Cylance® and the OPM Breach

AI and Machine Learning Move to the Frontlines of Cybersecurity

"This is crown jewels material… a goldmine for a foreign intelligence service."

— Joel Brenner,

Former NSA Senior Counsel, from The OPM Data Breach: How the Government Jeopardized our National Security for More than a Generation

"Swifter action by OPM to harden the defenses of its IT architecture could have prevented or mitigated the damage that OPM's systems incurred."

— Jeff Wagner,

OPM Director of IT Security Operations

The data breach at the U.S. Office of Personnel Management (OPM), which began in 2012 and went undetected until 2015, resulted in the theft of 21.5 million records on current, former, and prospective federal employees and contractors. Sensitive information syphoned from the breach included personnel names, birth dates, home addresses, biometric data, and Social Security numbers.

OPM, which serves as the central human resources department for the entire U.S. federal government, was a high-value target for this nation-state act of espionage. While the OPM breach was unprecedented, the agency's subsequent response demonstrates how organizations can successfully react and future-proof against threats. OPM took advantage of the CylancePROTECT® artificial intelligence (AI) and machine learning solution to remove threats deeply embedded in its systems. With assistance from Cylance Consulting Services, OPM identified the breach, performed mitigation activities, and secured its entire IT environment. In just ten days, OPM quarantined all identified malware. CylancePROTECT was leveraged on more than 10,000 devices, and more than 2,000 pieces of malware were detected and neutralized. As a result, OPM transformed its operations to provide superior security using a predictive, preventive, and proactive approach.

OPM and Cylance–A Partnership of Protection

In May of 2014, OPM contacted Cylance to gain an understanding of the company's capabilities for identifying and preventing advanced cyberattacks on the endpoint. Cylance briefed OPM and the agency purchased the CylanceV™ threat detection software, not the CylancePROTECT prevention platform. Throughout the budding partnership, Cylance continued to present its CylancePROTECT preventative platform, which automatically removes and quarantines threats, requiring no intermediary action.

On April 16, 2015, OPM discovered malicious software through the use of CylanceV. OPM engaged the Cylance Consulting team, which spent the next several days providing on-the-ground incident response assistance by optimizing software, providing breach analysis, and assessing OPM's enterprise systems.

As OPM began using Cylance software and services, including CylancePROTECT in demo mode, it discovered critical samples of malicious code on its network. Forensic analysis revealed a variety of findings, including the presence of malicious files to compress and encrypt data, as well as "command shells" that allow remote attackers to control a victim's machine, making it easier to move laterally through trusted networks.

Once it was determined that OPM was the victim of an advanced targeted attack, Cylance and OPM initiated full deployment of the CylancePROTECT platform to identify any additional malicious activity and eradicate the threat.

Cylance CEO Stuart McClure stated, "It's actually one of the poster-child examples of how to do it properly in an investigation, just as soon as you know that you've been breached…"

Cylance's AI and machine learning algorithms evaluated each piece of software on all of OPM's endpoints.

In addition to response and mitigation efforts, Cylance technology was employed to guard against future attacks by leveraging AI and machine learning to predict and prevent zero-day threats and sophisticated attacks that successfully bypass traditional security measures.

The predictive, proactive approach employed by Cylance is a complete shift from decades of traditional signature-based antivirus solutions which react to threats post-execution, after the damage has already begun. OPM installed CylancePROTECT without continuous management overhead and negative productivity impact on users.

The 2016 report titled *The OPM Data Breach: How the Government Jeopardized our National Security for More than a Generation*, released by the U.S. Congressional Committee on Oversight and Government Reform, states, "Cylance is breaking ground every day in detecting and preventing attacks predictively, before anyone in the world has seen it, all using the power of machine learning and artificial intelligence. While traditional solutions constantly miss these kinds of advanced and everyday attacks, Cylance consistently catches them in milliseconds."

The Data Behind the Breach:

- 21.5 million records
- Products deployed:
  - CylanceV
  - CylancePROTECT
- Number of devices protected: 10,000+
- Number of malware detected and neutralized: 2,000+
- Time to contain: ten days

OPM Moving Forward

Several important observations from the OPM breach serve as lessons for others:

- Deploying traditional antivirus for endpoint security fails to prevent today's sophisticated threats and adversaries, and does not protect systems from unknown or never-before-seen malicious software.
- AI and machine learning provides a level of prevention and protection that traditional signature-based, heuristic, or behavioral methods cannot match. These reactive, post-execution approaches cannot detect the advanced zero-day techniques used by modern threat actors.
- Cylance built its solution based on patented intellectual property, and CylancePROTECT successfully stops new and never-before-seen cyberattacks on millions of devices worldwide. It has proven effective in preventing advanced attacks.

OPM BREACH INCIDENT: THE FIRST 24 HOURS

Wednesday, April 15, 2015

First indicators of a malware-based cyberattack discovered.
Potentially lost:
- **4.2MM Personnel Records**
- **21.5MM Background Checks**
- **5.6MM Fingerprint Records**

OPM owns CylanceV but does not yet own CylancePROTECT.

April 15 @ 10:48 PM EDT

AssuranceData emails OPM recommending deployment of CylanceV across all endpoints.

April 15 @ 6:53 PM EDT

OPM's Computer Incident Readiness Team (OPM-CIRT) files a formal report with US-CERT, assigned number INC00000459698.

Morning of April 16

Cylance offers assistance in updating and resolving software incompatibility issues in OPM's systems.

April 16 @ 3:56 PM EDT

OPM discovers **FOUR** malicious executable files using CylanceV.

Malicious File Details:
- **THREE are rated UNSAFE**
- **ONE is rated ABNORMAL**
- **ONE file is found to be a Windows Credentials Editor (WCE) file-type.**

The Significance of Finding a WCE File:
"When you see something like a confirmed WCE or other types of credential dumping tools, that's usually a sign of an overt act, so something that somebody with ill intent actually was trying to achieve, versus just the presence of a malicious file."
~ Chris Coulter, *Worldwide Managing Director, Incident Reponse and Forensics*

April 16 @ 7:00 PM EDT

OPM discovers a McAfee dynamic link library (.dll) file.

The McAfee file was highly suspicious as OPM did not use McAfee in its systems.

Morning of April 17

Chris Coulter, Worldwide Managing Director, Incident Reponse and Forensics, arrives at OPM headquarters in Washington, DC to provide on-the-ground assistance and deploy CylancePROTECT.

The OPM/Cylance Timeline

2014: Cylance was called in to OPM by a reseller partner, Assurance Data, and OPM evaluated CylancePROTECT

2014: OPM's Director of IT Security Operations recommended deploying CylancePROTECT

2014-2015: "Internal politics and bureaucracy" delayed the adoption of the product

April 16, 2015: OPM discovered suspicious activity on its networks

April 16, 2015: OPM called Cylance consultants in "to help with the forensics" because "it was their tool that found the malware"

April 17, 2015: OPM IT Security Officer Jeff Wagner said in an email 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 or heuristics or indicators, like normal signatures in the past have been done. It utilizes a unique proprietary method."

April 18-19, 2015: Cylance Consulting used CylancePROTECT to identify and remove all instances of malware from the network

Further Reading

Download the full *OPM Data Breach Report* to learn more about the findings of the yearlong federal investigation into the OPM breach, as well as the vital role Cylance's technology played in identifying the breach.

Read more about how Cylance is protecting our government, and how we can protect your organization by visiting our *OPM Breach* page.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612