Understanding the FireEye Proof of Value Program

Thank you for engaging in a FireEye Proof of Value (POV). The POV process is designed to give you a first-hand look at a FireEye appliance and monitor for previously unknown threats that may have bypassed your existing security tools.

RESULTS FROM RECENT PROOF OF VALUE DEPLOYMENTS

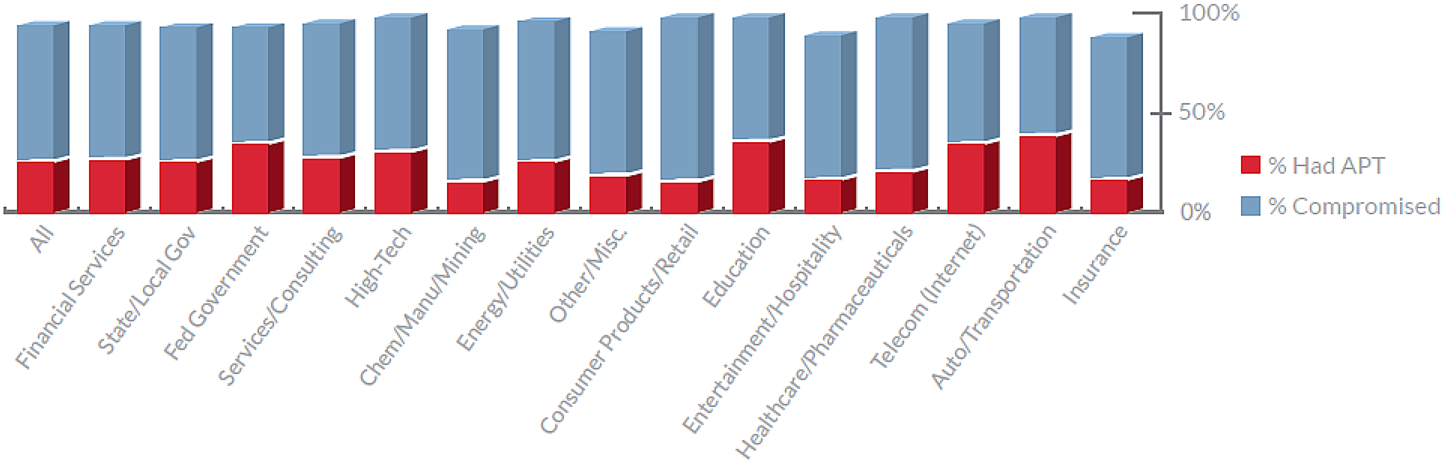
A recent FireEye analysis of POV participants examined 1,216 organizations across the globe. In each instance, the evaluators had traditional anti-virus protections. A portion also had file-based sandboxes that failed to detect the presence of advanced threat actors. In 97% of the cases, the POV revealed threats that the customers' traditional detection methods had failed to detect.

No single industry was spared, either. Our results indicated that compromises, and the presence of APT threat actors spanned all industries:

OTHER FINDINGS FROM THIS STUDY INCLUDE:

- More than 25% of all organizations experienced events known to be consistent with tools and tactics used by advanced persistent threat (APT) actors.
- 75% of organizations had active command-and-control communications, indicating that attackers had control of the breached systems and were possibly already receiving data from them.
- Even after an organization was breached, attackers attempted to compromise the typical organization more than once per week, on average.
- 75% of unique malware was detected only in one environment.

POV Results by Industry


% Had APT
% Compromised
All
Financial Services
State/Local Gov
Fed Government
Services/Consulting
High-Tech
Chem/Manu/Mining
Energy/Utilities
Other/Misc.
Consumer Products/Retail
Education
Entertainment/Hospitality
Healthcare/Pharmaceuticals
Telecom (Internet)
Auto/Transportation
Insurance