EXPANSE

State Police Department Reduces Remote Attack Surface With Expanse

Case Study

Overview

1) **The Problem.** A large state police department faced challenges in identifying and securing attack vectors across its remote attack surface. The department had unintentionally exposed more than 75 Remote Desktop Protocol (RDP) servers, the majority of which corresponded to state police cruiser vehicles, that could have left the department open to attack by malicious actors online.
2) **The Solution.** The department worked with Expanse to identify all exposed RDP servers and bring them under management.
3) **The Outcome.** The department eliminated all 75 exposed RDP servers and significantly reduced its overall attack surface and risk profile.

Remote Work Risks on the Rise

Due to the coronavirus (COVID-19) pandemic, organizations large and small, government and commercial, have seen a rise in their remote attack surfaces. For one large state police department, the coronavirus pandemic and subsequent rise in remote work led to more than 75 servers running Microsoft Remote Desktop Protocol (RDP) being left exposed on the public Internet.

RDP servers provide remote access to a computer over the Internet as though you were physically sitting in front of the computer and logging in through a graphical user interface. RDP is a useful protocol but was never intended to be exposed on the Internet. Externally accessible RDP servers pose a significant security risk and are a frequent target for attackers using a variety of documented exploits. The rise of rapid, Internet-wide scanning and machine-speed attacks makes it easier for bad actors to find and take advantage of exposed assets like RDP. Remote access exposures and attempts at compromise have only increased since the onset of the coronavirus crisis, and state-sponsored Advanced Persistent Threat (APT) groups are known to target them. Left unmitigated, each of those RDP servers would have presented an opportunity for a malicious actor to compromise the state police network.

Identifying RDP Exposures

The state police department first began working with Expanse when Expanse discovered an exposed RDP server and proactively reached out to the State Chief Information Security Officer (CISO) with the associated certificate, IP address, and other information to flag the risky asset and support remediation. After receiving the information, the CISO immediately initiated an internal investigation. The following day, Expanse discovered more than 75 additional examples of publicly accessible RDP servers following the same naming convention; most of these corresponded with state police cruiser laptops. The state agency was only able to find 36 of the 75 RDP servers Expanse had surfaced with an Internet scanning tool it had used previously.

In addition to surfacing the exposures for the state police department, Expanse alerted the state's CISO to seven additional exposed RDP servers belonging to the state's health department, the state legislature, environmental protection agency, and other state agencies. In less than a day, Expanse had reported the IP address, port, and certificate signature for each exposure to the CISO to inform and drive remediation efforts.

> *"RDPs are very concerning exposures, and we really appreciate the information Expanse provided to us," said the State CISO. "After Expanse's initial tip, we tried to find all additional exposures using publicly available tools, and we weren't able to do so. The data Expanse provided aided our investigation and helped us rapidly address a serious issue that could have had significant consequences for the operations of the state."*

Driving Remediation Processes

With the help of Expanse in identifying all exposed RDP services, the state government was able to remove each of these RDP servers from being publicly accessible. With a significantly reduced attack surface, the state government and police department are more secure and better able to focus on their mandate of serving the people of their state.