On September 22, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Siemens, Apple, VMware, and Google products.
See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
24 Sep	231,385,504	4,742,529

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
24 September 2021

In The News This Week

BlackMatter Strikes Iowa Farmers Cooperative, Demands $5.9M Ransom

Critical infrastructure appears to be targeted in latest ransomware attack, diminishing the hopes of governments to curb such attacks. - A ransomware group believed to be the latest incarnation of the infamous DarkSide cybergang is being blamed for taking out a farmers' cooperative online network, with extortionists demanding $5.9 million in ransom. The group BlackMatter is credited for the attack on an Iowa collective of farmers called NEW Cooperative. The incident occurred over the weekend, locking up computer systems. Threat actors behind the attack are demanding a $5.9 million ransom to provide a decryptor, which will increase to **$11.9 million** if not paid in five days, according to reports. The Iowa-based organization is a feed and grain cooperative, with 50 locations. It provides a variety of digital and software services to its network of farmers. As a result of the attack, it had to shut down its operations and also faces the threat of BlackMatter leaking stolen data if it does not pay the ransom, according to reports. This method of double extortion is now common and a hallmark of the former DarkSide group, whose members are believed to now be running the show at BlackMatter.
Read the full story by Elizabeth Montalbano here: ThreatPost

US Sanctions Cryptocurrency Exchange SUEX for Aiding Ransomware Gangs

The U.S. Treasury Department on Tuesday imposed sanctions on Russian cryptocurrency exchange Suex for helping facilitate and launder transactions from at least eight ransomware variants as part of the government's efforts to crack down on a surge in ransomware incidents and make it difficult for bad actors to profit from such attacks using digital currencies. "Virtual currency exchanges such as SUEX are critical to the profitability of ransomware attacks, which help fund additional cybercriminal activity," the department said in a press release. "Analysis of known SUEX transactions shows that over 40% of SUEX's known transaction history is associated with illicit actors. SUEX is being designated pursuant to Executive Order 13694, as amended, for providing material support to the threat posed by criminal ransomware actors." Read the full story by Ravie Lakshmanan here: The Hacker News

PH Army behind cyber-attacks on two alternative media outlets, DICT unit confirms

Metro Manila (CNN Philippines, September 24) — Two alternative media outfits said a unit under the Department of Information and Communications Technology has confirmed that the cyber-attacks on their websites were linked to the Philippine Army. Bulatlat and Altermidya, in a joint statement on Thursday, said Computer Emergency Response Team (CERT-PH) reported that the attacks originated from the internet protocol (IP) address assigned to the Philippine Army. "CERT-PH called DOST and confirmed the IP was assigned to the Philippine Army. This IP was also seen in the provided log file by Bulatlat/Altermidya which is 202.90.137[.].42," the groups said on Thursday. CNN Philippines is seeking confirmation from DICT. "This was similar to the report of Swedish digital forensics group Qurium that "brief but frequent" distributed denial of service (DDOS) attacks against the two websites. DDOS attacks intend to overwhelm a target website with fake traffic, making it inaccessible to users.
Read the full story here: CNN

VoIP company battles massive ransom DDoS attack

Canada-based VoIP provider VoIP.ms is still battling a week-long, massive ransom distributed denial of-service (DDoS) attack. The company, which provides internet telephony services to businesses across the US and Canada, was hit by a DDoS attack on September 16, with the company confirming via Twitter: "At the moment we carry on with the labor of alleviating the effects caused by the massive DDoS directed at our infrastructure. We continue to work full-on re-establishing all of our services so we can have you connected." Read the story here: ZDNet

South African based debt collector hit by massive ransomware attack

Debt-IN Consultants, a debt recovery solutions partner to many South African financial services institutions, says a ransomware attack by cyber criminals has resulted in a significant data breach of consumer and employee personal information. In a statement, Debt-IN Consultants says it is suspected that consumer and personal information of more than 1.4 million South Africans was illegally accessed from Debt-IN servers in April. However, it notes this breach only came to light last week, with the discovery that confidential consumer data and voice recordings posted on Dark Web internet sites. Read the full story here: ITWeb

The Dark Web/Net, what it is, and how to access it

A couple of weeks ago we spoke about how ransomware runs the underground economy. Today, I just want to revisit and write about the place where this so-called underground economy predominantly operates, the "Dark Net" A recent article by the CSO gives us a decent overview of what it is, how to access it, and what you can find. An important note though, the article contains links to dark web sites that can only be accessed with a Tor browser, **but please do not use a Tor browser on your work computer** or network, the security department will not find it very amusing. (The mobile version of Tor is called Onion, and it is in the AppStore)

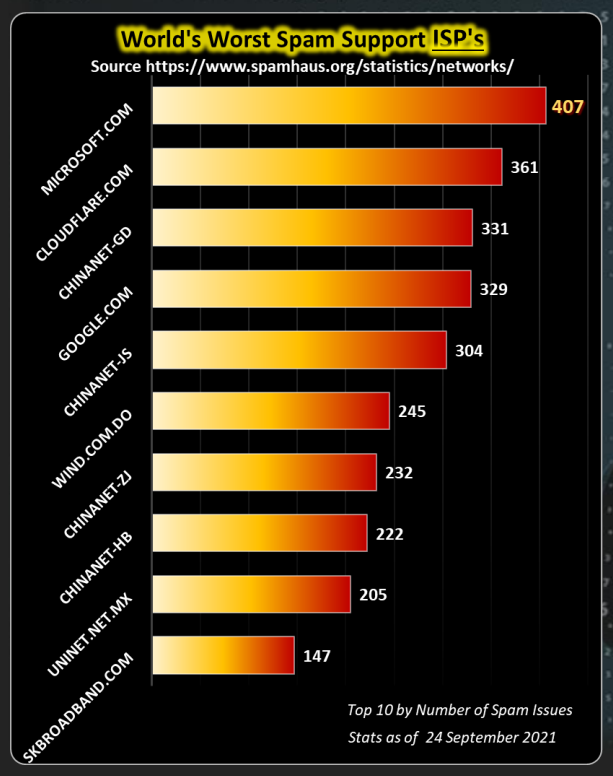
Dark web definition
The dark web is a part of the internet that isn't indexed by search engines. You've no doubt heard talk of the "dark web" as a hotbed of criminal activity — and it is. Researchers Daniel Moore and Thomas Rid of King's College in London classified the contents of 2,723 live dark web sites over a five-week period in 2015 and found that 57% host illicit material. A 2019 study, Into the Web of Profit, conducted by Dr. Michael McGuires at the University of Surrey, shows that things have become worse. The number of dark web listings that could harm an enterprise has risen by 20% since 2016. Of all listings (excluding those selling drugs), 60% could potentially harm enterprises. You can buy credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials and software that helps you break into other people's computers. Buy login credentials to a $50,000 Bank of America account, prepaid debit cards, or a "lifetime" Netflix premium account. You can hire hackers to attack computers for you. You can buy usernames and passwords. Not everything is illegal, the dark web also has a legitimate side. For example, you can join a chess club or BlackBook, a social network described as the "the Facebook of Tor."

Deep web vs. dark web: What's the difference?
The terms "deep web" and "dark web" are sometimes used interchangeably, but they are not the same. Deep web refers to anything on the internet that is not indexed by and, therefore, accessible via a search engine like Google. Deep web content includes anything behind a paywall or requires sign-in credentials. It also includes any content that its owners have blocked web crawlers from indexing. Estimates place the size of the deep web at between 96% and 99% of the internet. Only a tiny portion of the internet is accessible through a standard web browser—generally known as the "clear web". The dark web is a subset of the deep web that is intentionally hidden, requiring a specific browser, "Tor" to access, as explained below. No one really knows the size of the dark web, but most estimates put it at around 5% of the total internet. Again, not all the dark web is used for illicit purposes despite its ominous-sounding name.

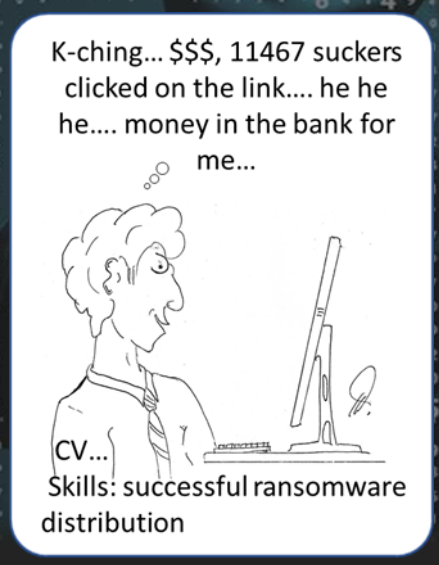
Dark web tools and services
The Into the Web of Profit report identified 12 categories of tools or services that could present a risk in the form of a network breach or data compromise: (1) Infection or attacks, including malware, distributed denial of service (DDoS) and botnets. (2) Access, including remote access Trojans (RATs), keyloggers and exploits. (3) Espionage, including services, customization and targeting. (4) Support services such as tutorials. (5) Credentials (6) Phishing (7) Refunds (8) Customer data (9) Operational data (10) Financial data (11) Intellectual property/trade secrets (12) Other emerging threats.
The report also outlined three risk variables for each category: (a) Devaluing the enterprise, which could include undermining brand trust, reputational damage or losing ground to a competitor. (b) Disrupting the enterprise, which could include DDoS attacks or other malware that affects business operations. (c) Defrauding the enterprise, which could include IP theft or espionage that impairs a company's ability to compete or causes a direct financial loss.
Ransomware-as-a-service (RaaS) kits have been available on the dark web for several years, but those offerings have become far more dangerous with the rise of specialized criminal groups like REvil or GandCrab. These groups develop their own sophisticated malware, sometimes combined with pre-existing tools, and distribute them through "affiliates". The affiliates distribute the ransomware packages through the dark web. These attacks often include stealing victims' data and threatening to release it on the dark web if the ransom isn't paid. This business model is successful and lucrative. IBM Security X-Force, for example, reported that 29% of its ransomware engagements in 2020 involved REvil. The criminal groups that developed the malware gets a cut of the affiliates' earnings, typically between 20% and 30%. IBM estimates that REvil's profits in the past year were $81 million.

Dark web browser & search engines.
All this activity, this vision of a bustling marketplace, might make you think that navigating the dark web is easy. It isn't. The place is as messy and chaotic as you would expect when everyone is anonymous, and a substantial minority are out to scam others. Accessing the dark web requires the use of an anonymizing browser called Tor. The Tor browser routes your web page requests through a series of proxy servers operated by thousands of volunteers around the globe, rendering your IP address unidentifiable and untraceable. Tor works like magic, but the result is an experience that's like the dark web itself: unpredictable, unreliable and maddeningly slow. Dark web search engines exist, but even the best are challenged. Even one of the best search engines, called Grams, returns results that are repetitive and often irrelevant to the query. Link lists like The Hidden Wiki and Dogpile are other options.

Dark web sites
Dark web sites look pretty much like any other site, but there are important differences. One is the naming structure. Instead of ending in .com or .co, dark web sites end in .onion. Browsers with the appropriate proxy can reach these sites, but others can't. Dark web sites also use a scrambled naming structure that creates URLs that are often impossible to remember. For example, "Dream Market" goes by the unintelligible address of "eajwlvm3z2lcca76.onion."
----- Unfortunately, that is all I have space for in this post… please visit CSO to read the rest of the article. (or Another source)

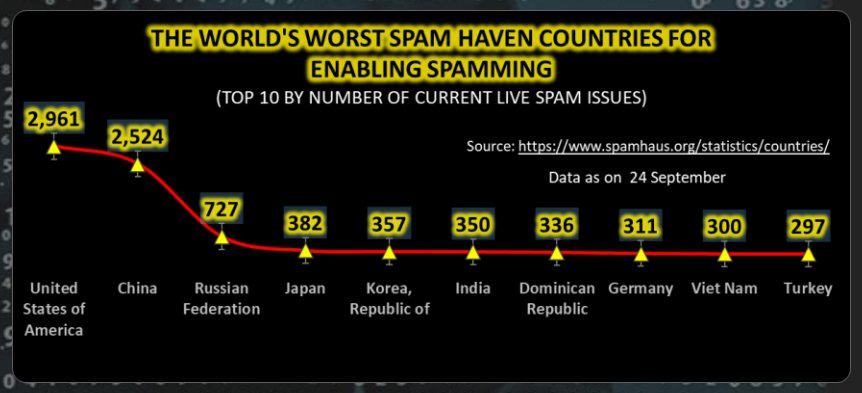


For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov



Other Interesting News and Cyber Security bits:

- OWASP updates top 10 vulnerability ranking for first time since 2017
- Verizon-plans-to-fight-quantum-attacks-with-these-quantum-safe-vpns
- AI Is Capable of Generating Misinformation and Fooling Cybersecurity Experts



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