On September 23, 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
25 September 2020

In The News This Week

Windows XP and Windows Server 2003 source code leaks online

Microsoft's source code for Windows XP and Windows Server 2003 has leaked online. Torrent files for both operating systems' source code have been published on various file sharing sites this week. It's the first time source code for Windows XP has leaked publicly, although the leaked files claim this code has been shared privately for years. The Verge has verified the material is legitimate, and we've reached out to Microsoft to comment on the leak. It's unlikely that this latest source code leak will pose any significant threat to companies still stuck running Windows XP machines. Microsoft ended support for Windows XP back in 2014, although the company responded to the massive WannaCry malware attack with a highly unusual Windows XP patch in 2017.
Read the full story here: The Verge

Activision denies Call of Duty accounts have been compromised

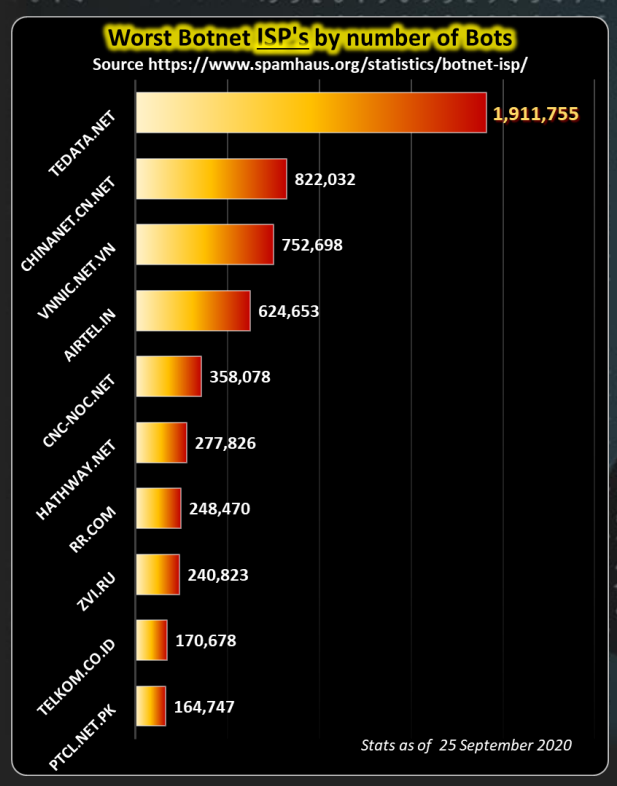
Reports of accounts being hacked have spread online this week, with some suggesting over 500,000 had been breached, a claim Activision attempted to shoot down in a statement on Twitter. "Reports suggesting Activision Call of Duty accounts have been compromised are not accurate," the publisher said. "We investigate all privacy concerns. "As always we recommend that players take precaution to protect their Activision accounts, as well as any online accounts, at all times. "You will receive emails when major changes are made to your Call of Duty accounts. If you did not make these changes, please be sure to follow the steps provided." Activision accounts are required to sign in to Call of Duty games like Modern Warfare and Warzone. It had been claimed that hackers were illegally accessing accounts and changing the log in details so the original owners could no longer access them.
Read the full story here: VGC

Hacking Group Used Malware to Bypass 2FA on Android Devices

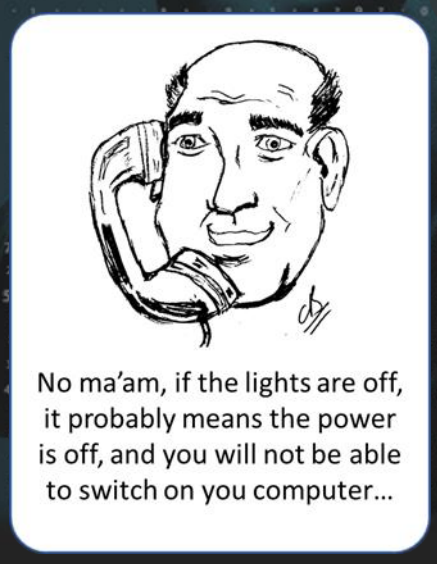
A recently uncovered hacking group that has targeted Iranian dissidents for several years has developed malware that can bypass two-factor authentication protection on Android devices to steal passwords, according to a paper published by Check Point Research last Friday. The hacking group, which Check Point researchers call "Rampant Kitten," also has developed other malicious tools used to steal information and personal data from Windows devices and Telegram accounts, according to the report. The group, active for at least six years, has mainly targeted Iranian dissidents and expatriates, according to the report. Check Point did not indicate whether Rampant Kitten works on behalf of the Iranian government or is conducting these espionage campaigns on its own.
Read the full story here: BankInfo Security

Polish police shut down major group of hackers in the country

Polish authorities have dismantled a major hacker group that was involved in multiple cybercrime activities, including ransomware attacks, malware distribution, SIM swapping, banking fraud, running rogue online stores, and even making bomb threats at the behest of paying customers. The gang, composed of four suspects, in believed to be among the most active groups in the country. "*Today, the Polish authorities are announcing the arrest of 4 suspected hackers as part of a coordinated strike against cybercrime. Those arrested are believed to be among the most active cybercriminals in the country." reads the press release published by the Europol. "This operation was carried out by the Polish Police Centre Bureau of Investigation (Centralne Biuro Śledecze Policji) under the supervision of the Regional Prosecutor's Office in Warsaw (Prokuratura Regionalna w Warszawie), together with the cybercrime departments of provincial police headquarters and Europol."* The arrests are the result of an investigation that begun in May 2019, when the group sent a first bomb threat to a school in Łęczyca after being paid by an individual named Lukasz K. According to local media, the hackers spoofed the email of a businessman that was a rival of the victim, for this reason, the police arrested him and detained the man for two days in prison. Read the full story by Pierluigi Paganini, and how they were caught here: Security Affairs



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



How to Tell if Your Phone Has Been Cloned

A family member of mine's Facebook account was recently hacked which ended up forcing her to create a brand new account losing all her Facebook history etc. When I looked into the matter, it was apparent that this happens quite often but most of the victims had other issues before they realised something went wrong with their Facebook account and they ultimately found out that their phone was cloned. Below is an adapted version of a recent article by Natasha Stokes from Techlicious that gives a good insight into this matter. I encourage you to read the full article that includes some handy information on how to prevent phone cloning.

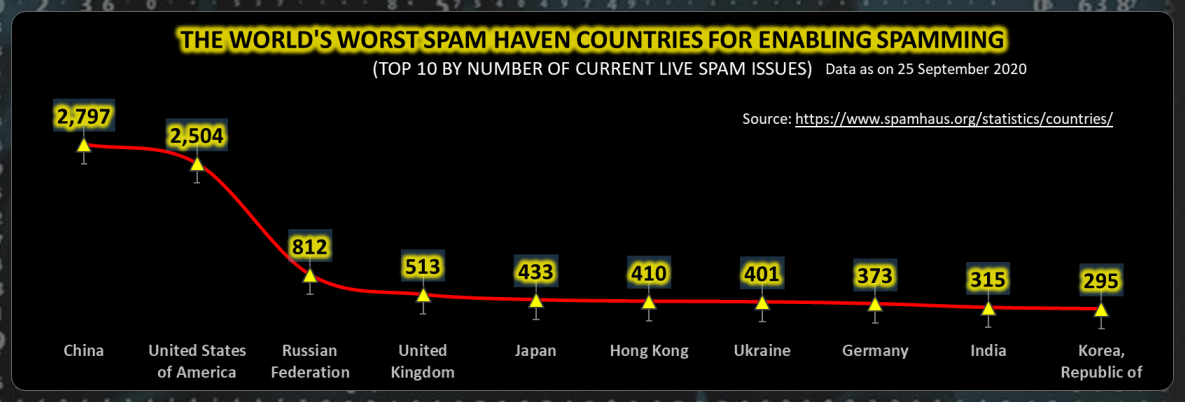
Our phones are the key to our digital identity, so it's no wonder that mobiles have become increasingly attractive targets for cybercriminals, who have at their disposal a fair number of ways to hack a smartphone, some of which require more access and technical savvy than others. Phone cloning – or the copying of the identification credentials a phone uses to connect to cellular networks – is one method that usually requires the perpetrator to have direct access to a device. That makes it less prevalent than, say, hacking an operating system vulnerability that hasn't been updated, but the consequences are equal to that of most phone hacks – your personal data is exposed, with potential financial consequences or identity fraud.

What is phone cloning? - Illegal phone cloning refers to the copying of a phone's complete cellular identity and using it in another device. In cloning a phone's cellular identity, a criminal would steal the IMEI number (the unique identifier for every mobile device) from the SIM cards, or the ESN or MEID serial numbers. These identifying numbers are then used to reprogram phones or SIM cards with the stolen phone number. Then there's also the threat of SIM hijacking, where hackers who have access to stolen phone numbers call up carriers and impersonate account holders to get a new SIM which the hacker then controls. This method, which relies on social engineering tactics to find out personal information that carriers use to authenticate customer accounts, differs from the highly technical method for SIM (or phone) cloning, but the end result is the same – to gain control over someone's phone service. Once the perpetrator has control of the phone service, they can send messages and make calls that appear to be from that phone number, with the bill footed by the victim. If a cloned phone and the original are near the same broadcast tower, it could even allow the perp to listen in on any calls made by the victim. The bigger danger is that text messages and calls intended for the rightful owner of the line can also be intercepted – **including two-factor authentication codes** that allow snoops to get access to critical accounts like banking. Phone cloners might also target political figures for surveillance: in February this year, South African state security ministers were reported to have had their cell phones cloned, the crime was detected when several people reported receiving text messages from a minister who hadn't sent them.

How phones get cloned - Most phones have SIM cards whose IMEI numbers are protected by secret codes that prevent over-the-air interception. But if someone is able to remove the SIM card and place it in a SIM reader for a few minutes, they can copy all its identifying credentials to load onto a blank SIM. Some older phones are more vulnerable to remote attacks. Those running on 2G or 3G CDMA frequencies, which are used only by the Sprint and US Cellular networks (Verizon retired its CDMA network at the end of 2019), broadcast to the operator in a way that would allow special equipment – like a femtocell – to eavesdrop on the connection and intercept handset ESN or MEID serials. That means older CDMA phones, such as flip phones or 3G-only regular and smartphones, that are locked to either Sprint or US Cellular may be at a slightly elevated risk of remote phone cloning. All that said, however, phone cloning is not as common as it was in the early days of mobile phone use, when the radio frequencies in use were much easier to eavesdrop on.

6 Signs that your phone might have been cloned - If you think your phone might have been cloned, check for these signs which can indicate someone else is using your cellular service, such as: **(1)** Receiving an unexpected text requesting you to restart your device - This may be the first sign that your phone or SIM has been compromised; restarting your device gives the attacker a window in which your device is off and they can load their phone with your cloned credentials. **(2)** Calls or texts on your cell phone bill that you don't recognize - Any outgoing texts and calls made on the cloned device will seem to be coming from your phone number – and land on your bill. Even if you don't have an itemized bill, international calls will show up here, so keep an eye on your monthly payments and double-check when you pay more than usual. **(3)** You stop receiving calls and texts - If someone else has control of your phone number, calls and SMSes may be diverted to their cloned device, or your cellular connection stopped entirely. Check this by having a friend or your partner call you to see if the call rings and if it comes through to your phone. **(4)** You see your device in a different location on Find My Phone - Logging into Find My iPhone or Google's Find My Device can be a way to check on the integrity of your SIM. If your phone's on your desk, but on the map appears to be somewhere else, someone else may be using your cell service. (Chances are, phone hackers would disable this setting, however.) **(5)** You get a message from your carrier saying your SIM has been updated - If your credentials have been activated on a new device, your network provider will probably send a message confirming your details have been updated – a major red flag if you haven't done anything. This can also be the point at which you find your device no longer has cellular service. **(6)** You're mysteriously locked out of your accounts - You might even find someone has commandeered your email accounts and social media handles. If someone having control over your phone service it means they can do things like trigger a forgotten password, receive a two-factor authentication code to the phone number they now have access to, then change the password and access any account they know your login name for.

That is all I have space for in this edition, please follow the link to Techlicious and read the full article.



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