

Space

'Return our moon dust'

NASA postpones asteroid 'mission'

NEW YORK, June 25, (AP) - NASA put an asteroid mission on hold Friday, blaming the late delivery of its own navigation software.

The Psyche mission to a strange metal asteroid of the same name was supposed to launch this September or October. But the agency's Jet Propulsion Lab was several months late delivering its software for navigation, guidance and control -- a crucial part of any spacecraft. Engineers "just ran out of time" to test it, officials said Friday.

Now the space agency is going to step back, and an independent review will look at what went wrong, when the spacecraft could launch again and even if it should go ahead, NASA planetary sciences chief **Lori Glaze** said.

NASA has already spent \$717 million on Psyche and its projected total cost, including the rocket to launch it, is \$985 million. The small car-sized spacecraft was originally supposed to arrive at its asteroid in 2026 after a journey of more than 1 billion miles.

Now that the software has been delivered, there's no known problems with the spacecraft except "we just haven't been able to test it," said **Lindy Elkins-Tanton**, the Psyche mission lead scientist.

"There is that one challenge we couldn't overcome in time to launch in 2022 with confidence," she said.

There are still at least two launch opportunities next year and more in 2024 to get to the asteroid that sits in the belt between Mars and Jupiter, said JPL Director **Laurie Leshin**. That means Psyche wouldn't arrive at its asteroid until 2029 or 2030.

But calculating launch times is complicated because the mission needs the proper sunlight conditions and the asteroid "is spinning like a rotisserie chicken instead of like a top," Elkins-Tanton said.

Two other small missions were going to ride along on the SpaceX Falcon heavy rocket and NASA is looking at what will happen to those.

Psyche is just the latest in NASA's fleet of asteroid-exploring spacecrafts. Osiris-Rex is on the way back to Earth with rubble from the asteroid Benu. Last year, NASA launched the ships Lucy and Dart to explore other space rocks and test if a rocket could knock off course an asteroid heading smack into Earth.

Rehearsal

Meanwhile, NASA said Thursday it has finished testing its huge moon rocket and will move it back to the launch pad in late August.

A date for the first flight will be set after a leak that popped up during a dress rehearsal is fixed, the space agency said.

Earlier this week, NASA fueled the 30-story Space Launch System rocket for the first time and pressed ahead with a critical countdown test despite a fuel line leak. Previous attempts were foiled by technical issues.

No one will be on board the debut launch that will hurl the Orion crew capsule atop the rocket to the moon and back. The initial flight will be followed by astronauts in 2024, looping around the moon and back. The third mission would attempt to land astronauts on the moon no earlier than 2025, more than a half-century after NASA's Apollo moonshots.

In another development, NASA said it wants its moon dust and cockroaches back.

The space agency has asked Boston-based RR Auction to halt the sale of moon dust collected during the 1969 Apollo 11 mission that had subsequently been fed to cockroaches during an experiment to determine if the lunar rock contained any sort of pathogen that posed a threat to terrestrial life.

The material, a NASA lawyer said in a letter to the auctioneer, still belongs to the federal government.

The material from the experiment, including a vial with about 40 milligrams of moon dust and three cockroach carcasses, was expected to sell for at least \$400,000, but has been pulled from the auction block, RR said Thursday.

"All Apollo samples, as stipulated in this collection of items, belong to NASA and no person, university, or other entity has ever been given permission to keep them after analysis, destruction, or other use for any purpose, especially for sale or individual display," said NASA's letter dated June 15.

Evidence

It went on: "We are requesting that you no longer facilitate the sale of any and all items containing the Apollo 11 Lunar Soil Experiment (the cockroaches, slides, and post-destructive testing specimen) by immediately stopping the bidding process," NASA wrote.

In another letter dated June 22, NASA's lawyer asked RR Auction to work with the current owner of the material to return it to the federal government.

The Apollo 11 mission brought more than 47 pounds (21.3 kilograms) of lunar rock back to Earth. Some was fed to insects, fish and other small creatures to see if it would kill them.

The cockroaches that were fed moon dust were brought to the University of Minnesota where entomologist **Marion Brooks** dissected and studied them.

"I found no evidence of infectious agents," Brooks, who died in 2007, told the Minneapolis Tribune for an October 1969 story. She found no evidence that the moon material was toxic or caused any other ill effects in the insects, according to the article.

But the moon rock and the cockroaches were never returned to NASA, instead displayed at Brooks' home. Her daughter sold them in 2010, and now they are up for sale again by a consignor who RR did not disclose.

It's not unusual for a third party to lay claim to something that is being auctioned, said **Mark Zaid**, an attorney for RR Auction.

"NASA has a track record of pursuing items related to the early space programs," although they have been inconsistent in doing so, Zaid said. By its own admission, NASA acknowledged in one of its letters that it did not know about the previous auction of the cockroach experiment items.

"We have worked with NASA before and have always cooperated with the U.S. government when they lay claims to items," Zaid said. "At the end of the day, we want to act appropriately and lawfully."

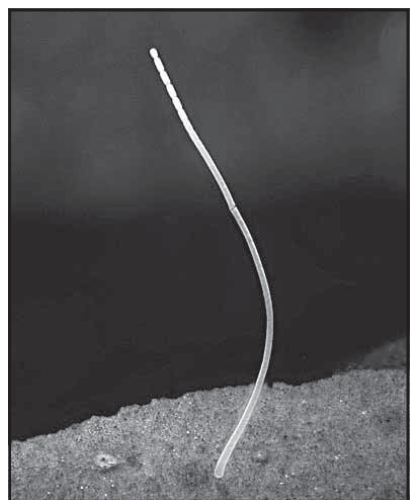
RR Auction is holding on to the lot for now, but ultimately, it's up to the consignor to work something out with NASA, he said.



Glaze



Technicians work on the Psyche spacecraft at the NASA Jet Propulsion Laboratory, April 11, 2022, in Pasadena, Calif. NASA put an asteroid mission on hold Friday, June 24, blaming the late delivery of its own navigation software. The Psyche mission to a strange metal asteroid of the same name was supposed to launch this September or October. But the agency's Jet Propulsion Lab was several months late writing and delivering its software for navigation, guidance and control. (AP)



This microscope photo provided by the Lawrence Berkeley National Laboratory in June 2022 shows a filament of a *Thiomargarita magnifica* bacteria cell. The species was discovered among the mangroves of Guadeloupe archipelago in the French Caribbean. A team of researchers at the Department of Energy (DOE) Joint Genome Institute (JGI), Lawrence Berkeley National Laboratory (Berkeley Lab), the Laboratory for Research in Complex Systems (LRC), and the Université des Antilles, characterized the bacterium composed of a single cell that is 5,000 times larger than other bacteria. (AP)

Discovery

**Agency decision irks group:** The US Forest Service has approved a new rule waiving fees for unauthorized grazing under some circumstances in a move blasted by an environmental group that says the agency is codifying lax enforcement.

The Forest Service issued the decision this month following a 2016 Government Accountability Office report that found the agency couldn't identify how much unauthorized grazing was occurring because it often handled cases informally with no documentation.

The agency issues permits to livestock producers that define when, where and how many animals - mostly cattle and sheep - are allowed on specific Forest Service grazing allotments. Violations occur when livestock are in areas outside of allowed times of the year, in unauthorized areas or when there are more animals in an area than allowed.

About 2 million cattle and 800,000 sheep and goats graze on about 150,000 square miles (390,000 square kilometers) of Forest Service land in 29 states. Most of the grazing is in the US West. The agency said it administers about 6,000 active livestock grazing permits and in the last five years has collected between \$5.4 million and \$9.2 million annually in grazing fees.

"Providing Forest Service line officers the authority to waive excess and unauthorized use fees, when certain conditions are met, provides the needed flexibility to resolve incidents using

Health

Monkeypox outbreak growing across Britain

'COVID vaccines saved 20m lives'

NEW YORK, June 25, (AP) - Nearly 20 million lives were saved by COVID-19 vaccines during their first year, but even more deaths could have been prevented if international targets for the shots had been reached, researchers reported Thursday.

On Dec. 8, 2020, a retired shop clerk in England received the first shot in what would become a global vaccination campaign. Over the next 12 months, more than 4.3 billion people around the world lined up for the vaccines. The effort, though marred by persisting inequities, prevented deaths on an unimaginable scale, said **Oliver Watson** of Imperial College London, who led the new modeling study.

"Catastrophic would be the first word that comes to mind," Watson said of the outcome if vaccines hadn't been available to fight the coronavirus. The findings "quantify just how much worse the pandemic could have been if we did not have these vaccines."

The researchers used data from 185 countries to estimate that vaccines prevented 4.2 million COVID-19 deaths in India, 1.9 million in the United States, 1 million in Brazil, 631,000 in France and 507,000 in the United Kingdom.

An additional 600,000 deaths would have been prevented if the World Health Organization target of 40% vaccination coverage by the end of 2021 had been met, according to the study published Thursday in the journal *Lancet Infectious Diseases*.

The main finding - 19.8 million COVID-19 deaths were prevented - is based on estimates of how many more deaths than usual occurred during the time period. Using only reported COVID-19 deaths, the same model yielded 14.4 million deaths averted by vaccines.

The London scientists excluded China because of uncertainty around the pandemic's effect on deaths there and its huge population.

The study has other limitations. The researchers did not include how the virus might have mutated differently in the absence of vaccines. And they did not factor in how lockdowns or mask wearing might have changed if vaccines weren't available.

Another modeling group used a different approach to estimate that 16.3 million COVID-19 deaths were averted by vaccines. That work, by the Institute for Health Metrics and Evaluation in Seattle, has not been published.

In the real world, people wear masks more often when cases are surging, said the institute's **Ali Mokdad**, and 2021's delta wave without vaccines would have prompted a major policy response.

"We may disagree on the number as scientists, but we all agree that COVID vaccines saved lots of lives," Mokdad said. The findings underscore both the achievements and the shortcomings of the vaccination campaign, said **Adam Finn** of Bristol Medical School in England, who like Mokdad was not involved in the study.

"Although we did pretty well this time - we saved millions and millions of lives - we could have done better and we should do better in the future," Finn said.

Funding came from several groups including the WHO; the UK Medical Research Council; Gavi, the Vaccine Alliance; and the Bill and Melinda Gates Foundation.

Also:

**LONDON:** British officials said the monkeypox outbreak in the UK is growing across the country, mainly among men who are gay or bisexual, or other men who have sex with men. They urged those with new or multiple sex partners to be vigilant for the symptoms of monkeypox.

In a technical briefing released on Friday, Britain's Health Security Agen-

cy said their data show monkeypox is spreading in "defined sexual networks of gay, bisexual, or men who have sex with men." Officials said there were no signs suggesting sustained spread beyond those populations.

Of the 810 monkeypox cases in the UK to date, five are in women. Among patients who completed a detailed survey, 96% of those infected were men who were gay, bisexual or had sex with other men. Among the nearly 50 countries reporting monkeypox cases globally, Britain has the biggest outbreak beyond Africa.

"If you are concerned that you may have monkeypox, don't go to events, meet with friends or have sexual contact," said **Dr. Meera Chand**, director of clinical and emerging infections at Britain's Health Security Agency. Doctors say people who have unexpected skin lesions or rashes that could be monkeypox should seek help at a sexual health clinic and avoid close contact with others until they have consulted a physician.

She said that anyone who was in close, physical contact with someone who had monkeypox was at risk of catching the disease, regardless of their sexual orientation.

"To assist with our contact tracing, we encourage everyone to ensure they exchange contact details with sexual partners, to help us limit further transmission where cases occur," Chand said.

The Health Security Agency said there were "a relatively high number of cases reported travelling to **Gran Canaria** in early May," suggesting they were infected there before returning to Britain.

Earlier this week, British officials said they were widening their vaccination policy to offer shots to gay and bisexual, and other men who have sex with men who were at high risk of catching monkeypox, which it defined as those who have multiple partners, participate in group sex or attend venues where sex occurs on the premises.

ing a common-sense approach that minimizes conflict," the agency said in an email to The Associated Press. "The economic activity generated from ranching is the lifeblood of many rural communities." (AP)

**Team hauls in 18-foot python:** A team of biologists recently hauled in the heaviest Burmese python ever captured in Florida, officials said. The female python weighed in at 215 pounds (98 kilograms), was nearly 18 feet

long (5 meters) and had 122 developing eggs, the Conservancy of Southwest Florida said in a news release.

The team used radio transmitters transplanted in male "scout" snakes to study python movements, breeding behaviors and habitat use, said **Ian Bartoszek**, wildlife biologist and environmental science project manager for the conservancy's program.

"How do you find the needle in the haystack? You could use a magnet, and in a similar way our male scout snakes are attracted to the

biggest females around," Bartoszek said. The team used a scout snake named **Dionysus** - or **Dion** for short - in an area of the western Everglades. "We knew he was there for a reason, and the team found him with the largest female we have seen to date."

Biologist **Ian Easterling** and intern **Kyle Findley** helped capture the female snake and haul it through the woods to the field truck.

A necropsy also found hoof cores in the snake's digest system, meaning that an adult white-tailed deer was its last meal. (AP)

By **Rahil Ghaffar**, Director, Sales for Middle East & Africa at **Virsec**

Protecting the financial sector with Deterministic Protection

With increasing connectivity and the continuous, on-going digital transformation, attackers are finding new ways to completely bypass most solutions. Their methods are increasing in sophistication, resulting in a higher success rate. This becomes particularly dangerous with regards to financial organisations as a result of all the sensitive and real-time data they store. To make matters worse, their deep pockets make them an attractive target for threat-actors looking for a quick pay-out. Security solutions that treat the application as a black box are no longer sufficient in securing organisations from being breached or targeted in an attack; protection must be layered and the mindset and culture of cybersecurity must shift to an application aware security approach that is deterministic in nature. This is the only way to fully protect customers and confidential data and assets.

As such, organisations and users are looking for better security. Specifically, one that protects their workloads rather than one that takes days or even months to respond, after the attackers have stripped the said workload of all its value.

Ransomware defence is moving away from searching for known malicious code or signature-based blacklisting. Instead, the fastest and most reliable protection involves equipping vendors with the ability to catalogue known good behaviours and detect deviations in real time on both workstations and servers. This technique, known as whitelisting, is popular for its ability to detect and stop malicious activity quickly without relying on analysis in the cloud.

Deterministic protection: What is it and how does it help?

A deterministic protection platform (DPP) can be used to secure the full workload. It fully understands all application processes by extracting their original intention function and how they are supposed to run depending on their purpose. It can automatically detect any diversions or abnormalities within software and applications that don't correlate with the original intentions. In this way, it's able to protect any vulnerable workloads that are typically targeted by threat-actors.

This approach to security allows organisations to detect and block known and unknown attacks. As a matter of fact, DPP can identify, precisely and reliably, when a protected workload starts executing code that was not part of the original code and it can alert and stop any type of attack within milliseconds. When it comes to ransomware, the damage occurs when threat-actors move laterally from desktops to servers. DPP, in this case map the sequence of processes and commands by all applications authorised to run on that server and waits for anything that differs. As soon as a foreign application or sequence shows up, the software raises an alarm and kills the process. As such, attackers are unable to perform command injections or hijack control. This provides much more desirable security in comparison to other solutions that simply detect attacks when it has already occurred and can no longer be stopped. As such, DPP reduces threat-actor dwell time to near zero and blocks threats before the attacker can execute their malicious code.

Cybersecurity in the financial sector

COVID-19 sped up the already ongoing digital transformation. Consequently, financial institutions are increasingly relying on technology and data to provide their products and services to their customers. Additionally, the rapid transition to digital left organisations vulnerable to breach because more and more transactions were and continue to be done online. This switch meant that many compromised security for speed, which simultaneously increased the attack surface, as it was easier for attackers to find weaknesses within applications and networks. Now, there are a vast amount of internet facing apps that are still often riddled with gaps and vulnerabilities, giving hackers an easy way into a company's systems.

Just last year, for instance, the average cost of a data breach in the financial sector was \$5.72 million. In fact, financial institutions were in the top five sectors with regards to the severity and frequency of cyber-attacks. This year, this isn't expected to change, as financial organisations will continue to

face threats including phishing, ransomware/malware and even SQL injections. In 2020, 80% of financial organisations reported losses due to phishing attacks. While such an attack seems harmless, the simplest attack vectors tend to have the highest success rate, which is why it is vital for organisations to secure against any and all threats to avoid suffering the consequences. Unfortunately, the costs of data breaches will undoubtedly increase, unless financial organisations take the right measures to protect themselves adequately. Defensive protection is no longer enough. Cyber criminals will

always take an opportunity to breach a company's network and cause as much damage as possible. In order to adequately protect themselves, it is vital for financial organisations and institutions to invest in more robust cybersecurity programmes and solutions.

Why would financial institutions benefit from DPP?

With the financial industry continuously being targeted by cyber criminals due to the vast amounts of sensitive data it houses and the assets it deals with, IT teams and leaders are making more conscious decisions to deploy security solutions and protect their networks. This is a step in the right direction as more and more attackers are holding financial organisations for ransom. The magnitude and speed of ransomware leaves financial organisations confounded, due to a lack of preparation and layering within their existing security. More worryingly, if the ransom is paid, organisations risk being targeted again, or losing vast amounts of important information to the dark web. This is why it is vital to detect and block threats as quickly as possible, preferably before

hackers have a chance to gain a foothold in the network, move laterally and launch large-scale attacks.

This is where DPP is very effective. It maps precisely how a specific application executes. Therefore, when the application starts executing code influenced by an attacker, DPP will stop the threat in milliseconds. Considering the fact that the financial sector not only deals with sensitive data, but processes transactions in real time, these milliseconds can be incredibly decisive in how an attack does or does not play out. In addition, financial institutions sighted in a survey that they value prevention over detection, and DPP would do exactly this; detect any deviations from the software's original purpose and prevent an attack from being carried out. As a result, financial organisations can better protect their customers by deploying DPP, as it secures their data and their assets even if the application is riddled with (un) disclosed vulnerabilities or if the app has not been patched.

The world runs on software, yet before DPP there was no way to achieve protection at the workload while the software or application is running. With the speed at which threats are evolving and hackers are improving their methods, financial organisations must place more emphasis on cybersecurity by having a way to secure themselves and their customers from both known and unknown attacks. Layered protection provides a robust base, however analysing financial intelligence takes time - time that gives adversaries the upper hand. DPP can provide the vital protection financial organisations need by alerting organisations to any deviations in the software within milliseconds and blocking the attacker in their tracks. By deploying DPP, companies will take away threat-actors' ability to dwell on servers and gain unauthorised access to confidential data or assets.

Ultimately, the only way to eradicate any type of attack or breach is to fully understand applications and software at their core, and make sure they are always running as they are supposed to.



Bobby Gupta