On September 27, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Drupal, Apple, and Mozilla products. (No new evaluation this week)
CIS Security Advisories

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
06 October 2023

In The News This Week

KillNet launches DDoS attack against UK royal family

A distributed-denial-of-service (DDoS) attack launched against royal.uk, the official website for the United Kingdom's royal family took the site offline. The attack was launched on October 1 and saw the site go offline for around 90 minutes. Once the site was functional again, a Cloudflare IP address checker was put in place to ensure those accessing the site were not automated bots. Responsibility for the DDoS attack was later claimed by Russian hacktivist group KillNet. KillNet has been responsible for DDoS attacks launched against the governments, critical infrastructures and private companied of countries including Germany, Italy and Romania, among others. In a Telegram post about the cyber attack, KillNet claimed that the attack was launched as part of an "attack on pedophiles". It is thought that this is referencing It is thought that this is a reference to the allegations of sexual abuse of a minor made against Prince Andrew, Duke of York. It has not yet been confirmed if KillNet were responsible for the attack. Read the full article by Olivia Powell here: Cyber Security Hub

Australian Home Affairs and Immigration websites hit by denial-of-service cyber attacks

People have not been able to access visa and citizenship applications online following an attack on the Home Affairs website. - The Department of Home Affairs said it was first made aware of the distributed denial-of-service (DDoS) attack overnight and an investigation had been launched. A DDoS attack is when someone attempts to disrupt other people's ability to access a server, service or network — typically by overloading it with requests. And the attacks are becoming increasingly common. In this case, the Home Affairs website, which includes pages where people can lodge visa applications online, was not available for the public to access. In a statement, the department said the attack meant people were "briefly prevented" from access the website and online portals overnight... Read the rest of the story by Stephanie Borys here: ABC News

St. Johns County loses over $1 million to hackers, investigation underway

ST. JOHNS COUNTY, Fla. — St. Johns County is working to get back over $1 million it lost to hackers. Over $600,000 of taxpayer money has been recovered as county law enforcement said it is ramping up its investigation. - No arrests have been made but law enforcement is involved and they're working with the sheriff's office and Secret Service to recover the rest of the money. The scam all started with 1 letter. The county was a victim to a business email compromise. It started in July when the county thought they were talking to and paying DBE Utilities Construction, saying they changed their payment processing. But it was coming from a DOT "CO" email and not DOT "COM." The county sent a payment of over $500,000. But it wasn't actually to DBE.... Documents show St. Johns County again paid the hackers for a separate payment of over $600,000 in September. But the actual company emailed them saying they hadn't received any payments. Tyler Chancy, head of cybersecurity for Scarlett Group said this style of hacking means hackers have been reading your emails for a while. "They learn the habits, they learn the account, they learn the job," Chancy said. "Once they have all the information and knowledge they strike at the right time. They launch the attack right when a bill is being changed or someone isn't paying attention and they do it in a way that looks legitimate." So far roughly 60 percent of the money has been recovered, Patty said in the county commissioners meeting they're finding third party solutions to the threats... Read the report by Ben Ryan here: Action News Jax

Hackers steal user database from European telecommunications standards body

A nonprofit institution for developing communications standards said hackers have stolen a database identifying its users. The European Telecommunications Standards Institute (ETSI) announced the incident last week. It is not yet clear whether the attack was financially motivated or if the hackers had intended to acquire the list of users for espionage purposes. Following the incident, ETSI, which is based in the Sophia Antipolis technology park in the French Riviera, said it brought in France's cybersecurity agency ANSSI "to investigate and repair the information systems." The nonprofit said the "vulnerability on which the attack was based has been fixed," although it did not identify the vulnerability. A spokesperson declined to clarify whether this had been a known vulnerability or a zero-day at the time of the attack. Read the full article here: The Record

South Africa - SSA spooked after daring cyber attack

The State Security Agency (SSA) has been keeping a top secret from the public for more than a month. - Sunday World can exclusively reveal that SSA believes that it has been hacked by Britain's MI6 and US' CIA. Insiders believe the hackers accessed sensitive and compromising information. Sunday World has seen a video clip which SSA maintains it is intelligence data showing that South Africa along with Russia and India were the targets of the cyber attack in August this year, shortly before the Brics Summit. They said their analysis shows that Russia was the first victim of the coordinated attack, followed by India. As a result, a top official, Joe Mbhambhu, was made to take the fall for the scandal and forced to resign, while a multi-layered investigation was launched to assess the damage and track down the mastermind. Read the rest here: SundayWorld

For Reporting Cyber Crime in the USA go to **(IC3)** , in SA go to **Cybercrime**, in the UK go to **ActionFraud**

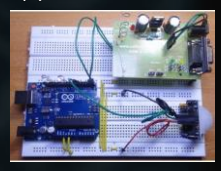
Using the humble Arduino for DIY home security projects

My son is currently busy with a small project to hook up physical switches to his flight simulator game to control things like the wing flaps, undercarriage, and so on, using a small Arduino microcontroller board that cost less than $20, and about the size of a credit card. He asked my help on a few things and as I was doing some research, I came across a ton of DIY home security and automation projects also using an Arduino. This could be a viable option for those who are budget-strapped and don't have the cash to flog out on a security company to do it for you. The projects range from simple PIR sensor systems to fully-fledged Wi-Fi and GSM-enabled alarm systems that will send you a message on your phone if the system is triggered. And most of it is within the technical grasp of a child, so almost anyone can do it. All you would typically need is some basic tools, like a screwdriver, side cutter, pliers, etc., and some code (which is mostly provided). You don't even need a soldering iron in most cases unless you want to be fancy J. So, my aim today is to first tell you a little bit more about the Arduino, and then direct you to some of the projects I found. Most of the components needed you can find at your local electronics store, or you can order them online. (*Locally in South Africa, I source most of my stuff from Micro Robotics and Communica.)*

What is an Arduino micro controller?

The Arduino platform was created in 2005 at the Interaction Design Institute Ivrea (IDII) in Italy. At the time, microcontroller boards were more geared for engineers than makers, and the design students at IDII needed an easier way to create their projects. Interestingly, the Arduino name comes from the pub the founding members used to meet at during its development. The picture shown here is of the Arduino Uno, probably one of the more popular of the Arduino family of microcontrollers and a popular choice for building 3D printers and things like security systems. Other similar-sized Arduino boards are the Leonardo and the Due, which one you choose depends on your project. Many of you probably also heard of or used a single board computer (SBC) like the Raspberry Pi. Although similar in size, these boards are different from microcontrollers. The biggest difference is that Raspberry Pi runs an operating system, and other software runs on that system. Arduino simply runs the code you upload to it. No frills, it simply does what it's told.

Security system projects



Project 1 – GSM Based Home Security Alarm System Using Arduino
Why not build a simple yet effective home security system? It calls the homeowner on a mobile number in the event of an intruder alert. To set up your personal alarm system, you'll need an Arduino Uno, a breadboard, some sensors, and a GSM module for calling your phone. The code for the Arduino is included, so the project shouldn't be too demanding even for beginners.

Project 2 – Bluetooth Door Lock (Arduino)
With this project, you can use your Android or Windows device to automatically lock and unlock a door via Bluetooth. You'll just need an Arduino Nano, a Bluetooth module, a servo, and a 5-V wall adapter. The idea is that I can easily lock and unlock my door without having to carry a key or even go near it. But this is only a fraction of what we can do. From here we could add a sensor like a knock sensor so we can unlock our door with a special knock or even voice recognition.

Project 3 – RFID Security System With Arduino
This project will basically teach you how to build an RFID Security System with Arduino. Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag, like the access control card you use at work. You will need: x1 RFID RC522 Card; x1 Arduino UNO; x1 Breadboard; x2 LED(Red, Green); x1 Buzzer; x1 Servo Motor and some jumper wires.

Project 4 - Upgrading your alarm system with an Arduino
When "Doug" moved into his new house, he found an old alarm panel set up — but it had no monitoring service anymore. Not wanting to pay a monthly fee to have it set up, he decided to try interfacing an Arduino with the system in order to push events to the net! He's using an Arduino Uno and an Ethernet breakout board to hook it up to the network.

Project 5 - Basement Flood Alarm (Using Arduino)
This compact but very helpful monitor will alert you to basement flooding, which is extremely practical if you live in a rainy area or are simply concerned about extra water or mold in your basement. The project uses an Arduino Uno with a moisture sensor and buzzers to create the alerting alarm effect. With thorough instructions and photos provided, the creator also suggests some possible modifications and explains false alarms (so you know what to expect if the alarm goes off).

Project 6 - Automatic Fish feeder using Arduino (Yes, I know its not a security project, but it could be fun ☺)
Suppose you are going out of town for a weekend or maybe for a few weeks and no one is there to feed your fish, then the question arises "Who will take care of your fish if you are running an aquarium?" This is a fun project, and you will need the following: Arduino Uno, Breadboard; Any empty plastic bottle; Servo motor; Jumper wires; DC adapter or battery; Cardboard; Glue, and some double side tape. (If you use a battery instead of a DC adapter, the fish feeder will work even if there is a power failure)

Some of the technical jargon explained

- If the project refers to a "Breadboard", it is not the board you cut bread on, it is simply a board for prototyping or building circuits on. It allows you to place components and connections on the board to make circuits without soldering.
- There is often a reference to a servo or servo motor. Servo motors or "servos", as they are known, are small electronic motors or actuators that rotate, push or pull components in your electronic project (like rotating the automatic fish feeder).

Resources: All3DP, Instructables, Hackaday, Circuit Digest, Hackster.io, MakeUseOf, The Arduino Handbook, Arduino Project Hub

Other Interesting News and Cyber Security bits:

- Nearly two-thirds of cybersecurity teams reportedly understaffed
- A Framework for Future Cybersecurity in Agriculture
- Who's Hacked? Latest Data Breaches And Cyberattacks (Cybercrime Magazine)
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
IRIS Interactive Earthquake Map
Marine Traffic
SatelliteXplorer Track satellites in orbit

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