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

On August 3, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Samba, Grails and Google products. (No further updates this week)
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

12 August 2022

In The News This Week

Cisco Confirms It's Been Hacked by Yanluowang Ransomware Gang

Networking equipment major Cisco on Wednesday confirmed it was the victim of a cyberattack on May 24, 2022 after the attackers got hold of an employee's personal Google account that contained passwords synced from their web browser. "Initial access to the Cisco VPN was achieved via the successful compromise of a Cisco employee's personal Google account," Cisco Talos said in a detailed write-up. "The user had enabled password syncing via Google Chrome and had stored their Cisco credentials in their browser, enabling that information to synchronize to their Google account."The disclosure comes as cybercriminal actors associated with the Yanluowang ransomware gang published a list of files from the breach to their data leak site on August 10. The exfiltrated information, according to Talos, included the contents of a Box cloud storage folder that was associated with the compromised employee's account and is not believed to have included any valuable data.
Read the rest of the post by Ravie Lakshmanan here: The Hacker News

Hackers issue 'ransom demands' to NHS IT supplier

United Kingdom - Fears MILLIONS of confidential patient records could be leaked after major cyber attack - Hackers are holding an IT firm that supplies NHS trusts to ransom following a cyber attack last week, according to sources. Health bosses are concerned criminals have access to confidential health records and could leak them if their demands aren't met. Call handlers across 85 per cent of the country are still without a crucial IT system and have had to resort to using pen and paper for the past week. Agencies including the National Crime Agency and GCHQ are now investigating the data breach. A source close to the investigation said the attackers have made 'some demands', according to the Health Service Journal, although it is not entirely clear what they are. But there is a suggestion cyber criminals are looking for payments in exchange for not leaking information and removing the malware. Read the article by Joe Davies here: Daily Mail

A massive cyberattack hit the website of the German Chambers of Industry and Commerce (DIHK)

Germany - A massive attack hit the website of the German Chambers of Industry and Commerce (DIHK) forcing the organization to shut down its IT systems as a precautionary measure for security reasons. - "Due to a possible cyber attack, the IHK organization has shut down its IT systems as a precautionary measure for security reasons . We are currently working intensively on a solution and defense. The IT systems are successively started up after testing, so that the services are then available again for companies." reads the announcement published by the German Chambers of Industry and Commerce (DIHK). DIHK states that phone and fax are the only channels to use to contact it.
Michael Bergmann, chief executive of DIHK, defined the attack as serious and massive, it also added that the organization was not able to estimate how long its systems will be down. Bergmann did not provide further details about the attack, but the circumstances suggest the German Chambers of Industry and Commerce was the victim of a ransomware attack. Read the article by Pierluigi Paganini here: Security Affairs

BazarCall attacks have revolutionized ransomware operations

BazarCall attack, aka call back phishing, is an attack vector that utilizes targeted phishing methodology and was first used by the Ryuk ransomware gang in 2020/2021. The BazarCall attack chain is composed of the following stages: Stage One - Attackers send a mail to the victims that notify them that they have subscribed to a service for which payment is automatic. The email includes a phone number to call to cancel the subscription. Stage Two - The victim is tricked into contacting a special call center. When operators receive a call, they use a variety of social engineering tactics, to convince victims to give remote desktop control, to help them cancel their subscription service. Stage Three - Once accessed the victim's desktop, the attacker silently extended a foothold in the user's network, weaponizing legitimate tools that are known to be in Conti's arsenal. The initial operator remains on the line with the victim, pretending to assist them with the remote desktop access by continuing to utilize social engineering tactics. Stage Four - The initiated malware session yields the adversary access as an initial point of entry into the victim's network..
Read the rest of the article by Pierluigi Paganini here: Security Affairs

The Hacking of Starlink Terminals Has Begun

It cost a researcher only $25 worth of parts to create a tool that allows custom code to run on the satellite dishes. - Since 2018, Elon Musk's Starlink has launched more than 3,000 small satellites into orbit. This satellite network beams internet connections to hard-to-reach locations on Earth and has been a vital source of connectivity during Russia's war in Ukraine. Thousands more satellites are planned for launch as the industry booms. Now, like any emerging technology, those satellite components are being hacked.
Lennert Wouters, a security researcher at the Belgian university KU Leuven, reveal one of the first security breakdowns of Starlink's user terminals, the satellite dishes (dubbed Dishy McFlatface) that are positioned on people's homes and buildings at the Black Hat security conference in Las Vegas. Wouters detailed how a series of hardware vulnerabilities allow attackers to access the Starlink system and run custom code on the devices..... Read the full the story by Matt Burgess here: Wired

Automotive hacking – the cyber risk auto insurers must consider

Up until the last few years, criminals hacking into your car and taking control seemed like the stuff of Hollywood movies. Not so today, as vehicles become increasingly connected. Global sales of connected cars are expected to surge to 115 million in 2025, from around 30 million sold in 2020, according to ABI Research. But the rise of smart, connective technology in vehicles has also exposed new weaknesses that hackers can exploit. A report by Upstream Security revealed that automotive cyber security incidents spiked 225% from 2018 to 2021. The majority (85%) of global attacks were conducted remotely. "When you think about how thefts of vehicles happened traditionally, somebody needed to hotwire or manually break into a vehicle,"... "Now you have more connectivity that potentially leads to more access points in the vehicle, as well as through the fobs that are used to access and remotely start them.".. Read the full post by Gia Snape here: InsuranceBusinessMag

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

The Dark Web or Deep Web keeps on popping up in conversations I have and all end up asking me, what the Dark Web really is. I have written about it previously and not much has changed since then, and I, therefore, decided to re-post the previous write-up, with a few updates, for those who missed out.
An 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 websites 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."

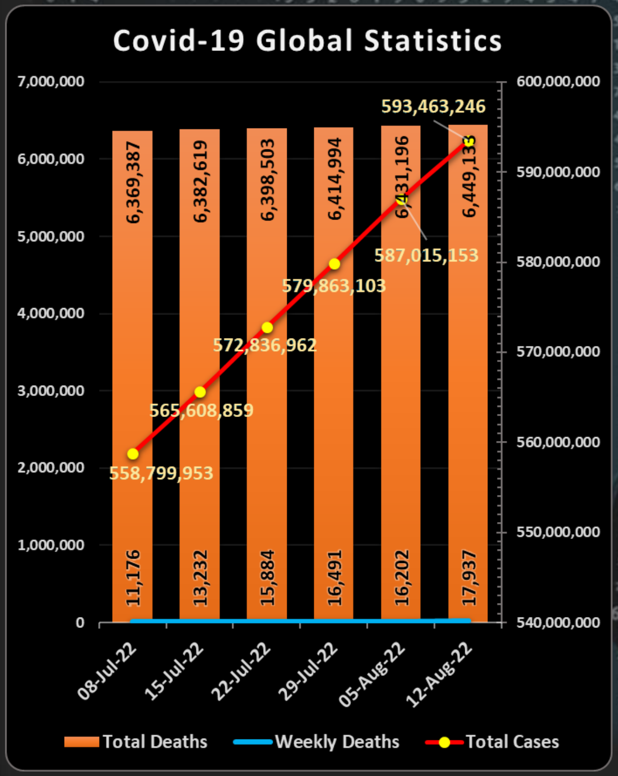
Deep web vs. dark web: What's the difference? - The terms "deep web" and "dark web" are sometimes used interchangeably, but they are not the same. Deep web refers to anything on the internet that is not indexed by and, therefore, accessible via a search engine like Google. Deep web content includes anything 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. Kilos, the successor of the now defunct Grams search engine still returns results that are repetitive and often irrelevant to the query. Link lists like The Hidden Wiki, Dogpile, and many more, are other options you can explore.

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. You can also read more here: Comparitech Step-by-Step Guide, Heimdal Security Step-by-Step Guide


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

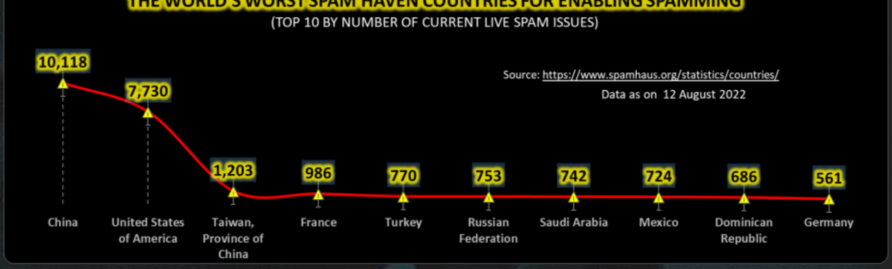
Olly, they say you have to deep dive into the dark web, with a special Tor something or another, but I didn't bring my swimming trunks today.
Stanley, I think we must surely check out this dark web thing everyone is on about. How do we get in?

Other Interesting News and Cyber Security bits:

- Black Hat - This Mac hacker's code is so good, corporations keep stealing it
- Zoom in – World map by Satellites Pro
- Surprise attack on Russian airfield destroyed as many as 13 war planes, satellite photos show
- Russia launches Iranian satellite into space from Kazakhstan base
- SANS Daily Network Security Podcast (Storm cast)

flightradar24
LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally


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 12 August 2022

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