On December 30, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in SolarWinds and ArubaNetworks 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

31 December 2020

In The News This Week

Op-ed: What nobody else will say about the new cybersecurity crisis

Marriott, Equifax, the Office of Personnel Management and the recent U.S. federal agencies — the big cyberattacks keep coming. They can start to seem like routine annoyances, like fender benders on the freeway. But anyone tempted to dismiss the recent SolarWinds and FireEye breaches as routine should think again.

This is no fender bender. It is a 75-car, road-closing pileup, and we know where the fault lies. The truth is, at the federal level, we're still dragging our feet on cybersecurity. Even though cybercrime now has a permanent roost atop the US intelligence community's annual Worldwide Threat Assessment report, there's a profound difference between identifying a problem and addressing it with Manhattan Project urgency. We have to shake off the complacency because we might not get a second chance. Why is the SolarWinds-FireEye crisis so troubling?

When you think of cyberattacks, imagine a hierarchy of chaos. On the lower levels, that includes stolen credit card or health data. These are inconvenient but not crippling. Higher on the hierarchy are attacks on a single company or agency. They steal intellectual property, from auto blueprints to vaccine recipes or hold their systems ransom until payment is made. These are costly and temporarily crippling. But this? This is peak chaos. This was a global supply-chain attack in terms of damage done with no precedent. It hit dozens of organizations from the United States Treasury to Intel and Cisco. We have not yet gauged the full impact. It may take years to sum up the costs..

Read the full article by Hitesh Sheth here: CNBC

Germany: 'Colossal' cyberattack knocks out Funke news group

Hackers knocked out one of Germany's biggest news organizations over the Christmas holiday. Such criminal attacks, which often come with ransom demands, have become a lucrative business model. One of the biggest media organizations in German-speaking territories has become the victim of a sustained cyberattack over the Christmas holiday, forcing several newspapers to cancel or offer severely curtailed "emergency" editions. The attack, which is still ongoing, began last Tuesday. The Funke Media Group, which publishes dozens of newspapers and magazines and runs several local radio stations and online news portals, said on Monday that some 6,000 of its computers had been "potentially infected" in the attack, which had affected several central computer systems at all its locations in Germany. Andreas Tyrock, editor-in-chief of the Funke-owned Westdeutsche Allgemeine Zeitung (WAZ), added in a statement that the "colossal" attack had left the data on its IT systems encrypted and made them "unusable for now." All IT systems had to be powered down to prevent further damage, which means that "all editorial systems and the entire technology for newspaper production had been switched off, and even remotely normal work is currently impossible," Tyrock wrote. "The newspaper pages are essentially built by hand, in many places from home.".. Read the full story here: DW.com

India: A Growing Cybersecurity Threat

Geopolitical tensions and a dramatic rise in offensive and defensive cyber capabilities lead India to join Iran, Russia, China, and North Korea as a top nation-state adversary.

Geopolitical Factors Boost India's Cyber-Threat Activity - India's cyber capabilities are growing, at least partially in reaction to activities across the border in China. The rise of China and its apparent expansionist activity is likely to motivate Indian actors with varying levels of state support to act. This provides fertile ground for the development of national offensive cyber capabilities and crime. Diplomatic relations between India and China are at a low point, with troops fighting along the border in the western Himalayas in mid-2020. China is also considering a plan to construct dams on a section of the Brahmaputra river, which could cause downstream water shortages through Bangladesh. At the same time, unemployment in India as a result of the COVID-19 pandemic has created a very large population of technically skilled people in need of income. Reports indicate that this has caused an uptick in cybercrime from India — presumably from the younger, tech-educated population.

Read the full story by Mike Hamilton here: DarkReading

Health to be on cyber-security's front line in 2021

Below is an extract of an article posted by the BBC this week. It is painting a bleak picture for cyber attacks aimed at the health care sector for the coming year. Please read the full article here: BBC Cyber Security Article

Covid-19 catapulted the health sector to the forefront of cyber-security in 2020, but the next year is likely to see the dangers continue and evolve.

Threats from nation states and criminals to the health system are a growing concern. The huge logistical challenge of rolling out vaccines faces the risk of disruption to complex supply chains. And criminal ransomware poses a threat at a time when the pandemic has increased our reliance on technology.

Supply chain

The distribution of the various coronavirus vaccines may bring relief, but it also brings with it a major challenge: many of those involved have not had to think hard about security in the past.

The complex global supply chain for vaccines ranges from factories in one country to internet-connected fridges in another.

It will create new pressure on doctors' surgeries, IT systems, and sometimes small providers who play a critical role.

IBM has already said it has seen suspected state-hackers target the "cold chain" used to keep supplies at the right temperature during transportation.

And in the UK, the National Cyber Security Centre, which worked quickly when the pandemic began to secure vaccine research, has since pivoted its efforts towards vaccine distribution.

At least the large pharmaceutical companies are no stranger to cyber-espionage. Their security officials say they first began thinking hard about the issue after a major espionage campaign back in Spring 2010.

But the issues around the pandemic have changed the sector's importance.

"We are now on a grander stage," is how one person involved puts it.

In July, the UK accused Russian intelligence of targeting research, including for the Oxford vaccine, while the US accused Chinese hackers of similar activity.

The emergence of "vaccine nationalism" led intelligence and security officials to raise questions about whether countries could try and undermine the efforts of others going forward.

"It could be trying to steal the intellectual property for financial purposes," Tonya Ugoretz of the FBI told a recent Aspen Institute Cyber Summit.

"It could be to undermine confidence... or to advantage another country's own development.

"We see our most determined nation-state adversaries not just relying on one method to target the supply chain, but combining cyber with using more traditional espionage and human sources."

One much discussed tactic is the deliberate spread of misinformation online about vaccinations, or questioning a country's safety and testing record.

The UK Army's 77th Brigade has supported a Cabinet Office investigation into whether foreign states are driving anti-vaccine fears within the UK. Most sentiment was domestically generated, head of Strategic Command General Sir Patrick Sanders said at a recent Chatham House event. And he raised the possibility of retaliation.

"Where these things are being fuelled from overseas, then we will take action, and if the NCF (National Cyber Force) has a part to play in that, it will."

Cyber-blackmail campaigns

But despite concerns about states, experts say, criminal ransomware - the locking of people out of their computers and data until they pay - remains the more serious and persistent threat.

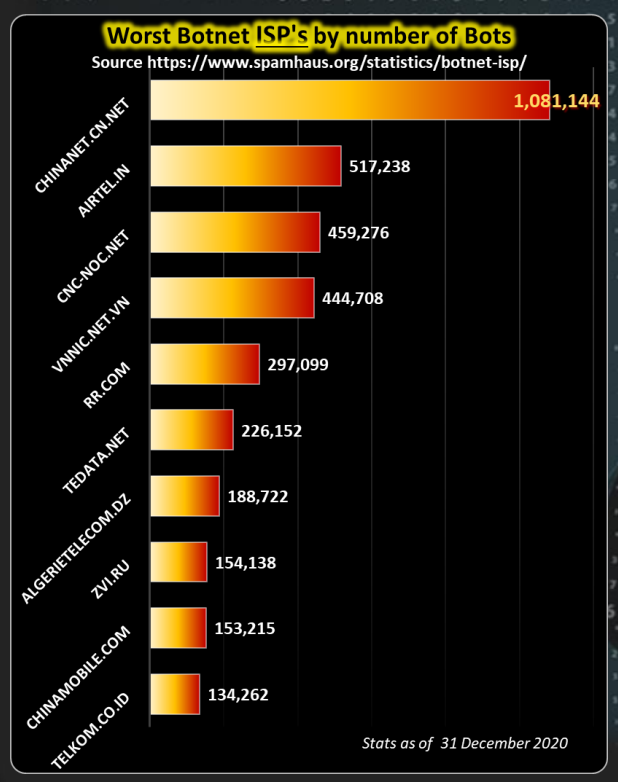
There was some talk at the start of pandemic from criminal gangs that they would not target health. But it did not last and attacks have multiplied.

A recent report from security firm Positive Technologies says half of all the cyber-attacks on healthcare were ransomware in the July-to-September quarter of 2020.

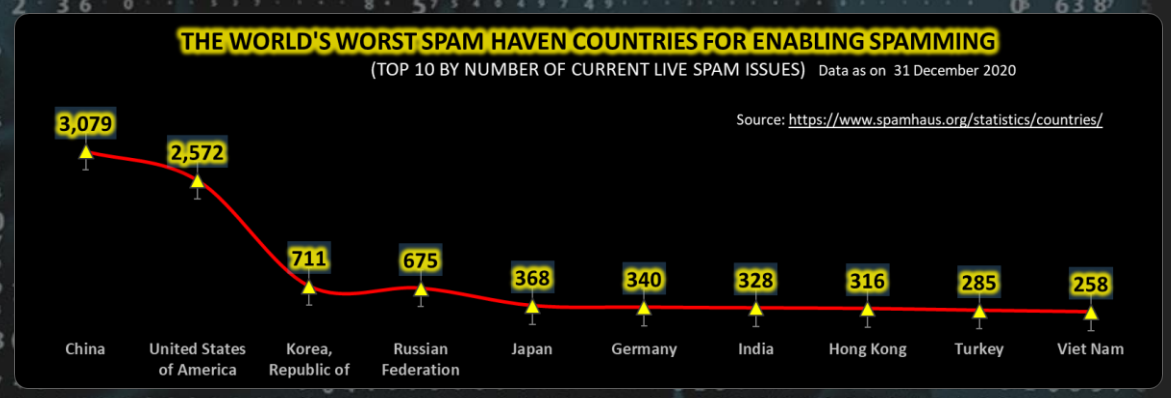
US hospitals have been worse hit than the UK. It is thought this is because criminals see them as richer than their NHS counterparts. In just 24 hours in October, six American hospitals received ransom demands of at least $1m (£810,000), leading to some cancer treatments being cancelled.

"The healthcare sector has become such a big, rich, juicy target," Greg Garcia, executive director for the US Cybersecurity of the Health Sector Co-ordinating Council, recently said. "It's as if they moved on from the financial services sector."

Please read the full article here: BBC Cyber Security Article



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



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