

The Cloud Computing News India

News And Info On Cloud Computing And Virtualization

<http://cloudcomputingnews.in/2016-congressional-report-cylanceprotect-halted-opm-breach/>

2016 Congressional Report: CylancePROTECT Halted OPM Breach

26/09/16

September 26, 2016



Congressional Report Concludes CylancePROTECT Played a Pivotal Role in Discovering, Stopping and Remediating Malware that Caused OPM Data Breach.

Cylance Inc, the company that is revolutionizing cybersecurity through the use of artificial intelligence to proactively prevent advanced persistent threats and malware, was named in a report today released by Chairman Jason Chaffetz (R-UT) with the House Committee on Oversight and Government Reform as having played a critical role in discovering, halting and remediating the data breach at the United States Office of Personnel Management in 2015.

The report says that the company's CylancePROTECT product was first used following discovery of the compromise to positively identify and stop the APT attack attributed to "Shell Crew" and/or "Deputy Dog" hacker teams, commonly associated with Chinese origin, and says, "The significance of the cutting edge preventative technology offered by Cylance in responding to the OPM data breach cannot be understated."

“We consider it an honor to have been able to help stop and clean up this vicious attack,” said Stuart McClure, founder, president and CEO at Cylance. “The OPM breach, and countless others like it, is exactly why we were compelled to apply artificial intelligence to fighting hackers, whether state actors, rogue hackers, organized criminal groups, or cyber terrorists. Our mission is to protect everyone under the sun and we are just getting started.”

“We knew at Assurance Data that CylancePROTECT was game-changing technology when it was first released,” said Matthew Morrison, president and CEO at Assurance Data, a long-time channel partner of Cylance and a leading information security consultant for the federal government.

“Seeing for ourselves how advanced malware was slipping past traditional endpoint security products, we recommended CylancePROTECT to the Office of Personnel Management and recommended its use on all computers and servers,” he added.

US-CERT issued a report on April 24, 2015 stating that OPM discovered suspicious activity on its networks on April 16, 2015. On April 17, 2015, Jeff Wagner emailed OPM’s then Chief Information Officer Donna Seymour to report that Cylance officials were “coming in to help with the forensics” because “it was their tool that found the malware.”

Today’s report notes that “CylancePROTECT was the first tool that OPM used after the agency learned its network was compromised, and the tool immediately found malware and set about cleaning OPM’s enterprise.”

The report quotes OPM’s IT Security Officer Jeff Wagner as saying that Cylance was able to find things that other tools could not “because of the unique way that Cylance functions and operates. It doesn’t utilize a standard signature of heuristics or indicators, like normal signatures in the past have been done, it utilizes a unique proprietary method.”

(NetEvents)