On August 12, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in TeamViewer, Apple, Apache, PHP, Google Chrome, SAP, Adobe Acrobat and Reader, Microsoft, and Citrix 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

14 August 2020

In The News This Week

Emotet Return Brings New Tactics & Evasion Techniques

Security researchers tracking Emotet report its re-emergence brings new tricks, including new evasion techniques to bypass security tools. The Emotet botnet recently resurfaced following five months of quiet. Now, researchers tracking the prolific threat share details about what's new and different in its latest wave — in particular, evasion detection tactics that help attackers fly under the radar of security tools.

Emotet is often used as the entry point for infecting a business, after which criminals stay in an environment for days or weeks. They often use the time to drop secondary payloads; in its latest iteration, Emotet has used TrickBot and QakBot to spread laterally and steal credentials.

Over the last few years, this threat has been "coming in waves," says Shimon Oren, vice president of research at Deep Instinct, where researchers have been analyzing its recent activity. "We see periods of very, very high volume of activity, both in terms of new samples that are generated and are being distributed under users, and also in terms of the targets… Read the full story by Kelly Sheridan here: DarkReading

In one click: Amazon Alexa could be exploited

Amazon's Alexa voice assistant could be exploited to hand over user data due to security vulnerabilities in the service's subdomains. The smart assistant, which is found in devices such as the Amazon Echo and Echo Dot -- with over 200 million shipments worldwide -- was vulnerable to attackers seeking user personally identifiable information (PII) and voice recordings. Check Point Research said on Thursday that the security issues were caused by Amazon Alexa subdomains susceptible to Cross-Origin Resource Sharing (CORS) misconfiguration and cross-site scripting (XSS) attacks. When Check Point first began examining the Alexa mobile app, the company noticed the existence of an SSL mechanism that prevents traffic inspection. However, the script used could be bypassed using the Frida SSL universal unpinning script. According to Check Point, it would only take a victim to click on a malicious link to exploit the vulnerabilities. A victim routed to a domain via phishing, for example, could be subject to code injection and the theft of their Amazon-related cookies. Read the full article here: ZDNet Article

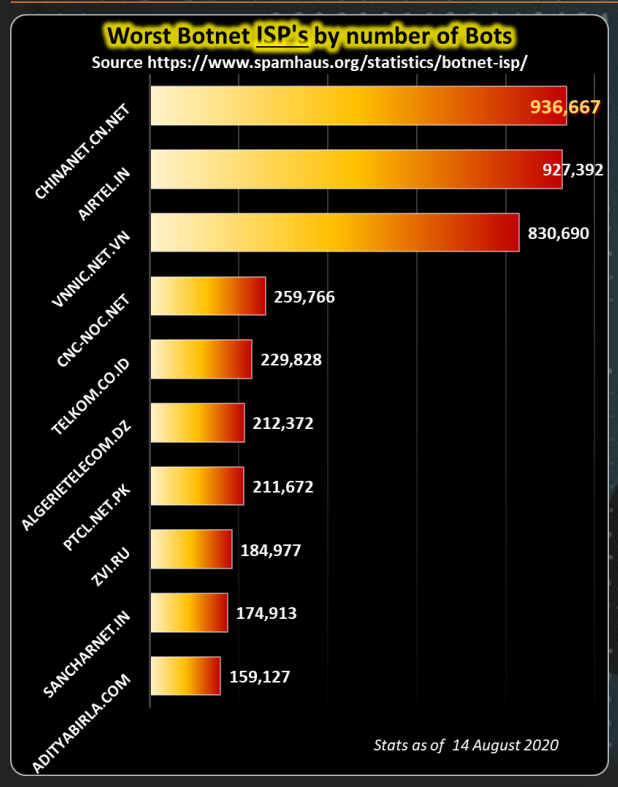
Flaws in Samsung Phones Exposed Android Users to Remote Attacks

New research disclosed a string of severe security vulnerabilities in the 'Find My Mobile'—an Android app that comes pre-installed on most Samsung smartphones—that could have allowed remote attackers to track victims' real-time location, monitor phone calls, and messages, and even delete data stored on the phone.

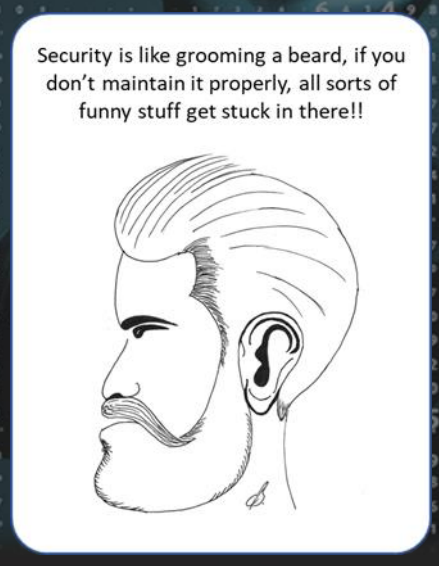
Portugal-based cybersecurity services provider Char49 revealed its findings on Samsung's Find My Mobile Android app at the DEF CON conference last week and shared details with the Hacker News. "This flaw, after setup, can be easily exploited and with severe implications for the user and with a potentially catastrophic impact: permanent denial of service via phone lock, complete data loss with factory reset (SD card included), serious privacy implication via IMEI and location tracking as well as call and SMS log access," Char49's Pedro Umbelino said in technical analysis. Read the full story here: TheHackerNews

Colorado City Pays $45,000 Ransom After Cyber-Attack

Lafayette, Colorado, officials announced Tuesday the city's computer systems were hacked and they were forced to pay a ransom of $45,000 to regain access. Officials said hackers disabled the city's network services and blocked its access until the city paid. The attack caused city emails, phones, online payments and reservation systems to temporarily shut down. The city's system servers and computers are still in the process of being cleaned and rebuilt. Once finished, the relevant data will be restored into the system and operations will resume. In the meantime, the city is using temporary phone numbers and emails.. Read the full story here: USNews



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



The Anatomy of a "BotNet"

In September last year we also touched on the subject of BotNets, but since many of the recent Ransomware attacks can be attributed to botnet activity, I decided to bring it up again. In today's piece I want to cover the basics of what a botnet is, the purpose of a BotNet, how easy it is to set up and some famous botnet of the past.

What does the word BotNet mean – The name Botnet is a blend of the words "Robot or Robotic" and "Network", normally with a malicious connotation as BotNets are generally used to launch digital attacks or other online criminal activity. When thinking about a botnet, it's helpful to visualize it as an army of connected devices working together as a single unit. You can also simplify it as one computer with a gazillion processors.

The Purpose of a BotNet - The purpose of a BotNet is to harness the combined processing power of thousands or even millions of corporate and/or privately-owned computers to launch a concerted exertion to orchestrate things like Denial of Service (Dos) or Distributed Denial of Service (DDoS) attacks, ransomware attacks, extensive crypto mining, infecting target hosts with credential harvesting malware and so forth, the list is endless. The Botnet will largely comprise of privately owned, or computers sitting on a home network, where security defences are by nature not as strong.

Here is a simplified description of how a BotNet is set up:

1. The criminals obtain user or server account credentials – This are achieved by various ways like social engineering, brute force attacks, phishing emails, dark web cafés and auctions, etc.
2. The criminal stealthy hack (break in) the target computer and deposits a malicious piece of code (malware) along with some sort of cloaking software or configuration items to hide the malware form onboard Anti-virus packages or other protection mechanisms.
3. The infected computer now sends a message (handshake) to the criminal controlled Command and Control (C&C) server in the backend, effectively telling it "I'm ready for service and are awaiting orders". The infected computer is now a "Bot" or otherwise known as a "Zombie" in the BotNet and the owner is none the wiser. (Your computer could be one of them)
4. The criminal, also known as the Bot Master, now connects to their backend Command and Control (C&C) servers and issue attack or action orders, normally using a script of some sort.
5. Depending on how it is set up, either the infected computers (zombies) retrieves the orders from the servers or the servers send the orders to the zombies. The latter is less used as it will attract more attention than the zombies retrieving the orders at random times and intervals. In some of the more complex BotNets, there could be any number of Command and Control servers scattered around the world.
6. The zombies now carry out the orders and attack the target to either break it (DDoS) or break into it. The orders might also be to break in, encrypt and/or steal the data.
7. At the height of an attack, the owner of the zombie or bot will experience a moderate to severe degrading of service and will be dumbfounded of what causes it.

How easy is it to set up a BotNet - Somewhat concerning is how easy it is to set up a BotNet. Internet criminals generally has a very low barrier to cross for entry. All you really need is an internet connection, a small amount of cash, the know-how and about a half hour of free time to set up a BotNet. You don't even have to plough your way trough the Darknet, most of the tools are freely available on the public internet. All you have t do is put in a Google search for a Botnet Building kit or search for "BYOB" (Build your own botnet). You will be amazed at the search results.

In essence, there is nothing illegal in setting up a botnet as long as you use your own computers or consenting computers, and there are many legitimate functions for BotNets in business hence the availability of building tools.

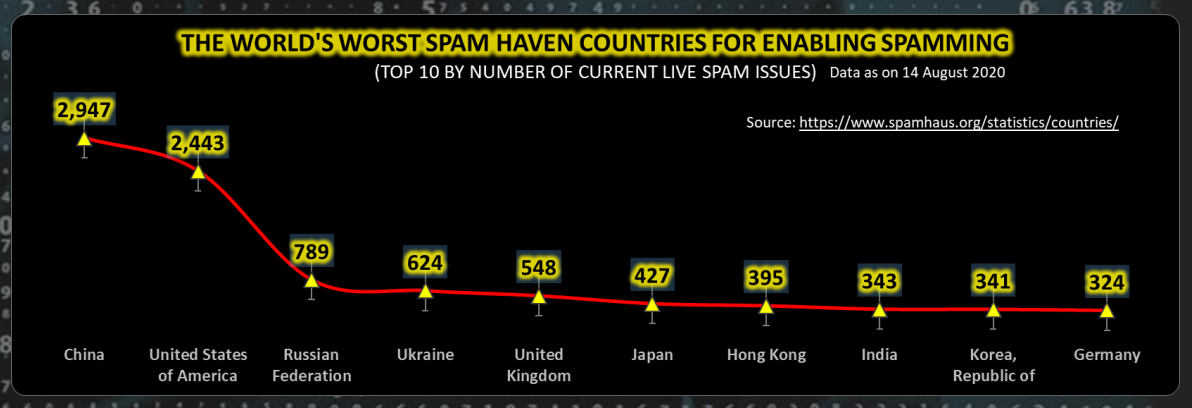
It is like making alcohol. Due to the Covid-19 regulations, the sale of alcohol is currently prohibited in our country but you can legally buy a beer making kit from the local store and make your own beer.

Some of the more famous and biggest BotNets in history

Mariposa - Originated in Spain in 2008, Mariposa botnet hijacked around **12.7 million** computers around the world in 2 years duration. The word "Mariposa" stands for butterfly in French. The botnet got its name because it was created with a software called Butterfly Flooder.

3ve – In 2018 3ve botnet gave rise to three different yet interconnected sub-operations, each of which was able to evade investigation after perpetrating ad fraud. It infected around **1.7 million** computers and a large number of servers that could generate fake traffic with bots. The malware also counterfeits 5,000 websites to impersonate legitimate web publishers along with 60,000 accounts of digital advertising companies so that fraudsters can earn from the ads received.

That all we have space for this week, see you again next week.



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