Among 121 SARS-CoV-2-associated deaths among persons aged <21 years reported to US CDC by July 31, 2020, 12 (10%) were infants and 85 (70%) were aged 10-20 years. 33% of deaths occurred outside of a hospital. Ongoing surveillance should be continued as schools reopen in the US.

Ongoing surveillance for SARS-CoV-2-associated infection, hospitalization, and death among persons aged <21 years should be continued as schools reopen in the United States.Persons aged <21 years constitute 26% of the U.S. population (4), and this report describes characteristics of U.S. persons in that population who died in association with SARS-CoV-2 infection, as reported by public health jurisdictions.Careful monitoring of SARS-CoV-2 infections, deaths, and other severe outcomes among persons aged <21 years remains particularly important as schools reopen in the United States.Persons aged <21 years who met the definition for a SARS-CoV-2-associated death and died during February 12-July 31, 2020, were included in this study.Fifty states, New York City, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands were asked to submit information on SARS-CoV-2-associated deaths among persons aged <21 years, including COVID-19 or MIS-C case status (as determined by each jurisdiction), demographics, dates of illness onset and hospitalization, underlying medical conditions, and location of death.These racial/ethnic groups are also disproportionately represented among essential workers unable to work from their homes (7), resulting in higher risk for exposure to SARS-CoV-2 with potential secondary transmission among household members, including infants, children, adolescents, and young adults.The findings in this report are subject to at least five limitations.More detailed review of available medical and death records is currently underway in collaboration with public health jurisdictions.Jasmine Abdelnabi, Judy Chen, Marie S. Dorsinville, Meredith Eddy, Michele English, Kevin Guerra, Fabiana Jeanty, Lucretia Jones, Kenya Murray, Marc Paladini, John Paul Quinn, Gloria E. Rivera, Brian Toro, New York City Department of Health and Mental Hygiene; Kimberly D. Machesky, Ohio Department of Health; Courtney Dewart, Ohio Department of Health and Epidemic Intelligence Service, CDC.Atlanta, GA: US Department of Health and Human Services, CDC; 2020. https://wonder.cdc.gov/population-projections-2014-2060.html Kim L, Whitaker M, O'Halloran A, et al.; COVID-NET Surveillance Team.US Department of Health and Human Services, CDC; 2020. https://www.cdc.gov/coronavirus/2019-ncov/community/health-equity/race-ethnicity.html Lange SJ, Ritchey MD, Goodman AB, et al.Among these, date of report to CDC was missing for 34,538 cases not shown here.Demographic and clinical characteristics of SARS-CoV-2-associated deaths among persons aged <21 years -- United States, February 12-July 31, 2020* CharacteristicNo.(%) Total 121 (100) Age group, yrs <112 (9.9)1-411 (9.1)5-913 (10.7)10-1312 (9.9)14-1723 (19.0)18-2050 (41.3)Age, yrs, median (IQR)16 (7-19) Sex Female45 (37.2)Male76 (62.8) Race/Ethnicity Hispanic54 (44.6)American Indian/Alaska Native, non-Hispanic5 (4.1)Asian or Pacific Islander, non-Hispanic5 (4.1)Black, non-Hispanic35 (28.9)White, non-Hispanic17 (14.0)Multiple/Other + 2 (1.7)Missing/Unknown3 (2.5) SARS-CoV-2-associated condition SS COVID-19120 (99.2)MIS-C15 (12.4) Underlying medical condition P No underlying condition30 (24.8)>=1 underlying condition91 (75.2)>=2 underlying conditions54 (44.6)Chronic lung disease**34 (28.1)Obesity ++ 33 (27.3)Neurologic and developmental SSSS 26 (21.5)Cardiovascular disease PP 22 (18.2)Cancer or immunosuppressive condition***17 (14.0)Diabetes mellitus +++ 11 (9.1)Chronic kidney disease5 (4.1)Chronic liver disease3 (2.5)Other PPP 37 (30.6) Location of death Home16 (13.2)Emergency department23 (19.0)Hospital79 (65.3)Other/Unknown3(2.5) Median interval from symptom onset to hospital admission, days (IQR)**** 3 (1-7) Median interval from hospital admission to death, days (IQR) ++++ 8 (4-21.5) Median interval from symptom onset to death, days (IQR) SSSSSSSS 11 (6-24) Abbreviations: COVID-19 = coronavirus disease 2019; IQR = interquartile range; MIS-C = multisystem inflammatory syndrome in children.* Persons aged <21 years were included if they were reported by state and local health departments as meeting case definitions for COVID-19 (https://wwwn.cdc.gov/nndss/conditions/coronavirus-disease-2019-covid-19/case-definition/2020/) or MIS-C (https://www.cdc.gov/mis-c/hcp/) with a fatal outcome that occurred before August 1, 2020.++ Decedents with body mass index >=30 kg/m 2 at or above the 95th percentile for age and sex.Suggested citation for this article: Bixler D, Miller AD, Mattison CP, et al. SARS-CoV-2-Associated Deaths Among Persons Aged <21 Years -- United States, February 12-July 31, 2020.CDC is not responsible for the content of pages found at these sites.All HTML versions of MMWR articles are generated from final proofs through an automated process.Questions or messages regarding errors in formatting should be addressed to mmwrq@cdc.gov .

Transport bosses in Greater Manchester confirmed a snake was not a valid face covering.

image captionOne passenger thought the snake was a "funky mask" before she saw it moveA man boarded a bus using a snake as a face covering.The commuter and his reptilian mask, which was wrapped around his neck and mouth, were seen on a bus from Swinton to Manchester on Monday.One passenger, said she thought the passenger was wearing a "funky mask" until she spotted it slithering over hand rails.Transport bosses in Greater Manchester confirmed a snake was not a valid face covering.The eyewitness, who asked to remain anonymous, said she found the incident "really funny", adding the animal did not seem to be bothering any of her fellow passengers.She said: "No-one batted an eyelid."image captionTransport for Greater Manchester said a snake was not a valid face coveringUsing a face covering on public transport is mandatory, except for children under the age of 11 or those who are exempt for health or disability reasons.A Transport for Greater Manchester spokesperson said: "Government guidance clearly states that this needn't be a surgical mask, and that passengers can make their own or wear something suitable, such as a scarf or bandana."While there is a small degree of interpretation that can be applied to this, we do not believe it extends to the use of snakeskin - especially when still attached to the snake."Why not follow BBC North West on Facebook , Twitter and Instagram ?You can also send story ideas to northwest.newsonline@bbc.co.uk

Virus Strands Hasidic Pilgrims on Ukraine-Belarus Border

Hundreds of Jewish pilgrims seeking to travel from Belarus to Ukraine to visit the grave of a revered rabbi were barred from entering because of virus restrictions.Jewish pilgrims visiting the grave of Rabbi Nachman in Uman, Ukraine, on Tuesday.Thousands of Israeli Hasidic Jews visit the town to celebrate Rosh Hashanah each year.Credit...Marian Kushnir/ReutersThey slumped in exhaustion on their luggage.For a second night in a row, hundreds of Hasidic Jewish pilgrims remained outdoors along a road between checkpoints on the border between Ukraine and Belarus on Tuesday, stranded by coronavirus travel restrictions.As Covid-19 cases in the country ticked up, Ukraine closed its borders last month, blocking the pilgrimage, which typically draws tens of thousands of people, many coming from Israel.Israeli health officials have supported Ukraine's decision.The pilgrims began arriving at a border crossing with Belarus on Monday afternoon, according to the Ukrainian border guard service.Authorities in Belarus let the group pass, and they gathered on a road in the buffer area between the two border stations.The Ukrainian and Israeli governments issued a joint statement asking pilgrims to cancel their trip because of the coronavirus.Credit...Breslev Live, via ReutersLittle boys, looking bored and sleepy, stood by watching.The pilgrims traveled to the Novi Yarylovychi border crossing after Belarus announced that it was open, Israel Public Broadcasting said in a tweet .Ukrainian authorities said the pilgrims had been warned about the border closure beforehand.Ukraine's border guard service said that 690 pilgrims had gathered along the border by Tuesday, and the agency's director, Serhiy Deyneko, said that more were expected on charter flights arriving in Belarus.Belarusian media reported a different number of pilgrims on the border, saying about 1,500 had already arrived.President Volodymyr Zelensky of Ukraine, who is Jewish, said that the border closure would be enforced."The State Border Service has enough forces and means for reliable protection of the state border," a presidential office statemen t said.Guards were reinforcing the border with a secondary barrier, several hundred yards inside Ukraine.Ukraine on Tuesday reported 2,905 new cases of coronavirus in the past 24 hours.The country's ban on foreign visitors, instituted last month, is in place until Sept. 28.

A non-academic recap of our newest peer-reviewed paper on pollution in humpback whales from Antarctica. Whales in our study had the lowest levels of man-made chemicals ever measured for the species. Good news for these populations, still recovering from industrial whaling.

We found long-banned pesticides and industrial pollutants in the blubber of humpback whales from Antarctica , suggesting these contaminants accumulate in Antarctic food webs.Our study on humpback whales from Antarctica just got published in Environmental Pollution and it is my first publication as a first author.Here is an explanation of the study in a non academic way with our main findings.Humpback whales we sampled for our project on pollution in Antarctica - Pierre GallegoIn particular, a type of man-made chemicals called " persistent organic pollutants " (POPs) include long banned industrial chemicals like PCBs and pesticides like DDT .These contaminants are persistent, meaning that even decades after their ban, they still circulate in the atmosphere and end up in Antarctica .They carry useful information from their feeding zones all around Antarctica.Since persistent organic pollutants accumulate in food webs, Humpback whales can give us a representation of which contaminants reach Antarctica and accumulate in Antarctic food webs .We just need to measure these chemicals in their blubber, where they are the most abundant.The goal of our research was to determine southern humpback whales feeding habits and measure their contaminants levels to help us measure pollution in Antarctica.To do so, we used samples of about 150 whales we sampled in both Ecuador and Mozambique , where they breed after they complete their migration.These Ecuador whales feed close to South America in the Antarctic Peninsula.The pesticide we found in the highest concentration is called hexachlorobenzene : a fungicide used in wheat agriculture was banned decades ago as well.This chemical is very volatile, like most persistent organic pollutants, and travels through the atmosphere to redeposit in Antarctica.Pollutant levels were low, so they are not a direct threat to the whales' health .Humpback whale from our sampling season in Mozambique - Pierre GallegoFor more information, you can read our just published peer-reviewed paper in Environmental Pollution .If you wish to know how exactly we did our analyses, let me know so I can write about it.Do not hesitate to share the good news everywhere!She is a PhD student at McGill University working on killer whale ecology and pollution.

Families meeting would break the rules

Media playback is unsupported on your deviceMedia captionHome Secretary Priti Patel explains why "mingling" is against the latest Covid-19 restrictionsFamilies stopping to talk in the street would be in breach of the rule of six restrictions, the home secretary has said.Priti Patel told the BBC that two families of four stopping for a chat on the way to the park was "absolutely mingling".The new measures mean police can break up groups larger than six, with fines of up to PS3,200 if people flout the rules.Speaking to BBC Radio 4's Today programme, Ms Patel said that two families of four stopping for a chat on the way to the park was "absolutely mingling"."You have got to put this in the context of coronavirus and keeping distance, wearing masks," she said."The rule of six is about making sure that people are being conscientious and not putting other people's health at risk."The home secretary added: "Mingling is people coming together.That is my definition of mingling."When asked if she would call the police on her neighbours if they breached the new coronavirus rules, Ms Patel told BBC Breakfast: "I don't spend my time looking into people's gardens."Pressed further on the topic, she said anybody would want to "take responsibility" to help to stop the spread of the virus, adding that if she saw gatherings of more than six, "clearly I would report that".It comes as the national chairman of the Police Federation of England and Wales called for guidance over enforcement of the measures.Speaking to Good Morning Britain, John Apter said that police officers on the frontline were "trying to interpret" the rules, and were being accused of "asking (people) to snitch on their neighbours".He added: "Maybe we should have guidance, because we haven't had any yet."Government guidelines include exemptions for physical activities that can be done in groups of more than six, such as football, hockey and netball, as well as sailing, angling and polo.Shooting - including hunting and paintball that requires a shotgun or firearms certificate licence - is also exempt as an organised sport.Earlier, Ms Patel defended the government's record on testing, following widespread reports of people struggling to get swabbed.She told BBC Breakfast the government was "surging capacity" where it was needed.Media playback is unsupported on your deviceMedia captionPriti Patel challenged on coronavirus testing delays"Clearly there is much more work that needs to be undertaken with Public Health England and the actual public health bodies in those particular local areas, and as a government obviously we work with Public Health England to surge where there is demand in local hotspot areas."

https://lg.lc/3/index.php?url=>944 2020-09-15 15:35:21

OneFuzz - A self-hosted Fuzzing-As-A-Service platform by Microsoft

Project OneFuzz enables continuous developer-driven fuzzing to proactively harden software prior to release.With a single command, which can be baked into CICD, developers can launch fuzz jobs from a few virtual machines to thousands of cores.This project welcomes contributions and suggestions.Most contributions require you to agree to a Contributor License Agreement (CLA) declaring that you have the right to, and actually do, grant us the rights to use your contribution.For details, visit https://cla.opensource.microsoft.com .When you submit a pull request, a CLA bot will automatically determine whether you need to provide a CLA and decorate the PR appropriately (e.g., status check, comment).Simply follow the instructions provided by the bot.You will only need to do this once across all repos using our CLA.

https://lg.lc/3/index.php?url=>913 2020-09-15 19:47:11

AboutPressCopyrightContact usCreatorsAdvertiseDevelopersTermsPrivacy Policy and SafetyHow YouTube worksTest new features Super Mario Bros. 3 in 3 minutes - World Record Speedrun Explained - YouTube

Super Mario Bros. 3 in 3 minutes - World Record Speedrun Explained

https://lg.lc/3/index.php?url=>994 2020-09-14 08:32:17

Featured PortalsArticles by TopicFeatured PortalsArticles by Topic

Researchers measured growth and milk output in two lactating mammals, mice and striped hamsters, at temperatures between 21-33C. They found differences in milk production, growth, & mortality, suggesting lactation is a period particularly vulnerable to ambient temperatures (and thus climate change).

https://lg.lc/3/index.php?url=>967 2020-09-15 18:56:36

Yoshihide Suga elected Japanese prime minister

Keep abreast of significant corporate, financial and political developments around the world.Stay informed and spot emerging risks and opportunities with independent global reporting, expert commentary and analysis you can trust.

https://lg.lc/3/index.php?url=>926 2020-09-16 11:44:21

Dismiss GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.Sign up No description, website, or topics provided.rootxharsh Harsh Jaiswal iamnoooob Rahul Maini

CVE-2020-15505 - [RCE on MobileIron MDM]

https://lg.lc/3/index.php?url=>836 2020-09-13 20:08:57

Europe PMC is an ELIXIR Core Data Resource Learn more >

Understanding ER+ Breast Cancer Dormancy Using Bioinspired Synthetic Matrices for Long-Term 3D Culture and Insights into Late Recurrence. - Abstract

https://lg.lc/3/index.php?url=>957 2020-09-15 15:56:53

Error502 Server Error: Bad Gateway for url: http://news.nau.edu/global-warming-study/

In the past 150 years, global warming has more than undone the global cooling that occurred over the past six millennia, according to a major study

https://lg.lc/3/index.php?url=>958 2020-09-15 18:36:38

AboutPressCopyrightContact usCreatorsAdvertiseDevelopersTermsPrivacy Policy and SafetyHow YouTube worksTest new features Aung San Suu Kyi falls from grace as humanitarian icon | DW News - YouTube

Suu Kyi and her fall from grace... Heartbreaking

https://lg.lc/3/index.php?url=>983 2020-09-16 01:10:39

Study shows difficulty in finding evidence of life on Mars. The researchers conducted simulations involving clay and amino acids to draw conclusions regarding the likely degradation of biological material on Mars.

In a little more than a decade, samples of rover-scooped Martian soil will rocket to Earth.While scientists are eager to study the red planet's soils for signs of life, researchers must ponder a considerable new challenge: Acidic fluids - which once flowed on the Martian surface - may have destroyed biological evidence hidden within Mars' iron-rich clays, according to researchers at Cornell and at Spain's Centro de Astrobiologia.Alberto G. Fairen, a visiting scientist in the Department of Astronomy in the College of Arts and Sciences, is a corresponding author.NASA's Perseverance rover, launched July 30, will land at Mars' Jezero Crater next February; the European Space Agency's Rosalind Franklin rover will launch in late 2022.The Perseverance mission will collect Martian soil samples and send them to Earth by the 2030s.The Rosalind Franklin rover will drill into the Martian surface, collect soil samples and analyze them in situ.In the search for life on Mars, the red planet's clay surface soils are a preferred collection target since the clay protects the molecular organic material inside.However, the past presence of acid on the surface may have compromised the clay's ability to protect evidence of previous life."We know that acidic fluids have flowed on the surface of Mars in the past, altering the clays and its capacity to protect organics," Fairen said.He said the internal structure of clay is organized into layers, where the evidence of biological life - such as lipids, nucleic acids, peptides and other biopolymers - can become trapped and well preserved.In the laboratory, the researchers simulated Martian surface conditions by aiming to preserve an amino acid called glycine in clay, which had been previously exposed to acidic fluids."We used glycine because it could rapidly degrade under the planet's environmental conditions," he said."It's perfect informer to tell us what was going on inside our experiments."Exposure to acidic fluids erases the interlayer space, turning it into a gel-like silica."When clays are exposed to acidic fluids, the layers collapse and the organic matter can't be preserved.They are destroyed," Fairen said."Our results in this paper explain why searching for organic compounds on Mars is so sorely difficult."The paper's lead author was Carolina Gil-Lozano of Centro de Astrobiologia, Madrid and the Universidad de Vigo, Spain.NASA/JPL/Caltech/Provided NASA's Perseverance rover, shown in this artistic rendering, will land at Mars' Jezero Crater in February 2021 and will start gathering soil samples soon after that.Scientists are now concerned about acidic fluids, once on Mars, may have ruined the evidence of life contained in the clays.

https://lg.lc/3/index.php?url=>950 2020-09-15 20:08:57

A Technical Analysis of the 4k Facebook Pishing Scam

tl;dr : Don't trust webview logins on native apps, they can read your cookies and use them to their advantage.Following the Hacker News thread " How I lost EUR4k in a Facebook scam ", we reverse engineered the app to see how this happens.How did Niek, a tech-savvy user who owns an e-commerce business, fell for this kind of attack?Instagram, TikTok, and even your local newspaper, there is almost always a need for user authentication to use any app.In the case of Facebook, for example, Android SDK presents the user with an overlay and asks the user to log into Facebook using his or her username and password.What happens when you involve Webviews in the login process?Any android app using a webview has full access to any data stored by the website - session storage, local storage, and most importantly, cookies.Niek isn't a typical user; He runs an e-commerce, online marketing and consultancy.I have 2FA on all my accounts, use a password manager, and I'm generally very cautious with account security.Niek trusted logging into the malicious app by using his Facebook username and password.But little did he know that the app he downloaded was malicious, and used webview to steal his Facebook cookies, log into his account, and steal EUR4k from him.Let's have a peak behind the scenes of Tiktok Ads Business, the malicious app that he downloaded.Niek opens the app, clicks on the big FB button, and is presented with a webview with Facebook's mobile page on it.After he logs in, the app runs this very simple line of code, taken from a decompilation of the app we did here at Sayfer:Too simple really - any user logging into any website through a webview on an app, is at risk of giving away full ownership of his or her account.A change is needed on two different levels.This makes users trust them too much, and results in users falling victim for real webview cookies hijacking scams.Secondly, a technical change is needed in Android's implementation of webview.Apps shouldn't be allowed to access the cookies of any website they load.Webviews should be sandboxed, and the app should communicate with it via a very thin and limited API, to prevent them from hijacking user credentials.

https://lg.lc/3/index.php?url=>911 2020-09-15 18:16:06

FIN6 Adversary Emulation Plan and Library

We are excited to announce the publication of the MITRE Engenuity Center for Threat-Informed Defense's (Center) FIN6 adversary emulation plan .On September 10, 2020 we announced the establishment of a public library of adversary emulation plans designed to enable red teams and cyber defenders to systematically test their defenses based on real-world adversary Tactics, Techniques, and Procedures (TTPs).As we discussed in last week's blog, we have brought together the combined knowledge and expertise of our Center Participants to create these intelligence driven resources.The plan itself is now available on GitHub.The FIN6 Intelligence Summary outlines 15 publicly available sources to describe FIN6, their motivations, objectives, and observed target industries.FIN6 is thought to be a financially motivated cyber-crime group.The group has aggressively targeted and compromised high-volume POS systems in the hospitality and retail sectors since at least 2015.Most of the group's targets have been located in the United States and Europe, but include companies in Australia, Canada, Spain, India, Kazakhstan, Serbia, and China1.The Intel Summary further describes the typical FIN6 Operation along with their publicly attributed TTPs and their most often used software, mapped to MITRE ATT&CK(r).Finally, the Intelligence Summary provides ATT&CK Navigator layers, separately illustrating FIN6 interactive TTPs (seen below) from the TTPs associated with each of their Software platforms.These scenarios will vary based on the adversary and available intelligence, but typically follow a sequential progression of how the actor breaches then works towards achieving their operational objectives within a victim environment (espionage, data/system destruction, etc.).The FIN6 Operations Flow chains techniques together into a logical flow of the major steps that commonly occur across FIN6 operations.Based on publicly available reporting, we found that FIN6 operations over time have typically been directed against: Point of Sale (POS) systems, e-commerce web-facing systems, and deploying ransomware to enterprise environments.The Emulation Plan includes an overview of each phase, an administrative section describing pre-requisites (toolsets required, supporting infrastructure, etc), and the Emulation Plan itself.The FIN6 Emulation Plan is organized into two phases.At that point, it walks the practitioner through discovery, privilege escalation, collection, and exfiltration TTPs reported to have been used by FIN6.Phase 2 , the operational effects phase, describes lateral movement, persistence, collection, and exfiltration, in 3 distinct scenarios as defined in the Operations Flow.Organizations can also choose to further customize the scenarios and/or behaviors within each emulation plan to better fit their specific environment, priorities, or to be shaped by additional intelligence.The Center is a non-profit, privately funded research and development organization currently comprised of 23 organizations from around the globe with highly sophisticated security teams.Together with our Participants, the Center builds on MITRE ATT&CK(r), an important foundation for threat-informed defense used by security teams and vendors in their enterprise security operations.

https://lg.lc/3/index.php?url=>912 2020-09-15 21:11:01

Mexico identifies submerged wreck of Mayan slave ship

Archaeologists in Mexico have identified a ship that carried Mayan people into slavery in the 1850s - the first time such a ship has been found.The ship was used to take Mayas captured during an 1847-1901 rebellion known as the "War of the Castes" to work in sugarcane fields in Cuba.(AP/AAP)Slavery was illegal in Mexico at the time, but operators of similar ships had reportedly bought seized captured combatants, or deceived Mayas left landless by the conflict to "sign on" as contract workers, often in Cuba, where they were treated like slaves.The La Union was on a trip to Havana in September 1861 when its boilers exploded, and it sank off the once-important port of Sisal, in the Mexican state of Yucatan.The ship was found about 3.7 kilometres off the port of Sisal in about 7 metres of water, after a local fisherman led archaeologists to the wreck.The unknown little town that could be hiding the Holy Grail TODAY IN HISTORY: What the first years of Australian television were like Rare new silver $1 coin celebrates Indigenous astronomyInstitute archaeologist Helena Barba Meinecke said the inhabitants of Sisal had passed down through generations the account of the slave ship , and one of them led researchers to it."One of the people in Sisal who saw how they led the Mayas away as slaves, told his son and then he told his grandson, and it was that person who led us to the general area of the shipwreck ."In October 1860, a ship had been caught in neighbouring Campeche state taking aboard 29 Mayas, including children as young as seven.Authorities prevented the ship from leaving, but clearly that didn't keep the trade from continuing.The ship was found about 3.7 kilometres off the port of Sisal in about 7 metres of water, after a local fisherman led archaeologists to the wreck.(National Institute of Anthropology and History)Mayas were often transported on ships which were taking sisal fibre, derived from a botanical plant, and paying passengers to Cuba.It was unclear if there were any Maya aboard on the ship's last voyage.The records are unclear because the Mayas would probably have been listed as cargo, not as passengers, or the ship may have tried to conceal their presence.Ms Meinecke noted that captured Mayan combatants were frequently sent to Cuba, from where many never returned.(Gamma-Rapho via Getty Images)But she said the next stage of research would involve trying to find their descendants."These people, or some of them, could be descendants of the Mayas who were taken by force or deception," she said."Research has to be done so these (Mayan) people can know where their grandparents or great-grandparents are."The Maya launched one of North America's last Indigenous revolts in the lower Yucatan Peninsula in 1847, fighting against domination by white and mixed-race Mexicans who exploited them.A few wrecks of African slave ships have been found in waters in the United States and elsewhere , but no Maya slaving ship had been identified.

https://lg.lc/3/index.php?url=>925 2020-09-16 11:22:49

Five Takeaways From The Lukashenka-Putin Talks: Who Got What?

Putin, one of few international leaders to back Lukashenka, was probably hoping to use the meeting to extract further concessions, especially on deeper integration between the two countries based on a 1999 "Union State" treaty that remains largely on paper.In 2013, as Ukrainian President Viktor Yanukovych was wavering over whether to sign an agreement strengthening Kyiv's ties with the European Union, Putin helped persuade him not to -- a decision that led to Yanukovych's ouster the following February -- by offering a $15 billion lifeline including a quick $3 billion loan.In their numerous telephone talks, Lukashenka has said Putin has vowed to "ensure security" in Belarus through the Russia-dominated Collective Security Treaty Organization (CSTO) and bilateral agreements.Longer-term, the Kremlin has its eye on establishing a permanent military base in Belarus -- and the latest developments are likely to raise concerns among Lukashenka's opponents that Putin has advanced this cause.In September 2019, Russian Foreign Minister Sergei Lavrov said Belarus's refusal to host a military base had been an "unpleasant episode."In Sochi, Lukashenka seemed at times to suggest that he did not need much help from Moscow.He downplayed the protests against him, which normally swell to some 100,000 people in Minsk on weekends, saying that Belarusians "live an ordinary life" on weekdays and that on Saturday and Sunday "we free up part of Minsk so that people can, if they wish, walk through this area."He suggested there was little or no threat to his rule and said that protesters had not yet crossed a "red line" and spoke of what he said had been Putin's "red line" in Chechnya, where the then-prime minister of Russia launched a war in 1999 that helped build his image and vault him to the presidency.On the other hand, Lukashenka looked and sounded subservient , making several conciliatory statements regarding increased integration with Russia."The body language says far more in this case than the Russian language," seasoned Swedish diplomat and Kremlin critic Carl Bildt wrote on Twitter, referring to footage showing Lukashenka leaning in eagerly and gesticulating at a seemingly disinterested Putin.Bildt's tweet was one of many social media posts making roughly the same point.Ahead of the meeting, Kremlin spokesman Dmitry Peskov said oil and gas cooperation, state debts, and other economic ties would be discussed, but no documents signed.Few details emerged, leaving Lukashenka's critics to wonder whether he made concessions that went unannounced.Svyatlana Tsikhanouskaya, the opposition leader who contends that she won the August 9 vote, called Lukashenka an "illegitimate" leader who has no authority to make agreements on behalf of Belarus.She told Current Time that a large round of arrests in Minsk on the eve of the Sochi meeting were an attempt by Lukashenka to show Putin that he's still in control."The mass show of force... was likely organized to frighten people so that they would not demonstrate.People have the intention, people have the desire to live in a new Belarus without someone usurping [power]," she said via Skype from Lithuania.Meanwhile, Putin's support for the authoritarian leader has done further damage to Russia's badly strained ties with the West -- and could end up alienating millions of Belarusians.Even as he asserted that the Belarusian people must decide their own fate without foreign influence, Putin left no doubt that Moscow will want to play a powerful part in shaping its future.He urged Lukashenka to work quickly to amend the country's constitution and made it clear that Russia would have a say in this process, participating "at the highest level."
https://lg.lc/3/index.php?url=>924 2020-09-16 11:53:55

Lateral Movement Detection GPO Settings Cheat Sheet

ErrorHTTPSConnectionPool(host='www.compass-security.com', port=443): Max retries exceeded with url: /fileadmin/Datein/Research/White_Papers/lateral_movement_detection_basic_gpo_settings_v1.0.pdf (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1108)')))
https://lg.lc/3/index.php?url=>826 2020-09-14 21:33:33

Error502 Server Error: Bad Gateway for url: http://www.financesherald.com/are-the-tories-planning-a-revolt-against-their-prime-minister/

Are the Tories planning a revolt against their prime minister?
https://lg.lc/3/index.php?url=>943 2020-09-15 13:34:43

Error502 Server Error: Bad Gateway for url: http://highaltitudehacks.com/2020/09/05/arm64-reversing-and-exploitation-part-1-arm-instruction-set-heap-overflow/

ARM64 Reversing and Exploitation Part 1 - ARM Instruction Set + Simple Heap Overflow
https://lg.lc/3/index.php?url=>828 2020-09-13 20:19:53

Featured PortalsArticles by TopicFeatured PortalsArticles by Topic

Open science, communal culture, and women's participation in the movement to improve science
https://lg.lc/3/index.php?url=>965 2020-09-16 01:19:16

Extending a Thinkst Canary to become an interactive honeypot

Building on Ollie's previous blog , in which he built a TCP proxying service into a Thinkst Canary device with their module capability, I took a look at practical use case for this functionality and how it can be used to make the facade of a Canary have more interactivity.A Canary is excellent at providing a low noise digital tripwire, which is a powerful tool to detect Red Teamers or malicious threat actors attempting to move laterally in an environment.It does this in part by presenting dummy services, something that is not real but a python script behaving as the application would whilst being present.Let's take a look at the SSH module that comes with OpenCanary .In this example we can see the Twisted framework used to present responses that an SSH service would, such as building in ways of handling bad packets or lost of connections (see the sendDisconnect and connectionLost functions) meaning that if profiled it looks consistent with an actual OpenSSH server:This module will never return a shell, instead returning an invalid credentials message every time using the error function twisted.cred library:We wanted to present them with an actual shell so that we can monitor and further understand any subsequent activity.Whilst it is possible to create a dummy terminal in Python, it doesn't seem wise as there are so many combinations of commands, files and techniques that an attacker might use that we would have to account for.As we also know the breakout points of the Canary devices we can we can use Network Address Translation (NAT) to route it to the correct container dynamically.Luckily for me Docker themselves had already provided documentation and an example build file to do that.Here's the code I ended up using:In addition, there are a few items to edit here; we could change the root password for example.Or we could create a user in the build file and with some trusted keys and a password deployed, which we could then sprinkle the associated private key around our environment.In this example I built a host in AWS so that it would be easier to make publicly available on the relevant ports.Install software dependencies for Docker to run Install the latest version of Docker Create the directories for the Dockerfiles and other config to exist and copy them over Build and run the containers on the box, exposing a specific port and give them a "normal" hostname Create a NAT for certain source IPs to route them to the correct exposed portHere's the rough Ansible code that I wrote to take care of this:In this example code I created two "environments", one named LiamTest and another called NCCGroup.And finally, a test logging into the NCC Group environment:In order to make the extension more effective there are few other things that still need doing:Instrumentation to monitor what is happening the container Deployment of credentials/SSH keys around the network to lead attackers here Add more custom environment artifacts to the container Emulate other services that are close to the environments configuration Build a small network that is accessible by the docker containers to encourage lateral movement attempts

https://lg.lc/3/index.php?url=>839 2020-09-15 15:36:12

What does NVidia's acquisition of ARM mean for the future of Data Science & AI

NVIDIA Acquires ARM for $40 Billion-- What Paradigm Shifts this Deal Might Bring About for the Data Science & AI Communities, and What Can We Expect in the Future?In this article, we are going to have a look at how this acquisition might pave a golden path for artificial intelligence in the coming years.But before we move on to that, let us first understand what are the current standings of these two companies, NVIDIA, and ARM, and why are they so important.This figure goes even higher if we consider just the more niche markets-- Deep Learning, Data Science, and Artificial Intelligence, as these sectors primarily rely on NVidia's CUDA technology for parallel computing.For those of you that don't know what that is, basically NVidia's CUDA-based GPUs allow AI models to be trained much at much faster speeds as compared to on a normal CPU.And as the saying goes, when it comes to business, time is money.In fact, the reason why Deep Learning has seen exponential growth over the last few years is that GPUs have gotten cheaper and faster as compared to, say, two decades ago.Now, as we can see, both these companies rule their respective areas of operation in the consumer markets.But how exactly is it affecting the AI industry in any way?The traditional GPU-powered computers, on the other hand, can not only run these models efficiently, in fact, but they are also being used to create and train these technologies.For example, Apple uses special hardware acceleration on its SoCs called Neural Engine to assist in running real-time machine learning applications locally on the device itself.Similarly, Google also came up with the Neural Net API for its Android framework as a software-based mechanism to run AI and ML models locally on smartphones.However, because these technologies are more of a substitute solution rather than actual GPU-based solutions, using these they require a lot of software workarounds on the developers' part, which is obviously not very efficient and might result in frequent during the production and development stage.Up until now, ARM was undoubtedly doing an exceptional job with its mobile chip designing.But now, with this merger of ARM and NVidia, you can expect some major improvements coming up.For a starter, we can expect NVidia, with its years of experience in desktop GPU development, to step forward for a joint venture with the team of ARM researchers and engineers.Who knows a company that excels in graphics-based solutions and the other with expertise in mobile chip designing might be able to come up with a product, say, a CUDA-compatible mobile SoC, that might be able to run fully-fledged AI models locally on the mobile phone itself, or in the extreme cases, support for on-device model training that will allow the device to learn based on the users' usage patterns.This might also mean that the users would not have to send their private data to some unknown location for the sake of getting "a tailored user experience".For the developers working on AI technologies, this will directly unlock the access to an entirely new area of development that till data had been either completely out of their reach due to existing technological limitations, or, it required so much work around that just was not worth it.With this agreement between NVidia and SoftBank for the acquisition of ARM now entering into a final stage, we can start expecting some major AI-related developments in the smartphone and other mobile computing divisions coming soon.

https://lg.lc/3/index.php?url=>971 2020-09-15 20:57:57

Trump's big lies reveal a truth: Right-wing science denial was never about ignorance, just cruelty

Republicans have denied or cast doubt on science in so many ways -- denying that condoms are effective, that evolution is real, that climate change is actually happening and largely caused by human activity -- and many liberals and progressives have felt legitimately confused about exactly why.That was confirmed again on Monday by a reporter for the Las Vegas Review-Journal , who confronted Trump about his decision to hold a packed (and largely mask-free) indoor rally in Henderson, Nevada, despite warnings from public health officials that such events easily spread the coronavirus."I'm on a stage and it's very far away," Trump told the reporter.Trump's odious attitudes towards the people who are being harmed by his failure to take science seriously were on display later in his trip, when he visited McClellan Park in Sacramento, California, where the skies are clogged from smoke from wildfires tearing up the West Coast.But when a California state official asked him about the issue, Trump simply responded , "It will start getting cooler."I don't think science knows," Trump insisted, while trying to pretend the problem on the West Coast is about forest management, instead of soaring summer temperatures that turn bone-dry wooded areas into kindling.(It was just nine months ago that similar summer fires in Australia reportedly .)It worked for many years, however, because the consequences of climate change weren't readily apparent to most people, and many people didn't grasp that snow in December doesn't negate the problems caused by record hot summers.The term "gaslighting" --when someone pretends not to know something that both they and their target know is true -- has been around in psychology for a long time and recently made the leap to politics, since it so perfectly describes the nature of Trump's obvious lies.That's also what Republicans have been doing all along when it comes to denying science.I spent years reporting on reproductive health care, and it soon became evident that no amount of common sense or scientific evidence would overcome the insistence by many conservatives -- such as Vice President Mike Pence -- that condoms don't work to prevent HIV transmission and other sexually-transmitted diseases.Pence is not the brightest bulb on the tree, but it doesn't exactly take a doctorate in molecular biology to see how a condom prevents virus from moving from one body to another.He was just feigning ignorance to justify his hostility to policies that protect the health of people he hates, especially LGBTQ people and women who have sex lives outside of heterosexual marriage.For one thing, that problem would seem to have a ready solution: Better education and reasoned discourse.It's a power play -- a demonstration that he can do or say whatever he wants, no matter how outrageous or offensive, and no one has the ability to stop him.This distinction matters, because it puts the fight over these issues squarely in the realm of a moral debate, instead of a debate about facts or science.And that's a debate conservatives don't want to have, because they know they'll always lose a moral debate over, say, whether it's OK to let the entire West Coast burn every summer and fall.The gaslighting and feigned ignorance was a tactic to keep the discussion mired in a pointless debate over facts that are abundantly clear, and to avoid these larger moral questions.Maybe now, with Trump giving the game away, we can stop letting the right waste our time with gaslight-fueled "debates" and turn to what really matters: Will our nation do the right thing, or will we continue to let a pack of bigots and sadists determine our national priorities?That fateful decision is long overdue, but with Trump in the White House trying to lie and cheat his way into a second term, we can no longer avoid it.

Whalescan is a vulnerability scanner for Windows containers, which performs several benchmark checks, as well as checking for CVEs/vulnerable packages on the container. It also checks the config and Docker files for misconfigurations

Released under Apache license 2.0, see LICENSE for more informationWhalescan is a vulnerability scanner for Windows containers, which performs several benchmark checks, as well as checking for CVEs/vulnerable packages on the container.It also checks the config and Docker files for misconfigurations.This tool can be used as part of a Windows container review on local copies of the containers, and on the host itself to enhance security.Whalescan performs the following checks on containers:Checks if containers are stored under C: drive - this could raise issues if there is a DoS attack, filling up the C: drive and making the host unresponsive Checks if container is running as a process or hyper-v. Hyper-v isolation offers enhanced security of containers Checks if there are any pending updates in the containers, and if so, how to update.Checks for unsafe commands being used in the dockerfile, for example docker ADD instead of docker COPY.Checks if hash verification is being performed on any files downloaded.Checks if any vulnerable packages are on the container, and pulls relevant CVE information Checks if .NET version being used is End Of Life Checks if Docker Engine is updated, and if not, gathers a list of CVEs for the version being usedChecks permissions of docker configuration filesChecks if additional devices have been mapped to containers

'Britain does not break treaties': EU president quotes Thatcher as she tells Boris Johnson he cannot change Brexit deal

And she quoted former Conservative UK prime minister Margaret Thatcher saying Britain should never break its word to other countries.The government's Internal Market Bill has prompted criticism both inside and outside the UK, following an admission by ministers that it would break international law.But the customs code requires new controls between Northern Ireland and Great Britain, which the prime minister first denied existed and now says he doesn't to want to implement.Addressing MEPs early on Wednesday, Ms von der Leyen quoted former Tory prime minister Margaret Thatcher to underline her point.Show all 66 A message projected onto the White Cliffs of DoverLONDON, ENGLAND - JANUARY 31: Pro Brexit supporters attend the Brexit Day Celebration Party hosted by Leave Means Leave at Parliament Square on January 31, 2020 in London, England.A pro-Brexit supporter jumps on an EU flag in Parliament SquarePro-EU campaigners take part in a 'Missing EU Already' rally outside the Scottish Parliament, EdinburghA large pro-EU banner is projected onto Ramsgate cliff in KentThe five-year old Elisa Saemann, left, and her seven-year old sister Katie hold a placard during a rally by anti-Brexit protesters outside the Scottish parliament in EdinburghPro Europe supporters gather on Brexit day near the British embassy in Berlin, GermanyPaddy from Bournemouth wears Union colours as he sits next to an EU flag decorated bag in Parliament SquarePro Brexit supporters dance in the street draped with Union Jack flags at Parliament SquareAn anti-Brexit demonstrator spreads his wings during a gathering near Downing Street-Britain on January 31 ends almost half a century of integration with its closest neighbours and leaves the European Union, starting a new -- but still uncertain -- chapter in its long history.Pro Brexit supporter wears a novelty Union Jack top hat outside the Houses of ParliamentCustomers Scott Jones and Laura Jones at the Sawmill Bar in South Elmsall, Yorkshire, where a Brexit party is being held throughout the dayLONDON, ENGLAND - JANUARY 31: Pro Brexit supporters hold up placards at Parliament Square as people prepare for Brexit on January 31, 2020 in London, United Kingdom.Newspapers and other souvenirs at a store, near Parliament SquareAfter half a century of membership and three years of tense withdrawal talks, the UK will leave the EU at midnight Brussels time (23.00 GMT) on January 31

Barbados to remove Queen as head of state by November 2021

Queen Elizabeth II, wearing a shimmering frock of blue and white taffeta glistening with diamante and a white fur wrap, is escorted by Mr Bernard Delfont in to the London Palladium for the Royal Variety Performance.England captain Bobby Moore holds the Jules Rimet Trophy, collected from the Queen, after leading his team to a 4-2 victory over West Germany, in an exciting World Cup Final that went to extra time at Wembley, London.Queen Elizabeth II opening the Victoria Line, London's first completely new underground railway for 60 years.A dazzling smile from Queen Elizabeth II in the Chelmsley Wood shopping centre during her visit to Birmingham.Queen Elizabeth II and the Duke of Edinburgh at Balmoral to celebrate their Silver Wedding anniversary.Catherine Cusack of Harrow presents a floral posy to the Queen on her arrival at Leicester Square Theatre.Queen Elizabeth ll toasts President Gerald Ford during a State Visit to the USA in July, 1976.Queen Elizabeth II on a walkabout among the crowds in Aberdeen, during her Silver Jubilee Tour of Britain.China's paramount leader Deng Xiaoping has died of complications from Parkinson's disease and a lung infection, the official Xinhua news agency said tonight.she later boarded a eurostar train to Calais for her inaugural trip through the channel tunnel.In results that correspond with three other polls since 1995, just 33% of 1,000 respondents nationwide said the Queen should make way for a republic.The pop superstar will celebrate her 60th birthday on Thursday, following a long career of reinvention and controversy.Britain's Queen Elizabeth II is greeted during her visit to Devonport Naval Base, Plymouth, Monday March 24, 2003.Britain's Queen Elizabeth II meets John Leese (far left with glasses), who was invited to a Christmas reception at Buckingham Palace.Prince Philip, Duke of Edinburgh kisses his granddaughter, Zara Phillips, as boyfriend, English rugby player Mike Tindall, shakes hands with Queen Elizabeth ll at a Buckingham Palace reception for the country's top achievers on December19, 2006 in London, England.Queen Elizabeth ll meets actress Thandie Newton at a Buckingham Palace reception for the country's top achievers on December19, 2006 in London, England.Queen Elizabeth ll meets comedian David Walliams at a Buckingham Palace reception for the country's top achievers on December19, 2006 in London, England.Britain's Queen Elizabeth II (L) meets British comedian Peter Kay (R) following the Royal Variety Performance in Blackpool.Queen Elizabeth II meets American singer Lady Gaga (right) following the Royal Variety Performance in Blackpool.Queen Elizabeth ll leaving after attending the Commonwealth Day Service at Westminster Abbey on March 09, 2020.

Iran warns the UAE and Bahrain they will bear 'severe consequences' after they signed an historic peace deal with arch-foe Israel

Israel, the UAE and Bahrain have signed a peace deal establishing diplomatic ties Iran blasted the leaders of both Arab states, warning of 'severe consequences' Palestinian leaders also attacked the deal, saying there can be 'no peace' in the Middle East until they are given a guarantee of statehood Donald Trump said the historic pact marked 'the dawn of a new Middle East'Iran has warned the UAE and Bahrain they will be responsible for 'severe consequences' caused by the signing of an historic peace deal with Israel.'How could you reach out your hands to Israel?And then you want to give them bases in the region?All the severe consequences that would arise from this are on you,' he said in televised remarks.Hassan Rouhani, president of Iran, has warned the UAE and Bahrain that they are facing 'severe consequences' after signing an historic peace deal with IsraelDonald Trump hailed the deal as 'a new dawn in the Middle East' as it was signed in Washington, saying he believed more Arab states would sign up soonAs the signing took place, two rockets were fired at Israel from Gaza, prompting the Israeli air force to strike targets it said belonged to Hamas (pictured), which controls the Gaza StripThe pact normalises diplomatic and economic relations between the three states, and breaks with years of consensus among Arab countries that a deal recognising Palestine is a necessary precursor to any accord with Israel.Egypt and Jordan are the only other Arab states to have recognised Israel.Palestinian leaders bitterly oppose the deal, fearing that it will prompt Israel to give up on the peace process, destroying their hopes of statehood.It also saw two rockets fired overnight from Gaza towards Israel, which were timed to coincide with the ceremony.At least two people received non-life-threatening injuries, emergency services said.The Israel Defence Forces said Wednesday that their fighter jets responded with air strikes on military targets belonging to Hamas, which controls the Gaza Strip.But the IDF levelled blame at Hamas and warned that it would 'bear the consequences for terror activity against Israeli civilians'.Egypt and Jordan are the only other Arab states to officially recognise Israel.Palestinians oppose the deal, fearing that it will prompt Israel to abandon the peace process and with it their hopes of establishing an independent Palestinian state.Bahrain Foreign Minister Abdullatif al-Zayani, Israeli Prime Minister Benjamin Netanyahu, President Donald Trump and UAE Foreign Minister Abdullah bin Zayed Al-Nahyan sign the Abraham Accords to normalize relations between the Israeli state and Arab nationsIn Gaza, protesters trampled on and set fire to placards bearing images of the leaders of Israel, the UAE and Bahrain.That latest rocket fire came after a month in which militants in the strip had stepped up incendiary balloon attacks against Israel, which responded with nighttime air strikes against Hamas.

https://lg.lc/3/index.php?url=>927 2020-09-16 11:38:57

New material can act as a super-fast magnetic switch. When struck by successive ultra-short laser pulses it exhibits "toggle switching" that could increase the capacity of the global fibre optic cable network by an order of magnitude.

Researchers at CRANN and Trinity's School of Physics have discovered that a new material can act as a super-fast magnetic switch.When struck by successive ultra-short laser pulses it exhibits "toggle switching" that could increase the capacity of the global fibre optic cable network by an order of magnitude.Switching between two states - 0 and 1 - is the basis of digital technology and the backbone of the internet.The vast majority of all the data we download is stored magnetically in huge data centres across the world, linked by a network of optical fibres.Obstacles to further progress with the internet are three-fold, specifically the speed and energy consumption of the semiconducting or magnetic switches that process and store our data and the capacity of the fibre optic network to handle it.The new discovery of ultra-fast toggle switching using laser light on mirror-like films of an alloy of manganese, ruthenium and gallium known as MRG could help with all three problems.Not only does light offer a great advantage when it comes to speed but magnetic switches need no power to maintain their state.More importantly, they now offer the prospect of rapid time-domain multiplexing of the existing fibre network, which could enable it to handle ten times as much data.The science behind magnetic switchingWorking in the photonics laboratory at CRANN, Trinity's nanoscience research centre, Dr Chandrima Banerjee and Dr Jean Besbas used ultra-fast laser pulses lasting just a hundred femtoseconds (one ten thousand billionth of a second) to switch the magnetisation of thin films of MRG back and forth.The direction of magnetisation can point either in or out of the film.Each pulse is thought to momentarily heat the electrons in MRG by about 1,000 degrees, which leads to a flip of its magnetisation.The discovery of ultra-fast toggle switching of MRG has just been published in leading international journal, Nature Communications.Dr Karsten Rode, Senior Research Fellow in the 'Magnetism and Spin Electronics Group' in Trinity's School of Physics, suggests that the discovery just marks the beginning of an exciting new research direction."We have a lot of work to do to fully understand the behaviour of the atoms and electrons in a solid that is far from equilibrium on a femtosecond timescale.In particular, how can magnetism change so quickly while obeying the fundamental law of physics that says that angular momentum must be conserved?"In the spirit of our spintronics team, we will now gather data from new pulsed-laser experiments on MRG, and other materials, to better understand these dynamics and link the ultra-fast optical response with electronic transport.We plan experiments with ultra-fast electronic pulses to test the hypothesis that the origin of the toggle switching is purely thermal."Next year Chandrima will continue her work at the University of Haifa, Israel, with a group who can generate even shorter laser pulses.The Trinity researchers, led by Karsten, plan a new joint project with collaborators in the Netherlands, France, Norway and Switzerland, aimed at proving the concept of ultra-fast, time-domain multiplexing of fibre-optic channels.

https://lg.lc/3/index.php?url=>966 2020-09-15 20:17:07

100-million-year-old giant sperm found preserved in amber is oldest ever, scientists believe

Fossilised sperm discovered inside a mussel-like crustacean that was trapped in amber 100 million years ago may be the oldest ever found, scientists say.The female ostracod was unearthed by an international team of palaeontologists .They believe it mated shortly before becoming trapped in the resin.Their findings, published in Proceedings of the Royal Society B , provide "an extremely rare opportunity" to learn more about the evolution of the reproductive process, they added.Until now the oldest known fossilised sperm resided inside a 50-million-year-old worm cocoon from Antarctica .The crustacean, a new species called Myanmarcypris hui, is thought to have lived in coastal and inland waters in what is now Myanmar, surrounded by trees that produced huge quantities of resin.A team led by Dr Renate Matzke-Karasz, a geobiologist at Ludwig-Maximilians-Universitaet (LMU) in Munich, analysed 39 ostracods trapped in a tiny piece of amber using 3D X-ray reconstruction.Reconstructed images of the extraordinary find(PA)The researchers found ripe giant sperm stored in a pair of receptacles inside the female ostracod, waiting for the eggs to mature, in what they said could also be the earliest direct evidence of a completed insemination.Most animals produce large quantities of very small sperm to increase chances of fertilisation.But some, like fruit flies and modern-day ostracods, produce a small number of oversized sperm, with tails several times longer than the animal itself.In these cases, the researchers say, chances of fertilising an ovum can increase with the size of the sperm cell.Understanding the evolution of such giant sperm may shed light on what the team described as "ancient and advanced instance of evolutionary specialisation".Dr Matzke-Karasz said: "The most significant part of our story is that we can now show that using giant sperm for reproduction is something that can last long in Earth history."Previously, we were not sure if animals that 'switched' to using these giant sperm at a certain point in their evolutionary history are doomed to become extinct very quickly."After all, these are enormous costs for the animals.Large sperm must be produced, the reproductive organs are much bigger than in other species, they take up a lot of space in the animal, and mating lasts long."This is a lot of biological energy that must be allocated to reproduction - so you might think that this doesn't make sense from an evolutionary standpoint."But in ostracods, it seemed to work for more than 100 million years."She added: "From an evolutionary point of view, sexual reproduction with the aid of giant sperm must, therefore, be a thoroughly profitable strategy."

https://lg.lc/3/index.php?url=>947 2020-09-16 10:34:45

New research finds people react better to both negative and positive events with more sleep

When people slept less than usual, they responded to these stressful events with a greater loss of positive emotions.Q&As New research from UBC finds that after a night of shorter sleep, people react more emotionally to stressful events the next day--and they don't find as much joy in the good things.The study, led by health psychologist Nancy Sin, looks at how sleep affects our reaction to both stressful and positive events in daily life."When people experience something positive, such as getting a hug or spending time in nature, they typically feel happier that day," says Nancy Sin, assistant professor in UBC's department of psychology."But we found that when a person sleeps less than their usual amount, they don't have as much of a boost in positive emotions from their positive events."People also reported a number of stressful events in their daily lives, including arguments, social tensions, work and family stress, and being discriminated against.When people slept less than usual, they responded to these stressful events with a greater loss of positive emotions.This has important health implications: previous research by Sin and others shows that being unable to maintain positive emotions in the face of stress puts people at risk of inflammation and even an earlier death.Using daily diary data from a national U.S. sample of almost 2,000 people, Sin analyzed sleep duration and how people responded to negative and positive situations the next day.The participants reported on their experiences and the amount of sleep they had the previous night in daily telephone interviews over eight days."The recommended guideline for a good night's sleep is at least seven hours, yet one in three adults don't meet this standard," says Sin."A large body of research has shown that inadequate sleep increases the risk for mental disorders, chronic health conditions, and premature death.My study adds to this evidence by showing that even minor night-to-night fluctuations in sleep duration can have consequences in how people respond to events in their daily lives."Chronic health conditions--such as heart disease, diabetes, and cancer--are prevalent among adults, especially as we grow older.Past research suggests that people with health conditions are more reactive when faced with stressful situations, possibly due to wear-and-tear of the physiological stress systems."We were also interested in whether adults with chronic health conditions might gain an even larger benefit from sleep than healthy adults," says Sin."For those with chronic health conditions, we found that longer sleep--compared to one's usual sleep duration--led to better responses to positive experiences on the following day."Sin hopes that by making sleep a priority, people can have a better quality of life and protect their long-term health.Erik Rolfsen UBC Media Relations Tel: 604-822-2644 Cel: 604-209-3048 Email: erik.rolfsen@ubc.ca

https://lg.lc/3/index.php?url=>968 2020-09-15 18:10:26

Smoke from western wildfires reaches East Coast; over 150 miles burned in Sequoia National Park

AccuWeather meteorologist Matt Benz said you can draw a line from California through St. Louis and on to Norfolk, Virginia - pretty much everyplace north of that line is looking at smoke-tainted skies.The crisis has forced 220,000 people to flee their homes in California, Oregon and Washington -- and it could be weeks before it's safe for them to return, the American Red Cross reported Tuesday."No matter which way the wind is blowing, the valley is getting smoke," said Jonathan Klassen, director of air quality science at San Joaquin Valley Air Pollution Control District."The valley is surrounded by fire, so no matter what happens, we will get smoke."Goldfarb urged people to stop working outdoors when air quality is unhealthy or worse."However, other airports in the West could be impacted by drifting smoke."The wildfire has burned through more than 1,100 square miles across five counties in Northern California and is on a westward path that threatens a region known for its marijuana farms, The Press Democrat reported.President Donald Trump repeated his claim this week that Democratic leaders in California deserve blame for the fires, having failed to clear leaves and dead trees from forest floors.Wally Covington, professor of forestry at Northern Arizona University, agreed that forests have become overgrown and need to be thinned, but "not with a lawn rake." Some of the policies that led to overgrown forests, such as aggressive fire suppression, were implemented more than 100 years ago, so blaming California's current leaders doesn't make sense, Covington said.Covington said people living in areas burning are paying the price because policymakers would not address climate change and the effects of fire suppression on forests 30 or 40 years ago."I was hopeful back in the '90s and '80s that maybe we would reverse climate change effects.Other vetoes will maintain a balanced budget as required by the state constitution.Senate Republican Leader Fred Girod said the vetoes are politically motivated, and more should have been done before this fire season to address forest management.Two major fires combined to burn more than 150 square miles in Sequoia National Park, tearing through groves of giant redwoods.Firefighters struggled against what have become familiar foes in recent weeks - gusty winds and dry, hot conditions.Residents of one wildfire-besieged Oregon county posted ominous signs such as "You loot, we shoot."Clackamas County Sheriff Craig Roberts said armed residents concerned about looters have been conducting stops on their own.In neighboring Multnomah County, Sheriff Mike Reese warned residents to stop setting up illegal roadblocks or they could face arrest."We understand everyone's concerns and anxiety, (but) roadways are open to all users."Contributing: Rebecca Plevin, Palm Springs Desert Sun; Tracy Loew and Connor Radnovich, Salem Statesman Journal; Joe Jacquez, Sheyanne N. Romero and James Ward, Visalia Times-Delta; Damon Arthur, Redding Record Searchlight; Joel Shannon, USA TThe Associated Press

The Story Behind TIME's Issue Marking Nearly 200,000 U.S. Deaths--and Why Its Border Is Black For the Second Time in History

In March, as the global pandemic hit New York, my colleague Kat Moon decided-wisely, it turned out, given what was ahead for the U.S.-to decamp to her childhood home, Taipei.Despite its proximity to mainland China, where the outbreak originated, Taiwan has seen only 495 cases and seven deaths among its more than 23 million people, making its response to the coronavirus one of the most successful in the world.So successful, in fact, that last month it was able to host one of the largest public gatherings reported since social distancing began: a 10,000-person live arena concert , which Moon and photographer An Rong Xu attended and covered for TIME.As one U.S. reader put it on Twitter, "An arena concert taking place with corona restrictions honestly seems like it's happening on another planet considering what's going on here in the U.S."While a great many mysteries remain around COVID-19 , the most effective ways to curb its spread are not among them.That is the theme of this week's cover story by Alex Fitzpatrick and Elijah Wolfson, echoing what scientists around the world have made clear now for many months.Do it all," says World Health Organization director-general Tedros Adhanom Ghebreyesus.And then there is the U.S., which will soon cross a devastating marker: 200,000 deaths caused by COVID-19.That death toll-equivalent to U.S. deaths in more than three Vietnams, or the entire population of Salt Lake City-is the world's largest by far and more deaths per capita than in all but 12 other countries.I spoke this week to Tom Ridge, the former Republican governor of Pennsylvania who later served as the first Secretary of the Department of Homeland Security-a role created after Sept. 11, 2001, out of the recognition that the threat of terrorist attacks on American soil would forever be part of the nation's reality.There are clear parallels not only with the continuing threat of COVID-19 but also with the likelihood of future pandemics that virologists predict may well be worse."We see in a painful and dramatic way the globalization of disease, and it's incumbent on us to make some rather substantive changes," Ridge says."If we don't, then shame on us and shame on our leadership."For this week's U.S. cover, we turned to artist John Mavroudis, who-using data from the Johns Hopkins Coronavirus Resource Center-handwrote the death counts in America on every one of the 193 days between Feb. 29, the first confirmation of a COVID-related death in the U.S., and Sept. 8, as it neared time to go to press.Creative director D.W. Pine then placed the illustration within a black border-only the second time in our history we have done so, the first being after 9/11."I really hope this cover is a wake-up call for those who are numbed to this catastrophe," says Mavroudis."Science and common sense are the answers to this crisis."And as TIME's Alice Park notes elsewhere in this issue, it's possible that at least one vaccine may be available by the time 2020 comes to an end , although distribution will create many new questions and challenges.In the meantime, it is not too late to do better.This appears in the September 21, 2020 issue of TIME.

Louisville has settled Breonna Taylor's wrongful death lawsuit

"I cannot begin to imagine Ms. Palmer's pain," Fischer said.The settlement comes more than six months after Louisville Metro Police officers broke down the door to Taylor's apartment and fatally shot her while executing a late-night, "no-knock" warrant in a narcotics investigation.Since her death, the police chief was fired in June after a separate police shooting , and the Louisville City Council passed "Breonna's Law," which banned no-knock search warrants .On Tuesday, Crump, attorney Lonita Baker and Palmer continued to push for criminal charges against the officers involved."It's time to move forward with the criminal charges, because she deserves that and much more," Palmer said."Her beautiful spirit and personality is working through all of us on the ground, so please continue to say her name : Breonna Taylor."Taylor's boyfriend, who said he believed the home was being broken into, shot and injured an officer, and police killed Taylor in the return fire.There is no body camera footage of the incident, police said."No amount of money will bring back Breonna Taylor," the group said."We see this settlement as the bare minimum you can do for a grieving mother.We need those involved in her murder to be arrested and charged.The police union did not immediately respond to a request for comment.One officer, Brett Hankison, was fired in late June for "wantonly and blindly" firing 10 rounds into her apartment, then-interim Louisville Police Chief Robert Schroeder wrote.Cameron is expected to announce a charging decision soon.An investigation, if done properly, cannot follow a specific timeline," Cameron tweeted last week.Correction: An earlier version of this story misspelled the last name of Brett Hankison, the officer fired after Breonna Taylor's death.Mayor Greg Fischer, Taylor's family and their attorneys announced the settlement at a joint press conference on Tuesday.Taylor, a 26-year-old EMT, was killed in her home by police on March 13.As part of the settlement, the city agreed to establish a housing credit program as an incentive for officers to live in the areas they serve; use social workers to provide support on certain police runs; and require commanders to review and approve search warrants before seeking judicial approval, among other changes."Justice for Breonna means that we will continue to save lives in her honor," said Tamika Palmer, Taylor's mother."No amount of money accomplishes that, but the police reform measures that we were able to get passed as a part of this settlement mean so much more to my family, our community, and to Breonna's legacy."

https://lg.lc/3/index.php?url=>990 2020-09-15 16:07:06

HTTP Toolkit - open-source tool with one-click MitM, inspecting & rewriting of HTTP(S)

Instantly intercept browsers, most backend & scripting languages (from Node.js to PHP), Android devices, Electron apps and more with one-click setup .Collect interesting traffic without intercepting everything on your whole machine, so there's no extra noise and no side-effects - just the traffic you care about .Inspect the full headers & body for every request & response from every client, to immediately see what's really being sent & received on the wire.Easily understand collected HTTP traffic , with inline documentation for all standard headers & responses statuses, plus body decoding, highlighting, folding, and other nicities, powered by the same internals as Visual Studio Code.Quickly find the data you care about, with exchanges highlighted by client and tagged by category (images, JSON responses, errors), and free-text search across all request & response metadata.Breakpoint live requests or responses, to rewrite HTTP traffic on the fly .Mock endpoints or servers , with a flexible rule configurations to match and handle requests automatically, to send responses, inject failures & timeouts, or transparently redirect requests elsewhere.HTTP Toolkit is driven by its community of users and their feedback.Have some ideas, problems or questions about HTTP Toolkit?If that's too public, you can also send a message directly .Would you like to help design the perfect HTTP debugging tool?HTTP Toolkit is 100% open source, so you can help shape it directly!All contributors get free HTTP Toolkit Pro (more background on this over here).That includes code contributions, but documentation improvements, article & blog posts elsewhere about the project, bug & security reports, and anything else that helps drive HTTP Toolkit forwards.Feel free to get in touch with any other questions about this too.All of that is open source, licensed as a mixture of copyleft AGPL (for the HTTP Toolkit-specific components, ensuring all direct derivative projects are open-source too) and permissive Apache-2/MIT licenses (for all the general-purpose reusable libraries).The main repos you might be interested in are:HTTP Toolkit UI - the core of the product, a TypeScript + React app that powers most of the functionality you use, except for things that can't be done in a web page (i.e. starting a proxy, and setting up client interception).Mockttp - the HTTP(S) proxy itself, and all low-level logic around that, as a standalone TypeScript library.Used in HTTP Toolkit for traffic interception, but also usable standalone as a testing tool, or as a programmatically controllable intercepting HTTP(S) proxy.

https://lg.lc/3/index.php?url=>995 2020-09-15 13:41:10

Notorious B.I.G's plastic crown sells at auction for almost $600K

A crown adorned with plastic jewels, famously worn by Notorious B.I.G .during his last ever photo shoot, sold for $594,750 at Sotheby's in New York on Tuesday evening.The item, signed by the rapper days before his death in 1997, smashed auction estimates that had initially valued it between $200,000 and $300,000.The crown was among a sizable collection of hip hop memorabilia auctioned off by Sotheby's in an sale dedicated to the genre's "history and cultural impact."is pictured on display in New York ahead of Tuesday's sale.Other lots included a five-piece drum kit, once used by Questlove of The Roots, and one of rapper Slick Rick's diamond eyepatches, which sold for $30,240 and $25,200 respectively.A pair of "Push It" Jackets worn by hip hop duo Salt-N-Pepa in a 2015 Super Bowl commercial went for just under $24,000.In a press statement released prior to the sale, vice president of Sotheby's books and manuscripts department, Cassandra Hatton, said that Biggie's crown and Tupac's love letters offered and "introspective look, in their own way, at the personalities behind their respective public personas."An archive of 22 love letters written by Tupac Shakur sold for over $75,000."Since its birth in the Bronx in the 1970s, hip hop has become a global cultural force, whose massive influence continues to shape all realms of culture: music, fashion, design, art, film, social attitudes, language and more," she is quoted as saying.was put up for sale by photographer Barron Claiborne, who had kept the item since styling the rapper as the "King of New York" in a photo shoot for Rap Pages magazine.Having acquired two crowns, Claiborne found that both were too small for Biggie's head, though he was able to use one by removing its foam cushioning.Sean "Diddy" Combs, who owned Biggie's label Bad Boy Records, was also present at the 1997 shoot.(King of New York)" crown, which is set to be auctioned off as part of Sotheby's hip hop sale Credit: Barron ClaiebornThe shoot went ahead nonetheless, and the resulting photos became some of hip hop's most recognizable and enduring portraits.In a press statement released through Sotheby's, Claiborne described the crown as an "iconic piece of hip hop history."became much more than a portrait -- the image transformed Biggie Smalls into an aristocratic or saint like figure, forever immortalized as not only the King of New York, but a king of hip hop music and one of the greatest artists of all time," the photographer said.Tuesday's auction also featured various hip hop-inspired luxury goods and contemporary artworks.Also among the 120 lots were a number of "experiences," including virtual wine tasting with Big Daddy Kane and a private styling session with Harlem fashion designer Dapper Dan.A portion of proceeds from the sale will be donated to charities including New York's Queens Public Library Foundation, which coordinates hip hop community programs.

Advanced Boolean-Based SQLi Filter Bypass Techniques

Learn how to bypass filters and Application Firewall rules using MySQL String Functions, Regex Functions, Conditional Select and Set Variables to exploit a blind (boolean-based) SQL Injection vulnerability.This article aims to show you some techniques to exploit a SQL Injection vulnerability bypassing libinjection (running inside a Web Application Firewall).libinjection is an open-source SQL / SQLi tokenizer parser analyzer created by Nick Galbreath from Signal Sciences that aims to detect SQL Injection and XSS payloads.Libinjection runs in many Web Application Firewall because it performs better than a regular expression based ruleset.Despite this, it works well and it detects many SQLi payloads, and it can be bypassed by using specific SQL syntaxes such as MySQL string functions or conditional select.Let's take a look at the following request that tries to check if the parameter id can be injectable with SQL syntax:/index.php?id=1 +AND+1=1It is successfully identified by libInjection as SQLi attempts.You can use a list of Arithmetic Operators, String Functions and Conditional Select syntaxes to bypass it.You can make it by replacing the number 2 with an arithmetic operation.OperatorDescriptionExampleInjection+Additionselect 1 + 1/index.php?id=1 %2b1 -Subtractionselect 3 - 1/index.php?id=3 -1 *Multiplicationselect 2 * 1/index.php?id=2 *1 /Divisionselect 2 / 1/index.php?id=2 /1 DIVInteger Divisionselect 2 DIV 1/index.php?id=2 +DIV+1 libinjection intercept most of SQLi classic attempts like 1+OR+1=1 but, speaking of MySQL, it's possible to bypass its filters by using MySQL functions:As you might know, a useful technique that could help in bypassing filters is to insert comments inside the SQL syntax, such as sEleCt/*foo*/1 .This kind of payload is well blocked by WAF that uses libinjection but the following syntax seems to bypass it well:For example, in a real scenario:curl -v 'http://wordpress/news.php?id=\ {`foo`/*bar*/(select+1)\} 'ExampleInjectionselect login from users where id={`foo`/*bar*/(select 2)};/index.php?id= {`foo`/*bar*/(select+2)} select login from users where id={`foo`/*bar*/(select--2)};/index.php?id= {`foo`/*bar*/(select--2)} select login from users where id={`foo`/*bar*/(select+2)};/index.php?id= {`foo`/*bar*/(select%2b2)} In a real scenario, if you found a boolean-based SQL Injection for example on a vulnerable WordPress plugin, and you need to bypass a WAF using libinjection to exploit it, you can bruteforce and exfiltrate the password hash of a user by using the following payload:*" -> error or different response body length RLIKE "(^)[$][c].*" -> error or different response body lengthRLIKE "(^)[$][c][b].You can perform multiple assignments in the same SET statement.You can perform multiple assignments in the same statement.This means you can use := in any valid SQL statement (not just in SET statements) to assign a value to a variable.We can use all syntaxes shown before (Expression, Comments, RLIKE, and Assignment Operator) too (thanks to @seedis https://github.com/seedis).

Vote Joe: Voter privacy issues in the Biden Campain app

Responsible disclosure: September 7th 2020: Vote Joe team is made aware of potential privacy issues.September 11th 2020: Developers have addressed issues and iOS version appears fixed.Disclaimer: The App Analyst is not an American website or associated with any political party.This is one of two election campaign apps analysed.It's been designed as an organization tool to help engage with voters.Once a user is signed up they can begin using the application's features such as sending canned Joe Biden support texts, and more importantly reporting information about your contacts in a practice called "relational organizing".As defined here , relational organizing is "when volunteers leverage their existing networks and relationships in support of our candidate, Joe Biden.".The way this is done in the app is by either syncing your phone's contacts, or by finding a voter in the Vote Joe App voter database, and reporting specific information about that contact/voter.The Vote Joe App allows any user who signs up with an unverified email access to the voter database compiled by Target Smart , a service who claims to have more than 191 million voter records.The Vote Joe App requires its users query the voter database using a first and last name, and state (age is required but it can be set as "All").The returned information will list which elections the voter has participated in with either a check-mark to signify their participation or an X otherwise.While this is already interesting information about a voter, the JSON object returned from the server contains much more voter data.The returned object appears to contain "Y" to signify "Yes they voted", but there are other values such as "B" and "R".There is additional hidden information about the voter such as their specific date of birth, "voterbase_id" (a value unique to Target Smart and not an official voter id), and some Target Smart fields (prefixed with "tsmart") corresponding to the voters senate, congressional, and house districts (more "tsmart" fields found here .When a user syncs their contacts with the Vote Joe App they will be presented with a corresponding voter entry from the Biden campaigns voter database.It should be noted that this voter's information may never have been inputed by themselves; it is very likely this data is collected via another user syncing their contacts or a third party data feed.It's not certain whether Target Smart is able to sell the data uploaded through the Vote Joe App to other third-parties, however they make no secret that their data on voters is being sold.Personal Information Sales Opt-Out and Opt-In Rights from the Target Smart privacy policy.While this likely violates their Terms of Service that does nothing to stop a bad actor.The Vote Joe App allows for users to query the Target Smart voter database and retrieve potentially sensitive voting records and addresses on unknowing American citizens.

Mass Job Losses and Other Economic Costs of President Trump's Inaction on Coronavirus

Accompanying this carnage is catastrophic economic fallout, which too can be attributed to the president's inaction and misdirection.With no end in sight to the recession, it is worth remembering that this economic crisis was not inevitable.In July, South Korea's harmonized unemployment rate, a metric calculated by the Organization for Economic Cooperation and Development (OECD) to enable the comparison of unemployment figures across countries, was 4.2 percent --just 0.9 percentage points higher than it was in February.Every OECD country with published July harmonized unemployment data (aside from Colombia) was performing markedly better than the United States relative to pre-pandemic levels.These measures, he argues, are the real reason consumer demand has crumpled.There is strong evidence suggesting that the fear of the virus's spread (perhaps compounded by an inadequate policy response) led to an economic slowdown before stay-at-home orders were even in place.States that gambled with their residents' lives by not shutting down or by reopening too quickly ended up with nothing to show for it economically.Since the beginning of the pandemic, states have been in a constant shuffle of reopening and shutting back down based on caseloads within their borders.Instead, he offered conflicting messages on wearing masks, downplayed the risks, pushed fake cures, and tried to turn state lockdowns into partisan issues .Now, the United States is virtually alone among wealthy countries in its mounting death count.Over August, that figure had dropped to 5, indicating a decreasing rate of growth.Germany, France, Italy, South Korea, New Zealand, and Singapore registered no change over the same period.Projecting each country's growth rates reveals that we will soon pass Italy, the United Kingdom, and Spain.Since the middle of June, however, consumer spending has remained around 7 percent below its February level.Similar trajectories have been observed in small business revenue, new job postings, and the overall employment level.Now, with the Senate still unable to pass its own bill and negotiations stalling yet again, the prospect of a new round of relief is starting to slip away.If he were to unveil a national plan to ramp up testing , work with states to minimize transmissions, and engage in negotiations with Congress to pass a new round of relief, it is still very possible that our country could get the pandemic under control and follow in the economic footsteps of some of our international peers.It seems though that the president is instead placing all of his faith in the successful development and wide distribution of a vaccine, which would surely lead to an economic rebound.Even if one of the vaccines successfully passes trials and is approved, there are already significant challenges to distributing and administering it to over 300 million Americans.Top image: OECD Chart (data.oecd.org) of United States and South Korea harmonized unemployment rates, Oct. 2019-July 2020

Starbucks billionaire Howard Schultz endorses Biden for president. "I admire Vice President Biden," Schultz told Taylor. "I know him, I've traveled with him. How could I not admire him? He served the country for 40-plus years -- he's a great man."

Former Starbucks CEO Howard Schultz publicly endorsed former Vice President Joe Biden for President in a letter published Monday.Schultz built a $4.2 billion fortune during his time at Starbucks, and pledged to donate at least some of it to Biden's campaign in the letter.Schultz considered running for president himself in 2019, but decided against it.Visit Business Insider's homepage for more stories .Howard Schultz is backing Biden for president.The future of democracy in America is on the ballot in November as America continues to battle the coronavirus pandemic and faces increasing political polarization, Schultz wrote in a letter posted to his personal website and distributed to his email list Monday.Schultz said he and his wife Sherri plan to vote for and donate to the former vice president's campaign, as well as support nonpartisan efforts to ensure the fairness of the election."Trump's defeat is but the first step to repair and rebuild our country," Schultz wrote in the letter ."The months and years to follow are a time not for Democrats to exact revenge and enact a far-left agenda.Rather, it will be a vital opportunity to bring a scarred, divided nation together."Schultz did two separate stints as the CEO of coffee giant Starbucks, first starting in 1986 and again in 2008, building himself a $4.2 billion fortune in the process.Schultz is now widely credited with growing Starbucks from a small chain in the Pacific Northwest to the international powerhouse it is today.Schultz has worked as a full-time philanthropist since departing Starbucks in 2017, he wrote in the letter .Schultz nearly competed head to head against Biden for the White House, but decided against it in September 2019.At the time, Schultz said that he feared that his planned third bid would make it easier for President Trump to get reelected."While my exploration revealed that a run for office was not the best way for me to give back to a country that has given me so much, I continue to believe that our nation can live up to our ideals, and that we all must envision and fight for a new American future," Schultz wrote in his letter of support for Biden.Regardless, the former CEO is a longtime admired of the former vice president, praising him in a March 2019 interview with Business Insider's Kate Taylor."I admire Vice President Biden," Schultz told Taylor.How could I not admire him?He served the country for 40-plus years -- he's a great man."

https://lg.lc/3/index.php?url=>972 2020-09-15 18:31:05

In shifting so much responsibility to individual people, America's government has revealed the limits of individualism: We all want to be free to make our own choices. But we need government that works well enough so we have good choices to make.

We couldn't shelter indoors, taking refuge with friends or family, because of the coronavirus .In America, our ideological conflicts are often understood as the tension between individual freedoms and collective actions.We are anything but free; our only liberty is to choose among a menu of awful options.And faced with terrible choices, we are turning on each other, polarizing against one another.You can see it in the way that people talk about personal responsibility, and the way that we see so much shaming about individual-level behavior." (You can hear my whole conversation with Marcus on this podcast .)People can choose safer activities over riskier ones -- though the language of choice too often obscures the reality that many have no economic choice save to work jobs that put them, and their families, in danger.The result is a maddening world of risk that individuals have been left to navigate virtually alone.And as the pandemic wears on, those differences sharpen, cutting into even loving bonds.Politics, too, is tipping into a darker, more dangerous place, with President Trump preemptively undermining the election, with millions out of work and furious at those they see as causing or dismissing their pain."A year from now we'll still be dealing with this situation.So I'm not here thinking about how to get through the next election.I'm thinking about how to get through the next few years."Imagine Joe Biden wins in November, and Democrats also take the Senate.Are we prepared, socially and psychically, for a vaccine that fails, or even just disappoints?Admitting that may, at some level, help us be more compassionate toward each other.But more of our ire should be directed at the government that has left us in these straits.If the US government had succeeded as Canada or Germany's governments succeeded , it would be easier to trust each other because we would pose less danger to each other.In the wreckage of state failure, though, it is nearly impossible for us to thrive.There, too, our failures as a polity have left us adrift as individuals -- free to flee our homes, but not free to breathe air that doesn't leave us choking.Our mission has never been more vital than it is in this moment: to empower you through understanding.

https://lg.lc/3/index.php?url=>982 2020-09-15 19:01:33

Life expectancy in the US increased 3.3 years from 1990 to 2015. Using vital statistics data and cause-deletion analysis, a team from Harvard determined 44% of the improvement was attributable to public health, 35% to medicines, 13% to other medical care, and 7% to unknown factors

Michael E. Chernew is the Leonard D. Schaeffer Professor of Health Care Policy and director of the Healthcare Markets and Regulation (HMR) Lab in the Department of Health Care Policy, Harvard Medical School, in Boston, Massachusetts.Mark Fendrick is a professor in the Department of Internal Medicine and director of the Center for Value-Based Insurance Design at the University of Michigan, in Ann Arbor, Michigan.David M. Cutler is the Otto Eckstein Professor of Applied Economics in the Department of Economics at Harvard University and a research associate at the National Bureau of Economic Research, in Cambridge, Massachusetts.Life expectancy in the US increased 3.3 years between 1990 and 2015, but the drivers of this increase are not well understood.We used vital statistics data and cause-deletion analysis to identify the conditions most responsible for changing life expectancy and quantified how public health, pharmaceuticals, other (nonpharmaceutical) medical care, and other/unknown factors contributed to the improvement.We found that twelve conditions most responsible for changing life expectancy explained 2.9 years of net improvement (85 percent of the total).Ischemic heart disease was the largest positive contributor to life expectancy, and accidental poisoning or drug overdose was the largest negative contributor.Forty-four percent of improved life expectancy was attributable to public health, 35 percent was attributable to pharmaceuticals, 13 percent was attributable to other medical care, and -7 percent was attributable to other/unknown factors.Our findings emphasize the crucial role of public health advances, as well as pharmaceutical innovation, in explaining improving life expectancy.ACKNOWLEDGMENTS All authors report grant support from Pharmaceutical Research and Manufacturers of America.Jason Buxbaum reports research support from the Agency for Healthcare Research and Quality (Grant No.Buxbaum has received consulting income from the University of Michigan.Michael Chernew is chair of the Medicare Payment Advisory Commission, in Washington, D.C.He has received speaking fees from American College of Cardiology, American Medical Association, America's Health Insurance Plans, BCBS of Florida, HealthEdge, Humana, MedAxiom and Washington University.He provides editorial services for Elsevier Inc. and MJH Life Sciences.He has research grants from Arnold Ventures, Agency for Healthcare Research and Quality, Centers for Medicare and Medicaid Services, National Institutes of Health, Blue Cross Blue Shield Association, Health Care Service Corporation, Ballad Health, Peterson Center on HealthCare, Robert Wood Johnson Foundation, and Commonwealth Fund.Mark Fendrick has received consulting income from AbbVie, Amgen, Centivo, Community Oncology Association, Covered California, EmblemHealth, Exact Sciences, Freedman Health, GRAIL, Harvard University, Health & Wellness Innovations, Health at Scale Technologies, MedZed, Penguin Pay, Risalto, Sempre Health, State of Minnesota, Department of Defense, Virginia Center for Health Innovation, Wellth, and Zansors.He has received research support from the Agency for Healthcare Research and Quality, Arnold Ventures, Gary and Mary West Health Policy Center, National Pharmaceutical Council, Patient-Centered Outcomes Research Institute, Robert Wood Johnson Foundation, State of Michigan, and Centers for Medicare and Medicaid Services.David Cutler has received consulting income from the American Economic Association, Colorado Center for Nursing Excellence, Journal of the American Medical Association, and the Scientific Advisory Board of F-Prime Capital Partners.He has been retained by counsel for plaintiffs to provide expert services in pending litigation involving opioid pharmaceuticals.

How Kamala Harris reflects a multiracial America | 2020 Election

How Kamala Harris reflects a multiracial America | 2020 electionMore Americans than ever consider themselves multiracial - including Kamala Harris, the Democratic vice presidential candidate for this November's election.But the multiracial experience in America is still misunderstood.We spoke with 11 people who shared their experiences and perspectives on being multiracial in America today.NewsletterGet our Essential Politics newsletterThe latest news, analysis and insights from our bureau chiefs in Sacramento and D.C.Sign Me UpYou may occasionally receive promotional content from the Los Angeles Times.Nani Sahra Walker is a video journalist and immersive producer at the Los Angeles Times.

Error404 Client Error: Not Found for url: https://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=12364708

Australia minister warns foreign journalists amid China spat

A wicked messenger falls into adversity, But a faithful envoy brings healing.--- ???Install the prerequisites:Update the submodules and build the demo:Client initiates an online key exchange:Client initiates an offline key exchange:Switch back to the server:

vault1317/signal-dakez: the improvement of public key concealing and deniablity based on OTRv3 and Signal protocol

A New Look at Iran's Complicated Relationship with the Taliban

These events led to a military mobilization on the Iranian side, and war appeared imminent.At Bonn -- where I was senior advisor to Brahimi -- Dobbins and Zarif jointly demarched me at breakfast one morning to ask why the United Nations had not included guarantees of elections and counter-terrorist cooperation in the draft agreement.Equating Iran to Saddam Hussein's Iraq, which had fought a bloody war of aggression against Iran with U.S. and Saudi help that cost the country an estimated one million lives deeply insulted Iranians, and not just regime sympathizers.After several years, Iran's position on the U.S. presence in Afghanistan turned more hostile, though it was still counterbalanced by common opposition to Sunni jihadist terrorism (though with differences on who qualified as a Sunni jihadist terrorist, notably Hamas) and Iran's need for stability along its 540-mile border with Afghanistan.These suspicions were confirmed on May 23, 2005, when Bush and President Hamid Karzai signed a " Joint Declaration of the United States-Afghanistan Strategic Partnership.On May 11, 2007, Cheney warned Iran -- while standing on the U.S. aircraft carrier John Stennis (named after a staunch white supremacist senator from Mississippi) -- that the United States was prepared to use its naval power against Iranian threats.To Iran and Russia, who had similarly hostile views of the Taliban, they emphasized a common interest in opposing the U.S. military presence in Afghanistan, while assuring them that they harbored no plans against any of Afghanistan's neighbors.At that time, the Taliban were still on speaking terms with Saudi Arabia, where King Abdullah hosted a reconciliation iftar among Afghans during Ramadan in September 2008.When Saudi intelligence chief, Prince Muqrin bin Abdulaziz, met Taliban political envoy Tayyib Agha in Jeddah, the two got into a heated argument over Taliban resistance to Saudi preconditions for acting as a mediator with the U.S. and Afghan governments.Two things happened after that meeting: Saudi Arabia became irrelevant to the peace process in Afghanistan, and Muqrin and his associates started telling their U.S. counterparts that Tayyib Agha was an Iranian agent being paid $10,000 per month by Soleimani.As a domestic counterpart of this policy, the Taliban also tried to downplay their Sunni sectarian allegiances.Periodically, intelligence reports surfaced claiming that Iran had started providing not only projectile components but also anti-aircraft weapons to the Taliban.Throughout this time Iran continued to enjoy warm relations with the Afghan government, aside from long-term interstate disputes over water, migrants, and drug trafficking.Iranian organizations such as Jundullah have adopted Sunni or even Salafi Islamism and received aid from Saudi Arabia operating through Pakistani territory.The narcotics threat became intertwined with Iran's concerns over Baloch separatism and Salafi terrorism.Subsequently, both Zakir and Mansour were reported to have spent time in Iran as guests of the Islamic Revolutionary Guard Corps.Zakir seems to have been looking for a base from which he could operate with more independence.Someone posted an image of his pseudonymous passport on the Internet, which was in a surprisingly pristine condition considering that it was supposedly salvaged from a taxi of which only charred embers remained (see photograph).In December 2018, Ali Shamkhani, secretary of Iran's Supreme Council for National Defense, visited Kabul to brief the Afghan government.More fundamentally, though Iran, like the United States, claims to be totally opposed to the drug trade and touts its efforts against it, in neither case has counter-narcotics policy prevented intelligence and military cooperation with traffickers when deemed necessary for national security.

Pennsylvania judge sets bail for accused rioters at $1M each

Several individuals accused of rioting in Lancaster, Pennsylvania, after the police shooting of Ricardo Munoz have had their bail set at $1 million .Of the nine who were given that bail amount, none were able to post it.Twelve adults have been charged with criminal conspiracy for arson, riot, institutional vandalism, failure to disperse, obstructing highways and other public passages, disorderly conduct, and defiant trespass.Nine of them had their bails set at $1 million.One of the 12 faced an additional charge of illegal possession of a firearm.According to police, at least eight of those charged are not Lancaster residents.One 16-year-old has been charged with riot, disorderly conduct, possession of instruments of crime, possession of a small amount of marijuana, propulsion of missiles onto a roadway, and institutional vandalism.The arrests happened early on Monday morning.An advocacy group called Lancaster Stands Up claimed that two of those charged were working as medics when they were arrested.The group tweeted, "The absurdly high bail amounts indicate that what we're seeing is not a measured pursuit of justice but a politically motivated attack on the movement for police reform and accountability."Protesters have taken to the streets in Lancaster over Munoz's death.The 27-year-old was shot by an officer after he ran toward the officer with a knife.Police said that the officer was responding to a call from Munoz's mother, who claimed her son was trying to break into her house.The family said that Munoz had been suffering from schizophrenia.

An extensive review of the newly published Ghidra Book

This review covers No Starch Press' Ghidra Book , which is written by Chris Eagle and Kara Nance.The book provides an extensive overview of Ghidra's capabilities, including screenshots and examples.The book starts with an introduction, stating it's not meant as a user manual, but rather how to use Ghidra when reversing.Unless you're really new to reverse engineering, most of the information in this chapter isn't too relevant.The different methods of disassembling were new to me, as I never looked into that.The usage is straightforward, but some more obscure cases are also explained in this chapter.Ghidra allows multiple analysts to work on the same binary in a shared project.Noteworthy is the comparison of Ghidra's version control commands to the commonly known Git terminology, which helps those who have experience with Git to quickly adopt Ghidra's way of working.It is possible to add more windows that are not connected in such a fashion, which can later be reconnected.These plug-ins can be written in Java and Python2, the latter is interpreted via Jython.My personal preference goes out to Java, which matches very well with Ghidra's API.In the previous chapter, an introduction into Ghidra's API functions is given.When making a simple script, one does not need the more extensive editor that Eclipse offers.Using Eclipse, three different shellcode loaders are created in a detailed and step-by-step manner.As such, this chapter will help out those who are interested in making their own loader.Additionally, one will learn about anti-virtualisation techniques, which can detect specific software, hardware, or CPU features, all of which can be used to discover more about the environment that the sample is executed in.Ghidra provides an emulator class to use within scripts, further helping the analyst.A detailed example on how to write and use the emulator is discussed within this chapter.This can help to more easily debug the sample using a debugger of choice.The Ghidra Book provides a thorough introduction for new users, using clear examples with plenty of background information.

https://lg.lc/3/index.php?url=>993 2020-09-14 13:15:20

Cyprus accuses Turkey of expanding 'illegal drilling' in East Med

Cyprus has accused Turkey of extending "illegal drilling" in disputed Mediterranean waters but said it is ready to engage in dialogue with Ankara to resolve differences over exploration rights.On Tuesday, Turkey extended the operations of its Yavuz energy drill ship in the disputed area off Cyprus until October 12, in a move that could stir tension between the island's Greek Cypriot government and Ankara."Yesterday, unfortunately a Turkish NAVTEX to expand illegal drilling by the Yavuz vessel was extended when at the same time, a series of initiatives are ongoing that seek an end to Ankara's unlawful actions and de-escalation," President Nicos Anastasiades said on Wednesday, after a meeting with European Council President Charles Michel in Nicosia.Yavuz will be accompanied by three other Turkish ships, according to a Turkish maritime notice that added "all vessels are strongly advised not to enter" the area, Turkish broadcaster TRT reported .Anastasiades's comments come a week ahead of a special summit of European Union leaders on September 24-25 to discuss how to resolve the crisis between Cyprus and Turkey.Anastasiades said Turkey was continuing its provocations in the Eastern Mediterranean, adding Cyprus would enter dialogue - but not under threats.Meanwhile, the European Commission's president on Wednesday warned Turkey against trying to intimidate Greece and Cyprus.In her annual State of the EU speech, Ursula von der Leyen said Ankara was a key partner doing important work hosting refugees but stressed "none of this is justification for attempts to intimidate its neighbours".Turkey, Greece and Cyprus have been locked in a dispute over energy resources and maritime borders in the region, with Ankara infuriating the EU countries by sending research ships with naval escorts to work in contested waters.There have been fears of conflict erupting and Cyprus is pressing the rest of the EU to impose fresh sanctions on Ankara over the drilling, a move Turkey has decried as lacking legal basis."Turkey is and will always be an important neighbour, but while we are close together on the map, the distance between us appears to be growing," Von der Leyen told the European Parliament."Yes, Turkey is in a troubled neighbourhood.And yes, it is hosting millions of refugees, for which we support them with considerable funding.But none of this is justification for attempts to intimidate its neighbours."Greece and Cyprus can count on Europe's "full solidarity on protecting their legitimate sovereignty rights", she added.Greek Prime Minister Kyriakos Mitsotakis has called for European "solidarity" on the issue and a renewed migrant crisis .Mevlut Cavusoglu, Turkey's foreign minister, said his country has been proposing to restart exploratory talks with Greece."Exploratory talks actually cover all disputed issues between Turkey and Greece ...The previous government [in Greece] ... didn't want to actually restart.And this government also has not been willing to restart the exploratory talks, so we have to make an agreement," he said.

https://lg.lc/3/index.php?url=>939 2020-09-16 11:33:41

Facebook gives in to pressure on climate-change myths -- including that antifa started deadly wildfires in western states -- with new 'science-based' hub

Facebook, long targeted by critics for allowing misinformation on global warming and other environmental developments to populate users' social-media feeds unchecked, announced it will launch a new information hub to provide "science-based information" about climate change.Now when users search for information related to climate change on Facebook or when certain posts related to the subject pop up, so, too, will a link to the Climate Science Information Center.On it, users will find data and commentary from sources including the Intergovernmental Panel on Climate Change, the U.N.The announcement comes just days after emergency responders in the Pacific Northwest had to fight misinformation on Facebook running counter to efforts to evacuate citizens in the line of the deadly wildfires.Wildfires are sparked by a variety of factors, but scientists increasingly point to climate change in contributing to the intensity and frequency of these events.The Facebook hub's launch -- in the U.S., U.K., France and Germany to start -- also comes ahead of the high-profile Climate Week, a conference to be run virtually next week by the United Nations and New York City.It's a position shift from a social-media giant that as recently as August offered push-back to mostly Democratic lawmakers seeking more action on behalf of truthful information."We asked Facebook leadership to close the loopholes that let climate disinformation spread on their platforms," Senators Elizabeth Warren, Tom Carper, Sheldon Whitehouse and Brian Schatz said in a statement last month."Their response: we should trust them to make and follow their own rules and procedures, even if it results in the distortion of facts and the mass dissemination of falsehoods.The future of our planet is at stake, and there should be no company too big, too powerful, and too opaque to be held accountable for its role in the climate crisis.Last year, Facebook removed a "false" rating from an op-ed published by the Washington Examiner that cast doubt on the accuracy of climate-change models.Initially, Facebook's independent fact checker flagged the article as "highly misleading," based on what it said was the inclusion of inaccurate information and cherry-picked data.But a nonprofit known as the CO2 Coalition, created by former Donald Trump adviser William Happer, protested the rating, and Facebook capitulated, dropping the warning and allowing the post under an "opinion" loophole.That labeling policy had always existed, Facebook stressed at the time.In addition to the information hub, Facebook said it will continue to reduce the distribution of posts containing false information on its News Feed feature and will label such posts as false.Facebook, however, says it will not remove the posts, and it was also not immediately clear how the company will deal with posts within private groups believed to contain information contradictory to what increasingly is mainstream adoption of the still-evolving science around man-made acceleration of climate change.Facebook has set its own goal, similar to those of many tech giants, to achieve net-zero carbon emissions and be supported fully by renewable energy in its own operations.The steps on climate change follow similar moves for the company surrounding information sharing on COVID-19 and voting in a presidential-election year.So far, Facebook says that over 2 billion people have been directed to resources from health authorities by its COVID-19 response.Facebook shares are up nearly 33% so far in 2020.

https://lg.lc/3/index.php?url=>938 2020-09-16 11:19:30

U.S. News & World Report Releases Best Colleges Rankings

A quality education from a top college can lead to many career opportunities for graduates.The best National Universities include a mix of public and private research institutions that offer a diverse range of undergraduate, graduate and doctoral programs.Find out which schools topped the 2021 Best National Universities rankings and see key details about each, including costs using the latest data available to U.S. News.Regular decision application deadline: Nov. 30Regular decision application deadline: Jan. 1Regular decision application deadline: Jan. 1Regular decision application deadline: Jan. 6Regular decision application deadline: Nov. 30Regular decision application deadline: Nov. 30Regular decision application deadline: Jan. 5Regular decision application deadline: Jan. 1Regular decision application deadline: Jan. 1Regular decision application deadline: Nov. 30Regular decision application deadline: March 1Regular decision application deadline: Jan. 15Massachusetts Institute of Technology4 (tie).California Institute of Technology9 (tie).University of Southern California26 (tie).University of North Carolina--Chapel Hill28 (tie).Georgia Institute of Technology35 (tie).

https://lg.lc/3/index.php?url=>977 2020-09-16 02:18:15

Error404 Client Error: Not Found for url: https://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=12365590

A 'crossroads' for humanity: Earth's biodiversity is still collapsing

https://lg.lc/3/index.php?url=>930 2020-09-16 11:33:40

Machine Learning Attack Series: Brute forcing images to find incorrect predictions

This post is part of a series about machine learning and artificial intelligence.Now it's time to start the attacks and build mitigations.It is like fuzzing (dumb or smart) to come up with malicious input that tricks a model.The operationalized Husky AI model is accessible over an HTTP endpoint.Equipped with a model that works decently well (or not, as we will see soon), it's time to create images to challenge the model.Hence, I thought of doing the same in this case.There is still one more experiment to perform amongst these simple scenarios.My initial plan was to create many random images in a loop until I get one that scores over 50%.It will be exciting to try more advanced attacks (includ ML based ones) after fixing these issues first.Now, let's discuss how to mitigate these issues, I had a couple of ad-hoc ideas:Transfer Learning A good improvement accuracy wise will be to use "Transfer Learning" and build on top of the shoulders of a more mature model.The results so far are quite interesting for my learning experience.Let's look how I trained the model for these adversarial images:These number are still bad, so I trained for more epochs.Overfitting did not seem too much of a concern as these images are far off real huskies.Testing the mitigation (brute forcing images) To check I built this basic brute force script, which just creates a random pixel image and then runs it through the new model.With the additional training we performed, it seems quite difficult to "guess" a husky picture now.I performed about 100000 tests and the highest score achieved via random pixels was about 30% now - still a bit high so I should probably add a few more "random pixel" adversarial examples.These are the core ML threats for Husky AI that were identified in the threat modeling session so far and that I want to research and build attacks for.Links will be added when posts are completed over the next serveral weeks/months.

Stricter regulation of glass tables could prevent millions of injuries a year. Most of the injuries occurred in children under age 7 and in young adults in their early 20s, and mostly affected arms, shoulders and forehead, ranged from minor abrasions and damage to major organs and vessels, to death.

Faulty glass in tables can cause life-threatening injuries, according to a Rutgers study, which provides evidence that stricter federal regulations are needed to protect consumers.The study , published in The American Journal of Surgery , reviewed 3,241 cases in the National Electronic Injury Surveillance System database and 24 cases from a level 1 trauma center.They found most of the injuries occurred in children under age 7 and in young adults in their early 20s.Injuries that mostly affected the arms, shoulders and forehead, ranged from minor abrasions and damage to major organs and vessels, to death.Glass table injuries are common, with more than 2.5 million per year reported, many of which are treated in trauma centers and emergency departments.According to the U.S. Consumer Product Safety Commission, tempered glass is mandatory for doors but voluntary for horizontal surfaces such as tabletops, which often are made with untempered glass and are more likely to break into sharp edges that can cause severe lacerations.In the national database, 1,792 of the faulty table injuries were lacerations and 24 were blunt injuries resulting from a fall after a table broke.Most frequently injured areas were the wrist, hand and finger.About 15 percent of the injuries were classified as severe, including those to the upper and lower trunk and the wrist.At the trauma center, half of the patients suffered injuries to their deep organs, upper torso, abdomen or joint cavities and required surgery; eight percent died within a month of injury.About 70 percent of those injured were male, with most injuries occurring in people under age 7 and in their early twenties.Injuries occurred when people fell into faulty glass tables, often breaking through, or from glass after the table was broken.People who had non-glass injuries, such as striking against or falling from a glass table, occurred most often in children under age 10, with injuries most often to the face, head and mouth."It is imperative to push for stricter regulation as consumers of glass tables should not be incurring life-threatening trauma injuries due to neglect of manufacturers in not using tempered glass," said study author Stephanie Bonne, an assistant professor of surgery at Rutgers New Jersey Medical School .

Police officers tend to blame the victim in cases of non-consensual distribution of intimate images

It has been well-established that the progress of cases through the criminal justice system reflects a highly selective process of elimination, also referred to as attrition, and that this is especially true for sexual assault cases (Soulliere, 2005).Over the past 6 years, many countries have made criminal law reforms or enacted legal and non-legal measures in order to combat NCII (Henry et al., 2018a).Drawing on interviews with these stakeholders, the authors identified five key barriers to law enforcement responses to image-based sexual abuse in Australia: inconsistent laws, a lack of resources, evidentiary limitations, jurisdictional boundaries, and victim-blaming or a harm minimization attitude.Based on the above, we hypothesized that police officers will engage in victim-blaming but at lower levels than students.The police officers were also expected to apply more objective reasoning regarding offender culpability and appropriate punishment.However, other phone calls from friends and family members made her realize that it was real.During summer vacation, she took some naked pictures of herself, but they were only for her own personal use.However, other phone calls from friends and family members made her realize that it was real.The three blaming items were taken from previous research on perceptions of criminal cases (e.g., Shechory-Bitton and Zvi, 2015 , 2016 , 2019).A significant gender difference was found as well [$F (1, 297) = 6.42$, $p = 0.012$, $e 2 = 0.021$], revealing that males tended to blame the victim more than females, with small effect size.The only significant difference found was a condition difference [$F (1, 297) = 31.51$, $p < 0.001$, $e 2 = 0.096$], with a moderate effect size, so that victim and offender shared blame was higher when the victim's photos were self-taken than when they were not.The general mean for supporting Maximum punishment was high (4.18 in a range of 1-5), with no significant differences by group, condition, or gender.Reality shows that many NCII victims were, in fact, photographed or video recorded by means of hidden surveillance.Regardless, according to this narrative, they may still be blamed for the mere violation of gendered social expectations.A victim who has chosen to express her sexuality may be perceived as defying social norms, resulting in greater victim-blaming.It seems that police officer training and experience may contribute to a more balanced approach toward NCII cases.It should also be noted that the study relied on self-reports, and may have thus been subjected to social desirability bias.However, recent research suggests that image-based sexual abuse actually involves female and male victims at similar rates (Powell et al., 2019).It is also possible that despite awareness, the entrenched gendered social perception, whereby only women can be victims of sexual violence remains dominant.Police perceptions of rape victims and the impact on case decision making: a systematic review.

Espressif ESP32: Bypassing Flash Encryption by leveraging a design weakness (CVE-2020-15048) in combination with EMFI

The typical approach of making modifications to the plain-text code or data stored in external flash is not possible any more once Flash Encryption is enabled.The decryption key is stored in OTP-memory and cannot be access directly from software.It's important to note that the decryption key is actually not used as-is.It is actually used to generate unique keys for each 32-byte block in the external flash.For example, when ECB mode is used it's possible to swap blocks and when CBC mode is used it's possible to flip bits.This is exactly what we leverage, in combination with several design and implementation issues, to bypass Secure Boot using a very similar attack as described in our previous post .Without further investigation we do not exactly know what the parts are.This information allows us to know, without analyzing the flash communication itself, exactly when what is copied.For example, the ROM will print the following if these values are set to 0x41414141 , even though it will result in a chip that does not boot as these values are invalid.Nonetheless, brute forcing an arbitrary value, considering we do roughly 10 experiments per second, takes more than 10 years (i.e. search space is 2^32).It allows us to identify if the attack is applicable using a fully controlled environment.Even though a real-world attacker is unable to do so, it's not unlikely an attack will do the vulnerability identification on a development board as well.We started our experiments by overwriting part ' E ', in a plain-text flash image, entirely with address pointers to a function in ROM that prints something on the serial interfaces.Nonetheless, this is definitely a valid approach for working towards attack identification.Even though this attack window is rather large, we are really affected by timing as we know that part ' E ' is entirely overwritten with the address pointer.Moreover, as it was late, and some test runtime was ahead of us, we decided to simply set only the last two 4-byte words of part ' E ' to the address pointer.Achieving success After roughly 300,000 experiments, which took roughly 12 hours, we got two successful glitches for which the results are shown in the picture below.We demonstrated an attack on the ESP32 that bypasses both Secure Boot , even when its Flash Encryption feature is enabled.Nonetheless, we believe the results described in this post are important as it shows that Fault Injection attacks are effective even when control over the environment is (very) limited.Stay tuned for our final post in this series on the ESP32 where we describe an attack that bypasses Secure Boot and Flash Encryption in order to extract the plain-text data from external flash using only a single glitch.

A study analyzing infections with four seasonal coronaviruses in humans shows that reinfections can occur within 12 months of initial infection, coupled with changes in virus-specific antibody levels. Thus, protective immunity against seasonal cornonaviruses, including SARS-COV-2, may be short-lived

A total of 513 serum samples from the Amsterdam Cohort Studies on HIV infection and AIDS 3 were examined.Whether the study individuals experienced acute infection by Epstein-Barr virus was not tested.Self-reported symptoms of influenza-like illnesses (ILIs) were documented at each study visit (Supplementary Table 4).Inclusion criteria for patients were as follows: age 18 years or older with an acute or worsened cough (<=28-d duration) as the main symptom or any clinical presentation considered by the general practitioner to be caused by a lower respiratory tract infection and consulting for the first time for this illness episode.The study was approved by the local ethics committees in all participating centers and by the competent authority in each country: Cardiff and Southampton (United Kingdom): Southampton & South West Hampshire Research Ethics Committee A; Utrecht (Netherlands) Medisch Ethische Toetsingscommissie Universitair Medisch Centrum Utrecht; Barcelona (Spain): Comite etic d'investigacio clinica Hospital Clinic de Barcelona; Mataro (Spain): Comite d'Etica d'Investigacio Clinica (CEIC) del Consorci Sanitari del Maresme; Rotenburg (Germany): Ethik-Kommission der Medizinischen Fakultat der Georg-August-Universitat Gottingen; Antwerpen (Belgium): UZ Antwerpen Comite voor Medische Ethiek; Lodz, Szeczecin and Bialystok (Poland): Komisja Bioetyki Uniwersytetu Medycznego W Lodzi; Milano (Italy): IRCCS Fondazione Ca Granda Policlinico; Jonkoping (Sweden): Regionala etikprovningsnamnden i Linkoping; Bratislava (Slovakia): Etika Komisia Bratislavskeho; Gent (Belgium): Ethisch Comite Universitair Ziekenhuis Gent; Nice (France): Comite de Protection des Personnes Sud-Mediterranee II, Hopital Salvator; and Jesenice (Slovenia): Komisija Republike Slovenije za Medicinsko Etiko.Detailed information on experimental design and reagents is supplied in the Life Sciences Reporting Summary.As a result, HCoV-NL63 (strain Amsterdam-1) is the only virus that can be used in neutralization tests.The N protein, and specifically its NCt, was chosen for this study because it is conserved within each species yet is the least conserved between species (Supplementary Table 1).After a washing, alkaline phosphatase-conjugated AffiniPure Goat Anti-Human IgG, Fc Fragment Specific (Jackson ImmunoResearch, catalog no.All sera were tested in duplicate or triplicate and normalized (replicates were performed on newly made dilutions of the same serum sample) to correct for differences in lumination times.LLC-MK2 cells were cultured in minimal essential medium with Earle's salt (Gibco), non-essential amino acids (Sciencell), L-glutamine 200 uM (Lonza) and penicillin-streptomycin (Lonza), 100 U ml -1 each, supplemented with 10% heat-inactivated fetal calf serum (Greiner Bio-One).The 96-well plates were incubated at 33 degC, and, after 7 d, cytopathic effect was scored visually and confirmed with a cell viability assay (CellTiter 96 AQueous One Solution Cell Proliferation Assay, Promega).We first measured the natural fluctuation among consecutive visits in measles virus antibodies for all ten individuals, assuming that measles infections did not occur during follow-up, as all individuals were vaccinated during childhood.Fold changes in antibody OD for measles virus ranged between 0.85 and 1.28 (Extended Data Fig.Indeed, reporting of any ILI symptom and fever (>38 degC > 3 d) alone were significantly associated with a >= 1.40 rise in antibodies (Fisher's exact test, P = 0.028 and P = 0.024, respectively; Supplementary Table 4).The low sensitivity for HCoV-HKU1 cannot be fully explained, but the unexpected low OD fold changes below 1.0 indicate that antibody levels were already elevated on V1 and started decreasing before V2, which might be a specific feature for this virus.For HCoV-NL63, HCoV-229E and HCoV-OC43, only one of 47 paired sera tested positive using our serological assay.Intra-betacoronavirus cross-reactivity: Cross-reactive antibody increases were observed for both seasonal betacoronaviruses, but, in all cases, a higher OD rise was observed to the NCt of the matching RT-PCR-confirmed virus (Extended Data Fig.We, therefore, concluded that there are no significant signs of cross-reactivity between the seasonal alpha- and betacoronaviruses.All analyses were performed using R version 3.6.2, with the following packages: reshape2, plyr, dplyr, zoo, EnvStats, survival and survminer.

New Climate Maps Show a Transformed United States

ProPublica is a nonprofit newsroom that investigates abuses of power.Sign up to receive our biggest stories as soon as they're published.According to new data from the Rhodium Group analyzed by ProPublica and The New York Times Magazine, warming temperatures and changing rainfall will drive agriculture and temperate climates northward, while sea level rise will consume coastlines and dangerous levels of humidity will swamp the Mississippi River valley.Taken with other recent research showing that the most habitable climate in North America will shift northward and the incidence of large fires will increase across the country, this suggests that the climate crisis will profoundly interrupt the way we live and farm in the United States .See how the North American places where humans have lived for thousands of years will shift and what changes are in store for your county.

Error502 Server Error: Bad Gateway for url: http://www.geochemicalperspectivesletters.org/article2029/

Diamond forms at low pressure setting in nature

Error502 Server Error: Bad Gateway for url: http://www.righto.com/2020/09/reverse-engineering-first-fpga-chip.html

Reverse-engineering the first FPGA chip, the XC2064

Tens of thousands forced to turn to food banks for first time as demand soars during pandemic, figures show - 'New wave' of UK families who have never needed help before struggling to make ends meet due to falling incomes and rising costs

Analysis published by the Trussell Trust, the UK's largest food bank provider, estimates that 846,000 food parcels will be distributed in October to December this year - with six given out every minute - as furlough comes to an end and unemployment is set to rocket.It comes as separate findings published by Action for Children indicate that a "new wave" of families who have never needed help before are struggling to make ends meet due to falling incomes and rising household costs - with 71 per cent of households supported by the charity's emergency appeal having not had financial issues before the pandemic.In one case, parents Leah Gale, 25, and Carl, 28, from Sherborne in Dorset, found themselves struggling to afford the basics for their three children - Jayden, six, Colby, four, and Evelyn, two - when work dried up for Carl, a self-employed painter and decorator, during lockdown.Leah Gale, who has three children -Jayden, Cloby and Evelyn - says she and her family has 'never struggled like this before'(Action for Children)"As Carl is self-employed, we're not entitled to any government help or furloughing or anything, so we've been forced to borrow left, right and centre from family and friends as well as take out a loan to cover the council tax.Covering life's basic expenses since March has pushed us into the most debt we've ever been in - and it doesn't look like things will get better for a long while yet."She said the rise was made up of a combination of people who had lost their jobs and weren't offered furlough or had no recourse to public funds, those still in work but with reduced hours, those whose benefits don't cover their needs and rough sleepers who were placed in hotels during lockdown but have now had to leave.Explaining that many had never used a food bank before, she said: "People turn up and break down into tears.Ms Woods said she was concerned about the months ahead, adding: "We are preparing for a tsunami.Right now it feels calm, but there will be increasing unemployment when the furlough scheme ends and more people lose their jobs and have to go on benefits."Sally Noden, who runs Action for Children's Newcastle family support service, which has been working in partnership with the city's West End food bank, said she and her team had supported many families who hadn't needed help before - often single parents who had lost their income due to the pandemic.Ministers are being urged to put a "protective shield" around struggling families by not withdrawing the PS20-a-week increase in universal credit, which was announced in response to the pandemic, and by boosting child benefit this winter, to prevent a generation of children from being "scarred by poverty".Jonathan Reynolds, Labour's shadow work and pensions secretary, urged the government to take "further, urgent action" to make sure that no one goes hungry during the public health crisis."Months into this crisis too many people are still falling through the gaps in the safety net and children are going hungry as a result.Emma Revie, chief executive of the charity, warned that food banks and other community charities could not "continue to pick up the pieces", adding: "Our research finds that Covid-19 has led to tens of thousands of new people needing to use a food bank for the first time.The Budget and comprehensive spending review present a pivotal opportunity to put things right."Carol Iddon, deputy chief executive at Action for Children, said families were "hanging by a thread" as they faced one of the "bleakest winters of their lives"."While parents on low incomes are starting to buckle, a new wave of families who've never needed help before are now also struggling to make ends meet," she added."The government must put a protective shield around struggling families by ensuring that November's Budget makes clear that universal credit will not be cut by PS20 a week in the spring."Students at South Hill School in Hemel Hempstead wave as they display a butterfly heart posterA government spokesperson said: "We have provided PS9.3bn extra welfare support to help those most in need, including increasing universal credit by up to PS20 a week, as well as introducing income protection schemes, mortgage holidays and additional support for renters.

https://lg.lc/3/index.php?url=>920 2020-09-16 10:52:52

malicious-hisilicon-scripts: Materials from my older (2018) HiSilicon research

Dismiss GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.Sign up Materials from my older (2018) HiSilicon research.When I watched the fantastic research talk from @PaulMarrapese at #defcon28 , just realized that I have some older, related, but unreleased stuff about IP cameras with HiSilicon firmware.Here are some of my older scripts.WARNING: these are intended for research use only, do not use it in production environment without prior testing, it could cause damage to the firmware.Discover IP cameras on current LAN.Reset password (unauthenticated).It is registered as a critical CVE (CVE-2020-9529) now by @PaulMarrapese Enable/Disable Telnet by the hidden backdoor command printscreen ;)pwn_cam.py : RCE by uploading malicious (wifi.conf) configuration.Please be careful, it could harm the device.Supported functions by the script:read /etc/shadow update /etc/shadow (useful for accessing the device by telnet because the factory default root password is still unknown) restore /etc/shadow to factory default (hardcoded in the script)resetting password (unauthenticated, that is without knowing the current one) setting our predefined root password in the OS (by exploiting RCE) enabling telnet by issuing the hidden backdoor command arbitrary RCE in the OS through the telnet interface as root

https://lg.lc/3/index.php?url=>833 2020-09-14 13:02:23

Cratons Mark the Spot for Sediment-Hosted Bonanzas - 85% of sediment-hosted base metals, including all giant deposits (>10 megatonnes of metal), occur within 200 kilometres of the transition between thick and thin lithosphere.

Metals are ingredients of many rocks, but to be exploitable, some process must concentrate them into localized deposits.For lead, zinc, copper, and nickel (collectively known as base metals), such deposits are either magmatic, associated with volcanism, or sedimentary, associated with material collected at the bottom of an inland body of water.Sedimentary deposits generally provide the biggest jackpot for mining companies, with some finds containing more than 10 megatonnes of metal.In-demand metals include "lead, zinc, copper, and nickel, but also lots of other metals that are accessories to these big deposits, such as cobalt, which goes into car batteries."Considering that about three quarters of the world's continents are covered by sedimentary basins, knowing to start looking there is of little help in detecting giant deposits.A first hint at how to limit the search space came from northern Australia, where Hoggard and his colleagues noticed that a number of large zinc deposits line up rather neatly along an arc.But it wasn't clear what geological feature was connected to that shape.The group had been working on improved models of how seismic waves travel through Earth's interior.A statistical analysis confirmed that what they saw was not due just to chance.That process generally starts with an inland sea becoming increasingly salty through evaporation.When compressed by subsequent layers of sediment, these precipitates turn into salt rocks, such as gypsum, anhydrite, and halite.The brine may keep circulating in this way through sedimentary layers for long periods (there is some debate whether those periods are millions of years at a stretch or come in shorter bursts), scavenging metals as it flows.Black shales, for instance, composed of mud sediments laid down in deeper portions of the inland sea, provide just such conditions, and build up metal deposits in their interstices.Such basins might even get stacked atop each other, as the lithosphere cycles through stretching and compressing phases."Our maps work everywhere, including in continents where a geologist's boot rarely hits the ground...and we can provide an actual probability that a deposit exists, which is what companies need to make financial decisions."The research documenting deposits on the craton's edge clearly has practical implications.According to Hoggard, "our maps work everywhere, including in continents where a geologist's boot rarely hits the ground--for instance, in parts of Africa and Antarctica--and we can provide an actual probability that a deposit exists, which is what companies need to make financial decisions."For instance, some sedimentary metal deposits in North America have been dated to 0.5-1.5 billion years old.But according to him, such relationships so far had not been established for sedimentary deposits.Even if someone had an inkling of the relationship before now, they wouldn't have been able to test it like we can today."Any reuse without express permission from the copyright owner is prohibited.

https://lg.lc/3/index.php?url=>945 2020-09-15 18:43:20

CVE-2020-16171: Exploiting Acronis Cyber Backup for Fun and Emails

You have probably read one or more blog posts about SSRFs, many being escalated to RCE.While this might be the ultimate goal, this post is about an often overlooked impact of SSRFs: application logic impact.This post will tell you the story about an unauthenticated SSRF affecting Acronis Cyber Backup up to v12.5 Build 16341 , which allows sending fully customizable emails to any recipient by abusing a web service that is bound to localhost.The fun thing about this issue is that the emails can be sent as backup indicators, including fully customizable attachments.The solution itself consists of dozens of internally connected (web) services and functionalities, so it's essentially a mess of different C/C++, Go, and Python applications and libraries.The application's main web service runs on port 9877 and presents you with a login screen:Now, every hacker's goal is to find something unauthenticated.So I've started to dig into the source code of the main web service to find something cool.Actually, it didn't take me too long to discover that something in a method called make_request_to_ams :The main interesting thing here is the call to get_ams_address(request.headers) , which is used to construct a Uri.The application reads out a specific request header called Shard within that method:When having a further look at the make_request_to_ams call, things are getting pretty clear.So this is a pretty straight-forward SSRF including a couple of bonus points making the SSRF even more powerful:While most of CyberBackup's routes are only reachable with authentication, there is one interesting route called /api/ams/agents which is kinda different:So we've found our attackable route without authentication here.Apart from doing meta-data stuff or similar, I wanted to entirely fire the SSRF against one of Cyber Backup's internal web services.There are many these, and there are a whole bunch of web services whose authorization concept solely relies only on being callable from the localhost.This service offers a variety of functionality to send out notifications.I'm not going through the send_external_email method in detail since it is rather complex, but this endpoint essentially uses parameters supplied via HTTP POST to construct an email that is send out afterwards.While both values tenant_id and jwt are not explicitly validated here, they are simply used in a new hardcoded call to the API endpoint /api/account_server/tenants/ which ultimately verifies the authorization:

https://lg.lc/3/index.php?url=>837 2020-09-15 15:55:04

San Francisco To Provide $1,000/Month To Pregnant Black, Pacific Islander Women To Improve Health Outcomes

SAN FRANCISCO (CBS SF) -- The City of San Francisco will pay Black and Pacific Islander women $1,000 a month during their pregnancies and after birth in a pilot program to study how the monthly support helps achieve better maternal health and birthing outcomes.The Abundant Birth Project will provide the monthly supplement to approximately 150 women in San Francisco for the duration of their pregnancy and the first six months of the baby's life, with the goal of eventually providing the supplement for up to two years post-pregnancy, according to a press statement from Mayor London Breed.The program is being launched in conjunction with Expecting Justice, a Black-led birth justice initiative lead by Dr. Zea Malawa at the San Francisco Department of Public Health and supported by the Hellman Foundation and the UCSF California Preterm Birth Initiative.Expecting Justice will study the resulting health impacts of the program, the first of its kind in the U.S.According to Expecting Justice, a Black infant in San Francisco is almost twice as likely to be born prematurely compared to a White infant, while the preterm birth rate for Pacific Islanders in the city is over 10%, nearly three points higher than the national preterm birth rate for Asians and Pacific Islanders.The disparity is not related to race, but rather racism, according to Expecting Justice, citing historically racist policies as well as modern-day discrimination which it says underscore the wealth gap among Black and Pacific Islander communities and other racial or ethnic groups in San Francisco.Black families also account for half of the maternal deaths and over 15% of infant deaths, despite representing only 4% of all births.Pacific Islander families face similar disparities, according to Expecting Justice."Providing guaranteed income support to mothers during pregnancy is an innovative and equitable approach that will ease some of the financial stress that all too often keeps women from being able to put their health first," said Mayor Breed in a prepared statement."The Abundant Birth Project is rooted in racial justice and recognizes that Black and Pacific Islander mothers suffer disparate health impacts, in part because of the persistent wealth and income gap."Funding for the public-private partnership includes grants from the Hellman Foundation, Twitter CEO Jack Dorsey's #startsmall campaign, Genentech, and the San Francisco Department of Public Health among other donors."Structural racism, which has left Black and Pacific Islander communities particularly exposed to COVID-19, also threatens the lives of Black and PI mothers and babies," said Dr. Zea Malawa in a prepared statement."Providing direct, unconditional cash aid is a restorative step that not only demonstrates trust in women to make the right choices for themselves and their families, but could also decrease the underlying stress of financial insecurity that may be contributing to the high rates of premature birth in these communities.It is exciting to be in a city that not only calls out racism as a problem, but also takes steps to heal the wounds left by decades of injustice and anti-Black sentiment."In San Francisco, the median annual household income for Black and Pacific Islander families is close to $30,000 and $67,000 respectively, compared with over $104,000 citywide, according to the city.The Abundant Birth Project will work with local prenatal care providers and the city's network of pregnancy support services to identify and enroll eligible clients over the next two years.The project will target low-income and middle-income pregnant people with the income supplement given the high cost of living in San Francisco.The Abundant Birth Project is a collaboration between the Department of Public Health, the California Preterm Birth Initiative at UCSF, UC Berkeley School of Social Welfare, the San Francisco Human Rights Commission, the San Francisco Treasurer's Office, the San Francisco Human Services Agency, and First 5 San Francisco.

https://lg.lc/3/index.php?url=>988 2020-09-15 18:11:56

BASH. Generate your reverse shell with proper IP address and port. Highly inspired by pentester monkey website

Dismiss GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.Sign up This script will generate your reverse shell with proper IP address and port.Ideal for CTF and HTB challenges .Use on your own risk

https://lg.lc/3/index.php?url=>824 2020-09-14 07:19:34

Bari fucking Weiss is their example?From what I've read, Weiss tattled on her coworkers who didn't toe the line she liked and was partly responsible for that pro-fascism op-ed by Cotton.This is a lot of words and ink for what essentially boils down to whining how unfair it is that they can no longer use the f-word and n-word.

cancel culture and speech regulation make a toxic mix

https://lg.lc/3/index.php?url=>974 2020-09-15 16:58:12

AboutPressCopyrightContact usCreatorsAdvertiseDevelopersTermsPrivacy Policy and SafetyHow YouTube worksTest new features Every Political Ad Ever - YouTube

Every Political Ad Ever

https://lg.lc/3/index.php?url=>986 2020-09-16 03:46:20

New Pew survey says US Image Plummets Internationally

German Chancellor Angela Merkel looks past then-International Monetary Fund Managing Director Christine Lagarde toward U.S. President Donald Trump during a working breakfast at the G7 Summit in Quebec City, Canada, on June 9, 2018.As a new 13-nation Pew Research Center survey illustrates, America's reputation has declined further over the past year among many key allies and partners.The publics surveyed also see Trump more negatively than other world leaders.For instance, supporters of Spain's Vox party are particularly likely to view Trump in a positive light: 45% are confident in his ability to handle international affairs, compared with only 7% among Spaniards who do not support Vox.Many demonstrations took place during or directly prior to the fielding of our survey.These opinions are in stark contrast to the very favorable assessments Germans had during Barack Obama's presidency, but roughly on par with views at the end of George W. Bush's tenure.In Germany, people who have a favorable view of the right-wing Alternative for Germany (AfD) are much more likely than those with an unfavorable view of the party to have a positive opinion of the U.S. (43% among party supporters vs. 22%) or to trust Trump's approach to international affairs (34% vs. 5%).Current ratings are back to their 2017 low: Only 17% believe Trump would do the right thing regarding world affairs.Still, South Korea stands out for its people's views of the U.S. as an economic leader.In every country surveyed, men have a more positive assessment of the U.S. than women.These numbers are particularly low when compared to how publics think other countries and organizations have handled the outbreak.Those who hold favorable views of right-wing populist parties are more likely than those who hold unfavorable views to think the U.S. has dealt with the virus effectively.Just one-in-five or fewer in Canada and Western Europe trust the president to do what is right.There has been some variability in Trump's confidence ratings over the last few years, but overall, current ratings are consistent with those at the start of his presidency in 2017.In contrast, Spaniards have more confidence in Trump now (16%) than they did four years ago, when they had one of the lowest levels of confidence measured (7%).In Australia, the UK, Italy, Canada, Sweden, the Netherlands and France, those with less than a secondary education have more confidence in Trump than those with more education.A similar pattern can be seen in every country surveyed except France.Mirroring the ideological divide, people who have a favorable opinion of right-wing populist parties in Europe also have more trust in the U.S. president than those with an unfavorable view of these parties.As is the case for ratings for the U.S. president, people who support right-wing populist parties in Europe are more likely to express confidence in Putin and Johnson than people who do not support these parties.The opposite pattern is true for Merkel and Macron; backers of populist parties in Europe tend to have less confidence in the leaders of Germany and France.

Brain Aromatase and the Regulation of Sexual Activity in Male Mice: Testosterone activates male sexual behavior in part via conversion to estrogen (estradiol) in the brain via the enzyme aromatase which is encoded by a single gene

Thus, local estrogen production via aromatase expression in these regions of the brain may be critical for normal reproductive function and behavior.Reverse transcription (RT) was performed using 1 ug of total RNA with qScript cDNA SuperMix (Quanta Biosciences, Gaithersburg, MD).Aromatase mRNA in the hypothalamus, testis, epididymis, and gonadal fat was analyzed by real-time quantitative PCR using tissue-specific primers (Fig.Overall, intact bArKO mice spent less total time engaged in sexual behaviors such as mounting or intromission (Fig.Sexual activity was measured in 12- to 14-week-old intact (noncastrated) bArKO, tArKO, and littermate control male mice over two 30-minute trials.Sexual activity was measured in 12- to 14-week-old intact (noncastrated) bArKO, tArKO, and littermate control male mice over two 30-minute trials.Mount and intromission behaviors were not observed in 5 intact tArKO mice analyzed across a total of 10 trials (Fig.Both castrated bArKO and heterozygous control mice treated with vehicle or E 2 alone showed negligible sexual behavior (mounts/intromissions, Fig.Note that brain E 2 levels in bArKO mice were significantly reduced compared with controls, as expected (see Fig.Serum FSH (K) and LH (L) levels following steroid hormone replacement in castrated bArKO mice were measured by RIA.Serum FSH (K) and LH (L) levels following steroid hormone replacement in castrated bArKO mice were measured by RIA.It is possible that alternative splicing events upstream of the first exons might result in previously unreported mRNA species.Additionally, no in-frame ATG codons are observed until exon 5, which if utilized would result in a severely truncated protein.Also, other whole-body ArKO models using our approach to ablate aromatase did not identify any abnormal mRNA or protein isoforms (27).However, we were not able to detect a statistically significant difference in circulating LH and FSH levels between bArKO, tArKO, or control/Het mice.In contrast to the previous studies, we employed LC-MS/MS that is much more sensitive and specific for measuring E 2 compared with antibody-based assays.It is also possible that T may be converted to E 2 at very small quantities in tArKO mice via an as yet unknown mechanism or through some low amount of aromatase expression in tArKO mice, which remained below the sensitivity of real-time quantitative PCR.Alternatively, perinatal T and dihydrotestosterone activation of brain androgen receptors may be sufficient for this process to occur in the mouse.Relatively few studies have investigated the direct effect of an aromatase inhibitor or estrogen supplementation on male sexual behavior (25 , 62 , 63).Shift from androgen to estrogen action causes abdominal muscle fibrosis, atrophy, and inguinal hernia in a transgenic male mouse model

Analysis: Trump Blames California for Fires. He Should Check to See Whose Land They're On.

Forest fire management is a complex issue, but one thing is clear: the federal commitment to it has been declining for years, and Trump has done little to reverse it.The federal government's spending on fire prevention has been shrinking; the budget for vegetation management fell from approximately $240 million in 2001 to $180 million in 2015, a decline of 24 percent.The problem, in part, is that until recently, the Forest Service had no way to increase its funding in bad fire years, so unanticipated costs of firefighting had to come out of funds originally set aside for other priorities, like land management.This same report noted that in 1995, firefighting made up 16 percent of the Forest Service's annual appropriated budget; in 2020, for the first time, firefighting constituted a majority of the Forest Service's annual budget.As a result, the agency was forced to redirect dollars and staff focused on measures that could reduce the risk of fires by improving forest health.Were this problem left unchecked, Forest Service would be devoting more than two-thirds of its budget to firefighting in 2025.The ask was simple--stop forcing the Forest Service to pay for firefighting with the money intended for forest management and other programs designed to protect fish and wildlife, provide outdoor recreation, and manage rangelands and wilderness areas--all part of the agency's legislated mission--and, instead, treat these extreme fire events like the disasters they are, and pay for them out of disaster assistance funds.After years of debate, Congress finally reached a compromise in 2018 to ease this zero-sum approach by allowing the Forest Service to tap into disaster assistance funding when firefighting costs exceeded the Forest Service's annual fire suppression budget.Fixing the funding problem for firefighting was very important.Because some Republican members of the House and the Senate refused to fix the funding problems unless measures were included to limit environmental reviews and legal challenges to future timber sales and insisted that funding for future national forest timber sales be increased.According to the California office of the U.S. Forest Service, returning California's national forests to a condition that reduces future extreme fire risk would require treating 6 million to 9 million acres a year.Currently, the agency treats a small fraction of that--approximately 200,000 acres per year.The agency would need to increase the number of acres restored to approximately 500,000 acres per year at a cost of at least $300 million a year to make significant progress in reducing future wildfire risk.It would seem that reducing fuel loads that contribute to fire risk and improving forest health should be the top priority.But, political leadership in the Department of Agriculture has reinstituted timber targets as a performance measure for Forest Service leaders in addition to improving forest health.In other words, as anxiety rises about fire risk across federal lands, national forest managers are being rewarded for shifting attention and dollars away from the goal of smart maintenance.Meeting timber production goals has little to do with improving the health and resilience of national forest lands.However, it is an easy metric to assess the performance of forest managers as well as a way to satisfy the timber industry.Efforts to politicize wildfire by questioning the connection to climate change--in spite of established science--and to cast blame or assign responsibility for catastrophic fire based on party affiliation (i.e., somehow it is a problem only for states with Democratic governors), or to short circuit required project reviews for health, safety or environmental impact are counterproductive--to say the least.As the president engages in partisan blame-shifting about a crisis happening on his own watch, there's one positive example to draw from, and it's far from Washington.

Instantly become Domain Admin by subverting Netlogon cryptography (CVE-2020-1472)

Requires the latest impacket from GitHub with added netlogon structures.Do note that by default this changes the password of the domain controller account.Yes this allows you to DCSync, but it also breaks communication with other domain controllers, so be careful with this!More info and original research hereRead the blog/whitepaper above so you know what you're doing Run cve-2020-1472-exploit.py with IP and netbios name of DC DCSync with secretsdump, using -just-dc and -no-pass or empty hashes and the DCHOSTNAME$ accountIf you install a version of impacket from GitHub that was updated on or after September 15th 2020, secretsdump will automatically dump the plaintext machine password (hex encoded) when dumping the local registry secrets.Alternatively on slightly older versions you can dump this same password by first extracting the registry hives and then running secretsdump offline (it will then always print the plaintext key because it can't calculate the Kerberos hashes).With this password you can run restorepassword.py with the -hexpass parameter.This will first authenticate with the empty password to the same DC and then set the password back to the original one.Make sure you supply the netbios name and IP again as target, so for example:

Learn Python & Ethical Hacking From Scratch - Medium Article

170+ videos on Python programming & ethical hacking Install hacking lab & needed software (on Windows, OS X and Linux) Learn 2 topics at the same time -- Python programming & Ethical Hacking Start from 0 up to a high-intermediate level Write over 20 ethical hacking and security programs Learn by example, by writing exciting programs Model problems, design solutions & implement them using Python Write programs in Python 2 and 3 Write cross platform programs that work on Windows, OS X & Linux Have a deep understanding on how computer systems work Have a strong base & use the skills learned to write any program even if its not related to hacking Understand what is Hacking, what is Programming, and why are they related Design a testing lab to practice hacking & programming safely Interact & use Linux terminal Understand what MAC address is & how to change it Write a python program to change MAC address Use Python modules and libraries Understand Object Oriented Programming Write object oriented programs Model & design extendable programs Write a program to discover devices connected to the same network Read, analyse & manipulate network packets Understand & interact with different network layers such as ARP, DNS, HTTP ....etc Write a program to redirect the flow of packets in a network (arp spoofer) Write a packet sniffer to filter interesting data such as usernames and passwords Write a program to redirect DNS requests (DNS Spoofer) Intercept and modify network packets on the fly Write a program to replace downloads requested by any computer on the network Analyse & modify HTTP requests and responses Inject code in HTML pages loaded by any computer on the same network Downgrade HTTPS to HTTP Write a program to detect ARP Spoofing attacks Write payloads to download a file, execute command, download & execute, download execute & report .....etc Use sockets to send data over TCP Send data reliably over TCP Write client-server programs Write a backdoor that works on Windows, OS X and Linux Implement cool features in the backdoor such as file system access, upload and download files and persistence Write a remote keylogger that can register all keystrikes and send them by Email Interact with files using python (read, write & modify) Convert python programs to binary executables that work on Windows, OS X and Linux Convert malware to torjans that work and function like other file types like an image or a PDF Bypass Anti-Virus Programs Understand how websites work, the technologies used and how to test them for weaknesses Send requests towebsites and analyse responses Write a program that can discover hidden paths in a website Write a program that can map a website and discover all links, subdomains, files and directories Extract and submit forms from python Run dictionary attacks and guess login information on login pages Analyse HTML using Python Interact with websites using Python Write a program that can discover vulnerabilities in websitesComputer with a minimum of 4GB ram/memory Operating System: Windows / OS X / LinuxWelcome this great course where you'll learn python programming and ethical hacking at the same time, the course assumes you have NO prior knowledge in any of these topics, and by the end of it you'll be at a high intermediate level being able to combine both of these skills and write python programs to hack into computer systems exactly the same way that black hat hackers do, and use the programming skills you learn to write any program even if it has nothing to do with hacking.From here onwards you'll learn everything by example , by writing useful hacking programs, so we'll never have any boring dry programming lectures.The course is divided into a number of sections, each aims to achieve a specific goal, the goal is usually to hack into a certain system, so we'll start by learning how this system work and its weaknesses, and then you'll lean how to write a python program to exploit these weaknesses and hack the system, as we write the program I will teach you python programming from scratch covering one topic at a time, so by the end of the course you're going to have a number of ethical hacking programs written by yourself (see below) from backdoors, keyloggers, credential harvesters, network hacking tools, website hacking tools and the list goes on .You'll also have a deep understanding on how computer systems work, how to model problems, design an algorithm to solve problems and implement the solution using python.ARP Spoofing -- redirect the flow of packets in a network.Spying on any client connected to the network -- see usernames, passwords, visited urls ....etc.Inject code in pages loaded by any computer connected to the same network.execute_and_report payload -- executes a system command and reports result via email.download_and_execute payload -- downloads a file and executes it on target system.download_execute_and_report payload -- downloads a file, executes it, and reports result by email.Download & upload files keylogger -- records key-strikes and sends them to us by email.Setting up a penetration testing lab to practice hacking safely.Installing Kali Linux and Windows as virtual machines inside ANY operating system.This course is created for educational purposes only and all the attacks are launched in my own lab or against devices that I have permission to test.you learn to build using Python a wealth of hacking tools.I totally recommend it to anyone keen on learning ethical hacking the programmer's way!Becoming an ethical hacker is simple but not easy, there are many resources online but lots of them are wrong and outdated, not only that but it is hard to stay up to date even if you already have a background in cyber security.Our goal is to educate people and increase awareness by exposing methods used by real black-hat hackers and show how to secure systems from these hackers.

Physicists Discover New Magnetoelectric Effect: In a very unusual way, the electrical and magnetic properties of a particular crystal are linked together

However, the phenomenon is much more complicated: electrical and magnetic properties of certain materials are also coupled with each other.Electrical properties of some crystals can be influenced by magnetic fields - and vice versa.In this case one speaks of a "magnetoelectric effect".It plays an important technological role, for example in certain types of sensors or in the search for new concepts of data storage.A special material was investigated for which, at first glance, no magnetoelectric effect would be expected at all.But careful experiments have now shown that the effect can be observed in this material, it only works completely differently than usual."Whether the electrical and magnetic properties of a crystal are coupled or not depends on the crystal's internal symmetry," says Prof. Andrei Pimenov from the Institute of Solid State Physics at TU Wien."If the crystal has a high degree of symmetry, for example, if one side of the crystal is exactly the mirror image of the other side, then for theoretical reasons there can be no magnetoelectric effect".This applies to the crystal, which has now been examined in detail - a so-called langasite made of lanthanum, gallium, silicon and oxygen, doped with holmium atoms."The crystal structure is so symmetrical that it should actually not allow any magnetoelectric effect."But if we increase the strength of the magnetic field, something remarkable happens: The holmium atoms change their quantum state and gain a magnetic moment."Polarization is when the positive and negative charges in the crystal are displaced a little bit, with respect to each other", explains Pimenov."This would be easy to achieve with an electric field - but due to the magnetoelectric effect, this is also possible using a magnetic field"."The relationship between polarization and magnetic field strength is approximately linear, which is nothing unusual," says Andrei Pimenov."The magnetoelectric effect will play an increasingly important role for various technological applications," says Andrei Pimenov."In a next step, we will try to change magnetic properties with an electric field instead of changing electrical properties with a magnetic field.If this succeeds, it would be a promising new way to store data in solids."They are generated with magnetic coils, which requires a relatively large amount of energy and time.Prof. Andrei Pimenov Institute for Solid State Physics TU Wien Wiedner Hauptstrasse 8-10, 1040 Vienna T: +43-1-58801-13723 andrei.pimenov@tuwien.ac.atIn a very unusual way, the electrical and magnetic properties of a particular crystal are linked together - the phenomenon was discovered and explained at TU Wien (Vienna).

Snowden warns that Assange extradition will lead free press to slaughterhouse as publisher's critics blinded by partisanship

The US drive to extradite and prosecute Julian Assange poses a grave threat to journalists everywhere, but the publisher's opponents have placed politics over principle, and even their own interests, said whistleblower Ed Snowden."I think a lot of it comes down to people forgetting what principles are and why they're important," Snowden said in an interview with Joe Rogan on Tuesday."You can hate Julian Assange, you can think he's a puppet of Russia, you can think he's the worst person on Earth - a reincarnation of Hitler or Stalin - and still realize that convicting him harms you."It harms your children's future.People forget about this in today's world where everything has become partisan.While Assange "fell out of favor" with a large segment of American society in 2016 over WikiLeaks' publication of emails belonging to then-Democratic presidential hopeful Hillary Clinton, his current extradition trial has "nothing to do with that," Snowden said."The US government... is trying to extradite this guy and put him in prison for the rest of his life for the best work that WikiLeaks ever did... which is the Iraq and Afghanistan War Logs, detainee records in Guantanamo Bay.Things that are about explicit war crimes and abuses of power," the whistleblower went on, adding that Assange's work with WikiLeaks spared no political party.Also on rt.comAssange extradition hearing adjourned after videolink failure, court fails to explain cause of problems Assange faces an 18-count indictment and up to 175 years in a US prison, with most charges linked to "espionage" over his role in securing classified leaks from Army analyst Chelsea Manning.But his case marks a clear break with American legal precedent, which has traditionally distinguished journalists and publishers from their sources, a "dangerous" development which Snowden said could impact the media as a whole."As abusive as these Espionage Act charges have run in the last 50 years, the government had a sort of quiet agreement.They never charged the press outlets... they charge their sources," he said."They are breaking that agreement with the Julian Assange case.Assange is not the source, he is merely a publisher.He runs a press organization."You cannot convict Julian Assange, the chief editor and publisher of WikiLeaks, under the Espionage Act without exposing the New York Times, the Washington Post, CBS, ABC, NBC, CNN, Fox, whoever, to the same kind of charges.Also on rt.comJulian Assange (and imperialism) on trial: In an age of 'lockdowns,' is there any hope left for the WikiLeaks founder?The WikiLeaks publisher's extradition hearing resumed last week in London after a lengthy hiatus due to the coronavirus outbreak.He remains in the maximum security Belmarsh Prison awaiting a decision, where he has spent 16 months under conditions that UN Special Rapporteur Nils Melzer has described as "torture."Think your friends would be interested?