On November 24, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Netgear, Microsoft and Fortinet products.. See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
26 Nov	260,311,551	5,199,480

Deaths this week: 52,307

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

26 November 2021

In The News This Week

New UK IoT law means huge fines and a ban on default passwords

The United Kingdom government has introduced new legislation designed to improve the security of "smart" internet-connected devices used in people's homes. With all manner of Internet of Things (IoT) gizmos - from smart TVs and internet-connected light bulbs to smart speakers and IoT washing machines - cluttering millions of Britons' homes, the Product Security and Telecommunications Infrastructure (PSTI) Bill requires manufacturers and sellers of IoT devices and gadgets to meet new cybersecurity standards to better protect customers' privacy and security. The UK says that the new legislation will allow it to force firms into being transparent with customers about what they are doing to fix security flaws, create a better public reporting system for vulnerabilities, and ban universal default passwords. And any organisation which fails to abide by the rules once the new bill comes into force could find itself fined up to £10 million or 4% of their global turnover, as well as up to £20,000 a day in the case of an ongoing contravention. Read the full story by Graham Cluley here: BitDefender

US, UK, and Australian Agencies Issue Joint Cybersecurity Advisory on Iranian APT Groups Targeting Critical Infrastructure

- The US, UK, and Australian agencies issued a joint cybersecurity alert over Iranian APT actors exploiting Fortinet and Microsoft Exchange ProxyShell vulnerabilities to compromise critical infrastructure entities. Post exploitation, the Iranian government-sponsored APT actors exfiltrated data and deployed ransomware to extort the victims. The agencies observed Iranian APT groups scanning for Microsoft Exchange ProxyShell vulnerability since October 2021 while they had actively exploited Fortinet vulnerabilities since March 2021. The joint advisory noted that Iranian APT groups actively targeted critical infrastructure in healthcare, transportation, and the public sector, and Australian organizations. However, they are focused on high-impact known Exchange Server and Fortinet FortiOS vulnerabilities instead of specific industries.
Read the full story by Alicia Hope here: CPO Magazine

Swire Pacific Offshore: Notice of Cyber Security Incident

Swire Pacific Offshore (SPO) has discovered that it was the target of a cyberattack which involved unauthorised access to its IT systems. The unauthorised access has resulted in the loss of some confidential proprietary commercial information and has resulted in the loss of some personal data. The cyberattack has not materially affected SPO's global operations. SPO has taken immediate actions to reinforce existing security measures and to mitigate the potential impact of the incident. It takes a serious view of any cyberattack or illegal accessing of data or any unlawful action that potentially compromises the privacy or confidentiality of data, and will not be threatened by such actions. SPO has reported the incident to the relevant authorities and will work closely with them in relation to the incident. SPO is contacting potentially affected parties to inform them about the incident.
Read the full statement here: Hellenic Shipping News

Popular adult cam chat exposed users data

Someone appears to have been careless with a database of users of the Stripchat adult video website. Security researcher Bob Diachenko says he found an unprotected database with a huge number of records of people who appear to be registered users of the site. "*The exposed database makes multiple references to Stripchat and consists of nearly 200 million records.*" Users can post videos of themselves in sexual situations. Information in the database includes email addresses, usernames and IP addresses. It isn't clear who owns the database, but after Diachenko notified Stripchat it wasn't openly available anymore. It isn't known how long the database was open for anyone to find or whether anyone else found and copied it. If they did, as Diachenko notes, the information could be used to harass and threaten people. Read the story by Howard Solomon here: ITWorldCanada

Vestas shuts IT systems in response to cyber security incident

Danish wind turbine manufacturer, Vestas, has released a statement confirming that on 19 November 2021 the company was impacted by a cyber security incident. - Details are currently scarce however Vestas has confirmed that in order to contain the issue, IT systems have been shut down across multiple business units and locations.
Read the full story here: PEi

Black Friday, why you should be vigilant and aware!

Once again, it is Black Friday, and retailers and civil departments alike are prepared for the frantic shopping craze that has become a worldwide phenomenon. With the advent of the Covid-19 pandemic, however, online shopping has increased in some areas close to 500%, if not more, and for this long weekend that closes out on Cyber Monday, the curve will shoot up even more. Great news for retailers but also ripe picking fields for Cyber Criminals. Business Live reported this week, "Check Point Research has identified 5,300 malicious websites a week leading up to Black Friday and Cyber Monday. It warns shoppers to be on the lookout for offers that are too good to be true. The company says it has seen a 178% spike in the past six weeks, compared with the average for 2021, with one in 38 corporate networks affected each week in November against one in 352 earlier this year."

To put the dangers of Cyber Crime in perspective, I include a feature form Crowdstaffing that remind us of the massive cyber crime incident involving the Target retail chain and others in 2013. The picture didn't change much from a criminal perspective, and the picking fields are still extremely lucrative. Below is an extract of the Crowdstaffing article highlighting the risk associated with the Digital age we all embraced as part of the new normal.

The Rewards of the Digital Age Aren't Without Risks

Few Americans can forget the panic of 2013's Black Friday, and not just because of the frantic rush to grab the hottest products off the shelves at "ridiculously" low prices. That was also the year over 110 million shoppers discovered that their credit card information had been stolen after hackers targeted a variety of retailers -- Target, chief among them.

In the weeks following the breach, Target revealed that the personal information of close to 70 million customers had been compromised, including names, addresses, phone numbers and email accounts. Yet, few other sellers were immune. Hackers also infiltrated the payment systems of Home Depot, Albertson's, Michaels, Neiman Marcus, P.F. Chang's, SuperValu, Adobe and others. In fact, by the conclusion of 2014, researchers at the Ponemon Institute estimated that 110 million Americans -- about the half the adult population of the country -- had fallen prey to cyber criminals who exploited allegedly secure systems to expose their victims' financial, transactional and personal details.

For all the wonders and conveniences of this digital world, we must not ignore the persistent threat of hackers. Technology graces us with new comforts every day -- and with them, new perils. The global cyberattacks that erupted in May offered another profound object lesson. A massive infection of malware plagued at least 75,000 computers across nearly 100 countries. The perpetrators targeted dozens of hospitals in England, multinational businesses such as FedEx and Spain's largest telecommunications provider. Companies in the United States were urged to place themselves on high alert and take precautions against intrusions.

Experts believe the attacks were inspired by a National Security Agency (NSA) tool kit that was leaked last year. The malicious software, called the Wanna Decryptor or WannCry, essential locks users out of a system until ransom is paid to the hackers. As NBC News reported, the malware spread through email phishing programs and specifically exploited a known bug in Windows operating systems: *"It was the size of the attack that shocked experts. "The scale of it — that's pretty unprecedented," Ben Rapp, the CEO of IT support company Managed Networks, told NBC News' British partner ITV News. "There's been a lot of ransomware in hospitals, but to see 16 hospitals, last time I looked, and reports of other people — this is probably the biggest ransomware attack we've seen."*

Yet the events of April 12 are not the headlines of the year in terms of data theft. Russia's interference in the U.S. elections became a chilling example of how far-reaching, sophisticated and consequential cyberattacks have become. Regardless of who orchestrated Friday's electronic ransom campaign, Michael Sulmeyer's piece in the Harvard Business Review illustrates the growing risks business around the world must confront as hackers develop more aggressive and penetrating attacks.

Sulmeyer's expose directly examines what the rise of Russian hackers means for our businesses – and the sensitive data we entrust to systems that may be more vulnerable than we suspect.

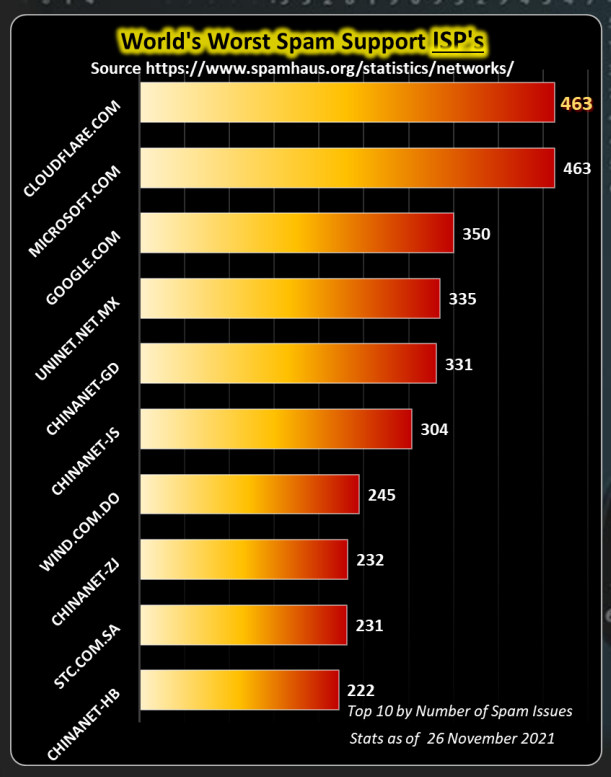
"On the geopolitical stage," he explains, "Russian hackers have been busy: Their targets have included Estonia (using overwhelming denial-of-service attacks), Georgia (supporting ground operations with cyber operations), Germany (achieving unauthorized access to servers in the legislature), and the United States (stealing data from the Democratic National Committee and emails from John Podesta). But with the U.S. Department of Justice's (DOJ) indictment of four Russian hackers for breaching Yahoo, the U.S. government is now on record that Russia's targets are not just geopolitical -- businesses are very much at risk as well."

To emphasize the latter point, look at the ramifications of the breaches that shook Yahoo. Not only were datasets compromised, the fallout led to severe indirect costs for the company. Sulmeyer noted that "Verizon reached new terms for its acquisition of Yahoo and exacted a $350 million discount toward its purchase price because of the Russian hacks."

However clever or overt some of these attacks have been, the U.S. government now worries about more insidious threats. Does anyone remember the 1979 film "When a Stranger Calls?" A psychopath terrorizes a babysitter in a fraught cat-and-mouse thriller. The big reveal, of course, is when the protagonist learns that the "call is coming from inside the house." Officials in the United States suspect that a similar menace could be lurking on millions of devices already -- an enemy stalking us from within. …

Please read the rest of the Crowdstaffing article as it gives us a glimpse of what the cybercriminal world has been up to.

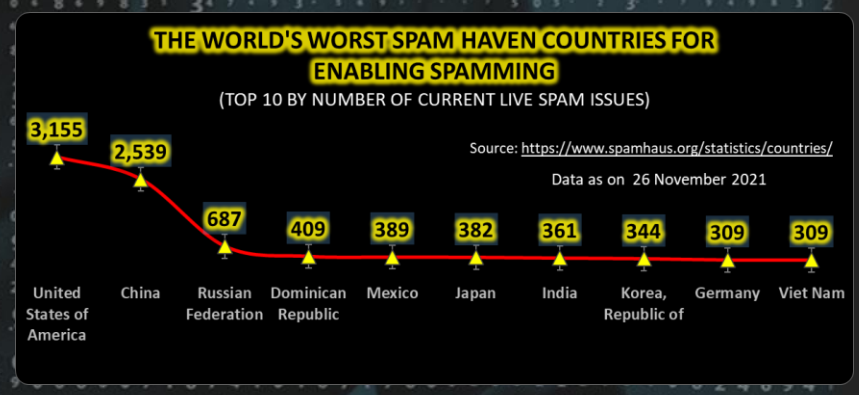
Other References: NBC News, KrebsonSecurity



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

Other Interesting News and Cyber Security bits:

- Drones, bots and self-driving cars
- The Threat from Drones and How You Can Prepare
- Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure,'



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