On June 3, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Google and Mozilla 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

05 June 2020

In The News This Week

Google faces $5 billion lawsuit in U.S. for tracking 'private' internet use

Google was sued on Tuesday in a proposed class action accusing the internet search company of illegally invading the privacy of millions of users by pervasively tracking their internet use through browsers set in "private" mode. The lawsuit seeks at least $5 billion, accusing the Alphabet Inc unit of surreptitiously collecting information about what people view online and where they browse, despite their using what Google calls Incognito mode. According to the complaint filed in the federal court in San Jose, California, Google gathers data through Google Analytics, Google Ad Manager and other applications and website plug-ins, including smartphone apps, regardless of whether users click on Google-supported ads. This helps Google learn about users' friends, hobbies, favorite foods, shopping habits, and even the "most intimate and potentially embarrassing things" they search for online, the complaint said. Google "cannot continue to engage in the covert and unauthorized data collection from virtually every American with a computer or phone," the complaint said. Read the full story here: Reuters

Nuclear missile contractor hacked in Maze ransomware attack

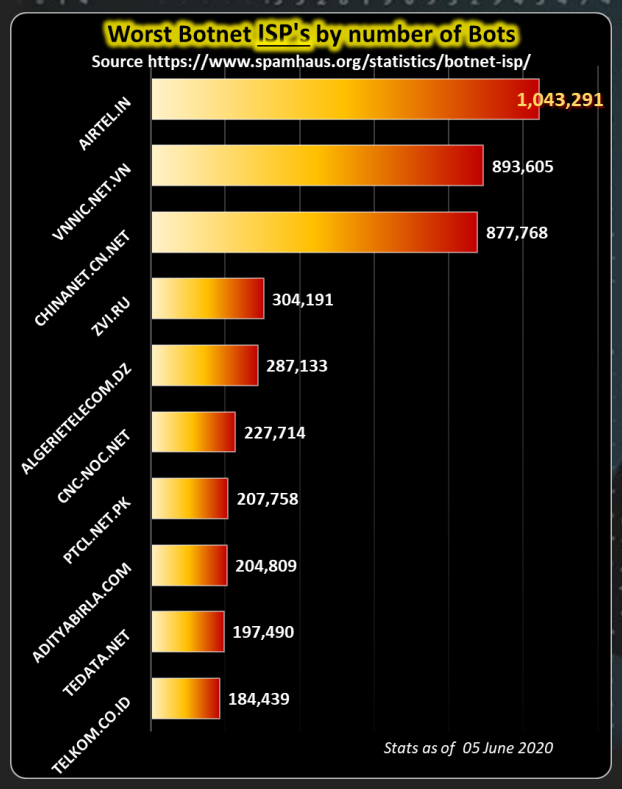
The US is protected by what's known as a nuclear triad: a three-pronged attack force that consists of land-launched nuclear missiles, nuclear missiles on submarines, and aircraft equipped with nuclear bombs and missiles. One of the triad's legs – the land-based LGM-30 Minuteman intercontinental ballistic missile (ICBM) – has been kicked by hackers who've inflicted Maze ransomware on the computer network of a Northrup Grumman contractor. Sky News reported on Wednesday that the contractor, Westech International, has confirmed that it's been hacked and that its computers have been encrypted. It's not yet clear if the extortionists managed to steal classified military information. Investigations to identify exactly what they got away with are still ongoing. However, the attackers have already leaked files that suggest they had access to sensitive data – including payroll and emails – that they copied before they encrypted it, Sky News reports. They're threatening to publish all of the files. Read the full article by Lisa Vaas here: Naked Security

Cisco hacked: Six backend servers used by customer VIRL-PE deployments compromised via SaltStack -

Six Cisco-operated servers were hacked via SaltStack security vulnerabilities, the networking giant revealed this week. The compromised systems act as the salt-master servers for releases 1.2 and 1.3 of Cisco's Virtual Internet Routing Lab Personal Edition (VIRL-PE) product, and customer installations connect to these Cisco-maintained backend boxes. SaltStack is a tool for managing software running on remote systems, and issued security patches at the end of April for two vulnerabilities in its code that can be exploited to gain control of host computers. Cisco patched the six VIRL-PE salt-master boxes – us-1.virl.info, us-2.virl.info, us-3.virl.info, us-4.virl.info, vsm-us-1.virl.info, and vsm-us-2.virl.info – on May 7, and discovered they had been hacked. *(Thank you to Yazan Shapsugh who pointed me to this news snippet)* Read the full article here: TheRegister

A new Java-based ransomware targets Windows and Linux

Security researchers have discovered a new kind of ransomware that uses a little-known Java file format to make it more difficult to detect before it detonates its file-encrypting payload. Consulting giant KPMG's incident response unit was called in to run the recovery effort at an unnamed European educational institute hit by a ransomware attack. BlackBerry's security research unit, which partners with KPMG, analysed the malware and published its findings Thursday. BlackBerry's researchers said that a hacker broke into the institute's network using a remote desktop server connected to the internet, and deployed a persistent backdoor in order to gain easy access to the network after they leave. After a few days of inactivity to prevent detection, the hacker re-enters the network again through the backdoor, disables any running anti-malware service, spreads the ransomware module across the network and detonates the payload, encrypting each computer's files and holding them hostage for a ransom. The researchers said it was the first time they've seen a ransomware module compiled into a Java image file format, or JIMAGE.
Read the full article by Zack Whittaker here: TechCrunch



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

How to tell if your Mobile phone has been hacked

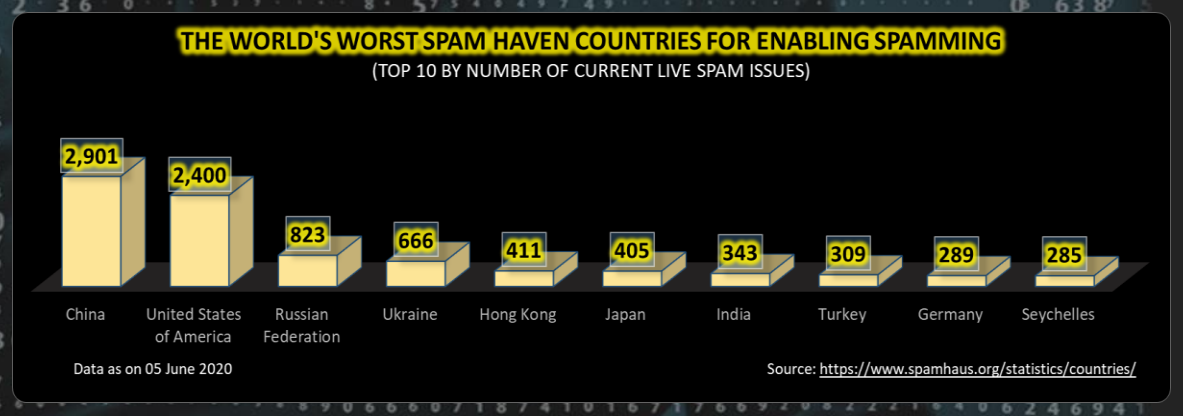
From kids to adults in this modern day and age, most of us are using cell or mobile phones as part of our daily lives. In fact, you might forget your wallet, spouse or even your kids when you go out, but you never forget your phone ☺. It has become one of the most important devices we have ever owned. And, as time goes by we want to believe that we have become some sort of an expert user. That is until that "funny" thing happens and you get some unexpected pop-up's or cryptic messages or your phone inexplicably runs out of space. Panic time! We don't want anything to go wrong with this little miracle device that can contain our whole life's history and more.
So, today we'll explore methods to try and establish if maybe, that "funny" thing is not a hack. I found a really nice and informative article by **Natasha Stokes** on just that. Below then is an appetiser and adapted version of the article that you can find on the techlicious web site. I encourage you to go and read the full article.

From email to banking, our smartphones are the main hub of our online lives. No wonder that smartphones rival computers as common targets for online hackers. And despite the efforts of Google and Apple, mobile malware continues to land in official app stores – and these malicious apps are getting sneakier. According to the McAfee 2020 Mobile Threat Report, over half of mobile malware apps "hide" on a device, without a homescreen icon, hijacking the device to serve unwanted ads, post bogus reviews, or steal information that can be sold or used to hold victims to ransom. And while iPhones can be hacked, more malware targets Android devices. In its 2020 State of Malware Report, MalwareBytes reported a rise in aggressive adware and preinstalled malware on Android devices designed to steal data – or simply victims' attention. Malware can also include spyware that monitors a device's content, programs that harness a device's internet bandwidth for use in a botnet to send spam, or phishing screens that steal a user's logins when entered into a compromised, legitimate app. It is often downloaded from non-official sources, including phishing links sent via email or message, as well as malicious websites. (While security experts recommend always downloading from official app stores – like the Apple App Store or Google Play – some countries are unable to access certain apps from these sources, for example, secure messaging apps that would allow people to communicate secretly.) Then there are the commercial spy apps that require physical access to download to a phone – often done by those well-known to the victim, such as a partner or parent – and which can monitor everything that occurs on the device. Not sure if you may have been hacked? We spoke to Josh Galindo, director of training at uBreakiFix, about how to tell a smartphone might have been compromised. And, we explore the twelve ways your phone can be hacked and the steps you can take to protect yourself.

6 Signs your phone may have been hacked

1. Noticeable decrease in battery life - While a phone's battery life inevitably decreases over time, a smartphone that has been compromised by malware may start to display a significantly decreased lifespan. This is because the malware – or spy app – may be using up phone resources to scan the device and transmit the information back to a criminal server.
   (That said, simple everyday use can equally deplete a phone's lifespan. Check if that's the case by running through these steps for improving your Android or iPhone battery life.)
2. Sluggish performance - Do you find your phone frequently freezing, or certain applications crashing? This could be down to malware that is overloading the phone's resources or clashing with other applications. You may also experience continued running of applications despite efforts to close them, or even have the phone itself crash and/or restart repeatedly. (As with reduced battery life, many factors could contribute to a slower phone – essentially, its everyday use, so first try deep cleaning your Android or iPhone.)
3. High data usage - Another sign of a compromised phone is an unusually high data bill at the end of the month, which can come from malware or spy apps running in the background, sending information back to its server.
4. Outgoing calls or texts you didn't send - If you're seeing lists of calls or texts to numbers you don't know, be wary – these could be premium-rate numbers that malware is forcing your phone to contact; the proceeds of which land in the cyber-criminal's wallet. In this case, check your phone bill for any costs you don't recognize.
5. Mystery pop-ups - While not all pop-ups mean your phone has been hacked, constant pop-up alerts could indicate that your phone has been infected with adware, a form of malware that forces devices to view certain pages that drive revenue through clicks. Even if a pop-up isn't the result of a compromised phone, many may be phishing links that attempt to get users to type in sensitive info – or download more malware.
6. Unusual activity on any accounts linked to the device - If a hacker has access to your phone, they also have access to its accounts – from social media to email to various lifestyle or productivity apps. This could reveal itself in activity on your accounts, such as resetting a password, sending emails, marking unread emails that you don't remember reading, or signing up for new accounts whose verification emails land in your inbox.
   In this case, you could be at risk for identity fraud, where criminals open new accounts or lines of credit in your name, using information taken from your breached accounts. It's a good idea to change your passwords – without updating them on your phone – before running a security sweep on your phone itself..

As I mentioned earlier, this is just an appetiser, there is a wealth of information on this topic on the techlicious site with tips on what to do if you are being hacked and so on.



Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com