Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On October 12, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Microsoft, Fortinet, Google and Adobe products.
CIS Security Advisories

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

14 October 2022

In The News This Week

Russian military 'exhausted,' Putin's judgment 'flawed,' U.K. spy chief says

LONDON — A British spy chief warned in a rare public speech Tuesday that Russian forces in Ukraine are overstretched and "exhausted" — and that President Vladimir Putin is committing "strategic errors in judgment." The assessment from Jeremy Fleming, head of the secretive GCHQ, Britain's intelligence, cyber and security agency, comes after Putin drafted reservists to bolster his war effort and claimed a "massive strike" across Ukraine this week. The missile attacks hit energy facilities and civilian infrastructure across the country, including in the heart of Kyiv, in retaliation for a weekend explosion on Russia's strategic Crimean Bridge. "Russia's forces are exhausted. The use of prisoners to reinforce, and now the mobilization of tens of thousands of inexperienced conscripts, speaks of a desperate situation," Fleming said. "Far from the inevitable Russian military victory that their propaganda machine spouted, it's clear that Ukraine's courageous action on the battlefield and in ***cyberspace*** is turning the tide," Fleming added. Read the rest of the story by Adela Suliman here: The Washington Post

Pro-Russian Group KillNet Claims Responsibility for 14 US Airport DDoS Attacks

On Monday, October 10, 2022, the websites of several US airports were disrupted due to a large-scale campaign of distributed denial-of-service (DDoS) attacks, in which servers were flooded with web traffic to knock websites offline. The victims include Los Angeles International Airport (LAX), Hartsfield-Jackson Atlanta International Airport (ATL), Chicago O'Hare International Airport (ORD), as well as other airports in Florida, Colorado, Arizona, Kentucky, Mississippi and Hawaii. The DDoS attacks meant that these airports' public-facing websites were either offline for a few hours, intermittent or slow to respond. They did not have any direct impact on airport operations. Some airport authorities, such as LAX, notified the Transportation Security Administration and the FBI about the incident. Later that day, the pro-Russian hacktivist group 'KillNet' claimed the attack and listed 14 targeted domains on a Telegram channel. Read the full story by Kevin Poireault here: Infosecurity

Researchers Warn of New Phishing-as-a-Service Being Used by Cyber Criminals

Cyber criminals are using a previously undocumented phishing-as-a-service (PhaaS) toolkit called Caffeine to effectively scale up their attacks and distribute nefarious payloads. "This platform has an intuitive interface and comes at a relatively low cost while providing a multitude of features and tools to its criminal clients to orchestrate and automate core elements of their phishing campaigns," Mandiant said in a new report. Some of the core features offered by the platform comprise the ability to craft customized phishing kits, manage redirect pages, dynamically generate URLs that host the payloads, and track the success of the campaigns... Read the story by Ravie Lakshmanan here: The Hacker News

Amid reports of JP Morgan cyberattack, experts call Killnet unsophisticated, 'media hungry'

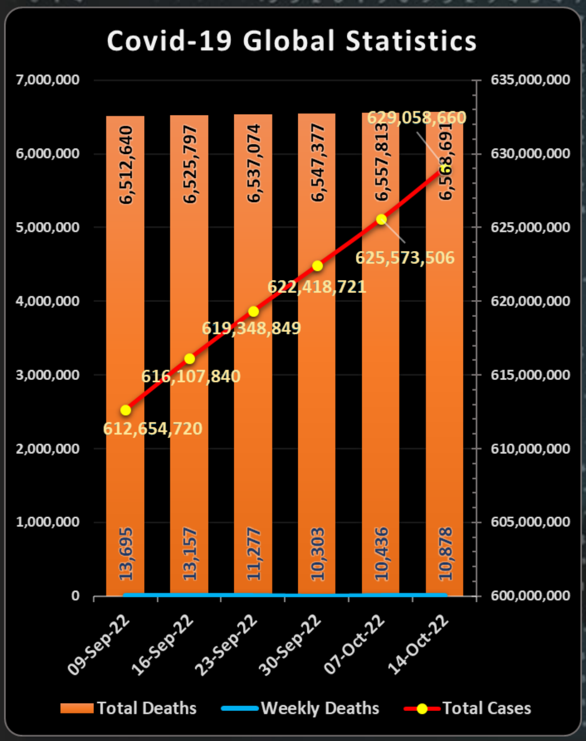
Russian hacktivist group Killnet, well-known for its flair for publicity, made more news today when it reportedly blocked J.P. Morgan's infrastructure, but failed to impact the bank's operations. These reports came one day after Killnet attacked airport websites in 24 states, disrupting service, but causing no real business damage or serious data exfiltration. Security researchers said Killnet's attacks remain relatively unsophisticated and unchanged, but the group is nonetheless persistent with its DDoS attacks. "While DDoS attacks can be classified as a nuisance, if successful, these attacks can result in websites or services being taken down for long periods of time," said Ivan Righi, senior cyber threat intelligence analyst at Digital Shadows. "This threat is notably higher for critical sectors, where even short downtimes can have significant consequences."...
Read the full story by Steve Zurier here: SC Magazine

Modified WhatsApp App Caught Infecting Android Devices with Malware

An unofficial version of the popular WhatsApp messaging app called YoWhatsApp has been observed deploying an Android trojan known as Triada. The goal of the malware is to steal the keys that "allow the use of a WhatsApp account without the app," Kaspersky said in a new report. "If the keys are stolen, a user of a malicious WhatsApp mod can lose control over their account. Typically spread through fraudulent ads on Snaptube and Vidmate, the app, upon installation, requests the victims to grant it permissions to access SMS messages, enabling the malware to enroll them to paid subscriptions without their knowledge. ... Read the story by Ravie Lakshmanan here: The Hacker News

BAE Releases New Cybersecurity System for F-16 Fighter Aircraft

Defense giant BAE Systems has unveiled Viper Memory Loader Verifier II (MLV II), a system whose role is to protect F-16 fighter aircraft against potential cyberattacks. - MLV II is the second version of a maintenance capability that should "reduce vulnerability to cyberattacks for F-16 aircraft". The system is used to load and verify software onto the fighter jet, ensuring that malicious software or files cannot get on the aircraft. The system supports mission data files, flight and fault data, and third-party software. It supports over 100 F-16 onboard systems, including flight- and mission-critical components such as radar, engine control, navigation, communications, crash data recorders, and electronic warfare, mission and flight control.
Read the full story here: BIBS Tech


Covid-19 Global Statistics

For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Cyber criminal services for sale

In our rapidly evolving digital world, Cyber attacks are commonplace, and the scary thing is that the perpetrator no longer needs to be an IT or Cyber expert to execute these attacks. He or she can just go on the Dark Web, pay a nominal fee for the service and the attack will be done on their behalf. Granted that for some of these Dark Web marketplaces, you need to know someone who knows someone who knows someone that can extend an invite to you. But for the most of it, it is quite easy to get onto some marketplaces that offer Phishing as a Service (PhaaS), or Ransomware as a Service (RaaS), and so on. As I reported some time ago, the digital underworld has an economy of its own and is highly lucrative for its equally dark and sinister participants. The business model is fairly simple when an attack is successful and a ransom is paid or data is sold, the service owner gets a cut of the revenue from its affiliate, normally between 25% and 40%. As we read about the new PhaaS called "Caffeine" in the news this week, I want to explore some of the more notorious service offerings available, and hopefully, give you a glimpse into that world.

DarkSide - DarkSide is a RaaS operation associated with a group dubbed by CrowdStrike as CARBON SPIDER. DarkSide operators traditionally focused on Windows machines and have recently expanded to Linux. DarkSide is believed to be based in Eastern Europe, likely Russia. The software checks the system's location and language to avoid machines in former Soviet countries. Darkside is most notable for the US Colonial Pipeline attack in May last year. (Some sources claim that Darkside has retired, but we will wait and see)

REvil – Revil (Ransomware Evil), also known as Sodinokibi or CrandCrab, was identified as the ransomware behind one of the largest ransom demands on record: $10 million. It is sold by criminal group PINCHY SPIDER. They sell RaaS under the affiliate model and typically takes 40% of the profits. REvil recruits affiliates to distribute the ransomware for them, and is though to be based in Russia, as they also do not target Russian organizations, or those in former Soviet-bloc countries.

Dharma - This RaaS trojan has been available on the dark web since 2016 and is mainly associated with remote desktop protocol (RDP) attacks. It was recently associated with attacks from a financially motivated Iranian threat group, but the source code originated in the Ukraine, and was created by an entity called "crss7777". Dharma today has several variants because of the sale and alteration of its source code by numerous malware developers. Affiliates pay for RaaS and then execute targeted attacks themselves by utilizing a standard toolkit. It made news in 2020 when it was used in a massive SPAM campaign in Italy.

LockBit – LockBit (original version also known as the ".abcd" virus), was in development since at least September 2019. LockBit is available as a RaaS, advertised to Russian-speaking users or English speakers with a Russian-speaking guarantor. LockBit is one of the most active groups around and was named as the culprit behind the devastating attack on a French hospital in August this year.

Satan – Satan is a Ransomware trojan offered as a Service (**RaaS**) focusing on Windows machines. It was created by "Cold-As-Ice" and is around since 2016. Following successful infiltration, Satan encrypts stored data using RSA-2048 and AES-256 cryptography. In addition, this virus appends the names of encrypted files with the ".stn", or ".satan". When successful, a ransom note is displayed which contains a unique victim ID and a URL to a TOR payment site.

BulletProftLink – Also know as BulletProofLink, a **PhaaS** that originated in Malaysia and discovered by OSINT in October 2020. It was later investigated by Microsoft after a campaign was identified that used a rather high volume of newly created and unique subdomains—over 300,000 in a single run. Phishing kits distributed via these campaigns are specifically crafted to bypass email threat detection technologies and are available for purchase as stand-alone products. It is notable that the type of large-scale phishing campaigns enabled by BulletProofLink use a "double theft" approach. This tactic, which is intended to increase the threat actor's profits, involves the distribution of credentials stolen in phishing attacks to a secondary server controlled by phishing-as-a-service operators.

EvilProxy – (also known as Moloch) A new phishing-as-a-service (PhaaS) toolkit recently discovered by Resecurity, is being advertised on the criminal underground as a means for threat actors to bypass two-factor authentication (2FA) protections employed against online services. The service is represented in all dark web forums, including XSS, Exploit, and Breached. It's offered on a subscription basis per service for a time period of 10, 20, or 31 days, with the kit available for $400 a month and accessed over the TOR anonymity network after the payment is arranged manually with an operator on Telegram.

Frappo – Also recently discovered and is similar to EvilProxy. "Frappo" a Phishing-as-a-Service (**PhaaS**) operator, provides anonymous billing, technical support, updates, and the tracking of collected credentials via a dashboard. Initially, the service popped up in the Dark Web around 22nd of March, 2021, and has been significantly upgraded since then. The security community believes it will most probably target major Financial Institutions and Online Retailers.

Cerber – Cerber is around since 2016 and is offered on the Darknet as a ransomware-as-a-service (**RaaS**). Said to be created by an entity called "crbr". The attacker licenses Cerber ransomware over the internet and splits the ransom with the developer. For a 40% cut of the ransom, you can sign-up as a Cerber affiliate and deliver all the Cerber ransomware you want.

MacRansom – Not as sophisticated as other offerings but worth mentioning as in 2017 it surfaced on the TOR network as the first RaaS targeting MacOS. This MacRansom variant is not readily available through the portal. It is necessary to contact the author directly to build the ransomware. An analysis at the time by Fortinet shows screenshots of the RaaS on the TOR portal and an email address to contact the author. MacRansom comes equipped with a "trigger time" that allows it to delay the encryption process until a time and date criteria have been met. Once triggered, it can encrypt the entire home drive in under a minute.

Resources: Crowdstrike, Kaspersky, Upguard, ManageEngine, Heimdal Security, Sophos

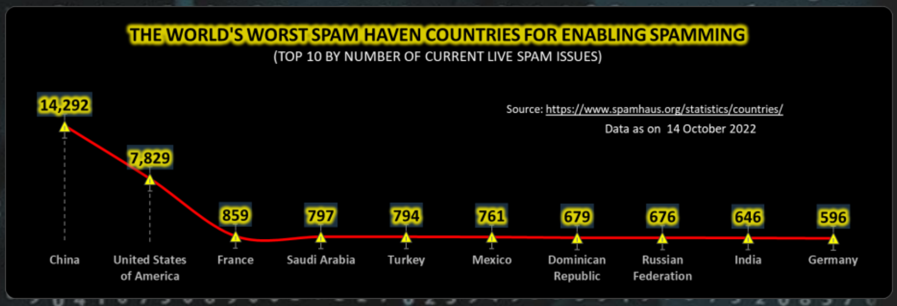
Other Interesting News and Cyber Security bits:

- **FBI and CISA Publish a PSA on Information Manipulation Tactics for 2022 Midterm Elections**
- **Forget about the car: Apple should make an e-bike**
- **The arrival of the first 4G network on the Moon is being prepared**
- **SANS Daily Network Security Podcast (Storm cast)**

flightradar24 LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally

SatelliteXplorer
Track satellites in orbit


THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)
Source: https://www.spamhaus.org/statistics/countries/
Data as on 14 October 2022

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