REDSPY^{365} CASE STUDY:

Averting Lateral Exploitation

CLIENT

A top banking institution.

SITUATION

A client had a good patch level and low threat surface, and was confident that a malware simulation would not produce insights of concern.

ACTIONS

RedSpy^{365} is able to begin simulations anywhere in the client's environment and test each layer for further risk and impact, including lateral movement. RedSpy^{365} analysts noted multiple findings once RedSpy^{365} passed through a potential attack path to execute on a desktop. The local admin user had been created in the domain admin group, and group policies contained admin passwords. Further testing revealed that admin access to this machine could have allowed ransomware to easily propagate.

RESULTS

The client immediately remedied the desktop-level misconfigurations, thereby avoiding potential significant loss of business continuity.

METRICS

Compensating controls were previously tested and failed to adequately detect deeper risk. RedSpy^{365} identified deeper risk that the client addressed, ensuring 100% business continuity.

RedSpy^{365}™

804.474.5269

RedSpy^{365}.com

Rev. 07012021