On November 25, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla, Drupal and VMWare 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
27 November 2020

In The News This Week

Personal data of 16 million Brazilian COVID-19 patients exposed online

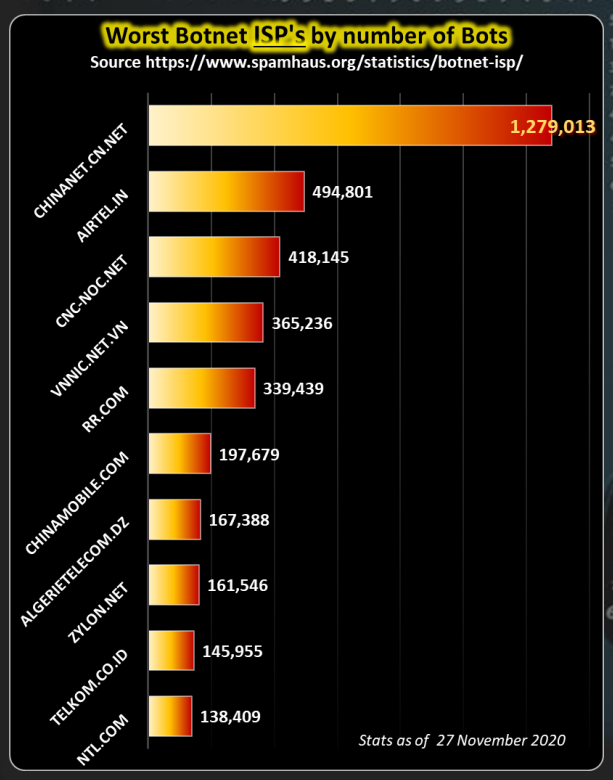
Among those affected by the leak are Brazil President Jair Bolsonaro, seven ministers, and 17 provincial governors. The personal and health information of more than 16 million Brazilian COVID-19 patients has been leaked online after a hospital employee uploaded a spreadsheet with usernames, passwords, and access keys to sensitive government systems on GitHub this month. Among the systems that had credentials exposed were E-SUS-VE and Sivep-Gripe, two government databases used to store data on COVID-19 patients. E-SUS-VE was used for recording COVID-19 patients with mild symptoms, while Sivep-Gripe was used to keep track of hospitalized cases. The two databases contained sensitive details such as patient names, addresses, ID information, but also healthcare records such as medical history and medication regimes. The leak came to light after a GitHub user spotted the spreadsheet containing the passwords on the personal GitHub account of an employee of the Albert Einstein Hospital in the city of Sao Paolo. Read the full story by Catalin Cimpanu here: ZDNet Article

Fertility Patients' Sensitive Personal Information Stolen During Ransomware Attack

Fertility clinics across the United States have been struck by a ransomware attack that has not only encrypted networks, but also stolen patients' sensitive personal and medical information. US Fertility, a network of fertility clinics which boasts 55 locations across the United States, has revealed that it became aware ransomware had infected its network on September 14 2020, encrypting data on servers and workstations. The company says that third-party experts were able to help it restore its systems six days later, but that a subsequent investigation has determined that a "limited number of files" had been accessed by an unknown hacker between August 12 2020, and the activation of the ransomware on September 14. Such tactics are not unusual in modern ransomware attacks, where criminal gangs increase pressure on their victims by not only locking them out of their organisation's computer systems by encrypting data, but also stealing sensitive files with the threat of publishing them online or selling them on to others. The company warned that the security breach might "affect the security of certain individuals' protected health information." According to US Fertility, the types of data accessed by the attackers included patients' names, addresses, phone numbers, email addresses, dates of birth, medical record numbers (MPI), and – in some cases – social security numbers. A list of infertility clinics affected by the attack are listed in US Fertility's press release. Read the full story here: hotforsecurity

Three Nigerians Arrested for Cybercrime Operation Targeting 150 Countries

Three Nigerian nationals have been arrested in Lagos for their suspected involvement in Business Email Compromise (BEC) scams. The three — identified only as OC, 32, IO, 34, and OI, 35 — are believed to be part of a larger organized crime group called TMT, which has been involved in malware distribution, phishing, and extensive BEC fraud. According to the Interpol, the three likely set up phishing links, domains, and mass mailing campaigns. By impersonating representatives of organizations, the suspects leveraged the campaigns to deliver 26 malware families, including spyware and remote access tools. Some of the malicious programs employed by the group include AgentTesla, Azorult, Loki, the nanocore RAT, Spartan, and Remcos RAT. In preparation for launching the scams and stealing funds, the malware was leveraged to gain access to and monitor the systems of victim organizations and individuals. Since 2017, the TMT group is believed to have targeted government and private sector companies in over 150 countries. Data extracted from devices pertaining to the three arrested members has helped identify approximately 50,000 victims. The three were arrested as part of Operation Falcon, a year-long investigation conducted by Interpol and Singapore-based security firm Group-IB, with assistance from the Nigerian police. Group-IB, which has been tracking the cybercrime ring since 2019, claims that roughly half a million government and private sector companies could have been compromised..
Read the full story by Ionut Arghire here: SecurityWeek



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

It's Black Friday Again

Black Friday is not just a lucrative event for retailers every year, it's highly lucrative for cybercriminals as well. This is the time of the year that criminals grab the opportunity to launch some of their own "hot deals" as they lure buyers into their web with phishing and other malicious campaigns. We therefore see tons of news articles covering the event from a security perspective and below is a couple I want to share this week.

One in Seven #BlackFriday Emails Are Malicious

More than one in seven emails sent on Black Friday today could be a scam, security experts have warned. Vade Secure claims to protect one billion inboxes around the world with AI-powered security for Microsoft 365. Its Current Events tracker has detected a predictable spike in malicious messages containing text about the shopping discount extravaganza today. It said 9% of US emails and 15% in Europe were malicious — spoofing big-name retail brands such as Lidl, Sephora, Target and, most popular, Amazon.

"We are issuing an alert about the Black Friday event in order to warn ISPs and businesses using Microsoft 365 to help them protect customers and clients from malicious emails. Seasonal threats of this nature can be predicted and monitored more easily than surprise attacks, so sysadmins should be aware of the surge in Black Friday email exploits," explained Vade Secure's chief product and services officer, Adrien Gendre.

"The rise of online shopping and home working has created new vectors for attackers, so security professionals need to guard carefully against new threats as they emerge. The best way to defeat email threats is to use complementary layers of protection involving both tech and humans." The United States Cybersecurity and Infrastructure Security Agency (CISA) also issued an alert today, warning that criminals may be looking to cash-in both online and in-person.

"Malicious people may be able to obtain personal information (such as credit card numbers, phone numbers, account numbers and addresses) by stealing your wallet, overhearing a phone conversation, rummaging through your trash (a practice known as dumpster diving) or picking up a receipt at a restaurant that has your account number on it," it claimed. "If a thief has enough information, he or she may be able to impersonate you to purchase items, open new accounts or apply for loans."

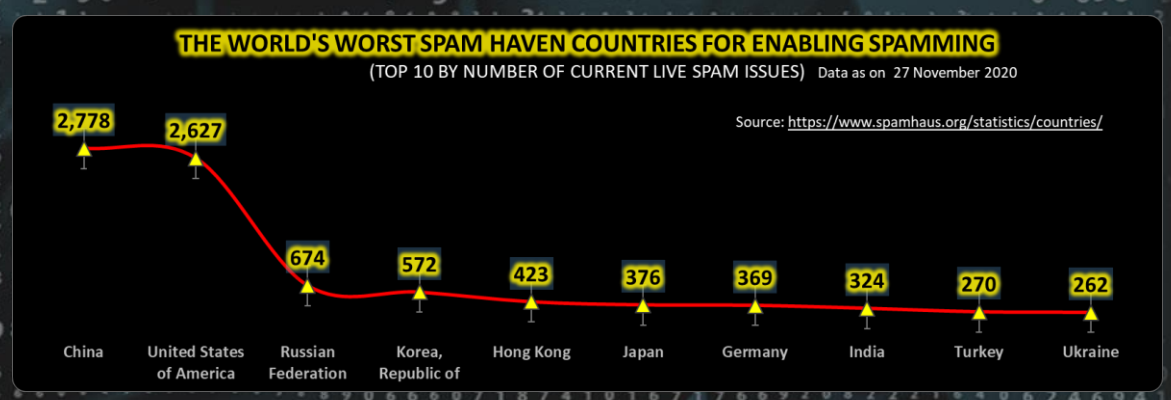
The agency urged shoppers to check company privacy policies, monitor their bank statements, use passwords and other security features where available and to avoid sharing personal information online..

Source Article by Phil Muncaster: InfoSecurity

10 Cyber Safety Tips For Black Friday & Cyber Monday (Adapted)

With more people expected to shop online this year due to the Coronavirus pandemic, cybercriminals have ramped up their scams ahead of Black Friday and Cyber Monday. Lockdown restrictions have forced many retailers to close the doors of their physical shops, meaning many Black Friday deals will only be available online. This has created the perfect environment for criminals to launch scams, phishing attacks, and other malicious activities. Black Friday is a major shopping event that originated in the United States but has since grown in popularity in the UK. It falls on November 27 this year, but many retailers have already started launching early deals to entice customers to start spending. The amount of money spent over this cyber weekend is escalating year on year, and last year in the UK, shoppers spent a staggering £2.5billion, an increase of 3.4% on the previous year. Cybercriminals follow the money and this weekend of crazed spending provides them with the perfect opportunity to scam a large number of people. According to Barclays, nearly a quarter of 18-34-year-olds have fallen for a Black Friday scam in the past five years and shoppers lose on average £661 after falling victim to such frauds. With attacks becoming more sophisticated, shoppers need to be extra cautious when looking for the latest bargains online. Below are 10 Cyber Safety tips to keep you safe online this Black Friday and Cyber Monday - 10 Cyber Safety tips to keep you safe online this Black Friday and Cyber Monday:
(1) **Watch out for fake websites** - This is one of the most popular ways criminals will try to trick shoppers into falling for their Black Friday and Cyber Monday scams. (2) **Only use secure sites** - Always check that the site is safe and secure. You should look for a padlock symbol in the address bar and check that the URL begins with a 'https://' or 'shttp://'. (3) **Use a credit card for shopping online** - When possible, it's always best to use a credit card when shopping online as it offers additional protection over other forms of payment. (4) **Beware of phishing emails** - Phishing is one of the most popular ways for criminals to steal your personal information and there is always a massive increase in these types of scams on Black Friday and Cyber Monday. (5) **Avoid deals that are too good to be true** - Cybercriminals know we'll be scouring the web for the cheapest deals and they take advantage of this by slipping in lots of fake offers. (6) **Use strong passwords** - You'll have heard it a million times, but is one of the easiest ways you can protect yourself. (7) **Watch out for social media scams** – Don't "Like" or "Share" an online deal, rather send a private message to your friend. (8) **Avoid Public Wi-Fi to go shopping** – It could open you up to a range of security risks. (9) **Ensure all your software is up to date** - Make sure that all your security software is up to date. (10) **Monitor bank statements for fraudulent activity** - It's always worth keeping a close eye on bank statements to make sure there are no unusual transactions on your account.

For the sake of space I had to adapt and shorten this article, please read the full article by Geraldine Strawbridge here: MetaCompliance



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