On February 17, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google Chrome.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
19-Feb	110,837,617	2,452,586

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

19 February 2021

In The News This Week

France uncovers cybersecurity breaches linked to Russian hackers

France's national cybersecurity agency said Monday it had discovered a hack of several organisations that bore similarities to other attacks by a group linked to Russian intelligence. It said the hackers had taken advantage of a vulnerability in monitoring software sold by French group Centreon, which lists blue-chip French companies as clients, such as power group EDF, defence group Thales, or oil and gas giant Total. The French ministry of justice and city authorities such as Bordeaux are also named as Centreon customers on the group's website. "This campaign mostly affected information technology providers, especially web hosting providers," said the French National Agency for the Security of Information Systems (ANSSI) in a report. ANSSI had discovered "a backdoor" on several Centreon servers which had given the hackers access to its networks. Centreon said later on Tuesday that none of its customers were affected. "This campaign bears several similarities with previous campaigns attributed to the intrusion set named Sandworm," said the report, referring to a group of hackers thought to have links with Russian military intelligence. Read the full story here: France24

France to Boost Cyber Security Defenses After Attacks

President Emmanuel Macron announced new investment to bolster France's cyber security defenses after two hospitals were struck by ransomware and the national security agency linked a large cyber attack spanning three years to Russian hackers. The government is earmarking around 500 million euros ($602 million) to help companies and public authorities boost their cyber defenses, an official in the president's office said Wednesday.
Read the full story by Ania Nussbaum here: Insurance Journal

Water Utility Hack Could Inspire More Intruders

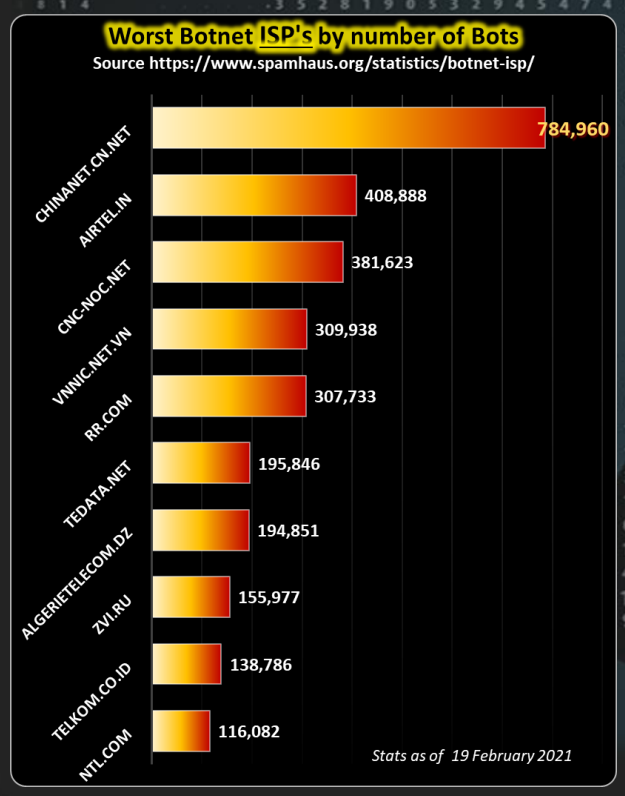
In the aftermath of the Oldsmar incident, where an unidentified attacker gained access to a water treatment plant's network and modified chemical dosages to dangerous levels, the FBI has sent out an alert on Tuesday, raising attention to three security issues that have been seen on the plant's network following last week's hack. The Oldsmar water treatment plant's network was accessed via TeamViewer on two occasions last Friday. If past cyberattacks are any indication, success begets imitation. In the wake of last week's hack of Florida water utility, other water utilities and users of remote desktop software would be wise to shore up defenses, experts say. The attack on the water treatment system in the small town of Oldsmar, Fla., lacked technical sophistication, showed no insider knowledge of the system, and had all the hallmarks of a hacker joyride through a critical system. Yet the fact that an unsophisticated attacker compromised a system, changed the chemical mix for treating the water, and could have potentially harmed people will likely have a ripple effect and attract more attackers to test the cybersecurity of municipal water systems, says Padraic O'Reilly, co-founder of CyberSaint, an IT risk management firm. Read the full story by Robert Lemos here: DarkReading

Kia Motors America suffers ransomware attack, $20 million ransom

Kia Motors America has suffered a ransomware attack by the DoppelPaymer gang, demanding $20 million for a decryptor and not to leak stolen data. Kia Motors America (KMA) is headquartered in Irvine, California, and is a Kia Motors Corporation subsidiary. KMA has nearly 800 dealers in the USA with cars and SUVs manufactured out of West Point, Georgia. On Tuesday, we reported that Kia Motors America was suffering a nationwide IT outage that has affected their mobile UVO Link apps, phone services, payment systems, owner's portal, and internal sites used by dealerships. When visiting their sites, users are met with a message stating that Kia is "experiencing an IT service outage that has impacted some internal networks". On Wednesday, BleepingComputer obtained a ransom note that we were told was created during an alleged Kia Motors America cyberattack by the DoppelPaymer ransomware gang. Read the full story by Lawrence Abrams here: BleepingComputer

Cybersecurity risks connected to AI in autonomous vehicles

By removing the most common cause of traffic accidents – the human driver – autonomous vehicles are expected to reduce traffic accidents and fatalities. However, they may pose a completely different type of risk to drivers, passengers and pedestrians. Autonomous vehicles use artificial intelligence systems, which employ machine learning techniques to collect, analyse and transfer data, in order to make decisions that in conventional cars are taken by humans. These systems, like all IT systems, are vulnerable to attacks that could compromise the proper functioning of the vehicle. A report by ENISA and JRC sheds light on the cybersecurity risks linked to the uptake of AI in autonomous vehicles, and provides recommendations to mitigate them.
Read the full story here: Helpnetsecurity



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

Cyber Attacks on Critical Facilities like Water & Electricity

The recent attack on a water utility in the US sparked a lot of interest and questions around the subject of securing automated computer systems that control part or complete critical infrastructure utilities. The attack on Oldsmar's water utility brought home the fact that lives could adversely be impacted on a massive scale. If the attack succeeded, the close to 15,000 inhabitants of Oldsmar could have become very ill or even worse, lost their lives. The threat actors could either be criminal or political. Criminal actors could hold a town or city to ransom once systems are compromised. Political or state actors are abound plentiful. If you take the tension between the Middle East and the USA as an example, can you just imagine what can happen if infiltrators take control of the water or power utilities of a large city like New York? Tricia Howard of Security Boulevard wrote an insightful piece this week on the state of water and other utilities today. Following is an extract of the article.

Utilities and Cybersecurity: Keeping the Lights On – Both On and Offline

Utilities have a very unique challenge in the cyber arena. You are not only responsible for keeping up with the evolving threats that plague other organizations, but also keeping people's lifelines open. Just look at what is happening in Texas right now. Thousands of people are without power and water in the middle of a storm that the infrastructure isn't built to deal with. Pipes are bursting. People are suffering. Electricity, water, gas… these things are what people need to survive. As we're seeing by the sheer outrage on social media and global news coverage of the Texas storm, the first ones to be blamed are the utilities and cooperatives. It only gets worse if it's a cyber incident. Let's look at an example – the water treatment facility near Tampa..

The state of water and utilities today

There has been a lot of attention in the news recently about the potential breach of the Water Treatment Facility near Tampa, Florida. It raises a major question about the security of similar facilities across the country. The supply of water in the Unites States comes in all shapes and sizes. This is primarily due to the nature of supply for suitable water. These companies aren't just dealing with living water, they also handle waste water. This means more treatment before delivery. It will depend on the geography and what water sources are available and what may need to be done to treat the water. There are large organizations that control the supply of water for major metropolitan areas and those organizations will have implemented some measure of cybersecurity controls. However, a large number of organizations that supply water are going to be small and very regionalized. In some cases they only supplying water to a single town or even just a portion of a town. For example, the Water Treatment Facility that was in the news only services 15,000 people. This is similar in the electric and power industries as well. Many smaller energy companies band together to form co-ops to service different areas. This is why an apartment complex can be without power but the parking lot across the street can have it on. It all depends on where the line falls.

Utilities getting hacked have real-life impact

The challenge is that many of these utility organizations have limited resources and budget to implement cybersecurity policies that are needed to protect their systems. When a retail organization has an incident that impacts their sales, people can get annoyed because they can't buy their shoes. If a power grid gets hacked – it can take people's living conditions away. Very big difference here. The backlash that the Tampa treatment center got from the cybersecurity community was staggering. It can seem that since they have a small landscape that cyber isn't as big of a priority. However, that limited attack surface can cause major damage to people's lives. It's important to pay attention to a few key controls which can significantly reduce your risk and potential exposure to attack. First, raise the awareness of the issue and be prepared to do something to improve your state. You cannot just decide your organization is too small and not a target. Cybersecurity awareness, especially at the top levels of the organization – including the Board, is a must if anything is to be done.

WHAT CAN BE DONE?

Back to Basics

Pay attention to the basics. Make sure you keep all software patched and up to date. If you have old systems in place with outdated operating systems, they do need to be replaced, so that investment is going to be needed but look now to map out how to replace them with updated operation systems that will be patched regularly and provide the needed cyber defense capabilities.

Multi-Factor Authentication

Pay attention to credentials and implement policies that significantly reduce risk. If your systems support MFA, then make sure it is implemented. Use complex passwords for all access especially to critical operational technology and set a policy to change passwords frequently. Separate privileged accounts from accounts used for daily operation – even when used by a single person.

Managing Remote Workers

With more people working from home today, you may need to implement additional controls to ensure only authorized individuals gain remote access.

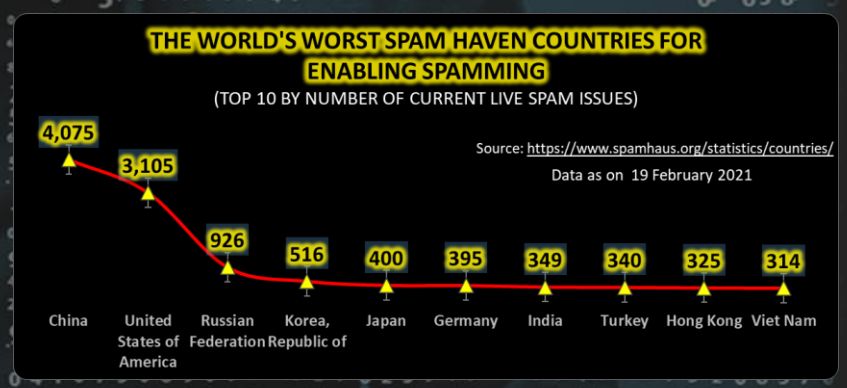
Additional Controls and Policies

Depending on the size of your organization and its associated complexity, you may need to ensure additional controls and policies are in place. These can include the implementation of firewalls, network segmentation, accurate inventory of all IT assets and systems, and the establishment of cyber security training programs for all employees. It is important to remember, that organizations of any size can and must do what they can to reduce risk and improve their overall cybersecurity state. Focus on the areas that can be implemented quickly and without massive cost – which often can significantly lower risk. This is most critical for utilities due to the nature of the business and the potential impact to the customers they serve.

Please visit the Security Boulevard page for more details and other stories.

Other Interresting News and Cyber Security bits:

- Ransomware: A company paid millions to get their data back, but forgot to do one thing. So the hackers came back again *(Thanks to Bill Graham for this one)*
- Home working increases cyber-security fears
- FEV SPORT framework addresses increased cybersecurity risks in new vehicles



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com