
**On September 11, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Firefox, Exim, Adobe Flash Player, Google Chrome and Microsoft 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
## 13 September 2019

## In The News This Week

**Meet 'Simjacker,' a nasty mobile vulnerability researchers say puts 1 billion phones at risk! -** A vulnerability in smartphone technology has made it possible for outsiders to conduct targeted surveillance against victims for the past two years, according to new security findings. Researchers from AdaptiveMobile Security said on Thursday 12 Sep 2019, they found an SMS-based hacking technique that actively is being exploited by a spyware vendor to track individual phone users. The company did not disclose who is behind the surveillance or the identities of the victims. Researchers warned that the attack, dubbed "Simjacker," has ramifications for more than 1 billion mobile phones worldwide. By relying on malicious text messages, hackers infect target phones to retrieve location information and other data. The attack leverages SIM cards, a circuit that stores customers' international mobile subscriber information in a way that isn't restricted to a single phone platform. "This is potentially the most sophisticated attack ever seen over core mobile networks," Cathal Mc Daid, AdaptiveMobile Security's chief technology officer, said in a statement. "It's a major wake-up call that shows hostile actors are investing heavily in increasingly complex and creative ways to undermine network security. This compromises the security and trust of customers, mobile operators and impacts the national security of entire countries." The SimJacker vulnerability exists in the S@T Browser, a kind of software that's embedded in most SIM cards produced by phone companies in 30 nations. It was designed to allow mobile carriers beam basic functions, like the subscription data or over-the-air updates, to customers. But the hackers in this case have exploited that intent, abusing the protocol to send an SMS to a phone and instructing the device to carry out malicious commands. "Now that this vulnerability has been revealed, we fully expect [that] exploit authors and other malicious actors will try to evolve these attacks into other areas," Mc Daid said in the statement.
Read the full story here: cyberscoop

**Texas Refuses to Pay $2.5M in Massive Ransomware Attack -** The ransomware campaign affected 22 local governments, none of which have paid the attackers' $2.5 million ransom demand. The state of Texas is so far refusing to comply with the demands of a ransomware attack that affected 22 local governments, the Texas Department of Information Resources (DIR) reports. None of the affected municipalities have paid the $2.5 million ransom demanded. On August 16, a coordinated ransomware campaign hit systems of cities and towns across Texas, prompting state officials to activate a task force consisting of the DIR, Texas A&M University System's Security Operations Center, the Texas Department of Public Safety, and emergency and military responders. By August 23, all affected entities had transitioned from assessment to remediation and recovery; now, more than half have resumed their normal operations. The DIR is now scheduling follow-up visits with governments to ensure their rebuilding efforts are successful, according to an update the organization published late last week. It is unaware of ransom being paid by any of the 22 affected municipalities in the aftermath of the attack. Ransom payments are a controversial topic among security professionals, most of whom disagree with paying attackers and fuelling their motivation to launch future campaigns. Still, depending on the size of the attack and amount of money requested, ransom payments may amount to less than the cost of rebuilding networks from scratch — a burden that could potentially fall on taxpayers' shoulders, commented ImmuniWeb CEO Ilia Kolochenko..
Read the full story here: DarkReading

## What is Social Engineering?

Social engineering is the art of manipulating people, so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information or access your computer to secretly install malicious software–that will give them access to your company passwords and bank information as well as giving them control over your computer. Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak). Security is all about knowing who and what to trust. It is important to know when and when not to take a person at their word and when the person you are communicating with is who they say they are. The same is true of online interactions and website usage: when do you trust that the website you are using is legitimate or is safe to provide your information? Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value.

What Does a Social Engineering Attack Look Like?

Email from a friend - If a criminal manages to hack or socially engineer one person's email password they have access to that person's contact list; and because most people use one password everywhere, they probably have access to that person's social networking contacts as well. Once the criminal has control, they send malicious emails or messages to anyone in your contacts list. Taking advantage of your trust and curiosity, these messages will potentially (1) Contain a link that you just have to check out–and because the link comes from a friend and you're curious, you'll trust the link and click–and be infected with malware so the criminal can take over your machine and collect your contacts info and deceive them just like you were deceived. (2) Contain a download of pictures, music, movie, document, etc., that has malicious software embedded.

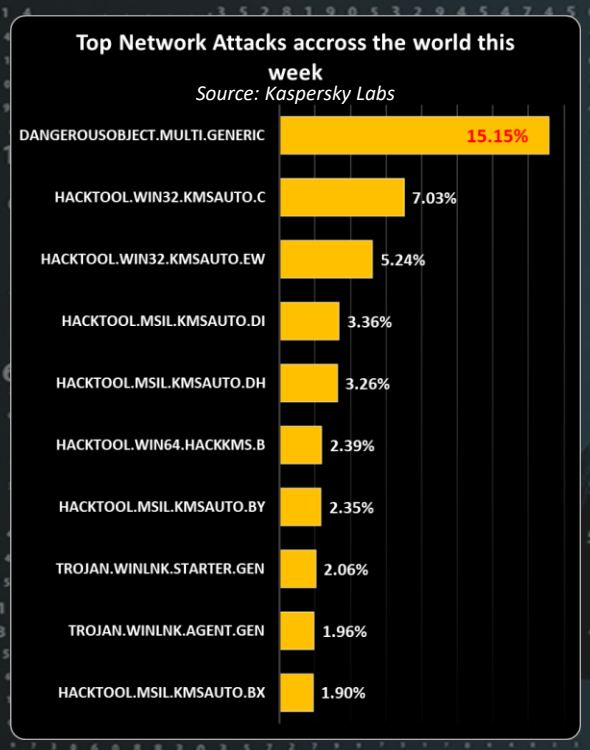
Email from another trusted source - Phishing attacks are a subset of social engineering strategy that imitate a trusted source and concoct a seemingly logical scenario for handing over login credentials or other sensitive personal data. According to various reputable sources, social engineering attacks including phishing and pretexting (see below) are responsible for around 93% of successful data breaches. Using a compelling story or pretext, these messages may (1) Urgently ask for your help. Your 'friend' is stuck in country X, has been robbed, beaten, and is in the hospital. They need you to send money, so they can get home and they tell you how to send the money to the criminal. (2) Use phishing attempts with a legitimate-seeming background. Typically, a phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution. (3) Ask you to donate to their charitable fundraiser, or some other cause. Likely with instructions on how to send the money to the criminal. Preying on kindness and generosity, these phishers ask for aid or support for whatever disaster, political campaign, or charity is momentarily top-of-mind. (4) Present a problem that requires you to "verify" your information by clicking on the displayed link and providing information in their form. The link location may look very legitimate with all the right logos, and content (in fact, the criminals may have copied the exact format and content of the legitimate site). (5) Notify you that you're a 'winner.' Maybe the email claims to be from a lottery, or a dead relative, or the millionth person to click on their site, etc. In order to give you your 'winnings' you have to provide information about your bank account so they know how to send it to you or give your address and phone number, so they can send the prize, and you may also be asked to prove who you are often including your social security number. (6) Pose as a boss or co-worker. It may ask for an update on an important, proprietary project your company is currently working on, for payment information pertaining to a company credit card, or some other inquiry masquerading as day-to-day business.

Baiting scenarios - These social engineering schemes know that if you dangle something people want, many people will take the bait. These schemes are often found on Peer-to-Peer sites offering a download of something like a hot new movie, or music. But the schemes are also found on social networking sites, malicious websites you find through search results, and so on. To allay your suspicion, you can see the seller has a good rating (all planned and crafted ahead of time).

Response to a question you never had - Criminals may pretend to be responding to your 'request for help' from a company while also offering more help. They pick companies that millions of people use such as a software company or bank. If you don't use the product or service, you will ignore the email, phone call, or message, but if you do happen to use the service, there is a good chance you will respond because you probably do want help with a problem. For example, even though you know you didn't originally ask a question you probably have a problem with your computer's operating system and you seize the opportunity to get it fixed. For free! The representative, who is actually a criminal, will need to 'authenticate you', have you log into 'their system' or give them remote access to your computer so they can 'fix' it for you, etc.

Creating distrust - Some social engineering, is all about creating distrust, or starting conflicts; these are often carried out by people you know and who are angry with you, but it is also done by nasty people just trying to wreak havoc, people who want to first create distrust in your mind about others so they can then step in as a hero and gain your trust. If the crook gained access to your mails, they may alter sensitive information (including images and audio) using basic editing techniques and forward these to other people to create drama, distrust, embarrassment, etc.

There are literally thousands of variations to social engineering attacks. The only limit to the number of ways they can socially engineer users through this kind of exploit is the criminal's imagination. Don't become a victim!
Adapted from an article posted by WEBROOT with much more information which you can find here: Article

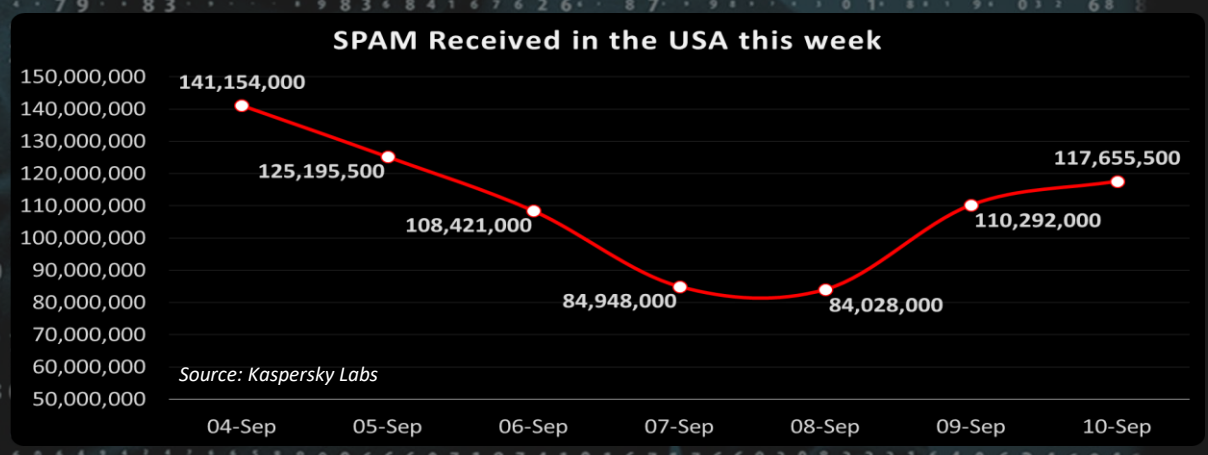



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

**Did you know?**
According to ZenOffice,

**54%**
of workers copy, print or scan confidential work and

**60%**
of workers are not prompted to enter a password before printing.




**Author: Chris Bester**
chris.bester@yahoo.com