CyberSec Weekly

Happy Monday!

Welcome to the 28th issue of CyberSec Weekly.
In this issue:

FBI is Investigating Malicious Activity

The U.S. Federal Bureau of Investigation (FBI) is reportedly investigating malicious cyber activity on the agency's network.
The federal law enforcement agency says it already contained the

"isolated incident" and is working to uncover its scope and overall impact.

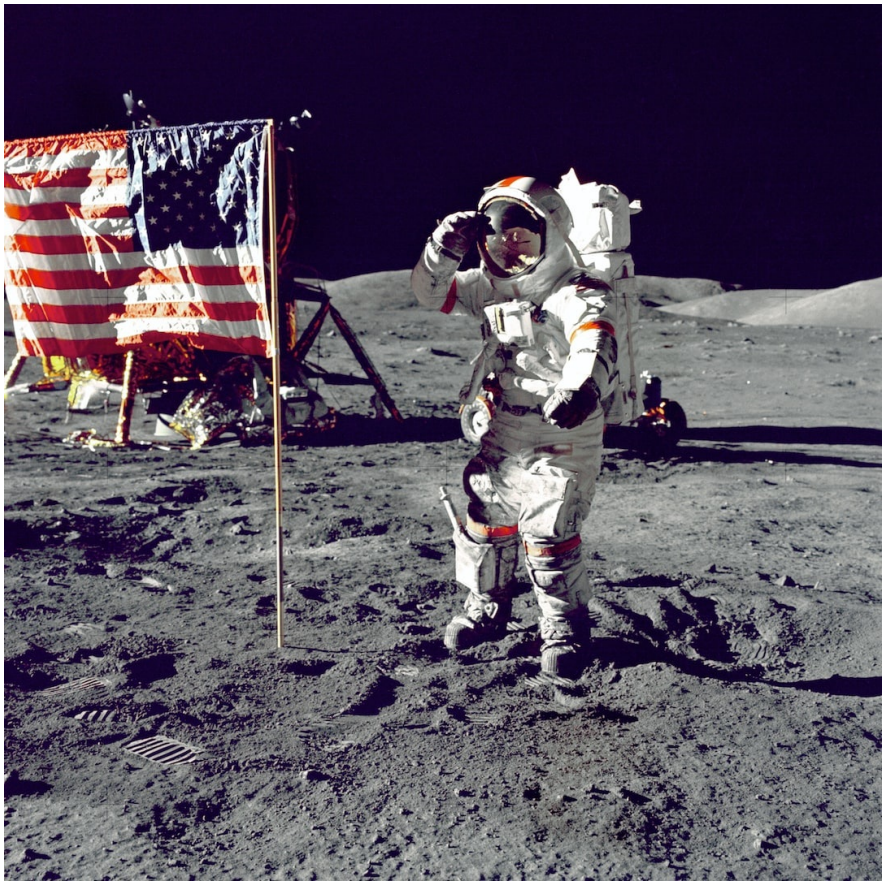
"The FBI is aware of the incident and is working to gain additional information," the U.S. domestic intelligence and security service told BleepingComputer.
"This is an isolated incident that has been contained. As this is an ongoing investigation the FBI does not have further comment to provide at this time."

To read the full story...

Click Here

What's the best thing about UDP jokes?

It doesn't matter if nobody gets them.



NASA Conducting Cybersecurity Review of Deep Space Network Tracking Site

A popular public website that tracks activities on NASA’s Deep Space Network (DSN) has been taken offline for what NASA calls a

“cybersecurity review” linked to future Artemis missions.

NASA’s long-running DSN Now website provided a graphical presentation of activities at the DSN’s three sites in Australia, California and Spain. The site provided realtime information about what antennas at each site were transmitting to or receiving data from missions across the solar system, illustrating the level of activity of the network and sometimes providing insights about the status of missions before formal announcements.

To read the full story…

Click Here

Could a Hacker Launch a Nuke?

Watch Video

GoDaddy Customer Accounts Hacked

GoDaddy, one of the world’s largest web hosting services, said in a filing this week that it fell victim to a two-year security breach that saw unknown attackers steal customer and employee login details and seize company source code.

In the Securities and Exchange Commission filing, the company said the attackers also installed malware that redirected customer websites to malicious sites. The attackers were allegedly responsible for three security breaches between 2020 and 2022.

To read the full story…

Click Here

CyberSec Weekly