On July 29, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe 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

31 July 2020

In The News This Week

Antitrust showdown: Apple, Amazon, Facebook, and Google CEOs report to Capitol Hill

- Alongside his Big Tech counterparts, Amazon CEO Jeff Bezos made his first-ever appearance before Congress, telling lawmakers that "just like the world needs small companies, it also needs large ones. "After years of getting overlooked in Washington, the technology industry has finally become too big for lawmakers to ignore. For the past year, a bipartisan group in Congress has zeroed in on the outsized influence of a few key industry giants. On Wednesday, the leaders of those companies -- Amazon CEO Jeff Bezos, Apple CEO Tim Cook, Facebook CEO Mark Zuckerberg and Alphabet CEO Sundar Pichai (also chief executive of Alphabet subsidiary Google) -- collectively appeared before Congress for the first time to defend their market dominance.

"I love garage entrepreneurs—I was one," Bezos said in written remarks, prepared for his first-ever appearance before Congress. "But, just like the world needs small companies, it also needs large ones. There are things small companies simply can't do. I don't care how good an entrepreneur you are, you're not going to build an all-fibre Boeing 787 in your garage."

During Wednesday's hearing before the House Judiciary Antitrust Subcommittee, Bezos did not deny allegations, as reported by the Wall Street Journal earlier this year, that Amazon has used data about the third-party sellers on its e-commerce platform to give a competitive advantage to its own, competing products.

Read the full story here: ZDNet Article

Average Cost of a Data Breach: $3.86 Million

The latest edition of IBM's annual cost-of-a data-breach study shows that security system complexity and incident response testing are two factors that have the biggest impact on the total cost of a breach. The 2020 IBM study — conducted by the Ponemon Institute — is based on data gathered from executives at 524 organizations around the world that experienced a data breach between August 2019 and April 2020. For purposes of the study, Ponemon only considered data breaches that involved between 3,400 and 99,730 compromised records. To calculate how much a breach might have ended costing a company, the research considered the costs associated with four process-related activities: the costs involved in detecting a breach, including investigation and forensics activities, assessment and audit; notification costs; lost business from system downtime and disruption and; legal fees and costs related to activities like providing help desk services, credit monitoring, and ID protection for victims. The analysis showed that globally, a data breach cost companies $3.86 million per incident during the nine-month period of the study. The average breach cost in the US as usual was more than twice that, at $8.64 million on average. Healthcare organizations globally once again shelled out more on average for a data breach — $7.13 million — than organizations in any other sector. Read the full article here: DarkReading

Russia-aligned hackers running anti-Nato fake news campaign

Hackers "aligned with Russian security interests" have been engaged in a sustained campaign to compromise news websites in Poland and Lithuania to plant false stories aimed at discrediting NATO, according to a new report. Part of the campaign – labelled "Ghostwriter" – involved gaining access to news sites publishing systems, deleting stories and replacing them with false news that sought to delegitimise the transatlantic alliance. In one example, a Lithuanian news site was compromised last September and a false article was inserted into its archive wrongly claiming that German soldiers serving with NATO had desecrated a Jewish cemetery. In May this year, a series of Polish sites were targeted and stories published with fake quotes attributed to the commander of the US army in Europe, in which he was said to have ridiculed the capability of the Polish military. Emails purporting to be from a local news service with links to the doctored articles were then sent out to other media and public institutions in an attempt to disseminate the fakes and give them further credibility... Read the full story here: TheGuardian

Social Media crimes on the rise

Social media, the technology invention of the decade. It is estimated that around 2.5 billion users are exchanging messages, pictures, videos and other what-nots in Facebook every month (That probably includes WhatsApp message). The same goes for Instagram with approximately 1.2 billion and Twitter around half a million to name a few. That is a lot of clicking thumbs and the landscape is ever increasing. It is difficult to imagine your life without social media and the convenience of instant messaging and sharing that goes from one-to-one chit chat to full on business meetings. I believe, now that the world is in lockdown in the midst of the Covid-19 pandemic, social media activity has grown exponentially. It would be interesting to see the figures if someone do a study to compare usage before and now amidst the pandemic. I said earlier it is the invention of the decade but in fact, the major social media apps has been around for quite some time. Here is when some of these has started up to give some context: LinkedIn – 2002; Facebook – 2004; Twitter – 2006; WhatsApp – 2009; Instagram – 2010; iMessage – 2011; Telegram – 2013; Google Hangouts – 2013; Signal – 2014; TikTok – 2016; once again, just to name a few, there are many more and the list is ever growing.

With this explosion in social media, apart from non-cyber crimes, the cyber security fraternity has had its challenges to deal with these endless and wide-open platforms. If I say wide-open, I am talking about the users, not the technology. Some people are so vigilant they are almost like a human firewall and question everything but most are totally ignorant and unaware of the real dangers lurking under the cover of these apps. No matter how many awareness campaigns you conduct it seems that no one takes notice and I'm sure many of my fellow security workers will echo that.

We have seen a major increase criminal activity since the Covid-19 pandemic took the world at ransom and the attacks are getting remarkably refined. We also see an increasing number of new actors and I believe this is directly related to the fact that people are forced to be at home and the only outlet for boredom are their computers that opens the world to them in a digital reality.

In 2012 already, the guardian reported that Social media-related crime went up by 780% in four years, I wonder what the compared statistics looks like today. According to the 2019 Bromium report "Social Media Platforms and the Cybercrime Economy", nearly 1 in 5 organizations worldwide are now infected by malware distributed by social media. Moreover, the problem of social media cyber crime is growing at an astonishing rate. In the U.S., for example, social media cyber crime increased nearly 300-fold in the period from 2015 to 2017. In January this year Info Security Magazine reported that Facebook Crime Rises 19% in the UK.

CPO Magazine sums it up nicely in an article on their website on why cyber criminals are targeting Social Media platforms and the trade of personal information harvested on these platforms. Below is a small extract of the article but I encourage your to follow the link and read the whole thing.

Why social media platforms are so desired by cyber criminals

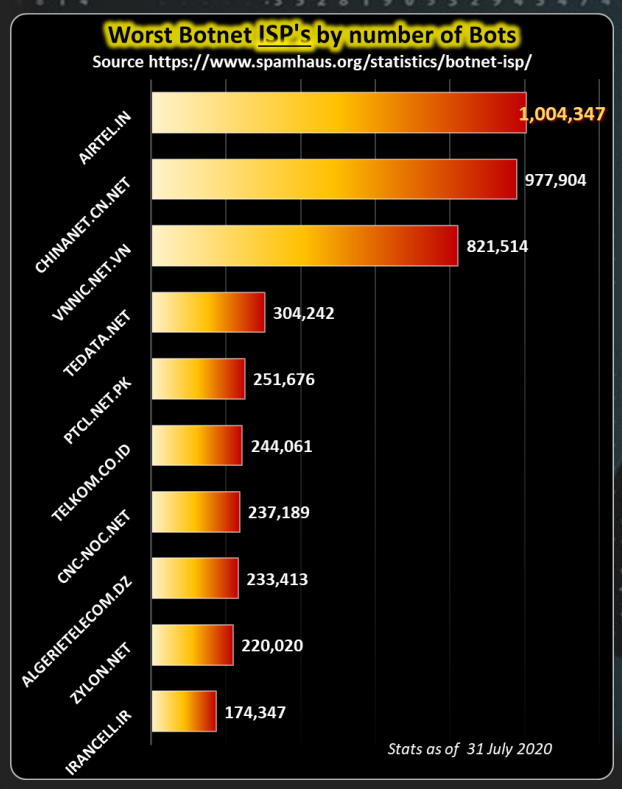
Given the rapid pace of growth and the near ubiquity of social media cyber crime on the Internet, the inevitable question becomes: Why have cyber criminals chosen to focus on social media platforms like Facebook, Twitter, Instagram, and YouTube? One easy answer is that these sites make it very easy to share and pass on just about anything – and that includes malware. In fact, the security researchers found that social media platforms, on average, have 20 percent more methods to scam and rip off consumers than other websites. These methods include adverts, sharing buttons and plug-ins. Plus, the fact that most people have hundreds, if not thousands, of connections on these social media platforms make it very convenient to distribute malware to a wide audience with surprisingly few negative consequences.

In fact, the researchers even went so far as to characterize every social media platform as a "Trojan horse" that could be used by hackers and cyber criminals to pull off increasingly sophisticated and brazen criminality. In the past two years, for example, "cryptojacking" (i.e. the taking over of another computer's computing resources to mine cryptocurrency) has emerged as one way to monetize malware. Once the malware has been inserted into someone else's browser, it can go to work mining cryptocurrency for cyber criminals located thousands of miles away. As a result, 4 of the top 5 sites hosting cryptojacking code are social media platforms. And, of the top 20 sites hosting cryptojacking code, 11 are social media platforms. The researchers specifically called out Facebook Messenger for its role in propagating the Digmine cryptomining strain.

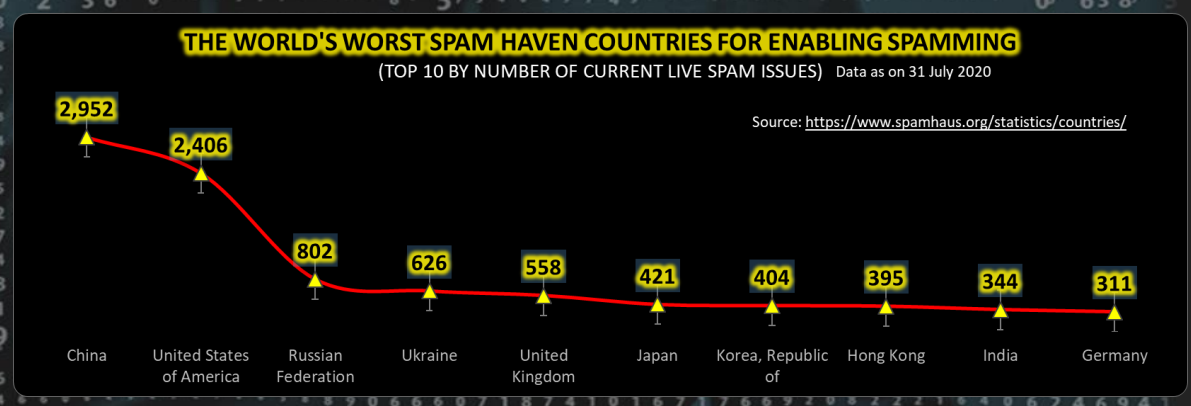
Data breaches and the illegal trade in personal information

One popular form of social media cyber crime involves the illicit trading of personal data from hacked social media accounts. In the past five years, says the Bromium report, nearly 1.3 billion social media users worldwide have had their social media accounts hacked. As a result, anywhere from 45 to 50 percent of all illicit trading of personal information – including stolen credit card information as well as username and password combos – could be traced back to social media platforms. Now that people share every detail of their personal lives online, it makes it easier than ever before for hackers to carry out these cyber crimes. According to the report, the underground economy for stolen personal data is now worth as much as $630 million each year to cyber criminals.

Moreover, social media accounts are sometimes hacked with the sole intention of using it as a way to generate fake accounts to ensnare even more web users. The Bromium report mentioned that hackers liked to masquerade as famous web or Internet personalities (e.g. Elon Musk). Once they've set up a fake account, they can then ask users to send them money, perhaps with the goal of winning a prize or getting free cryptocurrency deposited into their account. ....Read the rest here: CPO Magazine



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



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