Major intelligence website hacked in search for CIA spying secrets

washingtontimes.com/news/2025/jul/24/major-intelligence-website-hacked-search-cia-spying-secrets/

By Bill Gertz

A version of this story appeared in the daily Threat Status newsletter from The Washington Times. Click here to receive Threat Status delivered directly to your inbox each weekday.

Unidentified hackers recently compromised a major intelligence website used by the CIA and other agencies to submit details of sensitive contracts, according to the National Reconnaissance Office, the spy satellite service that runs the site.

The breach targeted proprietary intellectual property and personal information submitted on the Acquisition Research Center website in support of several innovative CIA spying programs.

In addition to the intelligence website hack, Microsoft revealed this week that Chinese state hackers compromised the Department of Energy's National Nuclear Security Administration, a central nuclear weapons agency.

A National Reconnaissance Office spokesman told The Washington Times: “We can confirm that an incident involving our unclassified Acquisition Research Center website is currently being investigated by federal law enforcement. We do not comment on ongoing investigations.”

The extent of the breach is not fully known, but people familiar with the activity said hackers likely obtained information on key technologies for CIA operations.

Other potential areas of compromise could include the Space Force, its efforts to build surveillance satellites and space weapons, and the Golden Dome missile defense program.

Data from one highly sensitive program, Digital Hammer, was compromised, said people familiar with the hacking.

Digital Hammer compiles cutting-edge technologies for human intelligence gathering, surveillance and counterintelligence operations. The program focuses on the threat of Chinese intelligence and information operations.

Portions of many Digital Hammer programs are unclassified. However, others submitted to the National Reconnaissance Office acquisition center are classified and involve capabilities essential to covert operations and strategic intelligence collection.

Digital Hammer is a closely guarded program working to develop open-source intelligence platforms, analytics, and items such as miniaturized sensors and hidden surveillance tools.

Other programs seek to develop acoustic and communications systems, artificial-intelligence-powered data collection, analysis and behavior prediction tools.

Countersurveillance and signature reduction technologies also are part of the program.

Lori Ann Duvall-Jones, CIA deputy director of the Office of Acquisition Management, said in a 2023 speech that Digital Hammer is a contracting vehicle that allows vendors to present offerings “within a CIA space.”

The program allows the CIA to assess new capabilities and consider how to apply them in an innovative way to a mission set, she said.

Critics say using the unclassified Acquisition Research Center for contracts created security vulnerabilities that hackers exploited.

The CIA states on its website that the center is “the industry’s unclassified and classified access point for acquisition information, new business opportunities, and outreach activity involvement.”

The CIA uses the center as an access point for market research, identifying business solutions and communicating with industry.

Companies seeking to do business with the CIA register with the acquisition center and then explain their core competencies.

Once registered, companies can use the center for solicitations, capabilities briefings, sharing innovative ideas and “identifying sub-prime opportunities.”

A CIA spokesman referred questions about the incident to the National Reconnaissance Office.

L.J. Eads, a former Air Force intelligence officer, said China would gain much from obtaining intellectual property on Digital Hammer, especially technologies designed in partnership with or directly for the intelligence community.

“This wasn’t a breach of opportunity,” said Mr. Eads, founder of Data Abyss. “Given the sensitivity and exclusivity of the Digital Hammer program, this compromise almost certainly points to a state-sponsored actor, likely China.

“When proprietary innovations intended for CIA-backed programs are exfiltrated, it’s not just a vendor issue but a serious national security breach,” he said.

The National Reconnaissance Office recently uncovered that the unclassified portion of the Acquisition Research Center was compromised and sent notices to several companies affected. The security breach impacts a number of acquisitions supported by the center among several government agencies.

The office’s notice said the compromise so far does not appear to involve classified information but rather losses as a result of unauthorized access to proprietary and personally identifiable information.

The agency is working to ensure that the full details of the compromise are identified and appropriate countermeasures are taken to prevent further losses.

During a speech last summer, National Reconnaissance Office Director Christopher Scolese said his agency was expanding its satellite capabilities and building innovative capabilities to counter China and Russia.

Mr. Scolese said Russia poses a very focused and capable space threat to U.S. intelligence, surveillance and reconnaissance capabilities.

However, the threat from China is more diversified, he said.

“Russia is pushing into more disruptive capabilities of space,” he told a security conference.

U.S. officials said Moscow is developing a space-based nuclear anti-satellite weapon.

“China, however, represents a different threat,” Mr. Scolese said. “They are a very capable country, technologically smart, and they’re economically strong. They’re developing capabilities across the spectrum of systems, and they are competing with us. We have right now the strongest capability and we have the best ISR, but China is coming on strong. It represents an additional threat to what we’re doing.”

The National Reconnaissance Office is working to advance its capabilities in space and on the ground to become faster, more agile and more resilient, he said.

“That complicates the calculus of anybody who wants to do us harm,” Mr. Scolese said.

On the National Nuclear Security Administration breach, Microsoft said the large-scale cyberattack involved Chinese hackers who exploited a Microsoft SharePoint zero-day vulnerability on Friday. The hackers were able to penetrate the agency’s network.

So far, the agency has been unable to determine whether the hackers stole sensitive or classified information from that network.

The National Nuclear Security Administration is the agency in charge of maintaining and building U.S. nuclear weapons for the Pentagon.

“As of this writing, Microsoft has observed two named Chinese nation-state actors, Linen Typhoon and Violet Typhoon exploiting these vulnerabilities targeting internet-facing SharePoint servers,” the company said in a security blog post Tuesday.

“In addition, we have observed another China-based threat actor, tracked as Storm-2603, exploiting these vulnerabilities to deploy ransomware.”

• *Bill Gertz can be reached at bgertz@washingtontimes.com.*