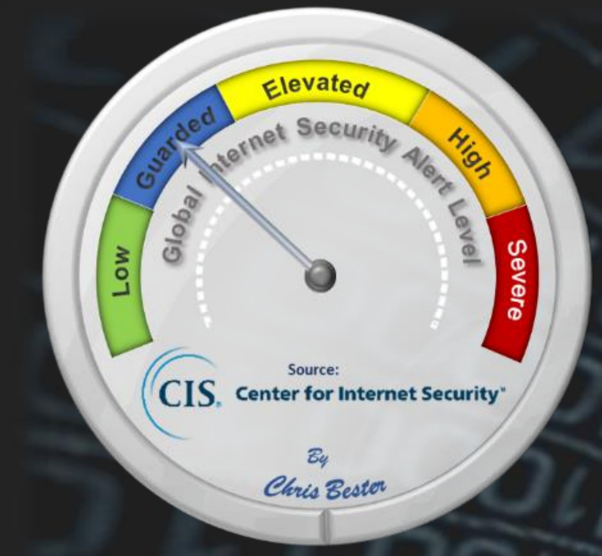

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On April 1, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in DrayTek 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

03 April 2020

In The News This Week

As I said last week, the current news reels are dominated by the COVID-19 pandemic and criminals prying on the general fear, ignorance and paranoia of people worldwide, which may overshadow other important cyber security news bits. Therefore, the news clips of the week will focus on other cyber security events that needs to be highlighted.

Zoom Lets Attackers Steal Windows Credentials, Run Programs via UNC Links

The Zoom Windows client is vulnerable to UNC path injection in the client's chat feature that could allow attackers to steal the Windows credentials of users who click on the link. When using the Zoom client, meeting participants can communicate with each other by sending text messages through a chat interface. When sending a chat message, any URLs that are sent are converted into hyperlinks so that other members can click on them to open a web page in their default browser. The problem is that security researcher @_g0dmode discovered that the Zoom client will convert Windows networking UNC paths into a clickable link in the chat messages as well. *(A big thank you to Yazan Shapsugh who pointed this story out to me)* Read the full article by Lawrence Abrams here: BleepingComputer

Operation Poisoned News used local news links to hit iPhone users with spyware

Research published by security firms Trend Micro and Kaspersky reveals details of a watering-hole campaign targeting iPhone users. Dubbed Operation Poisoned News, the campaign used malicious links on local news websites to install the LightSpy malware. Hackers have been exploiting vulnerabilities in iOS to install the spyware which can gather huge amounts of information and can also be used to take remote control of a device. The campaign was discover in the middle of January, and appears to have been designed to target iPhone users in Hong Kong. The perpetrators ensnared victims by posting links in various forums which purported to be local news stories. In reality, a hidden iframe was being used to load malicious code and install LightSpy. Read the full story by Mark Wyciślik-Wilson here: BetaNews

Marriott Got Hacked…. Yes, Again!

The hotel chain has suffered its second major breach in 16 months. - IN NOVEMBER 2018, hotel giant Marriott disclosed that it had suffered one of the largest breaches in history. That hack compromised the information of 500 million people who had made a reservation at a Starwood hotel. On Tuesday 31 March 2020, Marriott announced that it had once again been hit, with up to 5.2 million guests at risk. Which is a kind of progress, in a way? The details of this latest hack seem to be not quite as devastating as the last one, too, given that sensitive information like passport numbers doesn't seem to be affected. Still, that a major company could get hit twice in such a relatively short time frame underscores how at-risk your data is—and how not enough is being done to protect it.. Read the full story by BRIAN BARRETT here: Wired

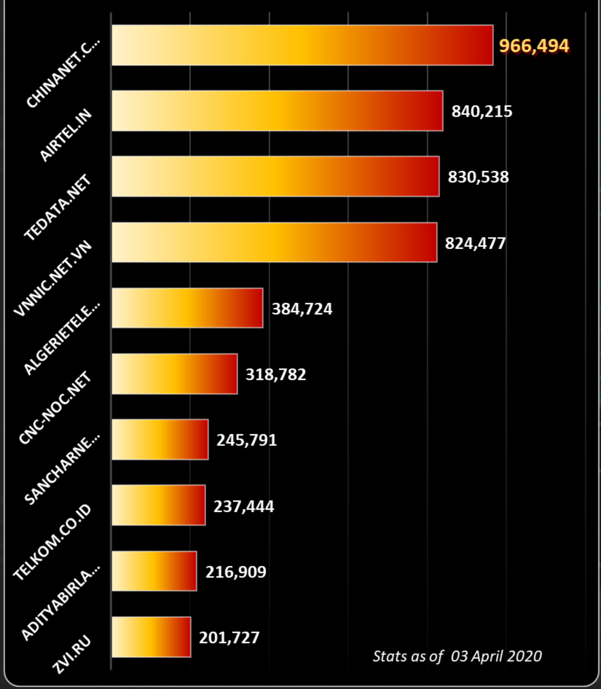
News snippets from the past - Computer crime

The dawn of computer crime: Theft today…is murder next? - 1978

The following news snippet by Hellen Kearns was published in The Gazette – May 17, 1978 – *"An electronic impulse races through a line from a computer to a machine regulating the life support system for a patient in the hospital. The system stops and the patient dies. Murder by computer? Sounds fantastic, but according to Don B. Parker, author of "Crime By Computer" and a computer consultant with Stanford Research Institute in California, it is entirely possible. Parker was the main speaker at a day-long seminar here on computer security yesterday which brought together more than 30 representatives from major Montreal-area corporations. The conference focused on computer crime in business, which Parker said cost US industry about $300 million every year."* Read the full story and more here: GoogleArchives

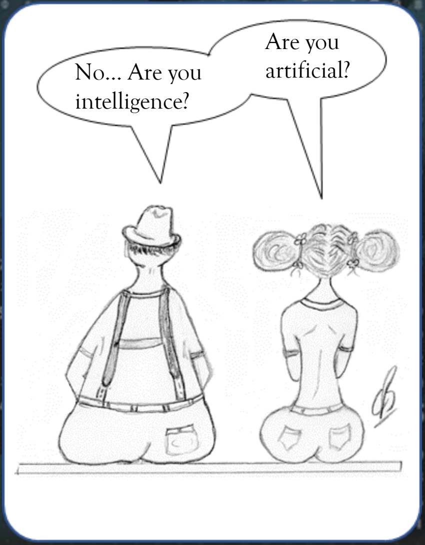
Worst Botnet ISP's by number of Bots

Source https://www.spamhaus.org/statistics/botnet-isp/



Stats as of 03 April 2020

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



Logic Bombs, what is it and how does it work?

In my daily walk of life many people, including family members, ask me questions about Cyber Security acronyms or other terms they hear about or read about somewhere. Just the other day I was asked about logic bombs and what they are, which prompted me to write something about it.

Wikipedia describes a logic bomb as follows: *"A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company."* The "code" they refer to here is lines of computer instructions written in one of an array of programming languages, which instructs the computer to perform one or many functions. This piece of code can be used for good or bad things depending on the intentions of the author(s). The job of the cyber security professional is then to distinguish between the good and bad ones and stop the bad ones before they cause any damage.

Most notorious logic bombs in history

The Original Logic Bomb

Many professionals refer to this incident as "The Original Logic Bomb", and at the time was said to be the biggest cyber-attack in history. During the cold war in the year 1982, USA's Central Intelligence Agency (CIA) found a way to disrupt the operation of a Siberian gas pipeline of Russia without using traditional explosive devices like missiles or bombs. The CIA allegedly caused the Siberian gas pipeline to explode using a portion of a code in the computer system that controlled its operation in what they tagged as "logic bomb." The chaos that ensued was so monumental that the resulting fire was even seen from space.

The 2006 crashing of the UBS servers

The logic bomb came courtesy of Roger Duronio, a systems administrator for the UBS Group AG. Duronio was a disgruntled worker attempting to wipe out the servers. His motivation was apparently because he was unhappy with his bonus. The bomb was successful. 2,000 servers at 400 office branches fell victim to the attack. However, his plan to drive down the stock of UBS ultimately did not pan out. Accordingly, Duronio was sentenced to 8 years in prison. Additionally, he had to pay 3.1 million dollars to UBS.

The Siemens Spreadsheet bomb

The Siemens Corporation spreadsheet debacle involved contract employee David Tinley, who provided software to Siemens' Monroville PA offices. He was a trusted employee for nearly a decade and would create spreadsheets to manage equipment orders. However, Tinely planted a logic bomb within one of the spreadsheets. The bomb went undetected for two years. Every time a script would malfunction, Siemens would have to call Tinley, who would "fix it" for a free. The scheme eventually ended though, when Tinley was out of town, and gave the spreadsheet password to Siemens' IT staff during another crash. The logic bomb was found, and Tinley pled guilty in May of 2019.

US Army logic bomb

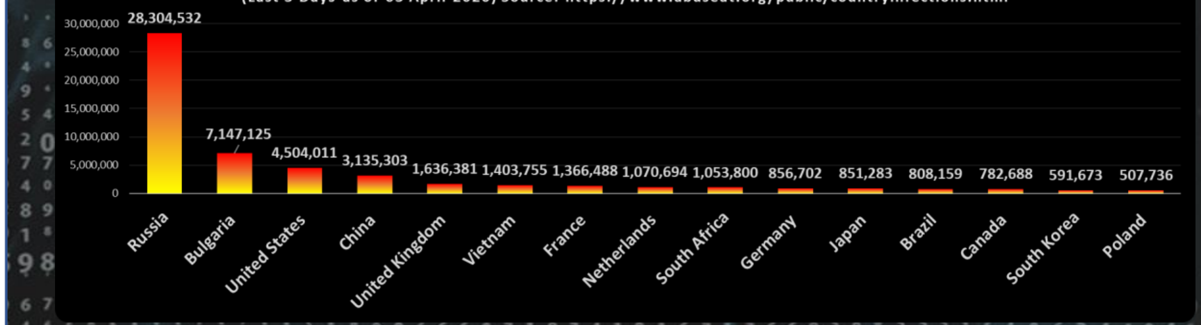
In 2017 Mittesh Das of Atlanta, Georgia, was found guilty by a jury in North Carolina of knowingly transmitting malicious code with the intent of causing damage to an Army computer used in furtherance of national security. Das deliberately introduced malware code seemingly designed to delete files, into the US Army Reserve payroll systems after his employers lost the contract to provide the technology. The military estimates it cost $2.6m to fix the damage. In 2012 Das was in charge of managing the servers controlling the payroll systems, located in Fort Bragg, North Carolina. But in November 2014, the contract was handed over to another company and shortly afterwards things started to go seriously wrong.

The Chernobyl Virus

The virus, also known as CIH or Spacefiller, was written by Chen Ing Hau from Taiwan but was nicknamed Chernobyl by the security fraternity as the logic bomb trigger date coincided with the date of the nuclear disaster in Chernobyl, Russia. The virus was first discovered in 1998, and quickly became one of the most commonly encountered viruses in the wild. According to Wikipedia, "*Sixty million computers were believed to be infected by the virus internationally, resulting in an estimated US$1 billion in commercial damages*." Even today the Chernobyl virus is considered to be one of the most dangerous viruses in history because it was able to hide itself away in a computer's memory. Whilst undetected in memory the virus could then damage or infect any applications that were run on the machine. When the pre-programmed date arrived it rewrote the files on the infected PC's hard drive and completely destroyed its contents.

Composite Blocking List (CBL) - Number SPAM emails trapped - Top 15 Countries

(Last 3 Days-as of 03 April 2020) Source: https://www.abuseat.org/public/countryinfections.html



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