On April 5, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to a compromise in 3CX software and vulnerabilities in Google products.
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

07 April 2023

In The News This Week

FBI Cracks Down on Genesis Market: 119 Arrested in Cybercrime Crackdown

A coordinated international law enforcement operation has dismantled Genesis Market, an illegal online marketplace that specialized in the sale of stolen credentials associated with email, bank accounts, and social media platforms.
Coinciding with the infrastructure seizure, the major crackdown, which involved authorities from 17 countries, culminated in 119 arrests and 208 property searches in 13 nations. However, the .onion mirror of the market appears to be still up and running. The "unprecedented" law enforcement exercise has been codenamed Operation Cookie Monster.
Genesis Market, since its inception in March 2018, evolved into a major hub for criminal activities, offering access to data stolen from over 1.5 million compromised computers across the world totaling more than 80 million credentials.
Read the rest of the post by Ravie Lakshmanan here: The Hacker News

Check Point attacked - Israeli cyber security website briefly taken down in cyberattack

One of Israel's largest cyber-security companies, Check Point, was taken down by a group of hackers calling themselves "Anonymous Sudan" on Tuesday afternoon. However, after a short while, the website seemed to return to operating as normal. Earlier in the day, the websites of multiple major universities in Israel were also attacked by the same group and were down for several hours.... Statement from a Check Point spokes person "All our sites are functioning well despite a large-scale attack on them," Check Point's spokesperson said in a statement. "The company's website is protected against DDoS (Distributed Denial of Service) attacks at the highest level. [It is] one of the strongest websites in the world.
Read the story by here: JPost

Is ChatGPT Safe? 6 Cybersecurity Risks of OpenAI's Chatbot

Although many digital natives praise ChatGPT, some fear it does more harm than good. News reports about crooks hijacking AI have been making rounds on the internet, increasing unease among skeptics. They even consider ChatGPT a dangerous tool. AI chatbots aren't perfect, but you don't have to avoid them altogether. Here's everything you should know about how crooks abuse ChatGPT and what you can do to stop them. Read the article by Jose Luansing Jr. here: MakeUseOf

Criminal records office yanks web portal offline amid 'cyber security incident'

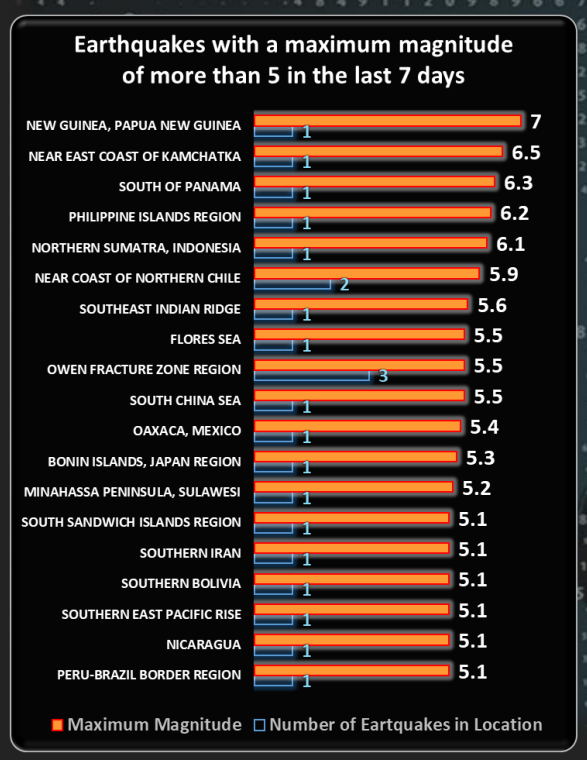
ACRO, the UK's criminal records office, is combing over a "cyber security incident" that forced it to pull its customer portal offline. As the name implies, the government agency manages people's criminal record information, running checks as needed on individuals for any convictions, cautions, or ongoing prosecutions. It doesn't just work with British police and businesses: it exchanges this data with other countries. This data, used by employers vetting potential hires and embassies processing visa applications, is drawn from UK's Police National Computer via an information sharing agreement ACRO has with the Cabinet Office. The data input typically includes a decade's worth of name and address history, extended family information, a new foreign address, legal representation, passport information, photo and data PIN cautions, reprimands, arrests, charges or convictions." Read the rest of the story by Paul Kunert here: The Register

The Pope's Security Gets a Boost With Vatican's MDM Move

The world's smallest and most antiquated army is taking a step towards modernizing its cyber defenses. Just ahead of the pre-Easter Holy Week for Catholics, Samsung announced that the Pontifical Swiss Guard (GSP) — the elite security force charged with protecting the Vatican and the Pope — is adopting the Knox Suite, a bundle of services for managing and securing mobile devices. Strange as the fit might be, multilayered security is necessary for an organization whose long history includes plenty of targeted cyberattacks. "Protecting the Vatican could be subtitled 'Mission Impossible,'" Approov CEO Ted Miracco says. "It's a high-profile target, with a vast array of sensitive information and valuable assets that make it attractive for cybercriminals, hackers, and other powerful groups opposing it." Read more by Nate Nelson here: Dark Reading

Garage Door Openers Open to Hijacking, Thanks to Unpatched Security Vulnerabilities

Garage door controllers, smart plugs, and smart alarms sold by Nexx contain cybersecurity vulnerabilities that could enable cyberattackers to crack open home garage doors, take over smart plugs, and gain remote control of smart alarms, according to the US Cybersecurity and Infrastructure Security Agency (CISA). And although independent cybersecurity researcher Sam Sabetan reported that he discovered several vulnerabilities in late 2022 and alerted Nexx to the issues, the company has yet to respond. Nexx has not replied to Dark Reading's request for comment, either. CISA's April 4 warning applies to three specific Nexx Internet of Things (IoT) products: Nexx Garage Door Controller (NXG-100B, NXG-200), version nxg200v-p3-4-1 and prior; Nexx Smart Plug (NXPG-100W), version nxpg100cv4-0-0 and prior; and Nexx Smart Alarm (NXAL-100), version nxal100v-p1-9-1 and prior.... Until Nexx issues a fix, Sabetan and CISA recommend that users unplug affected devices. "If you are a Nexx customer, I strongly recommend disconnecting your devices and contacting Nexx to inquire about remediation steps," Sabetan said in his disclosure. Read the full story here: Dark Reading



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

THE VIRTUAL EASTER EGG AND ITS HIDDEN BACK DOOR

If you are working in the cyber security space or are a programmer or a coder as the younger generation calls it, then you will most probably know what the term "Easter egg" means in relation to security. But, for common Joe out there, an Easter egg is an Easter egg, and are none the wiser about what it means in the digital world. I did a bit of digging in the Internet forest to find a reasonable explanation that I can share with you all and I found this article by Mirjam Burkard of InfoGuard (Swiss Cyber Security) that sort of capture what a digital Easter egg is.

"EASTER EGG" – THE VIRTUAL EASTER EGG AND ITS HIDDEN BACK DOOR.

Easter will be soon here again, and Easter egg hunts will be starting. It is fun and exciting, and at the end, we have the rewarded of an Easter nest filled with chocolate eggs and sweets. Hunting for Easter eggs is happening in the virtual world too. These Easter eggs are hidden surprises which are inserted by developers into things like operating systems, websites, applications and games. This kind of Easter eggs are fun but can also open up a hidden back door to attackers.

The virtual Easter egg - In the virtual world, Easter eggs are hidden codes that pop up within an application. Often developers or authors hide little funny surprises in their software known as Easter eggs, and so they become a permanent fixture in the application. Even the official software producer is often unaware of them, and they can be discovered quite by chance. To display or run an Easter egg in a program, you need to use certain key combinations, call up menu items or enter text and carry out certain other actions. For instance, Easter eggs might be pictures, videos, hidden text or even special functions, a secret level or applications hidden within a program.

No two eggs are alike - The same is true with both Easter eggs and virtual Easter eggs – no two eggs are alike. There is no single definition for Easter eggs, and this means that there are many different variants. Some of them are documented internally and are relatively innocuous, but some of them are undocumented and have adverse effects. Easter eggs are hiding in the most diverse applications:

- Video games are where Easter eggs are most widespread. Back in 1979, the developer Warren Robinett was able to build a secret room in the "Adventure" video game made for the Atari game console, which contains a script with the words "Created by Warren Robinett". It was the first action-adventure game and is also considered to be the first game to contain an Easter egg, but Easter eggs are also often found in movies in the form of allusions to other movies.
- Websites may also contain Easter eggs. One of Google's best known Easter eggs is when you type "do a barrel roll" into the search window. The browser screen then rotates through 360 degrees, or by typing "askew", the search engine tilts the Google search results page so that everything is on a slant.
- Even Microsoft developers have hidden Easter eggs in old versions of Microsoft Office, contributing their own sense of humour. In Word 97, for example, by entering secret key combinations, you could play pinball, or in Excel 97 you could use a flight simulator to fly over the names of the program developers which were carved into a virtual cliff. In Excel 2000 there was a motor racing game However, since then, doing this has been officially outlawed by Microsoft under the Trusted Computing Initiative because of the implications for security.
- An "Easter egg" was also discovered in connection with the Stuxnet virus, and Easter eggs were also found in Siemens PLC firmware – the system targeted by Stuxnet. These were embedded in an HTLM file and depicted dancing monkeys. The code was not documented and had not undergone any testing, which clearly called the quality management into question.

The hidden back door with Easter eggs - In principle, however, Easter eggs are relatively harmless, as their aim is not to unleash a harmful action, rather to reveal a fun surprise. However, any undocumented code poses a security risk, as it has no test procedures to be kept secret, and it may open up a potential hidden backdoor for attackers. Besides that, any software with these features is not very trustworthy. This is why many software companies forbid programmers from inserting Easter eggs or require them to undergo normal source code testing. These are then officially built-in fun features to entertain the users and are no longer secret, hidden messages from the programmer.
The term "logic bomb" often crops up in relation to Easter eggs. Like Easter eggs, logic bombs are also hidden programming code that is deliberately incorporated into the software. Again, there is no universal definition for what a logic bomb is, but unlike Easter eggs, logic bombs initiate a harmful or even a criminal process. The feature of these so-called "logic bombs" is that, in the same way as Easter eggs, they are triggered by entering special data, either at a specific time or via precisely defined actions, and then, unlike Easter eggs, they cause harm.
There have also been instances where former employees have planted logic bombs. One example is a former IT employee of the Fannie Mae mortgage lender who planted a logic bomb. Had it been triggered, it would have deleted countless customers' mortgage data and caused millions of dollars' worth of damage.

Hunting for "Easter eggs" is fun

Once again, this year, lots of children (as well as adults) will be out hunting for Easter eggs. This time, they will probably have to hunt within their own homes. This is what the FOPH recommends, and of course, we fully support that. However, for several years now, **the hacker community** has also been searching for hidden clues at Easter in the form of a CTF (Capture The Flag) game called "Hacky Easter", but they are not actually hunting for Easter eggs, they are searching for flags (solution words) that have been deliberately hidden. For example, these are concealed in images, programs, network traffic etc. The CTF participants know exactly what they are searching for.

What can you do as a company?

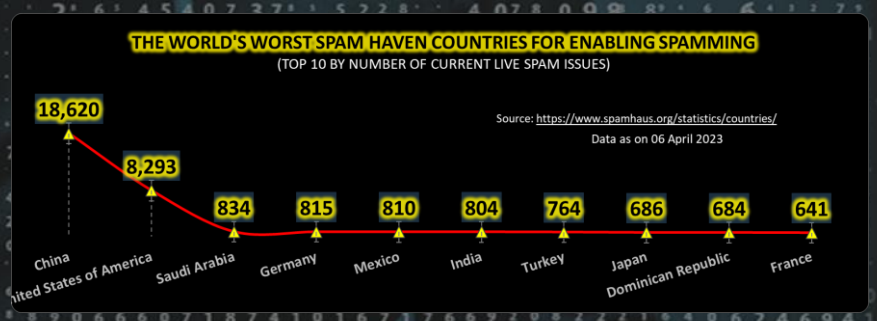
Although most Easter eggs are harmless and just undocumented code, they pose a real security risk, and the logic bomb aims to do damage. Consider these points in that light: - **(1)** When buying new software, we also recommend that you look at the software contract. How are non-documented functions or Easter eggs addressed and how are they dealt with? **(2)** You can also take precautions against possible unwanted applications (PUA for short), which may be installed directly by employees. Keep local administrator rights on end devices to a minimum. **(3)** With unknown programs, it is recommended that the application is first installed in a sandbox environment. You can also combine this with reverse engineering to verify that the software does what it is intended to do.

Read Mirjam's post here: InfoGuard

Other Interesting News and Cyber Security bits:

- Job scams powered by ChatGPT could try to rob you. How to protect yourself
- SpaceX's Next-Gen Starlink Satellites Have Started Falling From Space
- Researcher Tricks ChatGPT Into Building Undetectable Steganography Malware
- 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