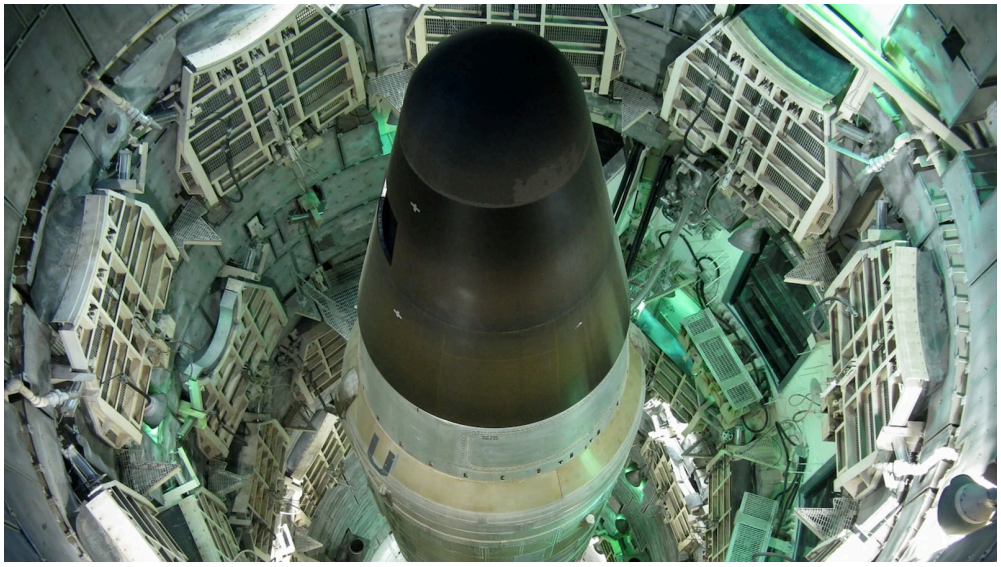
REvil ransomware hits US nuclear weapons contractor

By Lawrence Abrams

Published: 2021-06-14 · Archived: 2026-04-05 23:47:03 UTC



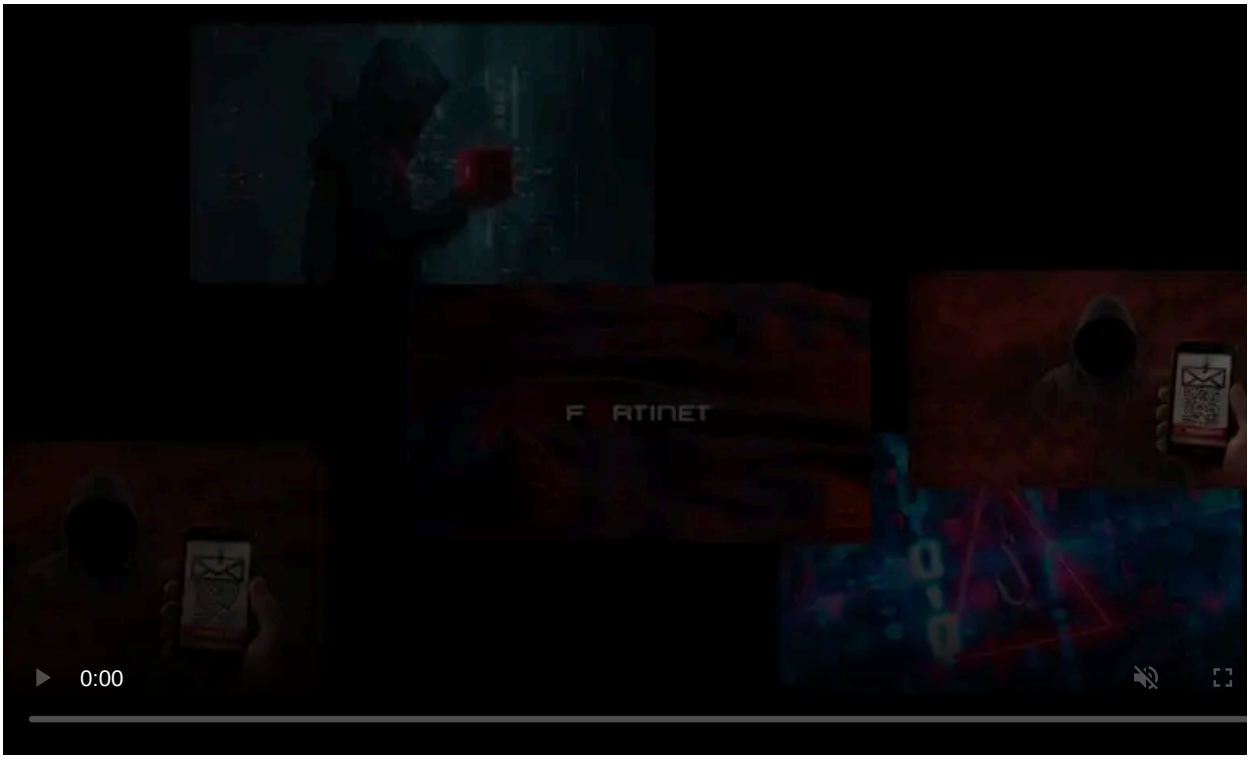
Source: Defense.gov

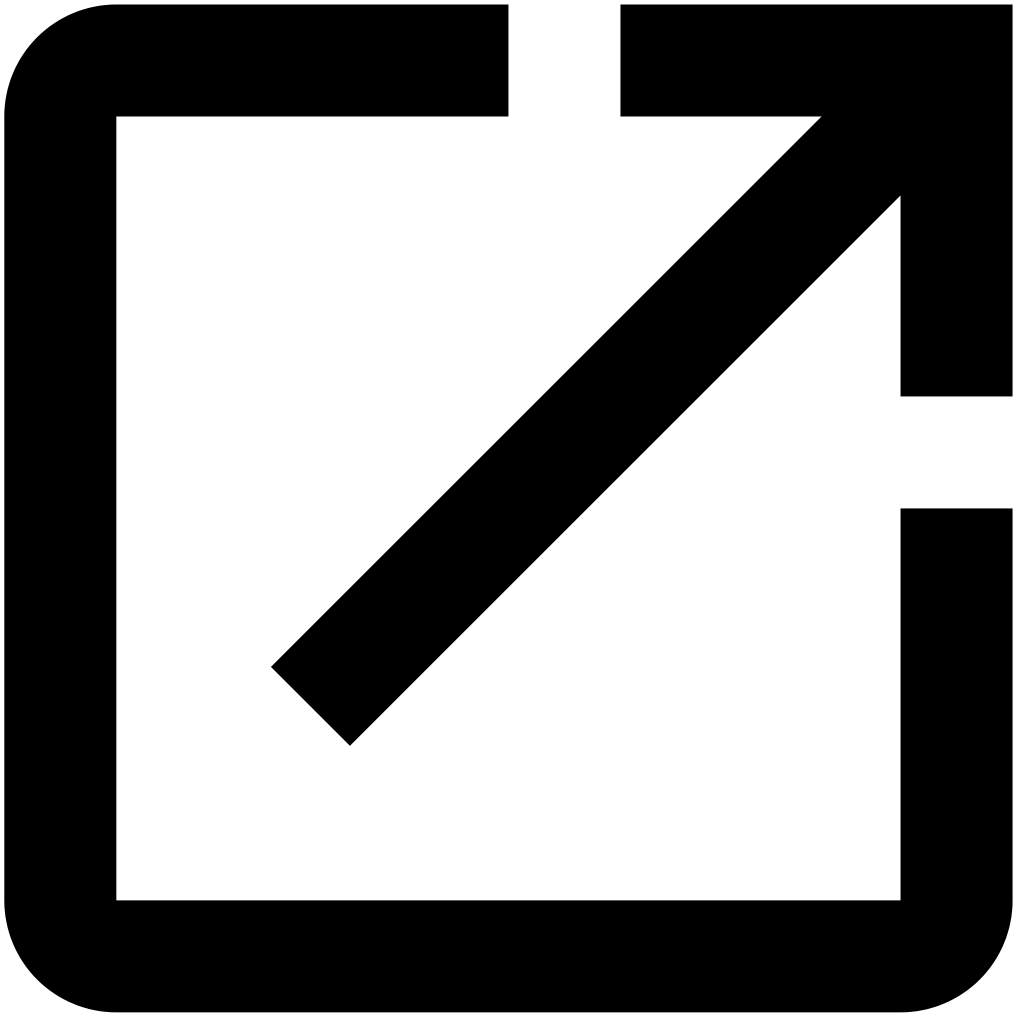
US nuclear weapons contractor Sol Oriens has suffered a cyberattack allegedly at the hands of the REvil ransomware gang, which claims to be auctioning data stolen during the attack.

Sol Oriens describes itself as helping the "Department of Defense and Department of Energy Organizations, Aerospace Contractors, and Technology Firms carry out complex programs."

However, job postings first spotted by CNBC correspondent Eamon Javers provide some insight into Sol Orien's operations, who are seeking program managers, consultants, and a 'Nuclear Weapon System Subject Matter Expert' to work with the National Nuclear Security Administration (NNSA).

"Sol Oriens LLC currently has an opening for a Senior Nuclear Weapon System Subject Matter. Expert with more than 20 years of experience with nuclear weapons like the W80-4. This. Subject Matter Expert works with NNSA Federal and other Contractor personnel to organize,. coordinate, implement, and manage technical program activities for the W80-4 Life Extension. Program.," says one of the job postings.


F RTINET
0:00



"Position Responsibilities. Planning and managing nuclear weapon life extension programs and associated. stockpile management as they relate to the maintenance of a highly reliable and safe. nuclear deterrent."

REvil claims to have stolen data from Sol Oriens

Last week, the REvil ransomware operation listed companies whose data they were auctioning off to the highest bidder.

One of the listed companies is Sol Oriens, where REvil claims to have stolen business data and employees' data, including salary information and social security numbers.

As proof that they stole data during the attack, REvil published images of a hiring overview document, payroll documents, and a wages report.

As a way to pressure Sol Oriens into paying the threat actor's extortion demands, the ransomware gang threatened to share "relevant documentation and data to military angencies (sic) of our choise (sic)."


Offer No. 2
Sol Oriens, LLC did not take all necessary action to protect personal data of their employees and software developments for partner companies. We hereby keep a right to forward all of the relevant documentation and data to military angencies of our choise, includig all personal data of employees.
sol*hiring.png sol*payroll.png sol_wages.png

Threat to share stolen data with military agencies

In a statement shared by Javers on Twitter, Sols Oriens confirmed a cyberattack in May 2021 that affected their network.

"The investigation is ongoing, but we recently determined that an unauthorized individual acquired certain documents from our systems."

"Those documents are currently under review, and we are working with a third-party technological forensic firm to determine the scope of potential data that may have been involved."

"We have no current indication that this incident involves client classified or critical security-related information. Once the investigation concludes, we are committed to notifying individuals and entities whose information is involved."

Like many other ransomware operations, REvil is believed to be operating out of Russia or another CIS country.

Over the weekend, G7 leaders issued a statement asking Russia to help disrupt ransomware gangs believed to be operating within its borders.

President Biden will also be discussing the recent ransomware attacks with Russian President Vladimir Putin at the June 16th Geneva summit.
