On January 20, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Siemens, Google, and Oracle products.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
22-Jan	98,086,977	2,100,341

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
22 January 2021

In The News This Week

This phishing scam left thousands of stolen passwords exposed through Google search

A mistake on the part of the cyberattackers led to their discovery, and that of the data they pillaged. - Operators of a phishing campaign targeting the construction and energy sectors exposed credentials stolen in attacks that were publicly viewable with a simple Google search. On Thursday, Check Point Research published a blog post describing the campaign, in which stolen information was dumped on compromised WordPress domains.
The recent phishing attack began with one of several fraudulent email templates and would mimic Xerox/Xeros scan notifications including a target company employee's name or title in the subject line. Phishing messages originated from a Linux server hosted on Microsoft Azure and were sent through PHP Mailer and 1&1 email servers. Spam was also sent through email accounts that had been previously compromised to make messages appear to be from legitimate sources. Attackers behind the phishing scam included an attached HTML file containing embedded JavaScript code that had one function: covert background checks of password use. When credential input was detected, they would be harvested and users would be sent to legitimate login pages.
"While this infection chain may sound simple, it successfully bypassed Microsoft Office 365 Advanced Threat Protection (ATP) filtering and stole over a thousand corporate employees' credentials," Check Point says.
Read the full story by Charlie Osborne here: ZDNet Article

Interpol: Dating App Victims Lured into Investment Scams

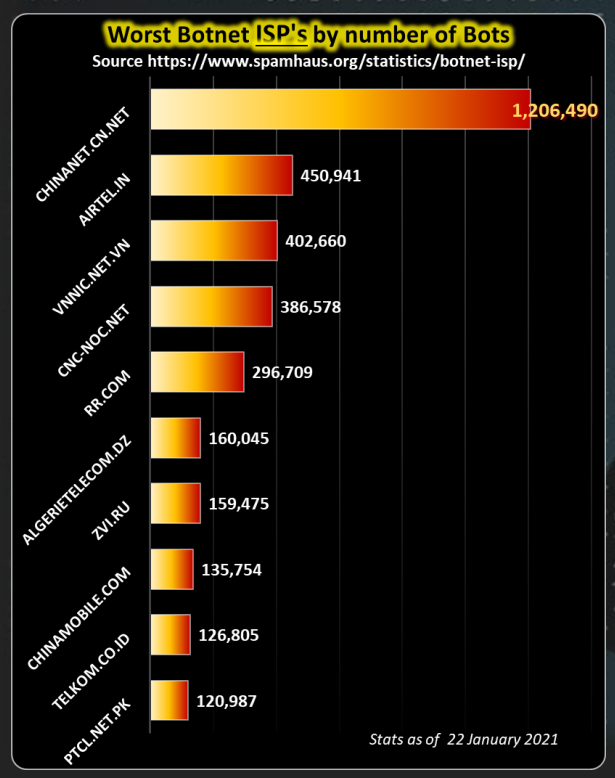
Interpol has issued a global warning that dating app users are being groomed for investment fraud scams. The policing body's Purple Notice claimed that lonely hearts are picked off online, when the fraudsters establish an "artificial romance" with their victims. Once they have built up a level of trust through regular communication, they share investment tips and encourage the victim to join up to a scheme. "Victims download a trading app and open an account, buy various financial products and work their way up a so-called investment chain, all under the watchful eye of their new 'friend.' They are made to believe they can reach Gold or VIP status," the notice explained. "As is often the case with such fraud schemes, everything is made to look legitimate. Screenshots are provided, domain names are eerily similar to real websites and customer service agents pretend to help victims choose the right products." However, eventually the victims are abruptly locked out of their accounts, having invested significant sums in the financial products. They're then left with a double whammy of financial loss and emotional pain. Read the full story by Phil Muncaster here: infosecurity

Malwarebytes breached by SolarWinds hackers

Malwarebytes becomes fourth major security firm targeted by attackers after Microsoft, FireEye, and CrowdStrike. US cyber-security firm Malwarebytes today said it was hacked by the same group which breached IT software company SolarWinds last year. Malwarebytes said its intrusion is not related to the SolarWinds supply chain incident since the company doesn't use any of SolarWinds software in its internal network. Instead, the security firm said the hackers breached its internal systems by exploiting a dormant email protection product within its Office 365 tenant. Malwarebytes said it learned of the intrusion from the Microsoft Security Response Center (MSRC) on December 15. "After an extensive investigation, we determined the attacker only gained access to a limited subset of internal company emails," said today Marcin Kleczynski, Malwarebytes co-founder and current CEO. Read the story here: ZDNet Article

Laptops given to British schoolkids came preloaded with malware and talked to Russia when booted

- A shipment of laptops supplied to British schoolkids by the Department for Education to help them learn under lockdown came preloaded with malware, The Register can reveal. The affected laptops, supplied to schools under the government's Get Help With Technology (GHWT) scheme, which started last year, came bundled with the Gamarue malware – an old remote access worm from the 2010s. The Register understands that a batch of 23,000 computers, the GeoBook 1E running Windows 10, made by Shenzhen-headquartered Tactus Group, contained the units that were loaded with malware. A spokesperson for the manufacturer was not available for comment. Read the full story here: The Register



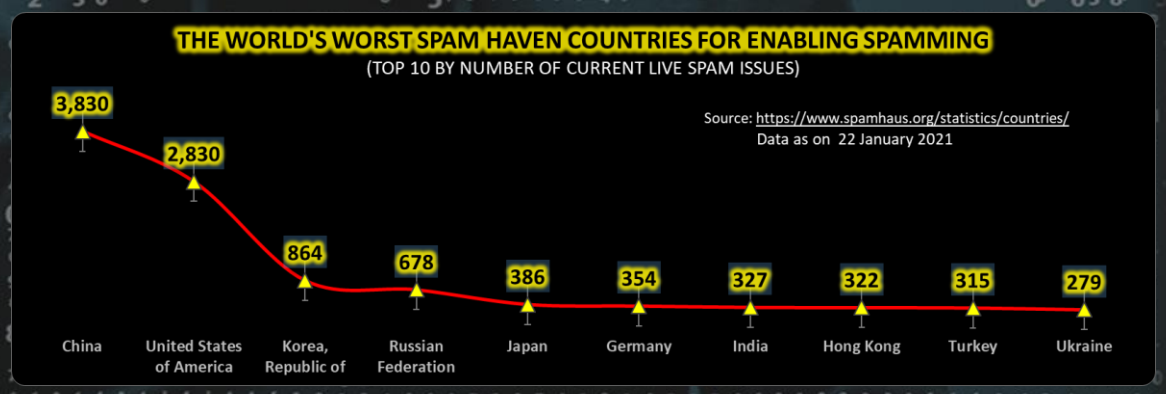
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Fake News, Misinformation & Disinformation

With the vast amount of information captured or manufactured and shared online, it surely makes it difficult sometimes to distinguish between what is real and what is not. In modern times, this very fact is used by criminals for financial gain or anyone with a personal or political agenda to either drum up support or for discord. How do we distinguish between what is true or not?
Let's first look at what the difference is between "Misinformation" and "Disinformation" and then also the "Misinformation Effect": Misinformation is false or inaccurate information that is communicated regardless of an intention to deceive. Disinformation is a species of misinformation that is deliberately deceptive, e. g. malicious hoaxes, spearphishing, and computational propaganda or as we all know it, Fake News. The "Misinformation effect" refers to the tendency for post-event information to interfere with the memory of the original event. Researchers have shown that the introduction of even relatively subtle information following an event can have a dramatic effect on how people remember.
The reason I brought this particular topic up is because I was bombarded this week with questions whether some of the messages or YouTube videos they received are true or not. In particular, the one that goes around regarding the so-called European hack that influenced and diverted votes in the recent US Presidential elections. Supposedly orchestrated by members of the World Economic Forum with connotations to "The Great Reset". Anyway, in my walk through the Internet forest to find the right answers, I came across many, many articles talking about it. The one that eventually got my attention as a reliable source is an article posted by Reuters this week. Below then is a small extract of the article, but please visit the site to read the full article to get the right perspective.
Sources: Wikipedia, Verywellmind, Reuters, YouTube

Fact check: Evidence disproves claims of Italian conspiracy to meddle in U.S. election (known as #ItalyGate)

On Jan. 6, 2021, the day supporters of President Donald Trump gathered in Washington, D.C. to protest the certification of the 2020 presidential election results by Congress and ultimately storm the U.S. Capitol, posts began to circulate widely social media claiming that an employee of an Italian security firm had interfered in the election to secure Joe Biden's victory. Shared online with the hashtags #ItalyDidIt and #ItalyGate, the claims are part of a conspiracy theory intended to sow doubt in the U.S. electoral system and bolster allegations by Trump and his allies that the election was rigged. The supposed evidence, analyzed by Reuters, contradicts the main claims presented in this theory. Examples of posts making these claims can be seen here , here and here.
WHAT IS #ITALYGATE? - This theory took off when an organization called Nations in Action published a press release on Jan. 6 with the headline "Senior IT Expert at Global Defense Contractor Testifies in Italian Federal Court; He and Others Switched Votes throughout America in the U.S. Presidential Race" (here).
According to its website, Nations in Action is based in Sarasota, Florida and was established in 2017 "to address the collapse of the civil society with families struggling to maintain faith, values and virtues" (nationsinaction.org/#about-us). Nations in Action did not respond to Reuters request for comment or elaboration on their "evidence" for these claims. If they do, this article will be updated accordingly.
The press release, which claims to have come from Rome, Italy on Jan. 5, alleges that an employee of the Italian defense, security and aerospace company Leonardo SpA "provided a shocking deposition detailing his role in the most elaborate criminal act affecting a US election." It names Arturo D'Elia as the employee and states that he "outlined the scheme that proved successful in using Leonardo computer systems and military satellites located in Pescara, Italy" to interfere in the U.S. election in favor of Joe Biden.
The press release quotes the group's chair Maria Strollo Zack as saying, "Make no mistake, this is a coup d'etat that we will stop in the name of justice and free and fair elections."
That day, several websites, such as "Shock Ya!" (here), "En Volve" (here) and "No Q Report" (here) began sharing the press release, which soon migrated to Facebook. In an editor's note at the top of the article, "No Q Report" acknowledged, "We have not independently verified it but felt it was necessary to put out there considering the late hour in this election cycle."
LEONARDO AND ARTURO D'ELIA - On Dec. 22, 2020, Reuters published an exclusive report here detailing an investigation into a data theft at Leonardo that took place between 2015 and 2017.
Italian police said on Dec. 5, 2020 that they had arrested Arturo D'Elia and Antonio Rossi, who had both worked at Leonardo, over their alleged role in hacking 94 computers, 33 of which were located at the group's plant in Pomigliano, a municipality in Naples. The hacking took place years prior to the 2020 U.S. election (between 2015 and 2017).
The 108-page arrest warrant examined by Reuters reporters showed that the hack appeared to target details of Europe's biggest unmanned fighter jet program and aircraft used by the military and police. There is no mention of the U.S. election anywhere in the document. (In the 108-page the judge cited different potential reasons behind the 2015-2017 hacking for which D'Elia is under investigation: "the use of data for industrial and commercial purposes, blackmail and military espionage activities or simply the intention to damage the image of the company by demonstrating ... its organizational and IT vulnerability.")
Reuters spoke via phone with D'Elia's lawyer Nicola Naponiello, who previously provided Reuters with comment for the Dec. 22 report on the Leonardo investigation. Naponiello said that when his client was questioned by Naples prosecutors on Jan. 12, he denied any involvement in an alleged plan to change the outcome of U.S elections. According to Naponiello, who was assisting his client during the questioning, D'Elia called any allegations of his involvement in a plan against Trump "pure fantasy." ... Read more.. (Final verdict: False)



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