On May 13, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Mozilla, Cisco, WordPress, VMware, Adobe and Microsoft 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

15 May 2020

In The News This Week

A hacker group is selling more than 73 million user records on the dark web

A hacker group going by the name of ShinyHunters claims to have breached ten companies and is currently selling their respective user databases on a dark web marketplace for illegal products. The hackers are the same group who breached last week Tokopedia, Indonesia's largest online store. Hackers initially leaked 15 million user records online, for free, but later put the company's entire database of 91 million user records on sale for $5,000. Encouraged and emboldened by the profits from the Tokopedia sale, the same group has, over the course of the current week, listed the databases of 10 more companies like Chatbooks, SocialShare, online dating app Zoosk and many more. The listed databases total for 73.2 million user records, which the hacker is selling for around $18,000, with each database sold separately. The hacker group has shared samples from some of the stolen databases, which has been verified to include legitimate user records. Read the full story here: ZDNet Article

Coronavirus: Israel turns surveillance tools on itself

Tom Bateman, BBC Middle East Correspondent, reported this week that he was shocked as he read messages from the Israeli government on local photographer, Hirsh Kotkovsky's phone. The messages read that he was next to someone that has corona... and that he must go into quarantine." He obeyed the order that came in late March, cancelling lucrative wedding shoots and shutting himself away from his wife and four small children, even though he had no symptoms. Mr Kotkovsky is one of thousands of Israelis who have been alerted by similar messages. In the fight to contain the coronavirus, Israel's internal security agency - the Shin Bet - was empowered to use covert systems to track people's movements. The Middle East's cyber-superpower has made extensive use of surveillance technology to try tackle Covid-19, as countries around the world grapple with the trade-off between privacy and monitoring infection. The Shin Bet can access the location data of millions of mobile phone users to trace those who have been in proximity to confirmed patients. Israel credits the system, among other measures, with reducing the rate of infection. *(Thank you to my good friend and all round IT specialist, Graham Cartwright, who pointed me in the direction of this news snippet)* Read the full article by Tom Bateman here: BBC

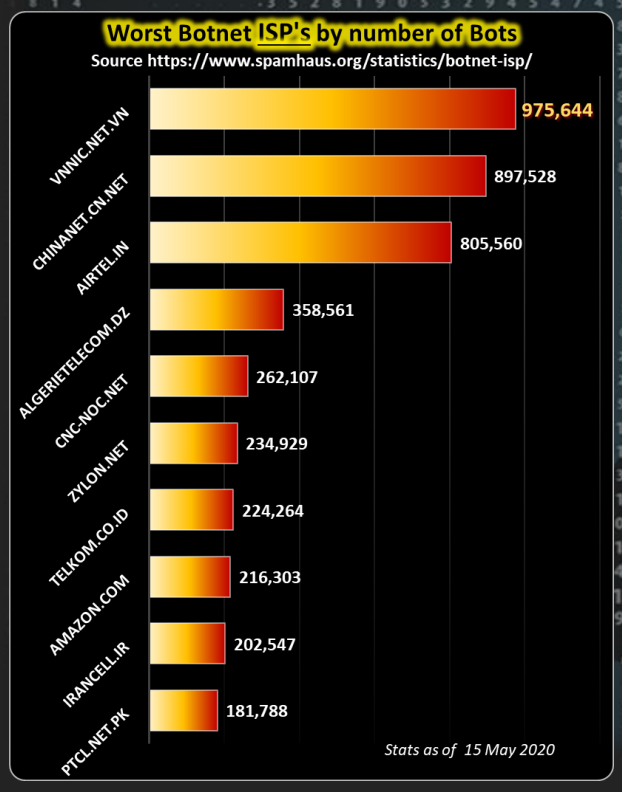
Europe's Largest Private Hospital Operator, Fresenius, Hit by Ransomware

Fresenius, Europe's largest private hospital operator has been hit by a ransomware cyber-attack on its technology systems. Fresenius is a major provider of dialysis products and services that are in high demand aiding in the COVID-19 pandemic. The company said the incident has limited some of its operations, but that patient care continues. This German-based organization told cybersecurity expert Brian Krebs that a "computer virus" has caused a disruption, but there is no impact on patient care. Fresenius employs 290,000 employees in more than 100 countries through a range of medical support businesses. Someone working for one of these businesses in the US told KrebsOnSecurity that computers had been roped off, and it was thought that the virus in question is the Snake ransomware. Read the story here: ZDNet02 & Krebs

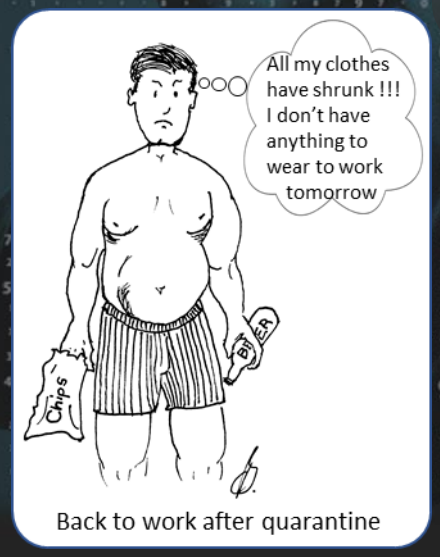
News snippets from the past - Computers & Security

Users Affected by Security Hole – August 2000

The following news snippet was found in the TimesDaily, August 8 2000 - WASHINGTON - Security experts were warning Internet users Monday about a security hole in Netscape's Web browser that already has infected almost 1,000 computers. Once a computer is infected, a hacker can click through the victim's computer and see, run and delete files on the target computer. The method, dubbed "Brown Orifice" in a reference to the popular hacker tool BackOrifice, has been making the rounds of computer security mailing lists and bulletin boards over the weekend. Netscape has not yet made a remedy available but are working on the problem.
Read the story here: GoogleArchives



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



The Security Threat of Employees Working from Home

The Financial Times published an article this week headlined "Companies wrestle with new cyber security threat: their own employees". Which for me is not a "new" threat but an old threat that is highlighted anew as organisations struggle with adapting to the distributed nature of their workforce in quarantine or lockdown. It reminds me of a time when Mainframe computers were the order of the day and we used to speak about the "Castle and Moat" approach to security. Here we had all the control within the castle and the perimeter was secure and we didn't worry too much about the "peasants" spread around the country side. Now there are no people in the castle but all the users ("peasants") still use the resources the castle provide to bake and store their "bread" at home. Thus control went out the window and we have to adapt, design and implement a whole bunch of new controls.

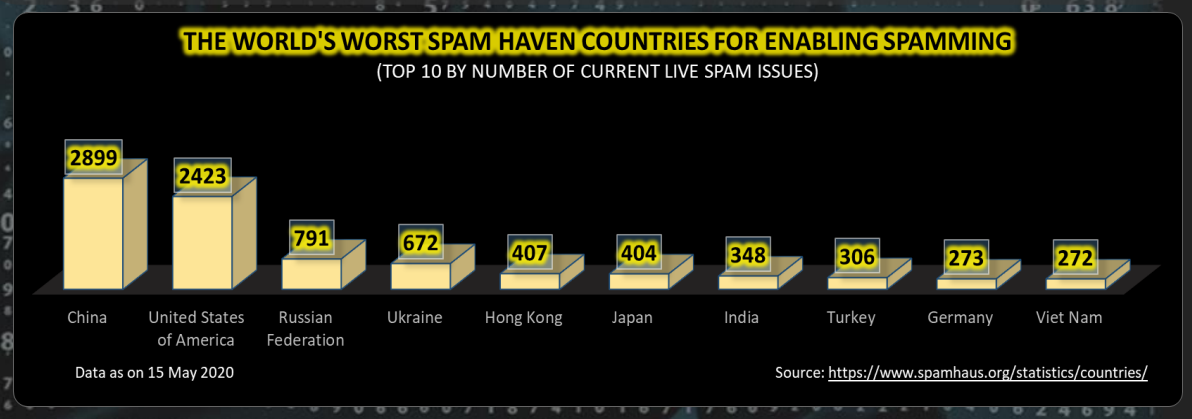
Now let's look at challenges from the employee or "peasants" outside the castle perspective. This global Covid-19 or Corona virus event will go down in history as the time where the most employees ever are forced to work from home. For most of us, this is a challenge as your home becomes your office, but that also means kids running around, dogs barking, dishes clanging in the kitchen and so forth. It is for sure not the quiet environment that you are used to in the office building. Your daily challenge is to find that quiet spot where you can have that meeting or work through a complex spreadsheet and so on. But that is just looking at a small portion of challenges from the employees perspective, can you now imagine the CISO's challenges from the corporate perspective.
All of a sudden, he doesn't have all that formal controls he had before and with 90% of the workforce working from home, the Cyber Security landscape is thrown wide open.

Sam Curry, Chief Security Officer at Cybereason, wrote an article in the Entrepreneur that highlights some of the risks we are facing in this new Cyber landscape, that struck a cord with me. Below then is an adapted version of his views.

What are the main risks?

1. Hackers can manipulate VPNs without a view of the whole - Virtual private networks, or VPNs, have become the new lifeline for many businesses, extending encrypted networks to our homes. However, many home networks are already infected with malware or compromised hardware that can be exploited for staging attacks through machines with VPN termini. A compromised identity or a machine, especially when behavioural baselining on the backend is in flux, can allow hackers to piggyback through the VPN. It's critical to have endpoint integrity checking and strong authentication in place at this stage once the VPN is in place and active. There are also vulnerabilities for VPNs that require really understanding and internalizing rather than blindly trusting, and many applications that are becoming the new critical IT infrastructure will see new vulnerabilities. This is not cause for panic, but it does mean you need to talk to vendors and plan for patching and failover. Remember, vendors, too, are going through change and doing triage on their support and escalations, but start the dialogue now. Contact your hardware or software providers to ensure configurations and policies are in order, starting with the VPN, endpoint and identity solutions.
2. Endpoint first, then mobile - Although there are many endpoint challenges, the first priority is to ensure critical business processes recover. Then, make sure the new enterprise footprint is brought into the fold from a policy and control perspective. Next, focus on mobile, which is the most pervasive and ubiquitous platform in our personal lives. Employees who have to learn new devices and applications will turn to their phones even more than usual because they feel familiar. Most companies have established policies defining what can and can't be done with mobile phones, but set these policies if you don't already have them. Cyber criminals will start with identity theft and classic machine exploits, but they'll think of new ways to target them before moving on to other devices. Get ahead of mobile threats before dealing with other devices.
3. Information can be weaponized - In the past few weeks, attackers have started taking advantage of human weaknesses. For example, hackers developed a malicious mobile application posing as a legitimate one developed by the World Health Organization. A vulnerable person could easily mistake this malicious app for a real WHO app. Once installed, the application downloads the Cerberus banking trojan to steal sensitive data. These types of attacks essentially weaponize tools and information, because they can easily be done with applications that provide legitimate benefits, too. Before, attackers had to plan their cons for diverse interests and lures, but right now the entire world has a shared crisis. COVID-19 has become our common watering hole, but with the right awareness and education, we will be able to defend ourselves.
4. Physical location matters again - When employees take their machines home or use their home machines for work, those machines now sit in a physical and digital space unlike any within the office. Between routers, printers, foreign machines, devices, gaming consoles and home automation, the average home has a more complex and diverse communication and processing system than some small companies. Employees might be taking conference calls within earshot of family members or even employees of other companies. Nothing should be taken for granted when it comes to the privacy of employee homes. Simple policies are important — these are relevant not only to security but also to privacy in general. Should employees have cameras on or off for meetings? Should they wear earphones? Should they take notes on paper or digital applications? How should they handle viewed or created IP or PII? What communications applications are acceptable? What happens when others intrude, see notes or overhear discussions? These questions might seem trivial, but you need to address them up front. Above all, listen and adapt when things aren't working.

These are by far not a complete list of the risks we are facing in these times as not a single one of us has been in this situation before. As we learn on the go, I encourage you to look at risks in a new way and from every and any angle and try to be one step ahead of the hackers and crooks out there who are doing exactly the same but from a gain perspective and not a security perspective.



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