers out of the company's data. A text file was left on infected Windows computers, telling the store that private data would be shared with the media if it was not prepared to begin negotiating with the hackers within three days. That's nothing unusual, but Egregor's novel twist is that it can also tell businesses that their computer systems are well and truly breached by sending its ransom note to attached printers. And in the case of a store like Cencosud, that means that printers at the checkouts of numerous retail outlets in Chile and Argentina were suddenly churning out the ransom demand as well. A Twitter user managed to capture a 'possessed' printer spitting out Egregor's extortion demand on camera, and uploaded a video. Read the full story here: Tripwire *(Thanks to my good friend Yazan Shapsugh who pointed me to this story)*



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

No, please understand it was not me you were talking to, my phone was hacked and cloned!!

When your phone has been cloned, the repercussion calls can go on for months. Consider changing your phone number

Bug Bounty Programs

I have spoken a little bit about bug bounty programs last week and I've mentioned it many times in previous bulletins. Today I want to share an extract of an article by Tammy Xu of builtin that give good insight into the topic. For the sake of space, I can only share a short extract for the bulletin, so please go ahead and read the full article at builtin once you're done with the appetiser below.

BUG BOUNTIES: A SHORT OVERVIEW

First, lets explain what a bug bounty program is: A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities. (Wikipedia).

X3n0N's story - While studying computer science in college in 2012, a young software developer who goes by X3n0N started to dabble with bug bounties. Armed with basic skills that he learned by reading online forums and articles, he tried his hand at white-hat hacking, combing through various websites for vulnerabilities and looking at web pages for user input boxes where cross-site scripting or SQL injection vulnerabilities might be lurking. Back then, cyber attacks resulting in losses of over $1 million was only one-fourth as prevalent as today, according to the Center for Strategic and International Studies. Although now there are multiple platforms for facilitating bug bounties and a robust bug bounty community, at the time there still wasn't a lot of infrastructure in place to support white-hat hackers, also known as ethical hackers. X3n0N's adventures soon earned him a lawsuit from a large internet service provider. He had come across a security vulnerability that made possible the hijacking of customer accounts, allowing him to change the bandwidth plans for any of the provider's customers, and he had reported the vulnerability in an email to the company. The company did not have a bug bounty program in place, he said, so he had not asked them for compensation and instead just alerted them to the vulnerability and asked them to secure it. But the company was far from grateful to receive X3n0N's email. Pretty soon, he started to receive calls from the company's lawyers, threatening to take him to court, he said. The whole situation found its way to the principal of his college, resulting in some "uncomfortable scenarios" for him.

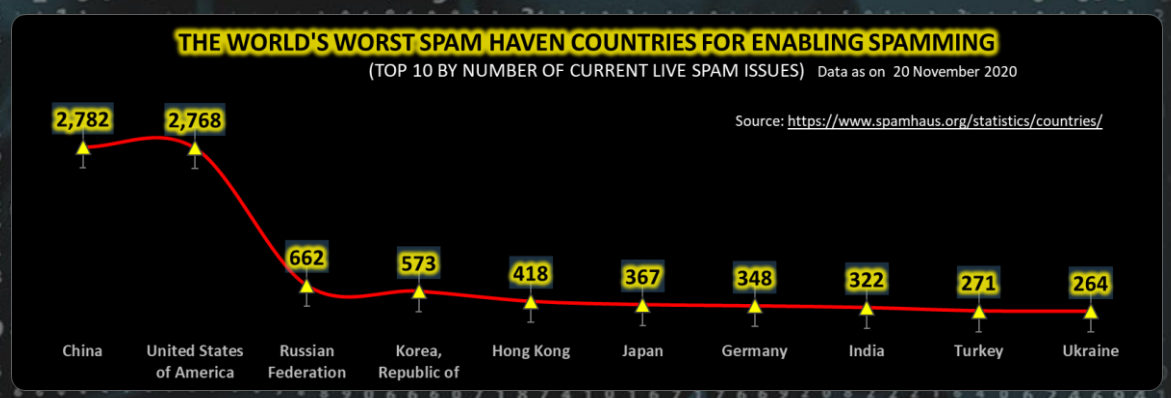
Because his actions were clearly not malicious, the whole situation was soon smoothed over. His email reporting the vulnerability helped prove that his intentions were to help the internet service provider be more secure, not to profit from its insecurity. The company dropped the suit, stipulating only that he formally apologize and sign a non-disclosure agreement promising not to go public with the company's vulnerability.

He was much more careful after that experience, but it didn't deter him from continuing to hunt for bugs. He learned that there were companies with official channels for reporting vulnerabilities, such as Google. Soon after, he came across a cross-site scripting vulnerability in Google's messaging service, which let him hack into users' accounts by injecting JavaScript into the phone number input box and stealing their cookies. He reported the vulnerability to Google, which paid him $500 for the find, then bumped up the reward to $2,000 after giving him credit for a related cross-site request forgery attack that he hadn't reported but his report had helped uncover. X3n0N was delighted with the experience. "I felt really, really happy and surprised," he said. "I never expected $2,000 when I was still studying." He was so motivated that he not only continued to pursue bug hunting, but also decided to work for Google "at least once" in his career.

Current Landscape - These days, the landscape of hacking has changed dramatically. It's no longer as easy to stumble across web application vulnerabilities at large internet companies. Bug bounty and bug reporting programs are more commonplace, and companies are also more open to employing the services of specialized penetration testing companies. Pen testers, as they're called, help to locate flaws in their clients' systems and operate like traditional consulting companies, with staff specializing in finding security vulnerabilities. Bug bounty platforms operate differently. These platforms act more like marketplaces that allow free-agent bug bounty hunters and the companies that are interested in their services find each other. They attract companies by giving them access to a large pool of hackers, and in turn attract hackers by providing a list of companies that are willing to pay for their services. Bugcrowd launched in 2011 as the first bug bounty platform of its kind, and many other platforms quickly followed. "The crowdsource security idea is that if you do a penetration test, you'd normally have one individual doing an assessment," said Grant McCracken, director of security operations at Bugcrowd. "If you have two people doing the assessment, you're probably going to find more than the one person, and 500 people are going to find exponentially more than one or two individuals. So it's taking the power of the crowd and the extensibility of the gig economy to fill the need in cybersecurity." It took some time for bug bounty platforms to be accepted into the mainstream. Katie Moussouris, who was the former chief policy officer of HackerOne, another early bug bounty platform, played an important role in helping to grow its program. She even successfully partnered with the famously guarded U.S. Department of Defence to set up its pilot bug bounty challenge in 2016, called Hack the Pentagon. Over a thousand hackers participated, and the government paid out roughly $75,000 for finding a total of 138 valid security vulnerabilities. The pilot was considered a successful proof of concept by the Department of Defence.

Read the full article by Tammy Xu here: Builtin

Other links with information on Bug Bounty programs: Top 30 Bug Bounty Programs in 2020, ZDNet Article, HackerOne Beginners Guide,



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