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

**(No change from last week)
On June 24, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Treck, Google and BitDefender 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 July 2020

In The News This Week

India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat

India's government banned nearly 60 Chinese mobile apps on Monday, including TikTok, citing national security concerns, after a deadly clash between their militaries this month raised tensions between the two countries to the highest level in decades. The fighting two weeks ago, along the disputed border between the world's two most populous countries, left 20 Indian soldiers dead and an unknown number of Chinese casualties. While India has vowed to retaliate, it lags far behind China in military and economic power, leaving it with few options. But Chinese telecommunication and social networking companies have long eyed India's giant market and its enormous potential. About 50 percent of India's 1.3 billion citizens are online. In addition to TikTok, the popular video-sharing social networking platform, the banned apps include WeChat, UC Browser, Shareit and Baidu Map. The Indian people are not particular happy about it as thousands of people around India appear to have made a living recording and broadcasting short videos, mostly of shimmying, lip-synching and prat-falling, for millions of other Indians to whom they would otherwise have remained utterly obscure. TikTok had about 1.2m content creators and 120m monthly viewers. It is said that up to a third of TikTok's global users are based in India. India's Ministry of Electronics and Information Technology said in a statement on Monday that Chinese Apps are "stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India" Read more about it here: NYTimes & Economist

USA - Nationwide Facial Recognition Ban Proposed By Lawmakers

Lawmakers proposed a new bill that would ban the use of facial recognition by law enforcement nationwide. Lawmakers have proposed legislation that would indefinitely ban the use of facial recognition technology by law enforcement nationwide. The new bill comes after months of public concerns surrounding facial recognition's implications for data privacy, government surveillance and racial bias. The Facial Recognition and Biometric Technology Moratorium Act was proposed Thursday by Sens. Ed Markey (D-MA) and Jeff Merkley (D-OR), and Reps. Pramila Jayapal (D-WA) and Ayanna Pressley (D-MA). While various cities have banned government use of the technology (with Boston this week becoming the tenth U.S. city to do so), the bill would be the first temporary ban on facial recognition technology ever enacted nationwide. The newly proposed bill would "prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance." That means federal agencies would be barred from using biometric surveillance systems (which in addition to facial recognition can also include voice recognition). Read the full article by Lindsey O'Donnell here: Threadpost

Hacker ransoms 23k MongoDB databases and threatens to contact GDPR authorities

A hacker has uploaded ransom notes on 22,900 MongoDB databases left exposed online without a password, a number that accounts for roughly 47% of all MongoDB databases accessible online, ZDNet has learned on Wednesday. The hacker is using an automated script to scan for misconfigured MongoDB databases, wiping their content, and leaving a ransom note behind asking for a 0.015 bitcoin (~$140) payment. The attacker is giving companies two days to pay, and threatens to leak their data and then contact the victim's local General Data Protection Regulation (GDPR) enforcement authority to report their data leak. Attacks planting this ransom note (READ_ME_TO_RECOVER_YOUR_DATA) have been seen as early as April 2020. In a phone call with ZDNet, Victor Gevers, a security researcher with the GDI Foundation, said initial attacks didn't include the data wiping step. The attacker kept connecting to the same database, leaving the ransom note, and then returning again to leave another copy of the same ransom note, a few days later. But Gevers told ZDNet that the attacker appears to have realized they made a mistake in their script. Since this week, the hackers has corrected their script and is now actually wiping MongoDB databases clean. Read the full article here: ZDNet Article

How ransomware is targeting industrial control systems

Other than Internet of Things (IoT) systems, Industrial Controls Systems (ICS) were traditionally locked down in isolated networks and could not be accessed unless you are inside the closed loop network at a specific site or location. This however changed over the last few years as remote management of these Industrial Controls Systems via Internet or Corporate IT network connectivity became more and more a necessity rather than a nice to have. This is even more so in the midst of the Covid-19 lockdown and truly isolated ICS networks are becoming few and far apart making it a lucrative target for disruptive threat actors as these networks became more accessible. Today we want to get a better understanding on how these guys go about hacking and disrupting these systems and I found this article published by ZDNet this week, focusing on the EKANS ransomware strain that gives us some insight. Below is an adapted version of the article but please visit ZDNet for full details and other useful security information.

This is how EKANS ransomware is targeting industrial control systems

New samples of the EKANS ransomware have revealed how today's cyberattackers are using a variety of methods to compromise key industrial companies.

In a research report published on Wednesday, FortiGuard Labs researchers Ben Hunter and Fred Gutierrez said that malware designed to attack industrial control systems (ICS) continues to be lucrative for threat actors.

While ransomware only accounted for roughly a third of all malware incidents over 2019 -- according to Verizon's 2020 data breach report -- when applied to core, critical systems, such as utilities and manufacturing, an infection can be devastating, disruptive, and key services may feel incredible pressure to pay a ransom.

The EKANS ransomware family is one such strain that has been used in targeted ICS campaigns.

The researchers were able to obtain two modern samples, one from May and another compiled in June, which revealed some interesting features.

Both Windows-based samples are written in GO, a programming language widely used in the malware development community as it is relatively easy to compile to work on different operating systems.

To help with analysis, FortiGuard created an EKANS-specific dissembler, discovering that despite a vast number of coding errors in the May version of the ransomware -- over 1200 strings, in fact -- the malware is still able to perform effectively in attacks against ICS systems.

It appears that EKANS has been designed to deliberately select its victims. The malware will try to confirm its target by resolving the domain belonging to a victim company and comparing this information to IP lists. If the target status is not confirmed, the routine exits.

Once a target is acquired, the ransomware will scan for domain controllers to compromise.

Both versions have the functionality of typical ransomware. Once it lands on a vulnerable machine, the malware is able to encrypt files and display a ransom note demanding payment in return for a decryption key which may -- or may not -- restore access to system files.

However, the June sample goes beyond these features and is capable of high-level functionality that could wreak havoc in an industrial setting, including the ability to turn off host firewalls.

This new addition to EKANS functionality was not the only improvement. In order to bypass any existing ICS protections, the ransomware will also attempt to turn the firewall off before encryption "probably to detect AVs and other defense solutions by blocking any communication from the agent," the researchers noted.

EKANS uses RSA encryption to lock up impacted machines and will go on a process killing rampage, terminating any system that could become a barrier to the malware's activities and deleting shadow copies in the process to make it more difficult to recover files.

Alongside the examination of this interesting ICS malware, FortiGuard also published a guide on what the cybersecurity firm believes are the most current techniques and tactics employed by industrial threat actors.

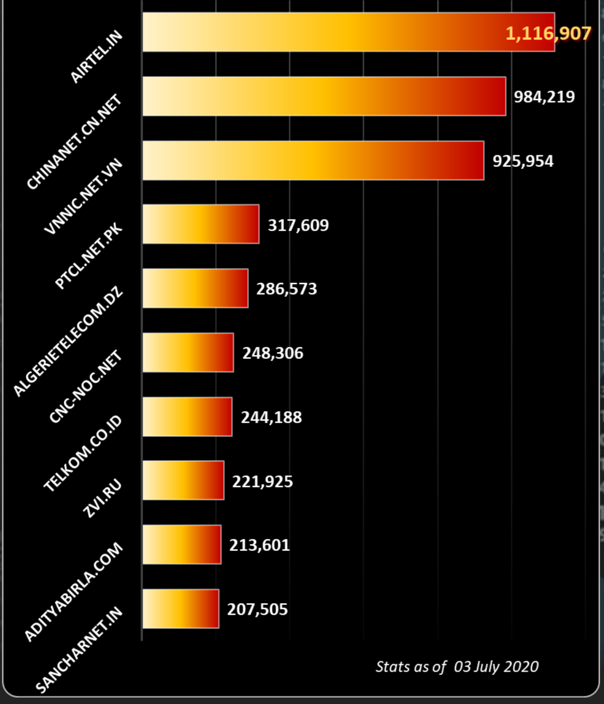
These include exploiting remote services, using credential dumps, moving laterally across networks, disabling or modifying cybersecurity tools, impairing defenses by disabling Windows event logs, and group policy modification.

In March, cybersecurity firm FireEye warned that the development of malware and hacking tools able to target ICS is on the rise, with the majority having been developed in the past decade. The majority of tools analyzed by FireEye are considered vendor-agnostic, but in some cases, software has been designed to compromise ICS setups offered by specific companies.

ZDNet Article

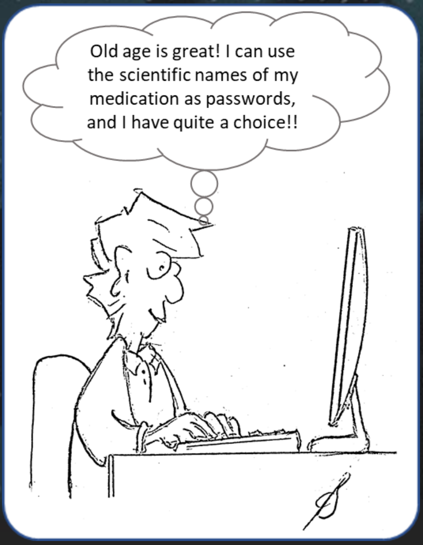
Worst Botnet ISP's by number of Bots

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



Stats as of 03 July 2020

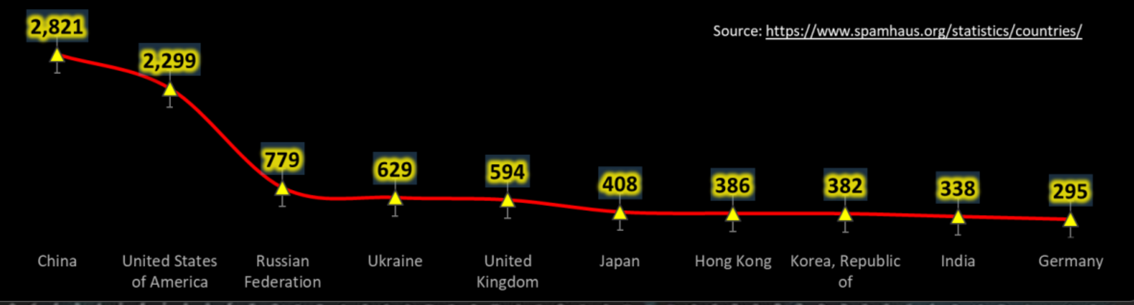
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov


Old age is great! I can use the scientific names of my medication as passwords, and I have quite a choice!!

THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING

(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES) Data as on 03 July 2020

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



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