On December 16, the Cyber Threat Alert Level was evaluated and is being raised to Yellow (Elevated) due to vulnerabilities in Cisco, SolarWinds and Apple 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

18 December 2020

In The News This Week

Microsoft unleashes 'Death Star' on SolarWinds hackers in extraordinary response to breach - This week Microsoft took a series of dramatic steps against the recent SolarWinds supply chain attack. In the size, speed and scope of its actions, Microsoft has reminded the world that it can still muster firepower like no one else as a nearly-overwhelming force for good.

Through four steps over four days, Microsoft flexed the muscle of its legal team and its control of the Windows operating system to nearly obliterate the actions of some of the most sophisticated offensive hackers out there. In this case, the adversary is believed to be APT29, aka Cozy Bear, the group many believe to be associated with Russian intelligence, and best known for carrying out the 2016 hack against the Democratic National Committee (DNC). While details are continuing to emerge, the SolarWinds supply chain attack is already the most significant attack in recent memory. According to SolarWinds, Microsoft, FireEye, and the Cybersecurity and Infrastructure Security Agency (CISA) the attackers compromised a server used to build updates for the SolarWinds Orion Platform, a product used for IT infrastructure management. The attackers used this compromised build server to insert backdoor malware into the product (called Solorigate by Microsoft or SUNBURST by FireEye).

According to SolarWinds, this malware was present as a Trojan horse in updates from March through June 2020. This means any customers who downloaded the Trojaned updates also got the malware. While not all customers who got the malware have seen it used for attacks, it has been leveraged for broader attacks against the networks of some strategically critical and sensitive organizations. Read the full story by Christopher Budd here: GeekWire

Tech savvy Mexican drug cartels find a new partner: Israeli spyware

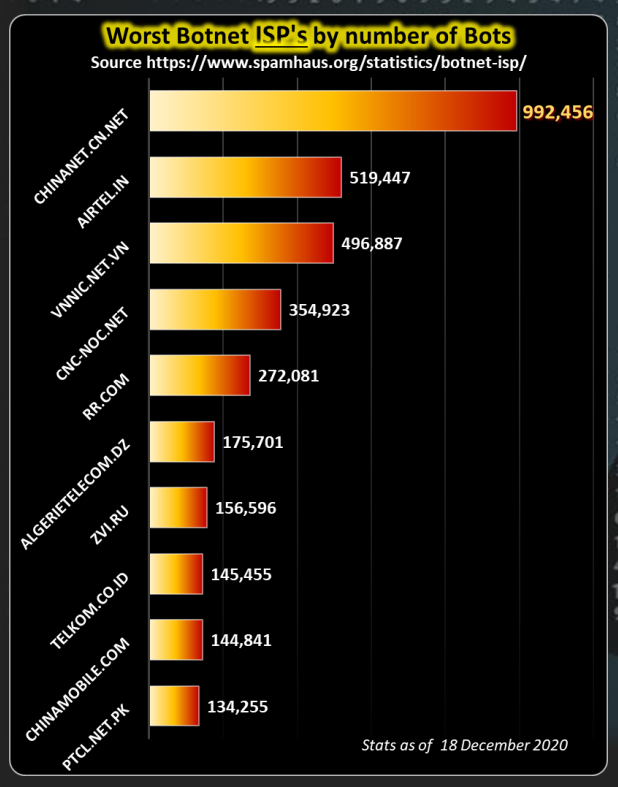
An investigation has found that journalists in Mexico are increasingly falling prey to Israel spyware that is being used by the state apparatus, even falling into the hands of some of the country's most dangerous drug cartels. The investigation, known as Cartel Project, an initiative coordinated by Forbidden Stories, found that leading Mexican journalist, Jorge Carrasco, has become the latest victim of such Israeli spyware. NSO Group, is an Israeli based spyware firm synonymous with selling software around the world, sometimes to authoritarian countries. NSO has been accused of, among other things, selling the hacking tool to places like Saudi Arabia and the United Arab Emirates, who have used it to spy on regime opponents. Over the last decade, Mexico has become a lucrative market for technology companies wishing to sell hacking software - the NSO Group is just one of more than 25 private security companies selling this software to Mexico. Read the full story here: TRTWorld

Medical Imaging Leaks Highlight Unhealthy Security Practices

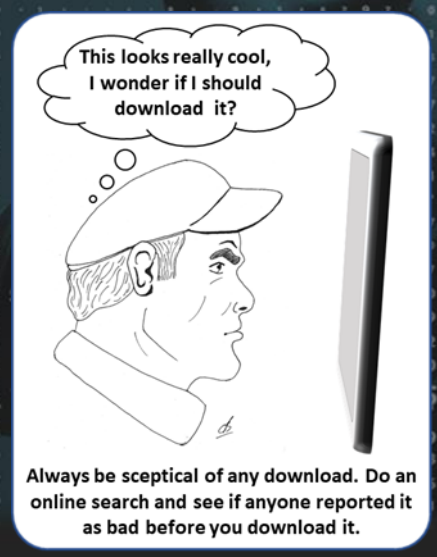
More than 45 million unique images, such as X-rays and MRI scans, are accessible to anyone on the Internet, security firm says. - Thousands of storage servers housing more than 45 million medical images can be accessed from the public Internet, with the majority using default ports and many showing signs of already being accessed by malicious actors, cybersecurity firm CybelAngel stated in a research report published on Dec. 15.

Over a six-month investigation, researchers from the firm discovered more than 3,000 servers that allowed connections to port 104 — one of the network ports used by the manufacturers of medical imaging machines — and presented a banner for the medical file format DICOM. A test of 50 randomly sampled servers found that 44 — or 88% — allowed connection attempts, according to the report. While the largest volume of files was stored in the server of a Russian health center, the largest number of unsecure servers— 819 — were located in the United States, says David Sygula, senior cybersecurity analyst at CybelAngel. These exposed servers "are totally widespread," he says. "There are some countries that are more secure than others. [While] we saw some smaller servers that were eye doctors, ... some of the biggest ones belong to medical centers." The research underscores that storage servers and cloud storage services continue to suffer from misconfiguration problems that expose them to data leaks and breaches. Read the full story by Robert Lemos here: DarkReading

(Thank you to my good friend and security expert Yazan Shapsugh for his week contributions and information)



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



Malicious Chrome or Edge extensions

All of us are using a web browser of sorts every day, whether it is on our computers or our mobile devices. Thus we are all susceptible to the risk of being online and our personal information being harvested for whatever sinister motive. To make our online life a bit easier, most of us will employ plugins or extensions to enhance our browsing experience. Sometimes these extensions are downloaded and installed on our browser unwittingly, and perpetrators are collecting data stealthily while we are non-the-wiser. Other times we see these cool extensions that we download and install without knowing if it contains some sneaky code that can either infect our computers with malware or harvest our personal information. In this light, I want to share a ZDNet article with you that highlights some extensions that were identified and reported as malicious this week.

Three million users installed 28 malicious Chrome or Edge extensions

Extensions could redirect users to ads, phishing sites, collect user data, or download malware on infected systems - More than three million internet users are believed to have installed 15 Chrome, and 13 Edge extensions that contain malicious code, security firm Avast said this week. The 28 extensions contained code that could perform several malicious operations. Avast said it found code to:

(1) redirect user traffic to ads, (2) redirect user traffic to phishing sites, (3) collect personal data, such as birth dates, email addresses, and active devices, (4) collect browsing history, (5) download further malware onto a user's device.

But despite the presence of code to power all the above malicious features, Avast researchers said they believe the primary objective of this campaign was to hijack user traffic for monetary gains. "For every redirection to a third party domain, the cybercriminals would receive a payment," the company said.

Avast said it discovered the extensions last month and found evidence that some had been active since at least December 2018, when some users first started reporting issues with being redirected to other sites. Jan Rubín, Malware Researcher at Avast, said they couldn't identify if the extensions had been created with malicious code from the beginning or if the code was added via an update when each extension passed a level of popularity. And many extensions did become very popular, with tens of thousands of installs. Most did so by posing as add-ons meant to help users download multimedia content from various social networks, such as Facebook, Instagram, Vimeo, or Spotify.

Avast said it reported its findings to both Google and Microsoft and that both companies are still investigating the extensions.

Google did not return a request for comment seeking additional information on the status of their investigation into Avast's report or if the extensions were going to be removed. Microsoft said it's still investigating the issue.

A day after Avast published its findings, only three of the 15 Chrome extensions were removed, while all the Edge add-ons were still available for download. A source familiar with the investigation told ZDNet that Microsoft has not been able to confirm the Avast report. Until Google or Microsoft finish their investigations and decide what's their course of action, Avast recommended that users uninstall and remove the extensions from their browsers.

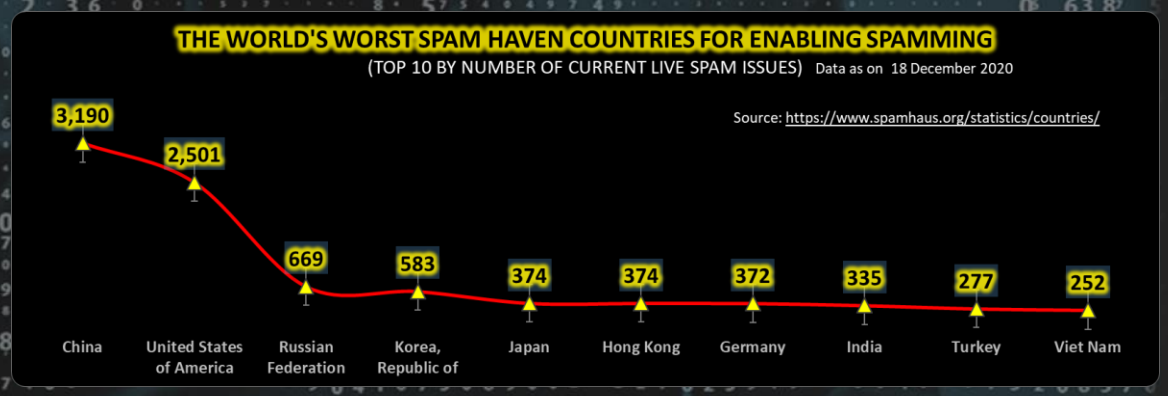
Below is the list of Chrome extensions that Avast said it found to contain malicious code:

- Direct Message for Instagram
- DM for Instagram
- Invisible mode for Instagram Direct Message
- Downloader for Instagram
- App Phone for Instagram
- Stories for Instagram
- Universal Video Downloader
- Video Downloader for FaceBook™
- Vimeo™ Video Downloader
- Zoomer for Instagram and FaceBook
- VK UnBlock. Works fast.
- Odnoklassniki UnBlock. Works quickly.
- Upload photo to Instagram™
- Spotify Music Downloader
- The New York Times News

Below is the list of Edge extensions that Avast said it found to contain malicious code:

- Direct Message for Instagram™
- Instagram Download Video & Image
- App Phone for Instagram
- Universal Video Downloader
- Video Downloader for FaceBook™
- Vimeo™ Video Downloader
- Volume Controller
- Stories for Instagram
- Upload photo to Instagram™
- Pretty Kitty, The Cat Pet
- Video Downloader for YouTube
- SoundCloud Music Downloader
- Instagram App with Direct Message DM

When you see a cool add-on or browser extension, do some snooping around on the net before you install it, you will easily see if someone reported it as a bad idea.



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