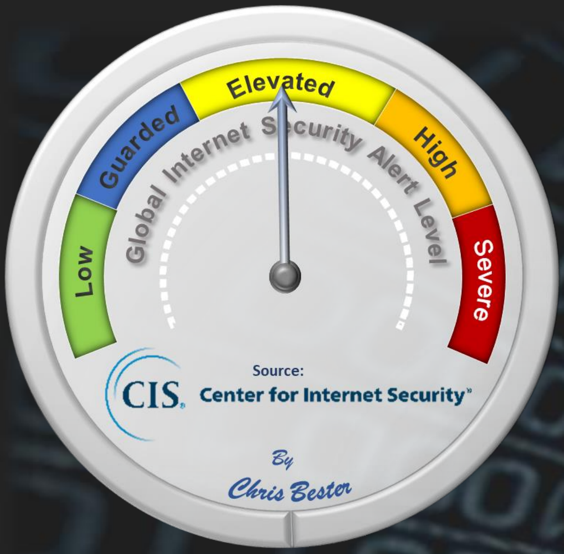

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS Center for Internet Security
By
Chris Bester

On October 28, 2020, the Cyber Threat Alert Level was evaluated and is being raised to Yellow (Elevated) due to vulnerabilities in Mozilla and Cisco products and for heightened awareness of cyber activity in advance of the upcoming General Election in the USA.

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

30 October 2020

In The News This Week

Donald Trump's Campaign Website Hacked And Defaced

The campaign website of President Donald Trump's re-election campaign was hacked and then defaced for a period on Tuesday, but a spokesman said that there was no access to sensitive data. Tim Murtaugh, communications director for the campaign, wrote on Twitter, "Earlier this evening, the Trump campaign website was defaced and we are working with law enforcement authorities to investigate the source of the attack. There was no exposure to sensitive data because none of it is actually stored on the site. The website has been restored." According to Tech Crunch, the campaign's "About" page was taken over by what appeared to be a cryptocurrency scam. A message read that the "world has had enough of the fake news spread daily by President Donald J. Trump." The hackers message was taken down within minutes. Read the full story here: Deadline

Google Removed 21 Gaming Apps from Playstore

Android apps packed with malware from HiddenAds family downloaded 8 million times from the online marketplace. Researchers have discovered a raft of malicious gaming apps on Google Play that come loaded with adware, signalling that the tech giant continues to struggle with keeping bad apps off its online marketplace. Twenty-one gaming ads discovered on Google packed with adware from the HiddenAds family were downloaded about 8 million times so far, according to new research Avast, which cited statistics from Sensor Tower on the number of downloads. The apps masquerade as a fun or useful application but actually "exist to serve up intrusive ads outside the app," according to a blog posted this week by Emma McGowan, a senior writer at Avast. Read the full story here: ThreatPost

Ransomware Hits Dozens of Hospitals in an Unprecedented Wave

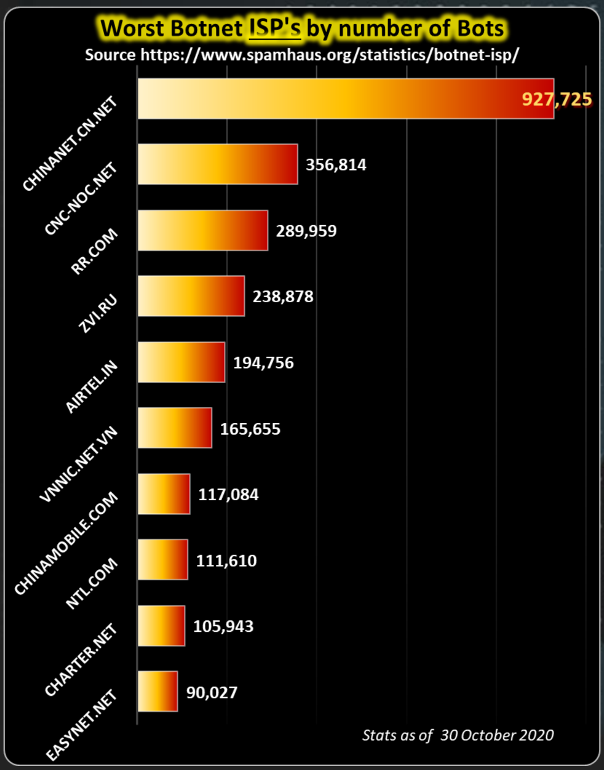
As Covid-19 infections spike in many parts of the US, malware gangs are wreaking havoc on the health care system. A FRESH WAVE of ransomware attacks has struck almost two dozen United States hospitals and health care organizations in recent weeks, just as Covid-19 cases spike across the US. According to US intelligence agencies and cybersecurity professionals, the situation could soon become much worse. On Wednesday evening, the Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Department of Health and Human Services warned that there is a "an increased and imminent cybercrime threat to US hospitals and health care providers," above and beyond the wave of attacks that have already occurred. The alert points to the notorious Trickbot trojan and Ryuk ransomware as the primary hacking tools involved in the attacks. Security analysts at private companies say that the activity is tied to the Russian criminal gang sometimes called UNC 1878 or Wizard Spider. Ransomware actors have for years targeted hospitals, because locking up a health care organization's digital systems can threaten patient care and create maximum urgency to pay up and recover. More recently, both rate of infections against the industry and the demands themselves have exploded; antivirus firm Emsisoft found that the average ransomware ask has increased from about $5,000 in 2018 to about $200,000 this year, with multimillion-dollar demands becoming increasingly common. Read the full story here: Wired

Invoice or payment fraud attacks that target group email boxes jump more than 200%

New research found that business email compromise (BEC) attacks focused on invoice or payment fraud and targeting group mailboxes increased 212 percent from second to third quarter. While invoice and payment fraud attacks on the c-suite are still prevalent, the sharp rise in attacks on group email boxes was significant because it pointed to a new favourite attack vector. "Sending to group email boxes is a great way for attackers to gain credibility," said Ken Liao, vice president of cybersecurity strategy at Abnormal Security, which posted its third quarter BEC report on Thursday. "The attackers can send the email around and once colleagues see that one or two of their co-workers have responded they are more likely to click. It's also a good line of attack because you don't need to get to the CFO or c-suite to get an invoice approved." - Read the story here: SCMagazine

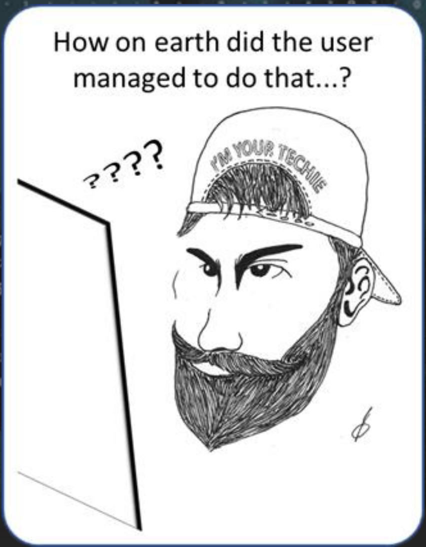
Worst Botnet ISP's by number of Bots

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



Stats as of 30 October 2020

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


How on earth did the user managed to do that...?

Fake News and Hoaxes revisited

In January 2019, I reported on how to spot fake news and hoaxes in social media. This topic came up again in a number of conversations I had over the past few weeks and with a barrage and exponential increase of fake news that hit our screens in current times, I decided to bring the topic up again.

First, what constitute fake news or a hoax? – Any form of untrue information presented as facts, news or stories of human endeavours distributed via social media, blogs or email platforms.

What is the general motivation behind fake news or hoaxes? - The general motivation can include anything from politics, monetary gain, social awareness and just plain pranks and so on. The run-up to the presidential election in the USA is quite a hot topic in the fake news arena, mostly to either discredit one party or drum up sympathy for another or sometimes to "expose" certain party members. As one of the most powerful nations in the world the election campaign also solicits international misinformation campaigns in an attempt to swing the scales toward a more beneficiary outcome for the instigators. In my country fake news are rife to fuel hate campaigns in particular and is sometimes used to solicit a response from the government on a particular issue.

In most countries Covid-19 has been the number one topic in fake news mostly to instigate supply fears for lockdown times to entice people to buy and stock up on items they would not buy or stock up normally.

We also see fake news that originates from the typical do-gooders who overheard something or pick up part of a conversation who feels that they absolutely have to share it or warn the world of this impending situation. Trouble is that they normally don't have all the facts straight and fill in the blanks so to speak and then this is picked up by someone else who add their own little snippet and before you know it, it spirals out of control and the world is going to "fall to pieces".

Then you also have the pranksters who'll create and share a false story or urban legend just for a laugh and see how far it goes.

Then there are the dreaded "Bots", which is short for "Robots", or "Botnets" used by political factions or cyber criminals for various unsavoury reasons. Bots are software applications running on an array of computers collectively teaming up to create a platform with incredible processing power and by using artificial intelligence (AI) can analyse human behaviour over the social network ether. (More on Bots here, or revisit the 14th of August bulletin "Anatomy of a Botnet") Bots pick up on keywords or hashtags in controversial topics and use computer algorithms to create and spread extreme views that emotionally arouse people. "Those messages can create a perception of serious political polarization and huge divisions in society," says Janey Lee, Ph.D., assistant professor of journalism at Lehigh University in Bethlehem, PA. Networks of bots can spread messages quickly, fooling social media platforms and creating the perception that a topic is trending, when in fact it's just being posted and retweeted by computers.

Whatever the motivation, the underlying aim is always to drum up an audience. Sam Huxley, of the communications firm LEVICK, once said "Mainstream media is motivated by getting an audience."

How can we validate a news snippet or story - No matter what the motivation or origins, if you receive a Twitter, Facebook, WhatsApp or Email message with this incredible news and you have this gut-feel that something is not right, there are a few things you can do to check or validate if it is true or not.

Firstly, use common sense, if it is too good or bad to be true, then it normally is. Secondly, you can validate news by visiting certain online platforms (which are listed below) and thirdly, check the source. If the news comes from a political party for instance, or any other questionable source, then it raises a question mark immediately. If a story comes from a newspaper, **is** it really a reputable site? In 2016, the Denver Guardian was often cited as a "reputable" source but it never existed and listed an empty car park as its address.

Listed below are a number of online platforms you can visit in attempt to validate the formation received. You can also visit your local law enforcement agency website to see if there is a specific fake news checking or reporting site in you own country.

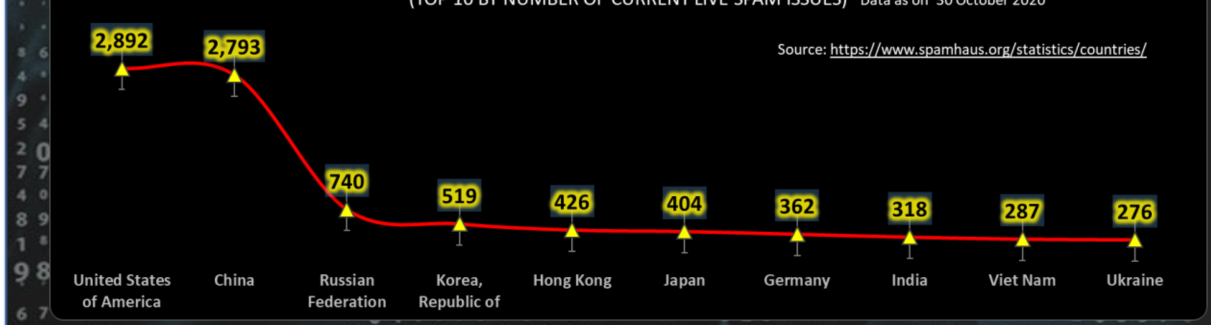
- Snopes
- Hoax-Slayer
- Politifact
- FactCheck
- Africa Check
- RMIT (Australia)
- Full Fact (UK)
- Lupa (Brazil)
- Chequeado (Argentina)
- ColombiaCheck
- ISPA (South Africa)
- Washington Post Fact Checking guide
- Wikipedia List of Fact Checking sites
- CIS – How to identify and what to do if you fall victim

Admittedly, though, fact checking has its limits. By the time a claim is researched and proven false, it may have already reached millions of accounts. Call out fake news you see in your network — but do it privately. "What polarizes people further is calling them out publicly. Then people get defensive because it makes them look stupid or gullible for posting it in the first place." Huxley says.

THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING

(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES) Data as on 30 October 2020

Source: https://www.spamhaus.org/statistics/countries/



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com