On May 1, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google and Oracle products..

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

10 May 2019

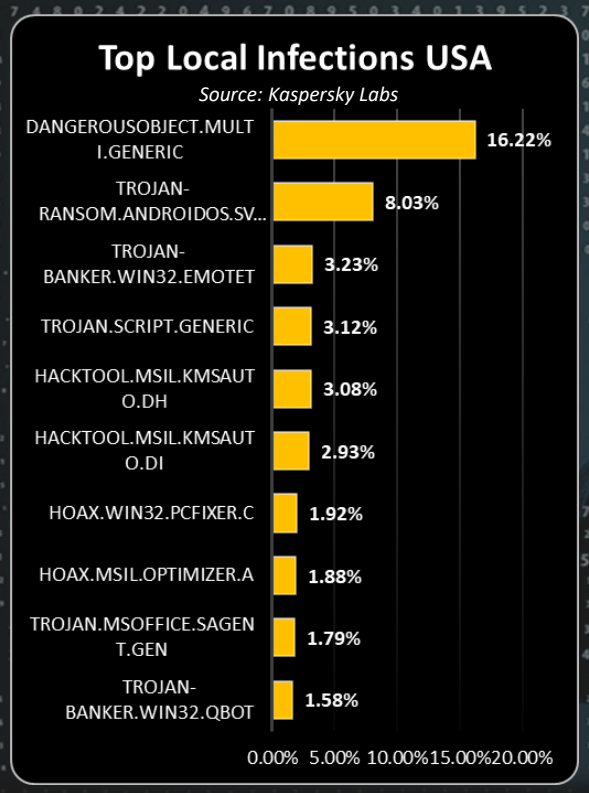
In The News This Week

Hackers Steal $40.7 Million in Bitcoin from Crypto Exchange, Binance.

Hackers stole more than 7,000 bitcoins from crypto exchange Binance, the world's largest by volume, the start-up reported Tuesday 7 May 2019. Binance announced that a "large scale security breach" was discovered earlier on May 7, finding that malicious actors were able to access user API keys, two-factor authentication codes and "potentially other info," the exchange's CEO, Changpeng Zhao, said in a letter. As a result, they were able to withdraw roughly $41 million in bitcoin from the exchange, according to a transaction published in the security notice. The disclosure comes hours after Zhao tweeted that the exchange was undertaking "some unscheduled server maintenance," writing that "funds are #safu." After the disclosure announcement, Zhao tweeted that the exchange would "provide a more detailed update shortly." The exchange may not yet have identified all impacted accounts, he said. And according to Binance's statement, the breach only impacted Binance's hot wallet, which contains roughly 2 percent of the exchange's total bitcoin holdings. "All of our other wallets are secure and unharmed," he said, adding: "The hackers had the patience to wait, and execute well-prepared actions through multiple seemingly independent accounts at the most opportune time. The transaction is structured in a way that passed our existing security checks. It was unfortunate that we were not able to block this withdrawal before it was executed." The withdrawal triggered internal alarms after it was executed, and Zhao said the exchange froze withdrawals following the discovery. While deposits and withdrawals will remain suspended for the next week, trading will be re-enabled, though he cautioned that "the hackers may still control certain user accounts." Read the full story here: CoinDesk

Airbnb "Superhost" Secretly Recorded Guests with Hidden Bedroom Camera.

The incident is only the latest in a string of disturbing horror stories of guests finding live, recording cameras hidden in their Airbnb flats. An Airbnb "superhost" in China has been arrested after a guest staying in his house found a hidden camera recording her in the bedroom. The guest, an unnamed woman who was staying in the Airbnb in eastern China last week, said she discovered the camera after spotting a light that looked unusual in the Wi-Fi router, according to local reports. The unfortunate guest told local news outlets that she worked in information security, and so was more vigilant than the average person when it came to always checking her hotel rooms for signs of surveillance devices. After inspecting and unscrewing the router, the guest found that there was a digital memory card inside. "I checked [the router] carefully and found the line arrangement was different from the usual ones," the woman told Beijing Youth Daily in a recent interview. The guest then called the police, who found that the host had been filming guests since March and arrested him. The home-sharing platform told Beijing Youth Daily that it removed the flat from apartment listings. However, the incident is making potential Airbnb users nervous – especially because the man was an Airbnb superhost, a title given to hosts who, in Airbnb's words, are experienced and seen as "a shining example for other hosts." This is disturbingly only the most recent horror story of traveling guests reporting that they were recorded. In March, Seoul police arrested four people who allegedly filmed about 1,600 motel guests in the past year in various states of undress and having sex. They did so with tiny wireless spy cameras set up in 42 motel rooms at 30 motels across South Korea, in 10 cities. The devices were hidden inside TVs, hair dryer holsters and electrical outlets. Airbnb has policies in place about electronic surveillance devices: Hosts must indicate the presence of any surveillance camera in their home, whether it is recording actively, or even if its not turned on or hooked up. A surveillance camera includes Wi-Fi cameras (including Nest Cam), nanny cameras, web cameras or baby monitors.
Read the full article by Lindsey O'Donnell here: ThreatPost



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

According to the Verizon 2019 Data breach Investigations report:

23%

of all investigated breaches involved actors identified as nation-state or state-affiliated threat actors

Phishing, Pharming, Vishing, and Smishing

Phishing

On the Internet, "phishing" refers to criminal activity that attempts to fraudulently obtain sensitive information. There are several ways a fraudster can try to obtain sensitive information such as your social security number, driver's license, credit card information, or bank account information, often luring you with a sense of urgency. Sometimes a fraudster will first send you a benign email (think of this as the bait) to lure you into a conversation and then follow that up with a phishing email. At other times, the fraudster will just send one phishing email that will direct you to a website requesting you to enter your personal information such as User ID and Password.

Here are some questions to ask if you think you have received a phishing email/attack:

- Do you know the sender of the email? If yes, still be cautious before clicking a link. If no, do not click any links.
- Are there any attachments in the email? If so, is the attachment an executable (a file with the extension ".exe, .bat, .com, .vbs, .reg, .msi, .pif, .pl, .php")? If so, do not click on the attachment. Even if the file does not contain one of the above mentioned extensions, be cautious about opening it. Contact the sender to verify its contents.
- Does the email request personal information? If so, do not reply.
- Does the email contain grammatical errors? If so, be suspicious.
- If you have a relationship with the company, are they addressing you by name?
- Have you checked the link? Mouse over the link and check the URL. Does it look legitimate or does it look like it will take you to a different Web site?

Pharming

Pharming is another scam where a fraudster installs malicious code on a personal computer or server. This code then redirects any clicks you make on a website to another fraudulent Website without your consent or knowledge. To avoid pharming, follow the basic computer safety guidelines published in various sites. Be especially careful when entering financial information on a website. Look for the 's' in https and the key or lock symbol at the bottom of the browser. If the website looks different than when you last visited, be suspicious and don't click unless you are absolutely certain the site is secure.

Vishing

Unfortunately, phishing emails are not the only way people can try to fool you into providing personal information in an effort to steal your identity or commit fraud. Fraudsters also use the phone to solicit your personal information. This telephone version of phishing is sometimes called vishing. Vishing relies on "social engineering" techniques to trick you into providing information that others can use to access and use your important accounts. People can also use this information to assume your identity and open new accounts.

To avoid being fooled by a vishing attempt:

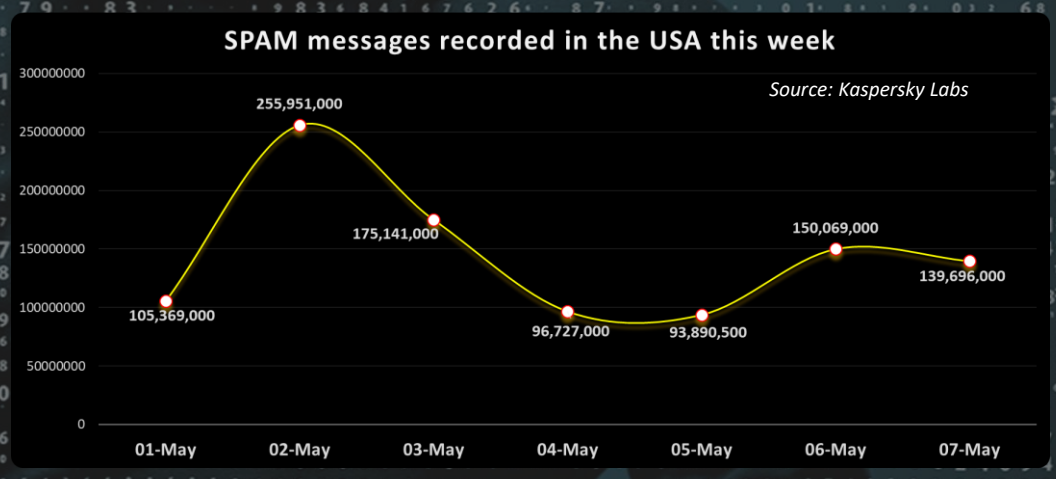
- If you receive an email or phone call requesting you to call them and you suspect it might be a fraudulent request, look up the organization's customer service number and call that number rather than the number provided in the solicitation email or phone call.
- Forward the solicitation email to the customer service or security email address of the organization, asking whether the email is legitimate.

Though vishing and its relative, phishing, are troublesome crimes and sometimes hard to identify, here are some tips from the Federal Trade Commission to protect your identity.

Smishing

Just like phishing, smishing uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. And again, just like phishing, the smishing message usually asks for your immediate attention.
In many cases, the smishing message will come from a "5000", "10" or some other arbitrary number instead of displaying an actual phone number. This usually indicates the text message was sent via email to the cell phone, and not sent from another cell phone. Do not respond to smishing messages.

Adapted from various sources



AUTHOR: CHRIS BESTER