On February 10, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco, SonicWall, SolarWinds, Google, Mozilla, Microsoft, and Apple products.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
12-Feb	108,273,536	2,377,002

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

12 February 2021

In The News This Week

Hacker modified drinking water chemical levels in a US city !!

The intrusion was detected right away and the hacker's modifications have been reversed right away. An unidentified hacker has accessed the computer systems for the water treatment facility in the city of **Oldsmar**, Florida, and has modified chemical levels to dangerous parameters. News of the attack was disclosed on Monday 8 February in a press conference by city officials. The intrusion took place on Friday, February 5, when the hacker accessed a computer system that was set up to allow for the remote control of water treatment operations. The hacker first accessed this system at 8 am, in the morning, and then again for a second and more prolonged intrusion at 1:30 pm, in the afternoon. This second intrusion lasted for about five minutes and was detected right away by an operator who was monitoring the system and saw the hacker move the mouse cursor on the screen and access software responsible for water treatment. **HACKER MODIFIED LYE LEVELS** - "Sodium hydroxide, also known as lye, is the main ingredient in liquid drain cleaners. It's also used to control water acidity and remove metals from drinking water in the water treatment plant," said Oldsmar Sheriff Bob Gualtieri.
"The hacker changed the sodium hydroxide from about 100 parts per million to 11,100 parts per million. This is obviously a significant and potentially dangerous increase." Oldsmar city staff said that no tainted water was delivered to local residents as the attack was caught in time before any lye levels could be deployed.
Read the full story by Catalin Cimpanu here: ZDNet Article

Following Oldsmar water facility attack, FBI warns about using TeamViewer and Windows 7 -

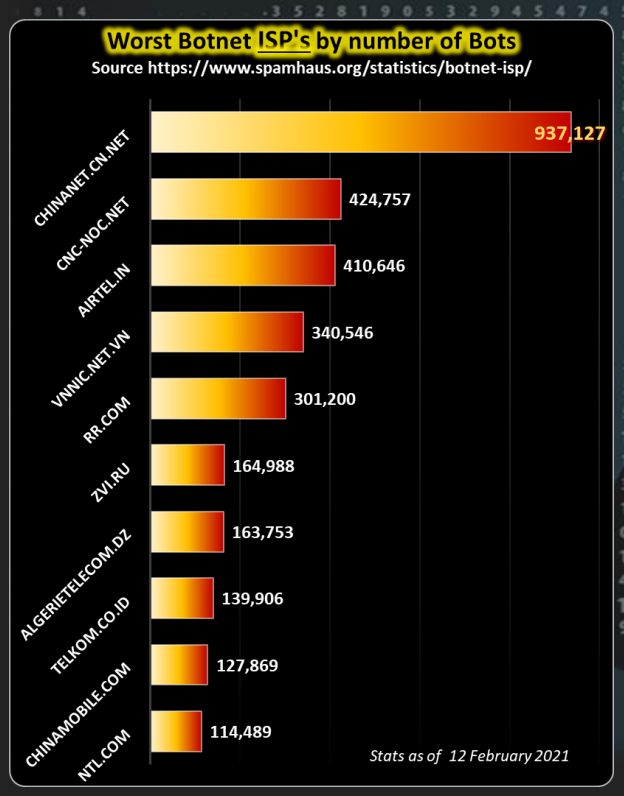
In the aftermath of the Oldsmar incident, where an unidentified attacker gained access to a water treatment plant's network and modified chemical dosages to dangerous levels, the FBI has sent out an alert on Tuesday, raising attention to three security issues that have been seen on the plant's network following last week's hack. The alert, called a Private Industry Notification, or FBI PIN, warns about the use of out-of-date Windows 7 systems, poor passwords, and desktop sharing software TeamViewer, urging private companies and federal and government organizations to review internal networks and access policies accordingly. The FBI PIN specifically named and confirmed the **TeamViewer** app as the attacker's entry point into the Oldsmar water treatment plant's network. According to a Reuters report, officials said the intruder connected to a computer on the Oldsmar water treatment plant's network via TeamViewer on two occasions last Friday.
Read the full story here: ZDNet Article

New phishing attack uses Morse code to hide malicious URLs

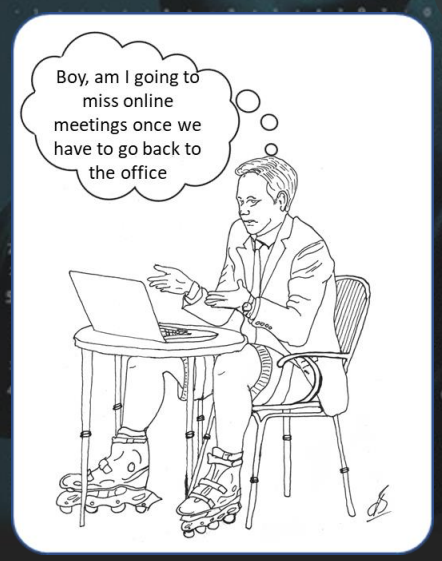
A new targeted phishing campaign includes the novel obfuscation technique of using Morse code to hide malicious URLs in an email attachment. Samuel Morse and Alfred Vail invented morse code as a way of transmitting messages across telegraph wire. When using Morse code, each letter and number is encoded as a series of dots (short sound) and dashes (long sound). Starting last week, a threat actor began utilizing Morse code to hide malicious URLs in their phishing form to bypass secure mail gateways and mail filters. BleepingComputer could not find any references to Morse code being used in phishing attacks in the past, making this a novel obfuscation technique. After first learning of this attack from a post on Reddit, BleepingComputer was able to find numerous samples of the targeted attack uploaded to VirusTotal since February 2nd, 2021. The phishing attack starts with an email pretending to be an invoice for the company with a mail subject like 'Revenue_payment_invoice February_Wednesday 02/03/2021'. Read the full story by Lawrence Abrams here: BleepingComputer

Cyberpunk 2077 game developer says it's been hit with a cyber attack

The Polish studio said hackers had managed to access its internal network, collected certain data and left a ransom note threatening to release the source code of its games. CD Projekt, the developer of sci-fi game Cyberpunk 2077, said Tuesday it's been hit with a "targeted cyber attack." The Polish studio said hackers had managed to access its internal network, collected certain data and left a ransom note threatening to release the source code of its games. "We will not give in to the demands nor negotiate with the actor, being aware that this may eventually lead to the release of the compromised data," CD Projekt said on Twitter Tuesday. "We are taking necessary steps to mitigate the consequences of such a release, in particular by approaching any parties that may be affected due to the breach." Read the full story by Ryan Browne here: NBCNews



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



Cyber Security Breaches and Events, 2020 in Review

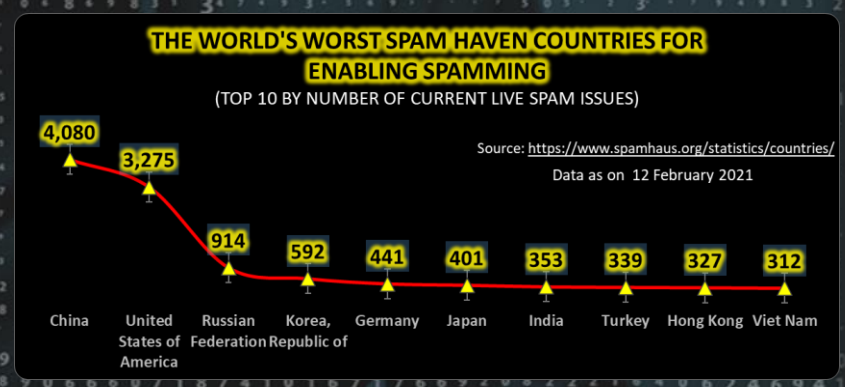
The year 2020 was earmarked by cyber attacks from criminals and Nation State actors alike, with a focus on Covid-19 soft spots and cyber intelligence. Below is an overview of some of the more significant adverse cyber events that took place across the globe. The inspiration and interest for this weeks piece comes mainly from the good work done by the folks at CSIS (Center for Strategic & International Studies) where you can find a comprehensive list dating back to 2006.

- **December 2020** - Hackers accessed data related to the COVID-19 vaccine being developed by Pfizer during an attack on the European Medicines Agency. BBC News
- **December 2020** - Multiple U.S. agencies and private firms were breached by Russian hackers who compromised the software provider **SolarWinds** and exploited their access to monitor internal operations. – Business Insider
- **December 2020** - Facebook has accused Vietnamese hackers of spreading malicious code and stealing user information from its platform. – VNExpress
- **December 2020** - African Union staff found that Chinese hackers had been siphoning off security footage from cameras installed in the AU headquarters. – Reuters
- **December 2020** - Hackers Breached Israeli Water Reservoir HMI System. Hackers with possible links to Iran appear to have breached an unprotected human-machine interface system at an Israeli water reservoir – Bank Info Security
- **November 2020** - A Mexican facility owned by Foxconn was hit by a $34 mil ransomware attack. The hackers claim that 1,200 servers being encrypted, 20-30 TB of backups being deleted, and 100 GB of encrypted files being stolen. – BleepingComputer
- **October 2020** - Hamas used a secret headquarters in Turkey to carry out cyberattack. Reports says the facility in Istanbul is overseen by terror group's military leadership in Gaza, and set up without the knowledge of Turkish authorities – Times of Israel
- **October 2020** - Iranian hackers targeted attendees of the Munich Security Conference in order to gather intelligence on foreign policy from the compromised individuals – POLITICO
- **October 2020** - The FBI and CISA announced that a Russian hacking group breached U.S. state and local government networks, as well as aviation networks, and exfiltrated data – ZDNet
- **October 2020** - The UN shipping agency the International Maritime Organization (IMO) reported that its website and networks had been disrupted by a sophisticated cyber attack – Reuters
- **September 2020** - A ransomware attack on a German hospital may have led to the death of a patient who had to be redirected to a more distant hospital for treatment. – The Verge
- **September 2020** - Georgian officials announce that COVID-19 research files at a biomedical research facility in Tiblisi was targeted as part of a cyberespionage campaign – US Embassy Georgia
- **August 2020** - New Zealand's stock exchange faced several days of disruptions after a severe distributed denial of service attack was launched by unknown actors – The Guardian, BBC News
- **August 2020** - Seven semiconductor vendors in Taiwan were the victim of a two-year espionage campaign by suspected Chinese state hackers targeting firms' source code, software development kits, and chip designs. – Wired
- **July 2020** - Israel announced that two cyber attacks had been carried out against Israeli water infrastructure, though neither were successful – Times of Israel
- **June 2020** - Nine human rights activists in India were targeted as part of a coordinated spyware campaign that attempted to use malware to log their keystrokes, record audio, and steal credentials – Amnesty
- **May 2020** - Israeli hackers disrupted operations at an Iranian port for several days, causing massive backups and delays. Officials characterized the attack as a retaliation against a failed Iranian hack in April on the Israeli water distribution systems – Aljazeera
- **May 2020** - Cyber criminals managed to steal $10 million from Norway's state investment fund in a business email compromise scam that tricked an employee into transferring money into an account controlled by the hackers – CyberScoop
- **April 2020** - Poland suggested the Russian government was being behind a series of cyber attacks on Poland's War Studies University meant to advance a disinformation campaign undermining U.S.-Polish relations. – CyberScoop
- **April 2020** - Suspected Vietnamese hackers targeted the Wuhan government and the Chinese Ministry of Emergency Management to collect information related to China's COVID-19 response. – Bloomberg
- **March 2020** - Saudi mobile operators exploited a flaw in global telecommunications infrastructure to track the location of Saudis traveling abroad - Privacy International
- **March 2020** - Chinese cybersecurity firm Qihoo 360 accused the CIA of being involved in an 11- year long hacking campaign against Chinese industry targets, scientific research organizations, and government agencies – Reuters
- **February 2020** - Mexico's economy ministry announced it had detected a cyber attack launched against the ministry's networks, but that no sensitive data had been exposed. – Economic Times
- **February 2020** - The U.S. Defense Information Systems Agency announced it had suffered a data breach exposing the personal information of an unspecified number of individuals – CNBC
- **January 2020** - Austria's foreign ministry has been targeted in a cyber-attack that is suspected to have been conducted by a nation state actor – BBC
- **January 2020** - Mitsubishi - a suspected Chinese group had targeted the company in a cyberattack that compromised personal data of 8,000 individuals as well as other information, including projects relating to defense equipment. – The Japan Times

New Book on the shelves:

The new book, ***"Cybersecurity 202: 'This Is How They Tell Me The World Ends'***, sheds new light on a global cyberweapons arms race.

Read the review here: Washington Post



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