No change in status - On November 28, 2018, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). The MS-ISAC released a Cyber Alert regarding the recent evolution of Business Email Compromise (BEC) scams targeting direct deposit accounts through emailed change requests being sent to Human Resources or Finance departments.

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
14 December 2018

In the news this Week

Australia Passes Anti-Encryption Bill

Australia's House of Representatives has finally passed the "Telecommunications Assistance and Access Bill 2018," also known as the Anti-Encryption Bill, on Thursday that would now allow law enforcement to force Google, Facebook, WhatsApp, Signal, and other tech giants to help them access encrypted communications. The Australian government argues the new legislation is important for national security and an essential tool to help law enforcement and security agencies fight serious offenses such as crime, terrorist attacks, drug trafficking, smuggling, and sexual exploitation of children. Since the bill had support from both major parties (the Coalition and Labor), the upper house could vote in support of the Assistance and Access Bill to make it law, which is expected to come into effect immediately during the next session of parliament in early 2019. Will other governments follow suit?

Read the full story at https://thehackernews.com

Watch out for a clever touch ID scam hitting the app store

One of the joys of Touch ID is how seamlessly it works. It rarely takes more than an instant to unlock your iPhone or approve a purchase. But recently a handful of scam apps have turned that ease of use against anyone unlucky enough to download them. In separately reported incidents, apps posing as health assistants invite users to use Touch ID before they show a calorie tracker, or take a heart rate measurement, or some other seemingly legitimate function. Once you scan your fingerprint, though, the apps briefly show an in-app purchase popup instead, charging anywhere from $90 to $120, and simultaneously dim the screen to make it hard to see the prompt. In some cases, even if you decline to use Touch ID to enable a feature, the app asks you to tap to continue—and try the in-app payment scam instead.

Read the full story at https://www.wired.com

BOMB THREATS! - THE NEW BITCOIN SCAM

In offices and universities across the USA last Thursday, the same threat appeared in email inboxes: Pay $20,000 worth of bitcoin, or a bomb will detonate in your building. Police departments sent out alerts. Workers from Los Angeles to Raleigh, North Carolina, evacuated their cubicles in the middle of the day. All over Twitter, people posted screenshots of the emails, many different versions of which appear to have been blasted out. As of Thursday afternoon, no bombs had been found, and cybersecurity experts largely dismissed the threats as an elaborate hoax. Not all police departments have confirmed it as a scam. But it certainly appears to be a steep escalation of a bitcoin blackmail tactic that took off this summer. In that scheme, victims received an email claiming that a hacker commandeered their webcam while they were watching pornography and would release the resulting photos publicly if the target didn't pay a small amount in bitcoin. It was an obvious lie but one that nevertheless earned its perpetrators half a million dollars. In an apparent attempt to increase the urgency, this wave of attacks swaps out sextortion in favour of fake bombs. Read the full story at https://www.wired.com

Proper Disposal of Electronic Devices

Why is it important to dispose of electronic devices safely?

Computers, smartphones, and cameras allow you to keep a great deal of information at your fingertips, but when you dispose of, donate, or recycle a device you may inadvertently disclose sensitive information which could be exploited by cyber criminals.

Some effective methods for removing data from your device

There are a variety of methods for permanently erasing data from your devices (also called sanitizing). Because methods of sanitization vary according to device, it is important to use the method that applies to that particular device. Methods for sanitization include: (Firstly make sure you have a Backup of your data)

(A) Deleting data - Removing data from your device can be one method of sanitization. When you delete files from a device—although the files may appear to have been removed—data remains on the media even after a delete or format command is executed. Do not rely solely on the deletion method you routinely use, such as moving a file to the trash or recycle bin or selecting "delete" from the menu. Even if you empty the trash, the deleted files are still on device and can be retrieved. Permanent data deletion requires several steps. Computers - Use a disk cleaning software designed to permanently remove the data stored on a computer hard drive to prevent the possibility of recovery. This could include (a) "Secure erase" which is a set of commands in the firmware of most computer hard drives. If you select a program that runs the secure erase command set, it will erase the data by overwriting all areas of the hard drive. (b) "Disk wiping" This is a utility that erases sensitive information on hard drives and securely wipes flash drives and secure digital cards. Smartphones and tablets - Ensure that all data is removed from your device by performing a **"hard reset"** This will return the device to its original factory settings. Each device has a different hard reset procedure, but most smartphones and tablets can be reset through their settings. In addition, physically remove the memory card and the subscriber identity module card, if your device has one. Digital cameras, media players and gaming consoles - Perform a standard factory reset (i.e., a hard reset) and physically remove the hard drive or memory card. Office equipment - (e.g., copiers, printers, fax machines, multifunction devices). Remove any memory cards from the equipment. Perform a full manufacture reset to restore the equipment to its factory default.

(B) Overwriting - Another method of sanitization is to delete sensitive information and write new binary data over it. Using random data instead of easily identifiable patterns makes it harder for attackers to discover the original information underneath. Since data stored on a computer is written in binary code—strings of 0s and 1s—one method of overwriting is to zero-fill a hard disk and select programs that use all zeros in the last layer. Users should overwrite the entire hard disk and add multiple layers of new data (three to seven passes of new binary data) to prevent attackers from obtaining the original data. (a) Cipher.exe is a built-in command-line tool in Microsoft Windows operating systems that can be used to encrypt or decrypt data on New Technology File System drives. This tool also securely deletes data by overwriting it. (b) "Clearing" is a level of media sanitation that does not allow information to be retrieved by data, disk, or file recovery utilities.

(C) Destroying - Physical destruction of a device is the ultimate way to prevent others from retrieving your information. Specialized services are available that will disintegrate, burn, melt, or pulverize your computer drive and other devices. These sanitization methods are designed to completely destroy the media and are typically carried out at an outsourced metal destruction or licensed incineration facility. If you choose not to use a service, you can destroy your hard drive by driving nails or drilling holes into the device yourself. The remaining physical pieces of the drive must be small enough (at least 1/125 inches) that your information cannot be reconstructed from them. There are also hardware devices available that erase CDs and DVDs by destroying their surface. (a) "Magnetic media degaussers" - Degaussers expose devices to strong magnetic fields that remove the data that is magnetically stored on traditional magnetic media. (b) "Solid-state destruction" - The destruction of all data storage chip memory by crushing, shredding, or disintegration is called solid-state destruction. Solid-State Drives should be destroyed with devices that are specifically engineered for this purpose. (c) "CD and DVD destruction" - Many office and home paper shredders can shred CDs and DVDs (be sure to check that the shredder you are using can shred CDs and DVDs before attempting this method).

Adapted from the source information at: https://www.us-cert.gov/ncas/tips/ST18-005

TOP – Network Attacks IN THE LAST WEEK (USA)

#	KNOWN AS	(%)
1	Bruteforce.Generic.Rdp.d	5.63%
2	Intrusion.Win.MS17-010.o	1.54%
3	Bruteforce.Generic.Rdp.a	1.50%
4	Bruteforce.Generic.RDP	0.29%
5	Intrusion.Win.CVE-2017-7269.cas.exploit	0.19%
6	Intrusion.Win.CVE-2017-0147.sa.leak	0.15%
7	DoS.Win.ICMP.BadCheckSum	0.10%
8	DoS.Generic.SYNFlood	0.04%
9	Intrusion.Win.MS17-010.p	0.03%
10	Intrusion.Win.NETAPI.buffer-overflow.exploit	0.02%

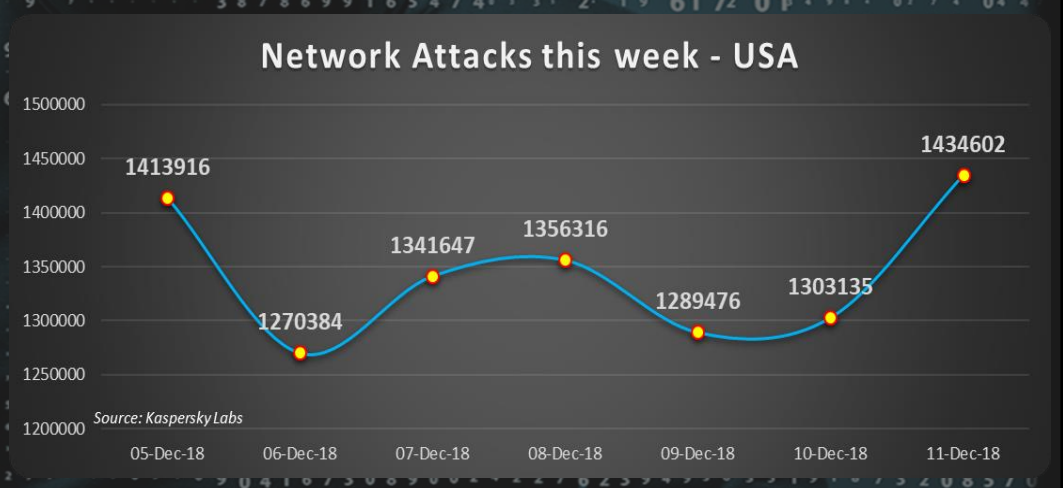
Source: Kaspersky Labs

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

According to Europol IOCTA 2018

In March 2018, Islamic State supporters attempted to come up with a Facebook alternative. Dubbed "Muslim's Network", it was made available in Arabic, English and French. However, the platform was not an in-house development but had been purchased online for a small amount of money showing their own internal capability appears limited.

(Read the Report for details)



Author: Chris Bester