Jamesbeam 14 hours ago | parent | context | favorite | on: 'We hacked the FBI:' Hackers say they have data on...

I will tell you where this gets really embarrassing for the FBI.

Oracle enterprise applications are a gold mine for attackers precisely because nobody treats them as security-critical systems.

In 2025 the Clop ransomware gang discovered that Oracle E-Business Suite has a critical vulnerability (CVE-2025-61882) that allows unauthenticated remote code execution.

Graceful Spider (tracked as Clop affiliates) started exploiting this in early August, well before Oracle issued a patch in October. That's a two-month window where attackers had free rein.

All you need to know about Clop is that they got fucked by SH as well just a few days ago.

ShinyHunters defaced Clop's Tor leak site and added its own branding and messages. SH claims it stole source code, system logs, plugins, and Tor onion service keys. SH says it plans to give Clop 72 hours to respond to an extortion message.

Say what you want but these kids got balls. Won't help them once SOCOM starts dealing with them, but they had a good run so far. I think hacking the FBI is as close as you can fly to the sun before the hammer drops.

In February this year they breached Wynn Resorts and lifted data on 800,000-plus employees. Can you guess the entry point?

If you guessed Oracle PeopleSoft, you were right.

Now you'd think the FBI IT people would have noticed that oracle software is a potential national security risk, if multiple ransomware groups keep focusing specifically on the shit Larry Elison personally have to seem vibe coded, over and over.

But Ka$h replaced most of the competent people at the FBI with Ka$h people and by pure luck Oracle won a $396m HR government contract this summer. Who wouldn't want to supply the most secure software product to manage some of the most sensitive data within the agency, if not the Oracle Moscow branch.

https://mesoclever.com/2026/06/11/oracle-wins-396m-hr-contra...

They even mentioned in the above June article:

> Separately, the cybercrime group ShinyHunters claimed to have exfiltrated student, financial-aid, immigration, health, and administrative records from PeopleSoft instances at more than 100 organizations, predominantly universities. The group stated it had previously targeted an *FBI PeopleSoft server* before pivoting to educational institutions already compromised in earlier campaigns. Oracle has not publicly confirmed the scope or remediation status of these incidents.

So the FBI knew, and had it coming, and if stuff like this happens, THE HEAD needs to roll. And all of his buddies in IT should permanently get to spend their time outside the government at the seafood buffet at Ka$hs favorite gentleman's club as well.

Fookin Big Idiots.

help

reply