On May 15, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Microsoft, and Adobe 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

24 May 2019

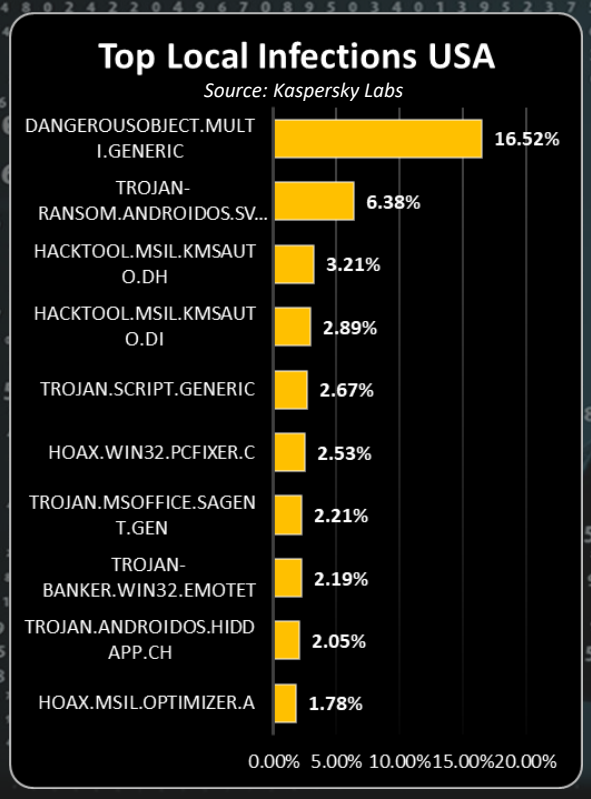
In the News this week

Google stored some passwords in plain text for the last fourteen years!

In a blog post earlier this week, Google disclosed that it recently discovered a bug that caused some portion of G Suite users to have their passwords stored in plain text. The bug has been around since 2005, though Google says that it can't find any evidence that anybody's password was improperly accessed. It's resetting any passwords that might be affected and letting G Suite administrators know about the issue. G Suite is the corporate version of Gmail and Google's other apps, and apparently the bug came about in this product because of a feature designed specifically for companies. Early on, it was possible for your company administrator for G Suite apps to set user passwords manually — say, before a new employee came on board — and if they did, the admin console would store those passwords in plain text instead of hashing them. Google has since removed that capability from administrators. Google's post goes to great pains to explain how cryptographic hashing works, likely in an effort to make sure the nuances surrounding this bug are clear. Though the passwords were stored in plain text, they were at least stored in plain text inside Google's servers, so they'd be harder to get to than if they were just out on the open internet. Although Google didn't say so explicitly, it seems like it wants to also make sure people don't lump this bug in the same category as other plain text password problems where those passwords have leaked out (Twitter & Facebook). - Read the full story here - TheVerge

Satan's Ransomware-as-a-service offering Adds More Evil Tricks.

The latest changes to the Satan ransomware framework demonstrate attackers are changing their operations while targeting victims more carefully. The operators and developers behind a 2-year-old ransomware framework, dubbed Satan, continue to expand the codebase, adding exploits for the Spring Web application framework, the ElasticSearch search engine, and ThinkPHP Web application framework popular in China, according to research from Fortinet. The refinements demonstrate a trend in ransomware: The malware is becoming more sophisticated and operations against victims more targeted, according to the company. In its quarterly threat report, Fortinet points to multiple debilitating attacks on manufacturers, chemical companies, and engineering firms, stating that attackers are moving from "indiscriminate ransomware attacks to more targeted and potentially more lucrative campaigns." "We are seeing more methodical techniques," says Anthony Giandomenico, a senior security researcher at Fortinet. "Some of the adversaries that are using ransomware — they are getting better at quickly incorporating new vulnerabilities that have recently been successfully exploited." The incorporation of three new exploits into the Satan ransomware framework highlights the continuing improvement in capabilities incorporated into the malicious software by operators and developers. Satan, which is the malware component of a ransomware-as-a-service offering on the Dark Web of the same name, had already included exploits for a variety of Web technologies, such as JBoss, Apache Struts, Web Logic, Tomcat, and the infamous EternalBlue exploit for Windows SMB services. While the addition of three new exploits does not appreciably increase the threat level of the malware, it does show that the developers are actively improving the code and the service, Fortinet's Giandomenico says. "The ransomware-as-a-service is successful in that it is taking advantage of those vulnerabilities that have been exploited much faster," he says. In January 2017, Satan made headlines as the first known ransomware-as-a-service offering — but not the first crimeware-as-a-service product — on the Dark Web. Subscribers can create tailored ransomware attacks, and the operators of the Satan service take a portion of any ransom paid. Read the full story by Robert Lemos here: DarkReading



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

Cyber Security Engineers are projected to be the highest paying and most recruited in the next few years

Smartphone Security (Part 2 of 5)

3. The third layer of protection: be careful with that web browsing

Install an ad blocker. No, not because ads are intrusive and have been failing potential customers, but because they can be exploited by cybercriminals. Malvertising can be served right on your smartphone through ad servers – and you don't even need to click on anything in order to get infected! Recently, over 14 million Android devices were infected by the CopyCat malware, with 8 million of them rooted. An ad-block app will help decrease your chances of infection. Blocking pop-ups will also help – you can easily do that from the browser settings.

For Chrome, for example, you just have to go to Settings -> Site Settings -> Pop-ups -> and make sure it's on Blocked. It's also recommended that you disable JavaScript in your mobile browser. This will also help you reduce the data you consume: according to recent studies, ad content is accountable for between 18 to 79% of transferred mobile data. That's especially true if you navigate through a lot of news websites. "JavaScript elements – often used by publishers for ads, but also for visual elements such as animations – added an extra 6% to 68%. Enders noted that the JavaScript it came across in the study wasn't central to the articles being loaded."

Watch out for where you tap your screen, be careful not to end up clicking by mistake where you didn't want in the first place. Ads can be placed close to legit content and you can accidentally end up clicking on them.

If your browser suddenly opens up without you opening it or you have adds suddenly popping up while using legitimate paid-for apps, then its quite possible that your phone or mobile device were infected in one of your recent web surfing stints. In this case, run an anti-virus scanner like Malwarebytes or Avast (or any other good Anti-Virus software you can find in the mobile stores), on you device and clean out the infection.

4. The fourth layer of protection: beware of phishing

First, let's define what is "Phishing": Phishing is the name given to the attempts and actions of cybercriminals to lure you into giving them sensitive information or money. The word "phishing" is similar to "fishing" because of the analogy of using bait to attempt to trap victims. By sensitive information we mean anything that ranges from your social security number and/or Identity number to passwords, bank account number, credit card details, PIN number, home address, social media account, birthday, mother's maiden name and so on.

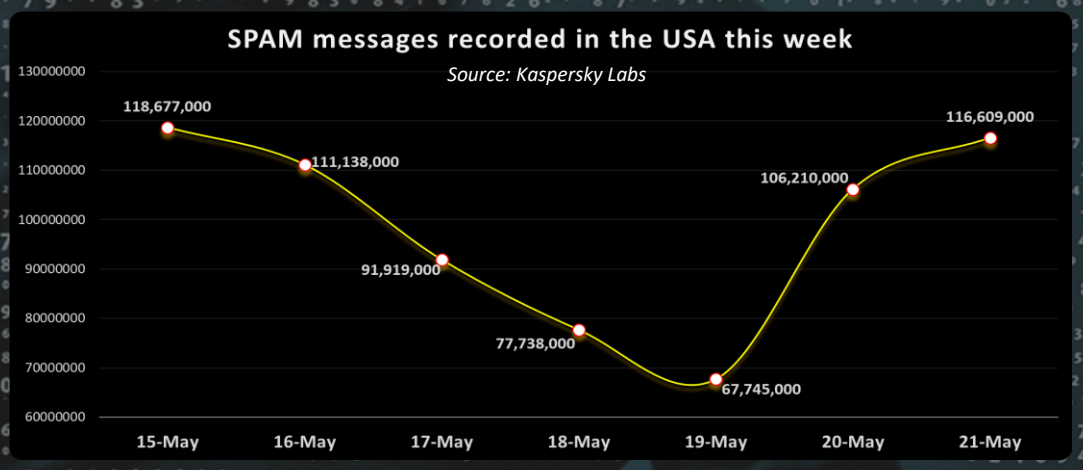
It's much harder to spot a phishing page on your mobile phone than on your PC or laptop. Keep your guard up against phishing on all your devices, no matter if it's a desktop, laptop, tablet or smartphone. No clicking on short, suspicious links, that you didn't request. And be careful with those attachments you download via email or instant messaging services.

Cyber attackers can use phishing techniques to withdraw money from you, steal your identity (here's a true story you should read), open credit card accounts in your name and much more. Not even the strongest antivirus will protect you from phishing and malware. The first truly massive mobile threat was Mazar BOT – a virus that our team detected in the early stages. It was spread via links sent in text messages and could give an intruder administrator rights on the victim's phone. This allowed the attackers to read, send and receive SMS, call people, and even erase the phone.

That's why it's important that you don't click on links that you never requested and don't know where they lead (especially short, hidden links). If somehow you end up clicking on them and they require you to sign-in, don't give away your credentials. Do you remember the "*Fappening*", the huge scandal from the summer of 2014? Lots of pics (especially naked ones) with celebrities were stolen from their phones and leaked online. One of the attackers involved pleaded guilty for the attack. His method to access celebrities' phones? Plain old email phishing: "From the court documents, it became clear that the victims of Collins' attack fell prey to a phishing scam. Collins allegedly sent e-mails to the victims that appeared to come from Google or Apple, warning the victims that their accounts might be compromised, and asking for their login details. The victims would enter their password information. Having gained access to the e-mail address, Collins was able to download e-mails, and get further access to other files, such as iCloud accounts."

Ryan Collins, 36, illegally accessed over 100 Google and Apple accounts of famous people, including that of Hunger Games star Jennifer Lawrence, between November 2012 and September 2014 and sold/distributed private photos and videos of these people. He was found guilty in 2016 and jailed for 18 months.

Adapted from an article by Cristina Chipurici, which you can find here - HEIMDAL SECURITY



Author: Chris Bester