Secret Service Investigates Breach at U.S. Govt IT Contractor

Published: 2019-09-09 · Archived: 2026-04-05 14:07:21 UTC

The **U.S. Secret Service** is investigating a breach at a Virginia-based government technology contractor that saw access to several of its systems put up for sale in the cybercrime underground, KrebsOnSecurity has learned. The contractor claims the access being auctioned off was to old test systems that do not have direct connections to its government partner networks.

In mid-August, a member of a popular Russian-language cybercrime forum offered to sell access to the internal network of a U.S. government IT contractor that does business with more than 20 federal agencies, including several branches of the military. The seller bragged that he had access to email correspondence and credentials needed to view databases of the client agencies, and set the opening price at six bitcoins (~USD $60,000).

A review of the screenshots posted to the cybercrime forum as evidence of the unauthorized access revealed several Internet addresses tied to systems at the **U.S. Department of Transportation**, the **National Institutes of Health** (NIH), and **U.S. Citizenship and Immigration Services** (USCIS), a component of the **U.S. Department of Homeland Security** that manages the nation's naturalization and immigration system.

Other domains and Internet addresses included in those screenshots pointed to Miracle Systems LLC, an Arlington, Va. based IT contractor that states on its site that it serves 20+ federal agencies as a prime contractor, including the aforementioned agencies.

In an interview with KrebsOnSecurity, Miracle Systems CEO **Sandesh Sharda** confirmed that the auction concerned credentials and databases were managed by his company, and that an investigating agent from the Secret Service was in his firm's offices at that very moment looking into the matter.

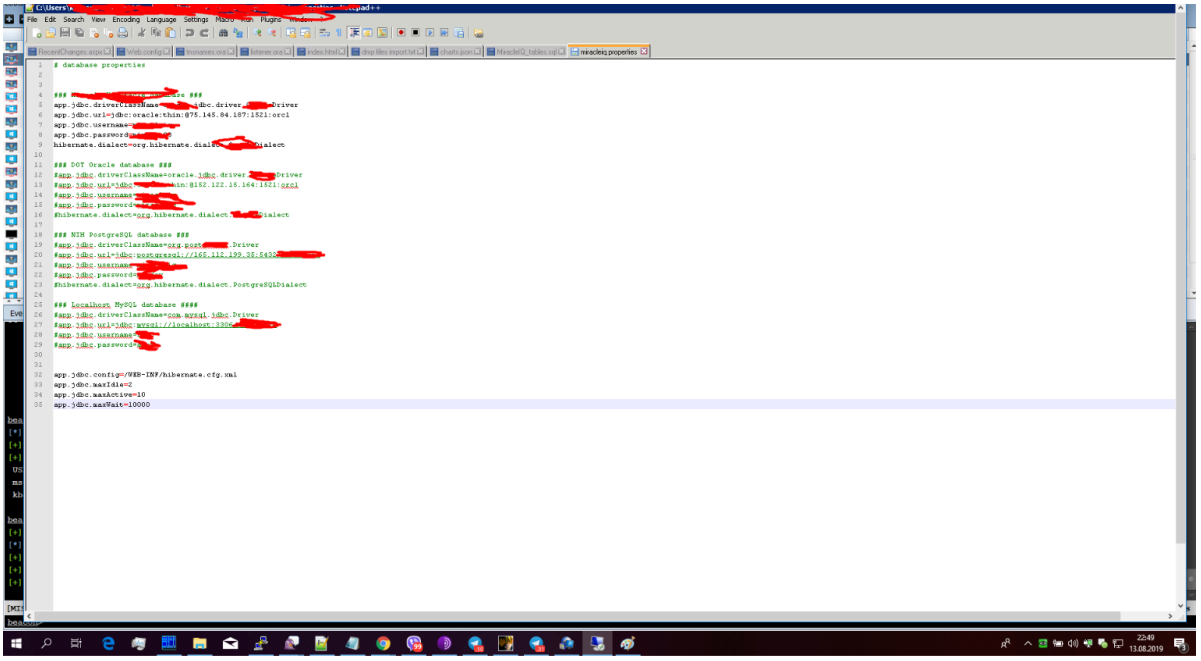
But he maintained that the purloined data shown in the screenshots was years-old and mapped only to internal test systems that were never connected to its government agency clients.

"The Secret Service came to us and said they're looking into the issue," Sharda said. "But it was all old stuff [that was] in our own internal test environment, and it is no longer valid."

Still, Sharda did acknowledge information shared by Wisconsin-based security firm Hold Security, which alerted KrebsOnSecurity to this incident, indicating that at least eight of its internal systems had been compromised on three separate occasions between November 2018 and July 2019 by Emotet, a malware strain usually distributed via malware-laced email attachments that typically is used to deploy other malicious software.

The Department of Homeland Security did not respond to requests for comment, nor did the Department of Transportation. A spokesperson for the NIH said the agency had investigated the activity and found it was not compromised by the incident.

"As is the case for all agencies of the Federal Government, the NIH is constantly under threat of cyber-attack," NIH spokesperson **Julius Patterson** said. "The NIH has a comprehensive security program that is continuously monitoring and responding to security events, and cyber-related incidents are reported to the Department of Homeland Security through the HHS Computer Security Incident Response Center."



One of several screenshots offered by the dark web seller as proof of access to a federal IT contractor later identified as Arlington, Va. based Miracle Systems. Image: Hold Security.

The dust-up involving Miracle Systems comes amid much hand-wringing among U.S. federal agencies about how best to beef up and ensure security at a slew of private companies that manage federal IT contracts and handle government data.

For years, federal agencies had few options to hold private contractors to the same security standards to which they must adhere — beyond perhaps restricting how federal dollars are spent. But recent updates to federal acquisition regulations allow agencies to extend those same rules to vendors, enforce specific security requirements, and even kill contracts that are found to be in violation of specific security clauses.

In July, DHS's Customs and Border Patrol (CPB) suspended all federal contracts with **Perceptics**, a contractor which sells license-plate scanners and other border control equipment, after data collected by the company was made available for download on the dark web. The CPB later said the breach was the result of a federal contractor copying data on its corporate network, which was subsequently compromised.

For its part, the Department of Defense recently issued long-awaited cybersecurity standards for contractors who work with the Pentagon's sensitive data.

"This problem is not necessarily a tier-one supply level," DOD Chief Information Officer **Dana Deasy** told the Senate Armed Services Committee earlier this year. "It's down when you get to the tier-three and the tier-four" subcontractors.

Source: https://krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/