On August 22, 2019, the Cyber Threat Alert Level was evaluated and is being lowered to Green (Low). Organizations and users are advised to update and apply all appropriate vendor security patches to vulnerable systems and to continue to update their antivirus signatures daily..

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

23 August 2019

In The News This Week

Even Apple gets it wrong some times -

Apple users are being warned to exercise particular caution over their cybersecurity for the next few days, after the company mistakenly reopened a security flaw in the latest version of iOS.

In iOS 12.4, released last month, Apple fixed a number of security bugs, as well as enabling support for the Apple Card in the US. But in doing so, the company accidentally reversed a security fix it had previously patched in iOS 12.3 at the end of April.

That vulnerability, discovered by Google's bug-hunting team Project Zero, theoretically allows "a malicious application … to execute arbitrary code with system privileges". In other words, if exploited, a malicious application can gain complete control over an iPhone – a dream for hackers and spies the world over. "No company is immune from making mistakes, even Apple, especially when the software is so complex as the iPhone," said Javvad Malik, a security awareness advocate at KnowBe4. Read the story here: The Guardian

23 Texas Government Agencies Knocked Offline in 'Coordinated Ransomware Attack' -

On Friday morning of last week, nearly two dozen state agencies across Texas reported having major computer issues. The state now believes that a single hacker is behind this crippling attack.

The Texas Department of Information Resources (DIR) said in a release on Friday that it is overseeing the response to a "coordinated ransomware attack" on several state agencies across the state. As of Saturday, DIR knew of 23 agencies that were affected in the attack, which the department believes was likely executed by a "single threat actor."

DIR say it is working with many organizations to bring the systems back online, including the state's Division of Emergency Management, military department, and Public Utility Commission, as well as the Federal Bureau of Investigation's cyber unit and Federal Emergency Management.

"Currently, DIR, the Texas Military Department, and the Texas A&M University System's Cyber Response and Security Operations Center teams are deploying resources to the most critically impacted jurisdictions," DIR said in a statement. Read the whole story here: Gizmodo

European Central Bank Breach: ECB Confirms Hack and Shuts Down Website -

The European Central Bank (ECB) has confirmed that it has suffered a breach that involved attackers injecting malware and led to a potential loss of data.

In a statement published August 15, the ECB confirmed that "unauthorized parties" had succeeded in breaching the security of its Banks' Integrated Reporting Dictionary (BIRD) website. The site, hosted by an external provider, appears to have been attacked in December 2018, according to a Reuters report. The breach was discovered months later as routine maintenance work was being undertaken.

"The BIRD website provides the banking industry with details on how to produce statistical and supervisory reports," the ECB statement said, "it is physically separate from any other external and internal ECB systems."

In confirming that it had closed down the BIRD site until further notice, the ECB statement also revealed that the personal data of some subscribers to the BIRD newsletter "may have been captured."

That data, affecting 481 subscribers, included names, position titles and email addresses but not passwords, according to the ECB which is contacting people whose data may have been compromised.

Read the full story here: Forbes

How to secure your "IoT" devices.

Last week we explored what "Internet of Things" (IoT) devices are and how it appears more and more in the cyber security spotlight. This week we will look into ways of securing your IoT devices.

Below is an adapted article by Luke James MakeUseOf (click to read the web article)

When you lead a busy lifestyle, anything that you can do to make it that little bit easier and more convenient can be a godsend. That is why kitting your home out with the latest Internet of Things (IoT) devices can be a tempting prospect. After all, wouldn't you like to be able to check up on the dog whilst you're away from home or see who's ringing your doorbell? If it's a cold caller then you can see this and simply ignore them, however, if it's the postman you can tell him to leave your package in a designated safe space.

Well, the thing is, you can do all of this and more with devices that are currently available. Heating your home, controlling the lights, turning on the oven and starting up your washing machine can all be done remotely from your phone or computer when you aren't there.

This is known as the Internet of Things and it is growing rapidly, spurred on by a culture that demands digital connectivity and smart devices that can be applied to all areas of life. Whilst this level of connectivity is great, there are some major drawbacks that you need to be aware of. Without proper management and security, your smart home full of connected IoT devices can become a living nightmare if it is targeted by hackers.

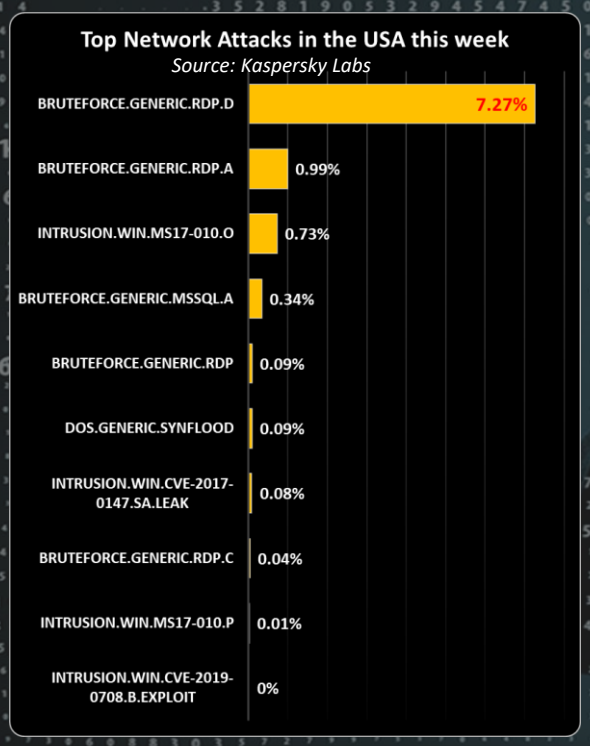
Many people naturally don't realize just how vulnerable they can be when making the most of the IoT. There are several security and privacy risks that pose a serious threat. Any device that shares a wireless network is inherently at risk of a security breach. When somebody gains access to your smart devices, they can harvest your data and manipulate them. With some smart home devices—e.g. cameras and ovens—this is downright dangerous. Luckily, there are plenty of security measures you can take to secure your IoT devices.

5 Ways to Secure Your Family of IoT Devices - If you haven't done any of these things yet or haven't at least checked your devices over to ensure they meet the following points, then you should do so right away if you use a lot of smart devices. **(1)** Start with your Router - Your router is the 'front door' to your smart home. Just like your physical front door, your router's front door should be secured with solid locks. You never know who's going to come knocking. **(2)** Create a Secondary or 'Guest' Network - You can create multiple networks on your Wi-Fi router. This is mostly used to create kids' networks with parental controls or guest networks for visitors. You may want to create an additional network that is solely for connecting your IoT devices to. By doing this, you prevent potential hackers from accessing sensitive data, shared files and other bits and pieces from your other devices if they breach your network.

All your Wi-Fi router's networks should be secured with a strong encryption method and robust password. For routers, the standard and most secure encryption method is called WPA2. This should always be used, even for guest networks.

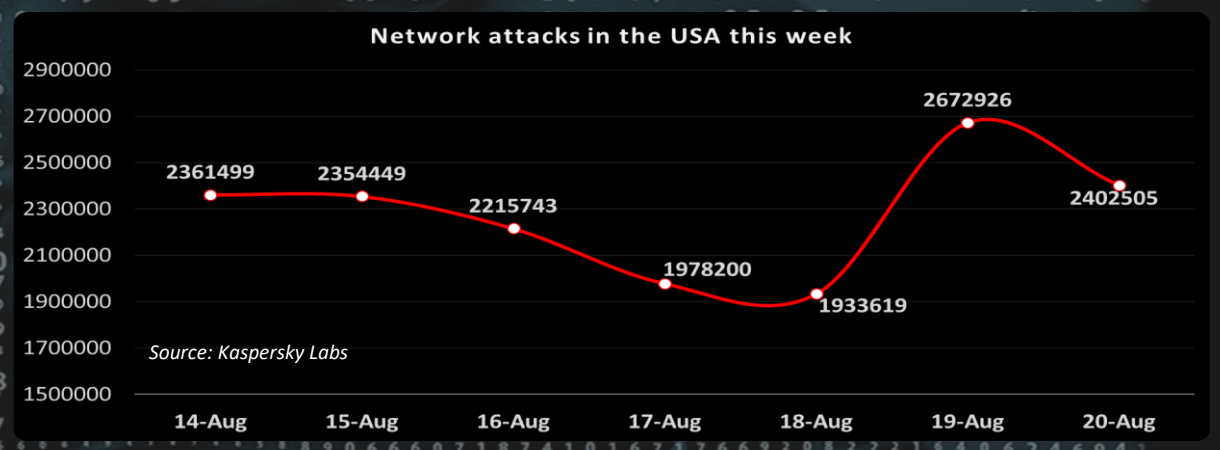
For passwords, avoid things that are common and easy to guess. Never use your router's default username and password. Creating a secondary and tertiary network is easy, and most routers let you do this through a user-friendly GUI. **(3)** Check Your IoT Device Settings and Keep Them Updated - Your IoT device probably comes with default security settings and you may want to consider changing them. Not all manufacturers have your best interests in mind and the default settings may work to benefit them more than you. Additionally, check that you don't have features enabled that you don't need. Avoid putting off software updates as these are often patches for security vulnerabilities. Many IoT devices will prompt you when an update is available, but it's good due diligence to check manufacturer websites often. **(4)** Enable Two-Factor Authentication - If any of your devices offer two-factor authentication, use it. Two-factor authentication is an additional security layer on top of a device's password that requires secondary authentication—a one-time code sent via email or SMS—before access is granted. When used properly, two-factor authentication can stop the bad guys gaining access to your accounts and taking control of your IoT devices. **(5)** Disable UPnP Features - IoT devices tend to have Universal Plug in and Play (UPnP) features, enabling different devices to find and connect to one another. Whilst this is convenient and eliminates the need to configure each device individually, the protocols rely on local networks to connect to each other and these are vulnerable to third-party attackers. When an attack occurs, UPnP lets multiple devices be accessed at the same time. It's far safer to just disable it and configure your devices manually.

Nobody's Going to Manage Security for You - Staying one step ahead of attackers and securing your network of IoT devices comes with the territory; it is the price you pay for convenience and benefiting from what IoT devices have to offer. Securing your devices isn't difficult and it is something you absolutely must be doing if you want a comprehensive smart home network.



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

According to Accenture's global survey, security breaches have increased by **67%** over the past five years



Author: Chris Bester
chris.bester@yahoo.com