On December 4, 2019, the Cyber Threat Alert Level was evaluated and is being raised to Blue (Guarded) due to vulnerabilities in 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

06 December 2019

In The News This Week

Ransomware attack hits major US data center provider

CyrusOne, one of the biggest data center providers in the US, has suffered a ransomware attack, ZDNet has learned. In an email after this article's publication, a CyrusOne spokesperson confirmed the incident and said they are currently working with law enforcement and forensics firms to investigate the attack, and help customers restore systems impacted systems. "Six of our managed service customers, located primarily in our New York data center, have experienced availability issues due to a ransomware program encrypting certain devices in their network," CyrusOne told ZDNet.

"Our data center colocation services, including IX and IP Network Services, are not involved in this incident. Our investigation is on-going and we are working closely with third-party experts to address this matter," the company said. Read the full story here: ZDNet Article

Millions of SMS messages exposed in database security lapse

A massive database storing tens of millions of SMS text messages, most of which were sent by businesses to potential customers, has been found online. The database is run by TrueDialog, a business SMS provider for businesses and higher education providers, which lets companies, colleges, and universities send bulk text messages to their customers and students. The Austin, Texas-based company says one of the advantages to its service is that recipients can also text back, allowing them to have two-way conversations with brands or businesses. The database stored years of sent and received text messages from its customers and processed by TrueDialog. But because the database was left unprotected on the internet without a password, none of the data was encrypted and anyone could look inside.

Security researchers Noam Rotem and Ran Locar found the exposed database

Read the full story by Zack Whittaker here: TechCrunch

What's in a Botnet? Researchers Spy on Geost Operators

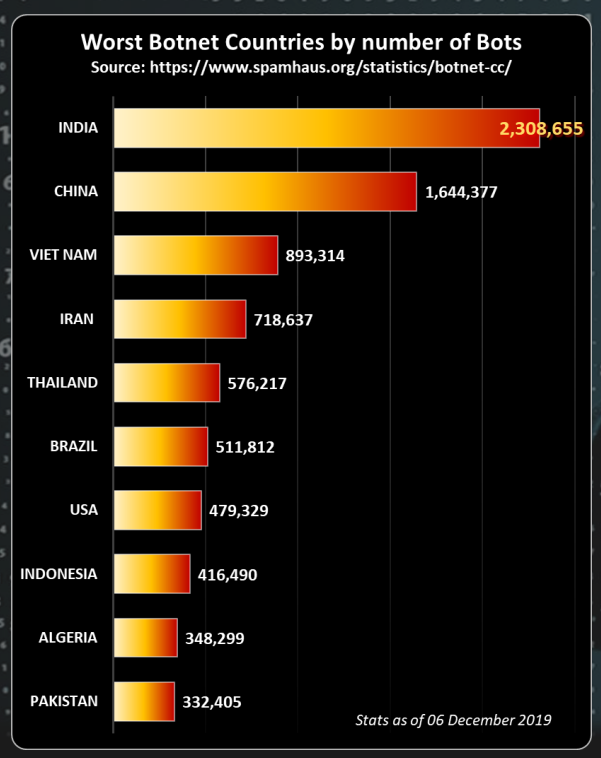
The investigation of a major Android banking botnet yields insights about how cybercriminals structure and run an illicit business. - Researchers who discovered one of the largest Android banking botnets to date also found its attackers' chat log, which they have been watching for nearly a year to learn the inner workings of this cybercrime operation, how its illicit business is structured, and how members interact.

The botnet, dubbed "Geost," was first detected in 2018. A team of security researchers representing Czech Technical University in Prague, UNCUYO University, and Avast Software noticed one of Geost's botmasters logging into a C2 domain while using the insecure proxy network created by HtBot malware. Machines infected with HtBot create an illegal network of proxies later sold to customers; the researchers' lab had one HtBot instance capturing traffic.

What they found was a massive botnet targeting Russian citizens. Geost has nearly 1 million victims, 15 C2 servers, thousands of domains, and thousands of malicious Android application packages (APKs), which are used to distribute and install applications on the Android OS. It has connections to victims' SMS data and direct links to the systems of five major European banks. Geost also sells and redirects traffic, harvests data, and accesses premium SMS services.

The discovery of Geost was made possible, in part, due to several OpSec failures by the attackers, says Avast Software researcher Anna Shirokova. One of their first mistakes was relying on proxies: "They assumed by default that it was secure," she explains. "They didn't expect researchers like us were going to be watching." This slip-up helped the research team uncover not only this banking botnet, but other criminal groups as well, she adds.

Read the full story by Kelly Sheridan here: DarkReading



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

What is a PUP and how is it different from malware

I've decided that from time to time, I'll explore and unpack some of the most common security acronyms that you came across at same stage and as a non-security person wondered, "what the heck is that? This week we'll look at PUP's (Potentially Unwanted Program/s), a term that pops up quite often when you run anti-virus or anti-malware programs..

What is PUP's (Potentially Unwanted Programs)

A PUP is similar to malware in that it may cause problems once it is installed on your computer. However, unlike malware, you normally consent to a PUP being installed, rather than it is installed by itself or by another illicit program or process without your knowledge. In other words, you agree to install it. In today's online world you are presented with so many things that you have to click on to approve or acknowledge, etc. and you found yourself, quite often, just clicking on the button to get it out of the way. Most PUPs are spyware or adware programs that cause undesirable behaviour on your computer.

Once installed, many of these programs can be difficult to remove and become more of a nuisance rather than a benefit. Many of them will display pop up ads, nag screens, or other types of alerts that are designed to convince you to purchase the software or perform some other actions. In some cases PUPs can be more damaging to a computer than traditional malware by causing application freezes, crashes, and other instability.

Chris Hoffman from How-To Geek wrote:

""potentially unwanted program" isn't the best name. Instead, these programs should really be called "almost certainly unwanted programs." In fact, if someone does want one of these PUP's installed, there's a good chance that person doesn't fully understand what that program is doing on their computer.

These are programs which don't really do anything good for you. For example, browser toolbars that clutter your browser, track your web browsing, and show additional advertisements to you are PUP's. A Bitcoin-mining program like the one uTorrent once included is a PUP."

There's a lot of money in this type of nuisance software . All the big free Windows software download sites bundle some sort of nuisance software — even SourceForge does! And it's now become normal for Mac freeware download sites to bundle potentially unwanted programs, too. If you download and install this stuff, your computer wasn't infected against your will — you agreed to some fine print and gave the company permission to run this stuff on your computer.

This is all completely legal, of course. Blocking such an application and labelling it "malware" would open up a company to lawsuits — at least, that appears to be the feeling across the industry. Antivirus companies like Avira have even been sued just for labelling software programs like these as "potentially unwanted programs." Avira won that particular lawsuit, but they might have lost had they gone farther and labelled that program flat-out malware.

By classifying these programs as just "potentially unwanted programs," antimalware software creators are attempting to shield themselves from legal action while detecting software most people don't want on their computers.

Whether an antimalware — or antivirus — application chooses to flag and detect PUPs is up to that individual engine. Some security software makers are more focused on malware, while others — Malwarebytes, for example — are more serious about detecting and removing PUPs."

Common Symptoms of a computer infected with Potentially Unwanted Program:

- Pop-up ads indicates infected PC
- Random web pages which keeps on opening new tabs
- Advertising banners injected into all web pages that you visit
- Browser pop-ups which recommend fake updates
- Unapproved programs installed without your knowledge
- Your browser homepage is changed without your knowledge

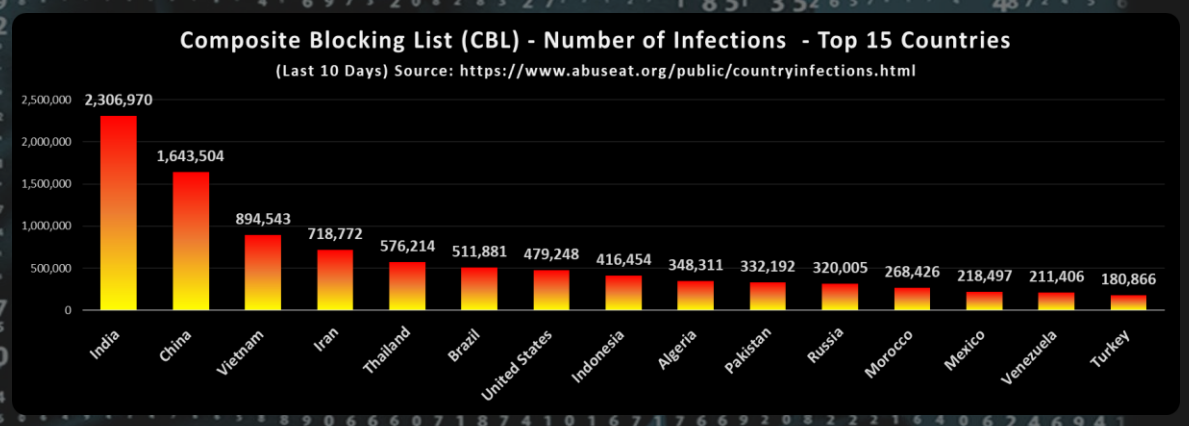
You can detect a PUP by accessing the list of programs on your PC and then locate programs which you are not familiar with, most especially programs with the term toolbar, adware, or even funny named programs. Follow this link to see a list of the most common PUP's or just google it.

How do I get rid of it?

There are many downloadable tools you can use to scan and remove PUP's from your computer, but the simplest way of removing Potentially Unwanted Program is by using Control Panel. If you are able to identify the unwanted program, then you can easily uninstall it from Programs and Features. Here's how to do this: Go to Start > Control Panel > Programs and Features, now, In the Programs and Features window, locate and uninstall any unwanted programs.

Alternatively, you can click on the "Installed On" column to sort your program by the installation date. Hence, scroll through the list, identify the most recent installed programs and uninstall any unknown programs. However, if you are unable to successfully uninstall the unwanted program(s) in Control Panel, you can advance to using a removal tool.

Popular PUP removal tools (and my favourites) include: AdwCleaner from Malwarebytes, Kaspersky Virus Removal Tool (KVRT), etc.



Author: Chris Bester
chris.bester@yahoo.com