

Healthcare Technology Company Thwarts Crypto-Miners Attacking Oracle ERP

A leading provider of IT and mobility applications for US hospitals and health systems stops an active WebLogic deserialization attack on its PeopleSoft environment — without code changes or downtime.

1,400

Employees

PeopleSoft 9.0

Products supported

<1 day

Initial installation time

<1 hr

Time to deploy on a new server, post-rollout

The Client offers end-to-end healthcare IT applications, hardware, and customization services, including business intelligence, disaster recovery, and help desk — and, like most organizations, must defend against a constant stream of automated attacks.

“This particular exploit was a WebLogic deserialization Java vulnerability,” says the Client’s CISO. “The attackers were attempting to install crypto-miner software that would let them use our servers to mine cryptocurrencies like Bitcoin.”

“Vendor patches don’t effectively address all vulnerabilities,” the CISO explains. The Oracle patch released on April 17, 2017 didn’t fully mitigate the threat, and systems continued to be breached. “Plus you have to perform regression testing and take your systems down to apply patches before hackers find you. When we discovered a successful attack on some of our PeopleSoft servers with a connection to the Internet, we immediately placed a call to our third-party support provider for assistance.”

CLIENT SUCCESS STORY

AT A GLANCE

A new strategy to thwart crypto-miners attacking Oracle ERP.

“Waratek was able to quickly identify the vulnerability and lead us to an effective solution that mitigates deserialization vulnerabilities through Java with WebLogic.”

— Chief Information Security Officer

Because of Waratek’s solution the attacks were immediately stopped, and the solution automatically alerted us to the attempt. All of the hacker’s malicious scripts failed, which took us to a new level of confidence — the Waratek virtual patch is providing the protection we need, better and faster than we ever thought possible.

CHIEF INFORMATION SECURITY OFFICER

Waratek's Solution

After identifying the nature of the attack, the client was introduced to Waratek. “Working with Waratek, we set up a demo scenario on a non-production server,” the CISO says. “They first used Metasploit to prove the vulnerability could be exploited. Next, we installed the Waratek patch software, which blocked the exploit and gave us confidence to install in production.” Because the solution doesn't touch source code, there is no regression testing and no system downtime required.

“Initial installation was easy and took less than a day,” notes the Client's senior security analyst. “Now that we're familiar with the software, we could set it up within an hour on a new server.”

Client Results

“A week after we installed the Waratek solution we got hit with more deserialization attacks,” the CISO says. “Because of Waratek's solution, the attacks were immediately stopped, and the solution automatically alerted us to the attempt. All of the hacker's malicious scripts failed, which took us to a new level of confidence.”

Client Benefits

- ✓ **Increased security protection** faster, less disruptive, and offers greater protection than typical vendor patching options.
- ✓ **Reduced support and maintenance spend** savings compared to previous annual PeopleSoft support and maintenance costs, alongside advanced security protection.



WARATEK

See what Waratek can do for your Java applications.

[Request a Demo](#)

Dublin Office

Third Floor, 42/43 Westland Row
Dublin 2, Ireland D02 YR86
+353 1 475 8803

Chicago Office

159 N. Sangamon, Suite 200
Chicago, Illinois 60607
+1 872 469 8605

Sales@Waratek.com
waratek.com