On February 13, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in PHP, Apple, Adobe, Microsoft, and Mozilla products. (No update from CIS at the time of publication)

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
22 February 2019

In The News This Week – Target Australia

Australia has become a significat target for cyber criminals and "state actors" alike recently starting with last year's breach at Perth-based Navy shipbuilder Austal, moving on to the recent attack on Parliament House and many more of which some are shown in the bulletin this week.

Cybercriminals encrypt 15,000 medical files belonging to Australian hospital and demand ransom

In the latest news, a cybercriminal group broke into a computer network that belonged to an Australian hospital and encrypted around 15,000 medical files. Cabrini Hospital, located in Malvern, Australia, was the victim of a ransomware attack. Melbourne Heart Group, which is based at the hospital, reported that it was not able to access patient files for three weeks, which led to the discovery of the attack. The attackers demanded a ransom to be paid in cryptocurrency in order to decrypt the files. The malware used in the attack is alleged to be created by a North Korean or a Russian hacker group. However, it is yet to be ascertained. The Australian Cyber Security Centre, which oversees cybersecurity matters in Australia, and the Federal Police, are looking further into the security incident. Cabrini Hospital told affected patients that their files had been lost but did not inform them of the breach. In fact, when some patients turned up for consultation, their records were missing from the database. The Age, which covered the incident, reported that despite the ransom payment being made, many files were still encrypted. "The protection of personal patient information is of the utmost importance...patient privacy has not been compromised in this instance," a Melbourne Heart Group spokeswoman told The Age. She pointed out that the encrypted files were not linked to cardiac device information of the hospital patients. (Read the full story by Ryan Stewart here: https://cyware.com/news/)

Toyota Australia hit by cyberattack; No customer data compromised

Toyota Australia, a subsidiary of Toyota Motor Corporation disclosed on February 21, 2019, that it has suffered a cyber-attack. However, the motor company confirmed that no private data of employees or customers were compromised in the attack. Upon learning about the incident, Toyota Australia's IT department started conducting investigations on the attack. The motor company is also working closely with international cybersecurity experts to get its systems back on track. However, the source of the attack still remains unknown. "At this stage, we believe no private employee or customer data has been accessed. The threat is being managed by our IT department who is working closely with international cybersecurity experts to get systems up and running again," Toyota Australia said. . (Read the full story by Ryan Stewart here: https://cyware.com/news/)

Cyber attach fears on Airports - Sydney Airport to establish cyber security centre

Sydney Airport to establish cyber security centre: Sydney Airport is preparing to establish an around-the-clock cyber security operation centre to protect its systems and data holdings from the threat of cyber-attack. The new centre, which is expected to be up and running by April, is aimed at enhancing "cyber defence capabilities, the airport said in its latest annual report released today. It is part of a broader cyber defence program to reduce security threats against the critical piece of national infrastructure and follows a refresh of airport's cyber security strategy last year. "With the security threat landscape evolving rapidly, we have continued to focus on managing current and emerging cyber risks," the airport said. (Read Justin Hendry's report on the matter here: https://www.itnews.com.au/news/)

Understanding Your Computer: Using Caution with USB Drives

What security risks are associated with USB drives?

Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

One option is for attackers to use your USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware, that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on their computers.

Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive. Victims may not even realize that their computers were attacked.

The most obvious security risk for USB drives, though, is that they are easily lost or stolen. If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. And if the information on the drive is not encrypted, anyone who has the USB drive can access all the data on it.

How can you protect your data?

There are steps you can take to protect the data on your USB drive and on any computer that you might plug the drive into:

- Take advantage of security features - Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost.
- Keep personal and business USB drives separate - Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.
- Use and maintain security software and keep all software up to date - Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions current. Also, keep the software on your computer up to date by applying any necessary patches.
- Do not plug an unknown USB drive into your computer - If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into your computer to view the contents or to try to identify the owner.
- Disable Autorun - The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically. In How to disable the Autorun functionality in Windows, Microsoft has provided a wizard to disable Autorun. In the "More Information" section, look for the Microsoft® Fix it icon under the heading "How to disable or enable all Autorun features in Windows and other operating systems."

Read the full article by Mindi McDowell here : **https://www.us-cert.gov/ncas/tips/ST08-001**

TOP Network Attacks last week in the USA

#	KNOWN AS	(%)
1	Bruteforce.Generic.Rdp.d	2.65%
2	Intrusion.Win.MS17-010.o	1.72%
3	Bruteforce.Generic.Rdp.a	0.83%
4	Intrusion.Win.CVE-2017-0147.sa.leak	0.21%
5	Bruteforce.Generic.RDP	0.16%
6	Intrusion.Win.CVE-2017-7269.cas.exploit	0.11%
7	Intrusion.Win.MS17-010.p	0.10%
8	DoS.Win.ICMP.BadCheckSum	0.05%
9	DoS.Generic.SYNFlood	0.04%
10	Bruteforce.Generic.Rdp.c	0.02%

Source: Kaspersky Labs

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

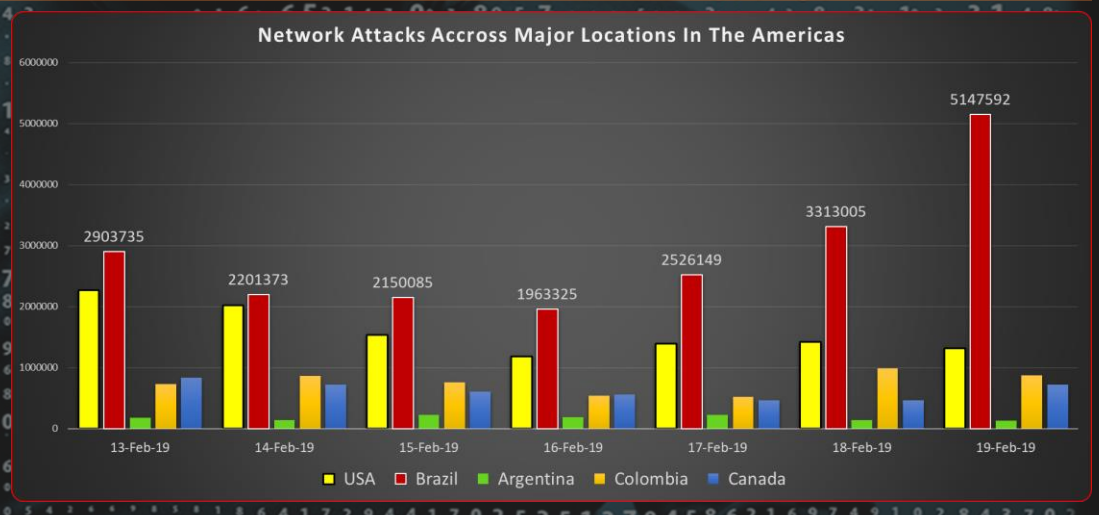
According to Cybint Cyber Solutions

There is a hacker attack every **39 Seconds.**

They also say that

43%

of cyber attacks target small business.



Author: Chris Bester