The Cyber Threat Alert Level was evaluated on May 12 2021, and was set to Blue (Guarded), and will remain at this level until a change is indicated by CIS.

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
25 June	180,775,213	3,916,202

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

25 June 2021

In The News This Week

Six Flags to Pay $36M Over Collection of Fingerprints

Illinois Supreme Court rules in favor of class action against company's practice of scanning people's fingers when they enter amusement parks - Theme park operator Six Flags has agreed to pay $36 million to settle a class-action lawsuit over its acquisition of the fingerprint data of visitors to its theme parks. The Illinois Supreme Court ruled in the case Rosenbach v. Six Flags that collecting biometric data at premises' gates by scanning fingerprints of people who enter the company's theme park violates Illinois Biometric Information Privacy Act (BIPA). Passed in 2008, the BIPA regulates how companies collect and use someone's biometric data, such as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. The law mandates that a company must obtain a person's written consent before acquiring and storing this type of data.
Read the full story by Elizabeth Montalbano here: ThreatPost

MTN and ZTE accused in US lawsuit of aiding Iraq terror

Africa's largest wireless carrier MTN Group Ltd. and Chinese technology company ZTE Corp. were accused in a U.S. lawsuit of indirectly supporting an Iranian terrorist campaign that resulted in Americans being injured and killed in Iraq. In a federal lawsuit filed Tuesday in New York, more than 50 Americans claim MTN and ZTE did business with the Islamic Revolutionary Guard Corps, even though they knew the transactions would help finance, arm and support the Iranian group's terror campaign in neighbouring Iraq. As a result, thousands of Americans were injured or killed between 2011 and 2016, according to the suit. "MTN is reviewing the details of the complaint and is consulting its advisers," the Johannesburg-based company said in an emailed statement. "It conducts its business in a responsible and compliant manner in all its territories and so intends to defend its position where necessary." ZTE spokeswoman Margaret Ma didn't immediately respond to an email sent after hours in China..
Read the full story here: MyBroadband, Bloomberg

Russia seeks productive dialogue with US on cyber security — Lavrov

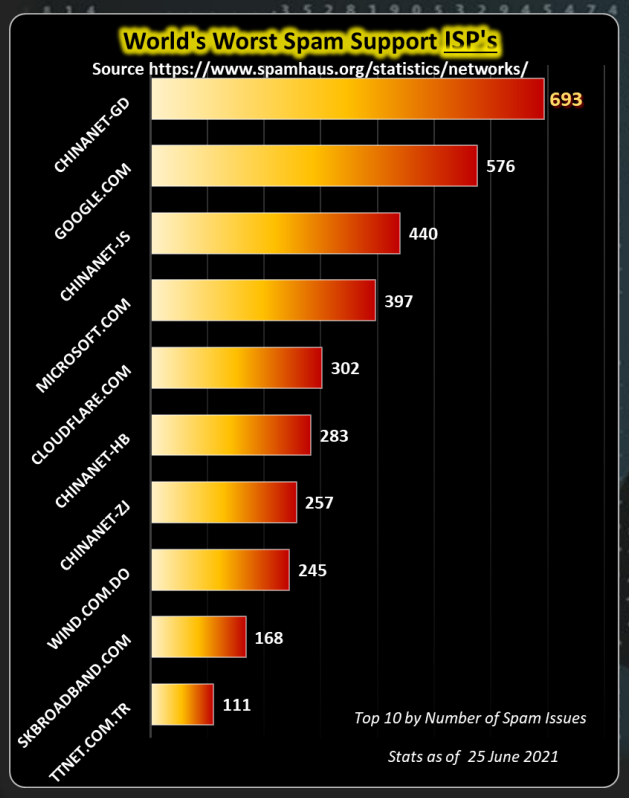
Moscow hopes to step up cooperation on cyber security in a bilateral format, and expects productive dialogue with the US in this direction, Russian Foreign Minister Sergey Lavrov told the Moscow Conference on International Security on Thursday. "We expect, of course, that our cooperation on cyber security will continue through bilateral channels, and we would like to also see productive dialogue on cyber security issues with the US side, as was discussed at the Geneva summit," said the top Russian diplomat. Moscow voices concerns over "the plans of certain states to militarize the Internet and unleash a cyber arms race there". "For our part, we are actively working on adopting a code of responsible behavior of states in the global information space, given the interests of each country in the field of military and political security. Simultaneously, we are promoting the project of a universal convention on combating cyber crimes," Lavrov said. Read the full article here: TASS

Israel's Rafael defense firm unveils consortium to provide cyber security in Dubai

Rafael defense company unveiled the Israeli Operational Technologies Cyber Consortium in Dubai, saying "war is not just about missiles today, it is also about harming critical infrastructure—the blood flow of a country," said Michael Arov, head of its Cyber Business Unit. Earlier this month, Rafael announced the establishment of a new consortium of Israeli companies to provide cyber security for operational technologies in Dubai. The new consortium will provide end-to-end, cyber-operational solutions for clients around the world. Story here: JNS

Anglesey cyber-attack affects island's five secondaries

All five secondary schools on the island of Anglesey have been hit by a cyber-attack. Officials said affected systems had been disabled to "contain the incident", but warned some personal data could have been compromised, including emails. Ms Morgan said: "We discovered the cyber-attack on Wednesday and moved quickly to bring in a team of specialised cyber-technology consultants to investigate. The National Cyber Security Centre will also be providing us with support to resolve matters.
Read the full story here: BBC



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

Credential Stuffing, what is it?

In a world where acronyms and technology phrases are the order of the day, we sometimes get lost in the mumbo jumbo jungle of tech language, especially in the Cyber space. I vaguely remember that some psychology guru once said that if you read something and come across a word or phrase that doesn't make sense, your interest level drops from 100 to 0 percent in 2 seconds flat. Only a small percentage of people will actually take the time to look it up and figure out what it means. A recent conversation I had on the topic prompted me to dedicate some time to this now and again, and today I'll talk about "Credential Stuffing" (What does it actually mean?). Unfortunately, in explaining it, more phrases and acronyms are used, but I'll provide links wherever I can.

Credential Stuffing – Checkpoint describes it as follows: "In a credential stuffing attack, cybercriminals take advantage of weak and reused passwords. Automated bots will take a list of username/password pairs that have been exposed in data breaches and try them on other online accounts. If the user has the same credentials on multiple sites, this provides the attacker with unauthorized access to a legitimate user account."

Anatomy of Attack - How it Works

Credential stuffing attacks use large lists of username/password pairs that have been exposed. In some data breaches, improper credential storage results in the entire password database being leaked. In others, cybercriminals crack some users' passwords via password guessing attacks. Credential stuffers can also gain access to usernames and passwords through phishing and similar attacks.
These lists of usernames and passwords are fed to a botnet (A network of compromised computers that act as slave robots), which uses them to try to log onto certain target sites. For example, the credentials breached by a travel website may be checked against a large banking institution. If any users reused the same credentials across both sites, then the attackers may be able to successfully log into their accounts.
After identifying valid username/password pairs, the cybercriminals may use them for a variety of different purposes, depending on the account in question. Some credentials may provide access to corporate environments and systems, while others may allow attackers to make purchases using the account owner's bank account. A credential stuffing group may take advantage of this access themselves or sell it on to another party.

Credential Stuffing vs. Brute Force Attacks

Brute force password attacks are a general term that covers a few different specific attack techniques. In general, a brute force attack means that the attacker is just trying different combinations for a password until something works.
The term brute force attack is most commonly used to refer to an attack where the attacker is trying every possible option for a password. For example, a brute force attack on an eight-character password may try aaaaaaaa, aaaaaaab, aaaaaaac, etc. While this approach is guaranteed to find the correct password eventually, it is slow to the point of being infeasible for a strong password.
Credential stuffing takes a different approach to guessing a user's password. Instead of looking at all possible password combinations, it focuses on those that are known to have been used by a person because they were exposed in a breach. This approach to password guessing is much faster than a brute force search but it assumes that passwords will be reused across multiple sites. However, since most people reuse the same password for multiple sites, this is a safe assumption to make.

How to Prevent Credential Stuffing

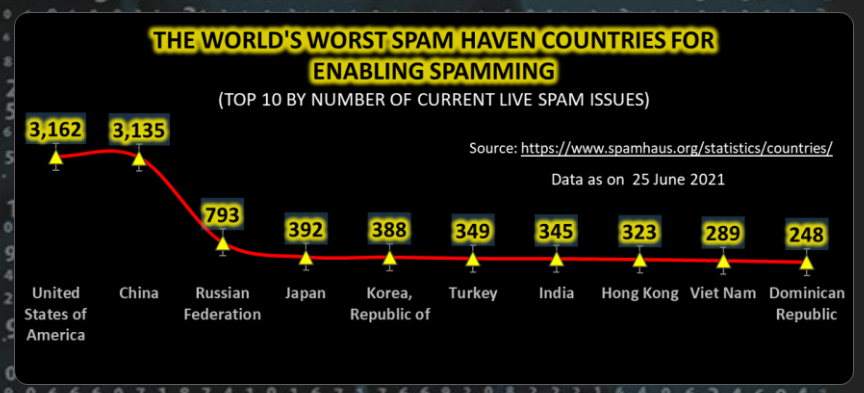
Credential stuffing presents a serious risk to both personal and corporate security. A successful credential stuffing attack gives the attacker access to the user's account, which may contain sensitive information or the ability to perform financial transactions or other privileged actions on the user's behalf. However, despite the well-publicized threat of password reuse, most people are not changing their password behaviours. (Check out The Hacker-Proof Password Formula, by the Leavitt Group)
Credential stuffing can also put the enterprise at risk if passwords are reused across personal and business accounts. Companies can take a few different steps to mitigate the risk of credential stuffing attacks, including:

- **Multi-Factor Authentication (MFA):** Credential stuffing attacks rely on the attacker's ability to log into an account with just a username and password. Implementing MFA or 2FA makes these attacks more difficult because the attacker also needs a one-time code to log in successfully.
- **CAPTCHA**: Credential stuffing attacks are typically automated. Implementing CAPTCHA on login pages can block some of this automated traffic from reaching the site and testing potential passwords.
- Anti-Bot Solutions: Beyond CAPTCHA, organizations can also deploy anti-bot solutions to block credential stuffing traffic. These solutions use behavioural anomalies to differentiate human and automated visitors to a site and to block suspicious traffic.
- **Website Traffic Monitoring**: A credential stuffing attack involves a massive volume of failed login attempts. Monitoring traffic to login pages may allow an organization to block or throttle these attacks.
- **Checking if your Credentials have been Breached**: Credential stuffing bots typically use lists of credentials exposed in data breaches. Checking user passwords against lists of weak passwords or services like HaveIBeenPwned can help to determine if a user's password is potentially vulnerable to credential stuffing. (You can also check the following sites if your credentials have been leaked or stolen: f-secure, Avast, BreachAlarm)

References: Checkpoint, paloalto networks, OWASP, Kaspersky, Leavitt Group, DigitalTrends

Other Interesting News and Cyber Security bits:

- 11 Security Certifications to Seek Out This Summer
- CIS Benchmarks: Configuration guidelines to safeguard systems against cyber threats.
- John McAfee: antivirus entrepreneur found dead in Spanish prison



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