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

On February 6, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Telerik, and Cisco 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 February 2020

In The News This Week

RobbinHood Ransomware installs Gigabyte driver to kill antivirus products

RobbinHood ransomware deploys novel technique to make sure it can encrypt files without being interrupted. A ransomware gang is installing vulnerable GIGABYTE drivers on computers it wants to infect. The purpose of these drivers is to allow the hackers to disable security products so their ransomware strain can encrypt files without being detected or stopped. This new novel technique has been spotted in two ransomware incidents so far. In both cases, the ransomware was RobbinHood [1, 2], a strain of "big-game" ransomware that's usually employed in targeted attacks against selected, high-value targets. In a report published by Sophos they described this new technique as follows:

> (1) Ransomware gang gets a foothold on a victim's network. (2) Hackers install legitimate Gigabyte kernel driver GDRV.SYS. (3) Hackers exploit a vulnerability in this legitimate driver to gain kernel access. (4) Attackers use the kernel access to temporarily disable the Windows OS driver signature enforcement. (5) Hackers install a malicious kernel driver named RBNL.SYS. (6) Attackers use this driver to disable or stop antivirus and other security products running on an infected host. (7) Hackers execute the RobbinHood ransomware and encrypt the victim's files.

This antivirus bypassing technique works on Windows 7, Windows 8, and Windows 10.

Read the full story by Catalin Cimpanu here: ZDNet Article

South Africa - Nedbank says 1.7 million of its clients may have been compromised

The ID numbers, addresses and contact details of some 1.7 million Nedbank clients may have been compromised after a "data security incident" at a direct marketing company. A company that sends out SMS's and emails on Nedbank's behalf may have been hit by a data breach. The "data security incident" may have released the names, ID numbers, telephone numbers, physical and/or email addresses of 1.7 million Nedbank clients. In a statement on Thursday morning, Nedbank said that there was a "data incident" at the direct marketing company Computer Facilities, which sends emails and mobile phone messages on its behalf. "No Nedbank systems or client bank accounts have been compromised in any manner whatsoever or are at risk as a result of this data issue at Computer Facilities."

Read the full story here: Business Insider

Facebook's Twitter and Instagram accounts hacked

Several of Facebook's Twitter and Instagram accounts were hijacked Friday night, and the group taking credit is the same one that said it hacked NFL and ESPN social media accounts last week. The hijacked accounts had returned to normal in less than 30 minutes. A group calling itself OurMine made multiple posts on Facebook's Twitter account, as well as on its separate Messenger account. The group says its agenda is to generate awareness about cyber vulnerabilities Read the full story here: The Verge

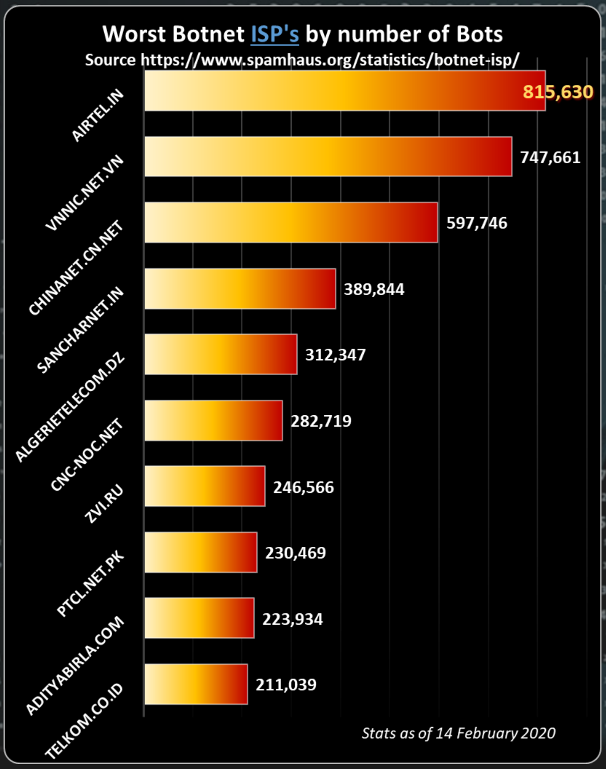
Craziest IoT Device Hacks - Parents nightmare: hacked baby monitor

Baby monitors started as simple one-way radio transmitters and evolved into sophisticated Wi-Fi-enabled smart devices with cameras, infrared vision, and other features. However, as everything IoT, those devices can be hacked as well. Late last year, a family from the US experienced a real nightmare. A hacker got into the wireless camera system used to keep an eye on the baby and threatened to kidnap him. This case is not an exception. There are several reported incidents of strangers' voices being heard over baby monitors.

Find more crazy hacks here: Finance Monthly

Worst Botnet ISP's by number of Bots

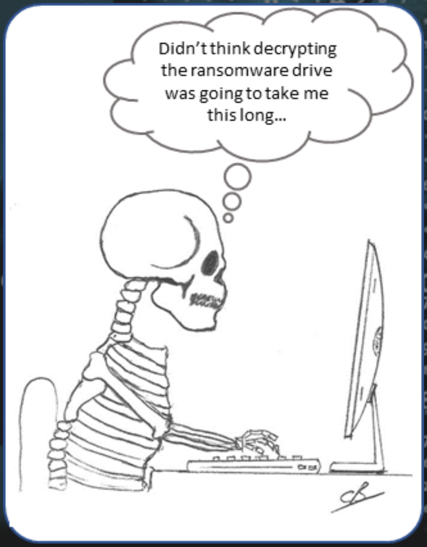
Source https://www.spamhaus.org/statistics/botnet-isp/



ISP	Bots
AIRTEL.IN	815,630
VNNIC.NET.VN	747,661
CHINANET.CN.NET	597,746
SANCHARNET.IN	389,844
ALGERIETELECOM.DZ	312,347
CNC-NOC.NET	282,719
ZVI.RU	246,566
PTCL.NET.PK	230,469
ADITYABIRLA.COM	223,934
TELKOM.CO.ID	211,039

Stats as of 14 February 2020

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


Didn't think decrypting the ransomware drive was going to take me this long...

Be wary of Romance scams on Valentine's day

It is that one special day in the year again where love, romance and spending go hand in hand and one can easily get caught up in the frenzy for romance and let your guard down. The whole idea of love and romance is overly stimulated by the media and retailers alike to maximise profits and exposure. Romance scams now account for the highest financial losses of all internet-facilitated crimes, according to the FBI. The Federal Trade Commission (FTC) received more than 25,000 reports about romance scams in 2019, a nearly threefold increase since 2015. Victims' losses totalled $201 million, almost 40 percent more than in 2018 and the most for any type of consumer fraud. The Australian's ACCC reported that dating and romance scams cost the victims more than $25 million in 2016. Traditionally online dating sites were targeted but with the social media revolution, the entry field for the scammers has broaden dramatically. Scammers are using Facebook, Twitter, Instagram, WhatsApp and any other social media means to lure the victims in.

Some tell-tale signs of a romance scam

1. Professes love quickly
2. Claims to be from the same country as you but is overseas for some reason or another.
3. Claims to be in a remote town and vising will be difficult.
4. Plans to visit but can't because of some emergency
5. Claims to need money for emergencies, hospital bills, travel, etc.

Some tips to avoid dating scams:

1. Whenever someone is rushing you for a decision, slow down, even if you think you know the person on the other side of the line, there is no certain way to know who it really is.
2. Never transfer money or load cash on an online gift or cash card, or physically send cash to a love interest. You will never see that money again. Be very wary if the amount asked is insignificant, that is normally just to lure you in with some fake proof of what the money was used for, then the next request comes!
3. Use Google Image Search or to Find and Identify Fake Profile Pictures. Most scammers will use a fake profile picture. See here how to do it – YouTube Video. You can also use other reverse image search engines like TinEye
4. When you think you have fallen prey to a scam and sent money to a scammer, contact your bank immediately, don't wait till the morning, all banks have a 24-hour help/fraud line. (keep the bank's help line number handy or store it on your phone's contact list, just in case)
5. Report the scam, see the "Reporting Cyber Crime" section on this bulletin for direction.

Hi-jacking your phone – Cyclist, runners and recreational walkers.

If you are a regular cyclist (like my wife), runner or recreational walker, that goes out in the wee hours of the morning or other weird times, this insert is for you.

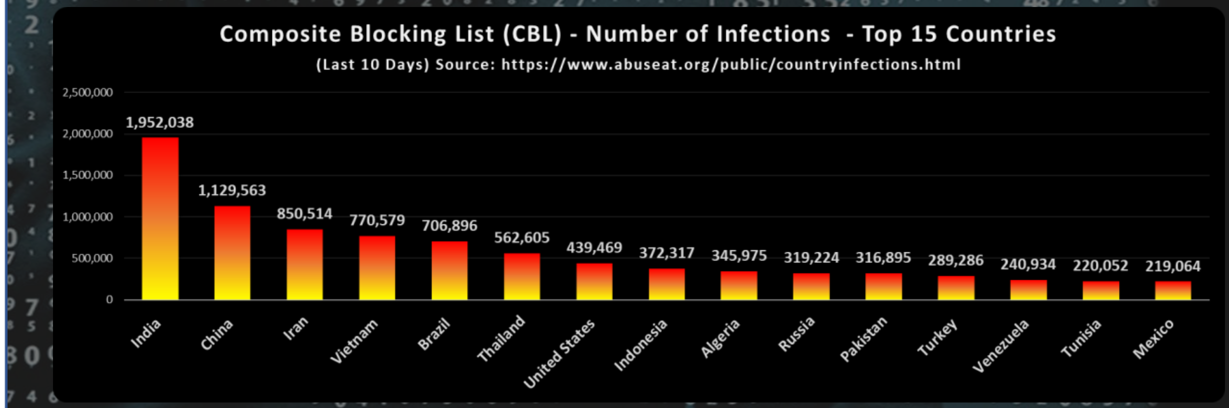
With security measures constantly being enhanced and upgraded on our smartphones, it becomes less attractive for thugs just to steal your phone. They are now more interested in what **you** can do with your phone under duress. More and more cases are reported where cyclists or runners are accosted and mugged by gangs that lay hiding on the side of the road. They then force the victim to unlock his or her smartphone, log on to their banking app and transfer money to an account they provide. You can imagine what can happen if the victim refuses to cooperate.

With this in mind, and the fact that you still need to carry a phone, some of these athletes has come up with a simple idea on preventing the criminals to at least get on your banking app or get other personal information that they can use to your detriment. What we are talking about is the use of a simple dial-only phone with no or very limited smartphone functionality for the exclusive use for your ride, run or walk. A dial-only phone can only make and receive calls. Many of us still have some old phones lying around that we can use for this purpose, but many providers are now offering tiny dial-only phones that can be used to this effect. Cheap pre-paid sim card account options are available everywhere which makes it viable to have a second phone just for use when you go out cycling or running. Hopefully the criminals will quickly loose interest if they realise the phone is useless for their sordid purpose.

Some non cyber safety notes: Stay safe on the road, if possible, never ride or run alone (safety in numbers). Always be vigilant, if you see a suspicious character lurking around, change your route if you can. Be visible, always wear bright clothes, cyclist put your lights on, runners/walkers wear one of those small blinking clip on lights..

Composite Blocking List (CBL) - Number of Infections - Top 15 Countries

(Last 10 Days) Source: https://www.abuseat.org/public/countryinfections.html



Country	Infections
India	1,952,038
China	1,129,563
Iran	850,514
Vietnam	770,579
Brazil	706,896
Thailand	562,605
United States	439,469
Indonesia	372,317
Algeria	345,975
Russia	319,224
Pakistan	316,895
Turkey	289,286
Venezuela	240,934
Tunisia	220,052
Mexico	219,064

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