On September 19, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla Thunderbird.

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

20 September 2019

In The News This Week

A flaw in LastPass password manager leaks credentials from previous site

Tavis Ormandy, the popular white-hat hacker at Google Project Zero, has discovered a vulnerability in the LastPass password manager that exposes login credentials entered on a site previously visited by a user.

Ormandy published a step by step procedure to exploit the flaw and display the credentials provided to the previously visited website. The expert explained that the bug is easy to exploit and required no other user interaction, the attacker could trick victims into visiting malicious pages to extract the credentials entered on previously-visited sites.

At the time of writing, there is no news about the exploitation of this bug in attacks in the wild.

LastPass implements an auto-update process for both mobile apps and browser extensions, users that have disabled it for some reason have to perform a manual update.

On September 12, 2019, LastPass has released an update to address the vulnerability with the release of the version 4.33.0. Read the full story here: Security Affairs

United States Files Civil Lawsuit against Edward Snowden for Publishing a Book in Violation of CIA and NSA Non-Disclosure Agreements!

On Tuesday 17 September 2019, the United States filed a lawsuit against Edward Snowden, a former employee of the Central Intelligence Agency (CIA) and contractor for the National Security Agency (NSA), who published a book entitled Permanent Record in violation of the non-disclosure agreements he signed with both CIA and NSA. *(For those lived in the dark ages, Edward Snowden was the American whistle-blower who copied and leaked highly classified information from the National Security Agency in 2013 when he was a Central Intelligence Agency employee and subcontractor).*

The lawsuit alleges that Snowden published his book without submitting it to the agencies for pre-publication review, in violation of his express obligations under the agreements he signed.

Additionally, the lawsuit alleges that Snowden has given public speeches on intelligence-related matters, also in violation of his non-disclosure agreements.

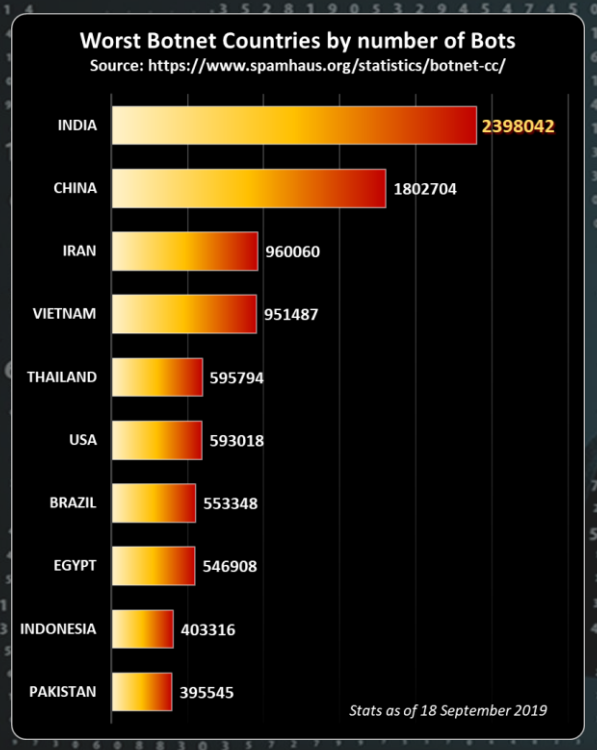
The United States' lawsuit does not seek to stop or restrict the publication or distribution of Permanent Record. Rather, under well-established Supreme Court precedent, Snepp v. United States, the government seeks to recover all proceeds earned by Snowden because of his failure to submit his publication for pre-publication review in violation of his alleged contractual and fiduciary obligations.

Read the full story here: Justice News

US sanctions 3 North Korean hacking groups behind Sony and WannaCry attacks

The US Treasury imposed sanctions on three state-sponsored North Korean hacking groups that have been found to engage in a variety of cyber attacks targeting critical infrastructure.

The groups are Lazarus, Bluenoroff, and Andariel, all of them notorious for a variety of financially-motivated operations ranging from cyber-espionage to data theft, so as to fund the country's illicit weapon and missile programs. Read the full story here: TheNextWeb



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

Cyber Attack Statistics According to HACKMAGEDDON:
(Motivations Behind Attacks)
Cyber Crime – 81.7%
Cyber Espionage – 16.0%
Cyber Warfare – 1.2%
Hacktivism – 1.2%

What is a RAT (Remote Access Trojan) and how is it used?

RATs Give Hackers Remote Access to Your Computer

If you've ever had to call tech support for a problem on your PC, then you're probably familiar with the magic of remote access. When remote access is enabled, authorized computers and servers can control everything that happens on your PC. They can open documents, download software, and even move the cursor around your screen in real time. They can literally take full control of your computer.

A RAT is a type of malware that's very similar to legitimate remote access programs. The main difference, of course, is that RATs are installed on a computer without a user's knowledge. Most legitimate remote access programs are made for tech support and file sharing purposes, while RATs are made for spying on, hijacking, or destroying computers.

Like most malware, RATs piggyback on legitimate-looking files. Hackers can attach a RAT to a document in an email, or within a large software package, like a video game. Advertisements and nefarious webpages can also contain RATs, but most browsers prevent automatic downloads from websites or notify you when a site is unsafe.

Unlike some malware and viruses, it can be difficult to tell when you've downloaded a RAT. Generally speaking, a RAT won't slow down your computer, and hackers won't always give themselves away by deleting your files or rolling your cursor around the screen. In some cases, users are infected by a RAT for years without noticing anything wrong. But why are RATs so secretive? And how are they useful to hackers?

RATs Work Best When They Go Unnoticed

Most computer viruses are made for a singular purpose. Keyloggers automatically record everything that you type, ransomware restricts access to your computer or its files until you pay a fee, and adware dumps dubious ads onto your computer for profit.

But RATs are special. They give hackers complete, anonymous control over infected computers. As you can imagine, a hacker with a RAT can do just about anything; as long as their target doesn't smell a RAT.

In most cases, RATs are used like spyware. A money-hungry (or downright creepy) hacker can use a RAT to obtain keystrokes and files from an infected computer. These keystrokes and files could contain bank information, passwords, sensitive photos, or private conversations. Additionally, hackers can use RATs to activate a computer's webcam or microphone discreetly. The idea of being spied on by some anonymous nerd is pretty upsetting, but it's a mild offense compared to what some hackers do with RATs.

Since RATs give hackers administrative access to infected computers, they're free to alter or download any files on a whim. That means a hacker with a RAT can wipe your hard drive, download illegal content from the internet through your computer, or place additional malware onto your computer. Hackers can also control your computer remotely to perform embarrassing or illegal actions online in your name or use your home network as a proxy server to commit crimes anonymously.

A hacker can also use a RAT to take control of a home network and create a botnet. Essentially, a botnet allows a hacker to utilize your computer resources for super nerdy (and often illegal) tasks, like DDOS attacks, Bitcoin mining, file hosting, and torrenting. Sometimes, this technique is utilized by hacker groups for the sake of cyber-crime and cyber warfare. A botnet that's comprised of thousands of computers can produce a lot of Bitcoin or take down large networks (or even an entire country) through DDOS attacks.

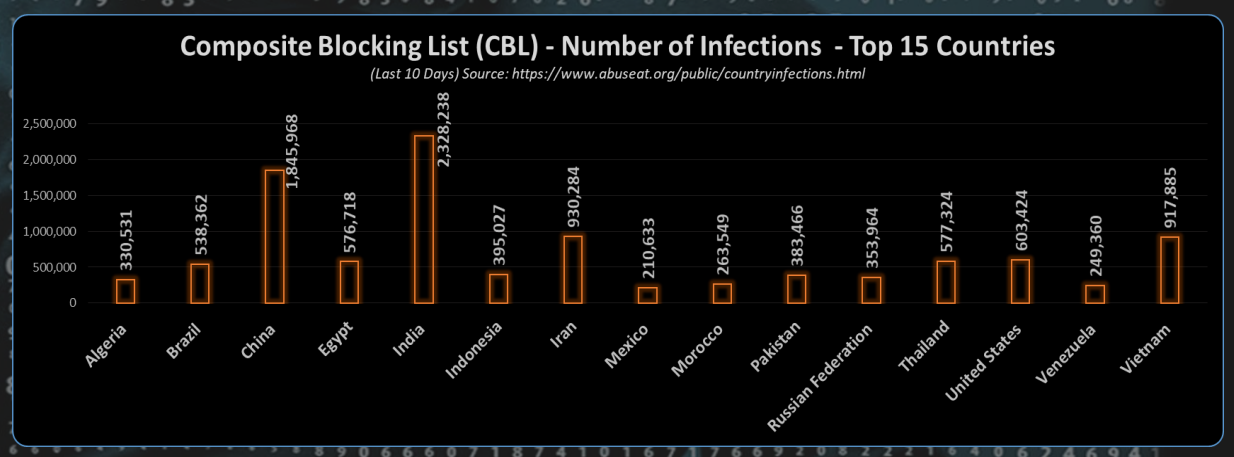
How to avoid a RAT infection

If you want to avoid RATs, then don't download files from sources that you can't trust. You shouldn't open email attachments from strangers (or potential employers), you shouldn't download games or software from funky websites, and you shouldn't torrent files unless they're from a reliable source. Keep your browser and operating system up-to-date with security patches, too.

Of course, you should also enable your anti-virus software. Windows Defender is included with your PC (and it's honestly a great anti-virus software), but if you feel the need for some extra security, then you can download a commercial anti-virus software program.

Since most hackers use well-known RATs (instead of developing their own), anti-virus software is the best (and easiest) way to find and remove RATs from your computer. Most commercial Anti-virus solutions have an extensive, ever-expanding database of RATs, so whatever you do, make sure your AV solutions is up-to-date.

Adapted from an article posted by ANDREW HEINZMAN of How-To-Geek which you can find here: How-To-Geek Article



AUTHOR: CHRIS BESTER
chris.bester@yahoo.com