On September 9, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in File Manager, Cisco, SAP, Microsoft, Google, and Adobe 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
11 September 2020

In The News This Week

France, Japan, New Zealand warn of sudden spike in Emotet attacks

Cyber-security agencies from France, Japan, and New Zealand have published security alerts over the past week warning about a large uptick in Emotet malware attacks targeting their respective countries. Emotet activity described in the alerts refers to email spam campaigns that originated from Emotet infrastructure and targeted companies and government agencies in the three countries. Victim organizations who received the emails, opened, and then ran the attached documents were at risk of getting infected with one of today's most dangerous malware. Joseph Roosen, a member of Cryptolaemus, a group of security researchers who track Emotet malware campaigns, told ZDNet that the Emotet botnet has been particularly active in recent weeks, and especially active in the three countries. Read the full story here: ZDNet Article

Collection of Metadata, as Done by the NSA, Likely Unconstitutional, US Court Suggests

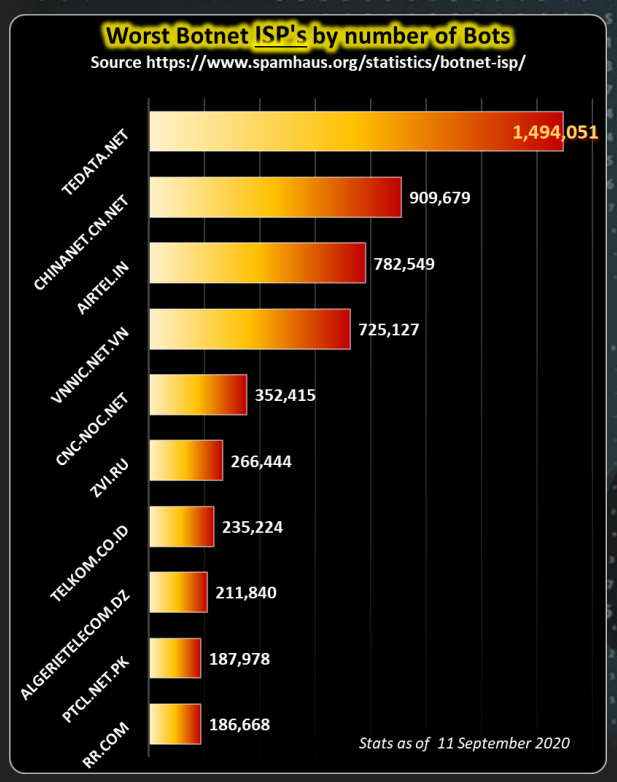
A ruling in an appeal by four men convicted of material support for terrorism finds that the National Security Agency's metadata collection program not only violated the prevailing law at the time but was also likely unconstitutional. **A post-9/11 program** that enabled the mass collection of telephone, cellular, and text metadata by the US National Security Agency (NSA) likely violated the constitution, a three-judge panel of the US Appeals Court for the Ninth Circuit concluded in a ruling on Sept. 2. The ruling involved an appeal by the attorneys representing four Somali immigrants to the United States convicted in February 2013 of providing financial aid to terrorists, based on the argument that the investigators used data collected from the NSA program as reason to wiretap and investigate the men. While the opinion denied the defendants a new trial, the judges concluded that the collection of metadata on millions of Americans is a substantially different proposition compared with limited requests for dialled phone numbers, which had legally been allowed without a warrant under previous precedents. The conclusion will make future attempts to revive such a program that much more difficult, says Mark Rumold, a senior staff attorney at the Electronic Frontier Foundation, a digital rights group.
Read the full story here: DarkReading

Hackers Shut Argentina Borders with $4 Million Bitcoin Ransom Demand

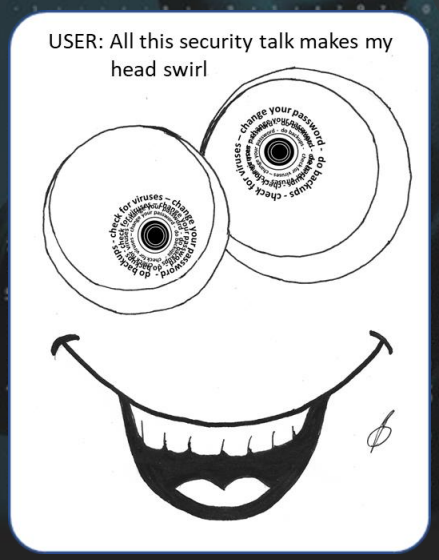
A ransomware attack by cybercriminals demanding Bitcoin led to the temporary shutdown of Argentina's international borders. Argentina's immigration agency, Dirección Nacional de Migraciones (DNM), was the victim of a ransomware attack that temporarily halted border crossings, with hackers demanding $4 million in Bitcoin. The attack was first reported by the Argentinean government on August 27 to the country's cybercrime agency, after multiple calls from border checkpoints suggested their computer networks were compromised, according to security news site Bleeping Computer. Read the full story here: Decrypt *(Thanks to My good friend Yazan Shapsugh who pointed me to this story)*

Ransomware: Huge rise in attacks this year as cyber criminals hunt bigger pay days

There's been a huge increase in the number of ransomware attacks over the course of 2020, with a **seven-fold rise** in campaigns compared with just last year alone, according to newly released data from cybersecurity researchers. Ransomware attacks have been on the rise and getting more dangerous in recent years, with cyber criminals aiming to encrypt as much of a corporate network as possible in order to extort a bitcoin ransom in return for restoring it. A single attack can result in cyber criminals making hundreds of thousands or even millions of dollars. It's something that cyber criminals have been capitalising on despite the changing working circumstances with more people working remotely during 2020, with Bitdefender's Mid-Year Threat Landscape Report 2020 claiming a **715%** year-on-year increase in detected – and blocked – ransomware attacks.
Read the full article by Danny Palmer here: ZDNet Article



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



19th Anniversary of the 9/11 Attack

As we all remember and as millions of us witnessed live on television - on September 11, 2001, 19 militants associated with the Islamic extremist group Al Qaeda hijacked four airplanes and carried out suicide attacks against targets in the United States. Two of the planes were flown into the twin towers of the World Trade Center in New York City, a third plane hit the Pentagon just outside Washington, D.C., and the fourth plane crashed in a field in Shanksville, Pennsylvania. Almost 3,000 people were killed during the 9/11 terrorist attacks, which triggered major U.S. initiatives to combat terrorism and defined the presidency of George W. Bush.

As traditional intelligence gathering and sharing failed to prevent the attack, did the world learn from this event and how was cyber security and cyber intelligence ramped up in a bid to prevent this from happening ever again?

The 9/11 event has opened the eyes of the intelligence community and Governments across the globe and literally tons of initiatives were spawned to improve the way we gather intelligence and more importantly, how we share intelligence. Over the last 20 years the cyber world has become immensely more complicated and terror groups are constantly finding ways to "hide" their activities and are using the Cyber Critical Infrastructure of countries to plan and launch physical as well as logical attacks. In the same realm, Cyber Intelligence gathering has become a massive challenge where Governments and the Private Sector are constantly bumping heads and citizens are demanding more privacy of their personal communications and data.

Although cyber intelligence gathering has improved leaps and bounds, the stumbling blocks are still plentiful due to the challenges mentioned above. The US for example, is still working out some disparity issues as stated in an article in Homeland Security Today.US last year - "*After the terrorist attacks of 9/11, the intelligence and law enforcement communities focused on connecting the dots, regardless of whether the information came from law enforcement, the intelligence community, the private sector, international partners or elsewhere. There was a concerted effort to increase information sharing among all stakeholders, and today there are strong mechanisms in place to share data seamlessly and globally around issues of security and terrorism.*

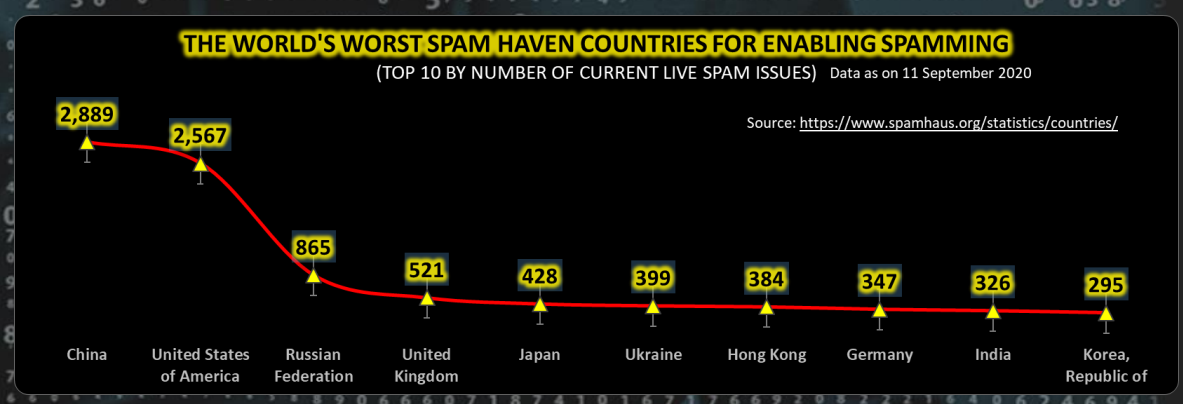
This is not the case for our cyber infrastructure. Instead, there is fragmentation and distrust between the government and the owners and operators of the critical infrastructure in the U.S., 85 percent held by private companies. This fragmentation creates seams that foreign adversaries are able to exploit. It is time that we create a mechanism to foster greater information sharing across critical infrastructure sectors, the federal, state and local government and the private sector. Information needs to be more readily available on a "need to have" basis instead of just "need to know." This effort will require more than just DHS and the new Cybersecurity and Infrastructure Security Agency (CISA) working closer with private industry. It will require buy-in and participation from across the federal government, international partners, private businesses, and state and local governments."

To address the communication and intelligence sharing blunders prior to the attack, a massive restructuring of the US Security and Intelligence agencies has seen the light as described in an article in the Department of Justice Archives. "*In 2006, the Justice Department created the National Security Division (NSD), the first new Justice Department division in 49 years, to merge the department's primary national security components into a single division to more effectively combat national security threats. The division brought together the former Office of Intelligence Policy and Review, the Counterterrorism Section and the Counterespionage Section from separate parts of the department. The new Office of Law and Policy, the Executive Office and the Office of Justice for Victims of Overseas Terrorism have completed the NSD. NSD's structure is designed to fuse the authorities and capabilities of the law enforcement and intelligence communities to strengthen the government's national security efforts.*

Since 9/11, the FBI has undertaken the most significant transformation in its history. The bureau has restructured its operations in order to better detect, penetrate and dismantle terrorist enterprises as part of its larger cultural shift to a threat-based, intelligence-driven, national security organization. Today, the FBI serves as a vital link between the intelligence and law enforcement communities, bringing the discipline of the criminal justice system to its domestic intelligence activities in a manner that is consistent with American expectations and protections for privacy and civil liberties. As part of this strategic shift, the FBI has overhauled its counterterrorism operations, expanded its intelligence capabilities, modernized its business practices and technologies, and improved coordination with its partners."

The reality of today is that enemies no longer need to launch missiles or fly airplanes into buildings to attack the United States or Russia or South Korea or any other country. The weapon of choice, cyber warfare, introduced into the world's arsenal in the last decade or so has no boundaries or rules, costs little, and has devastating potential. And we see evidence of that week on week in this bulletin alone.

Apart from Governments across the globe who stepped up to the plate in counter terrorism, the private sector has a massive role to play and the big technology conglomerates has to take responsibility in governing the tech they pump out in the world in such a way that terrorist activities can be proactively identified and stopped in it's tracks. Yes, it is a big statement, but it is possible if only they could cooperate and share intelligence (and intelligence they have!) in a timely manner and set aside their corporate and brand protection rules in those moments when it really matters and be instrumental in the prevention of terrorist atrocities.



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