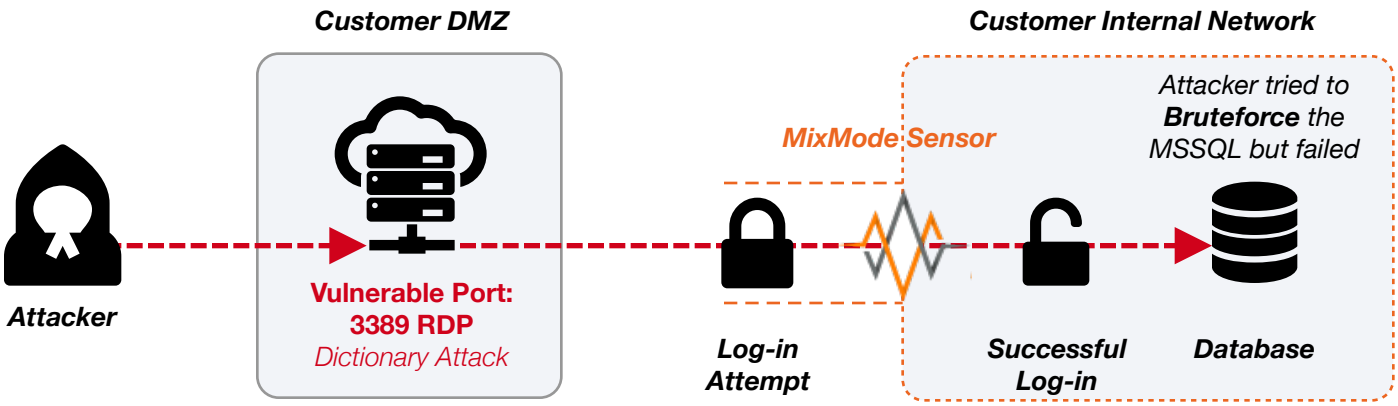
MixMode™

MIXMODE AI DETECTS ATTACK NOT FOUND ON THREAT INTEL

A MixMode customer experienced an incident where an external entity attacked a web server located in their DMZ, compromised it, and then pivoted internally through the DMZ to attempt access of a customer database. While the attacker was successful in penetrating the customer's network, MixMode was able to detect the event before they were successful in penetrating the customer database.

What Happened?

The attack described here occurred from an external IP Address to a machine that was sitting in the customer's DMZ. Through a scan or other method the attacker discovered an open port (Port: 3389) commonly used for RDP. Once discovered, the attacker used a brute force or dictionary attack on the machine, eventually discovering credentials that could be used to log into the web server within the DMZ.



Once the attacker gained access to the webserver in the DMZ, they used this machine to log into the internal network and attack the customer's SQL database. Unfortunately, the customer did not have a MixMode sensor in their DMZ so we are not able to see the initial attack, however, once the attacker penetrated the internal network, the activities hit the MixMode sensor and immediately caught by the MixMode AI. In fact, the AI not only saw the attack activities, but also recognized the behavior as anomalous and surfaced a Risk Level 10 indicator for the customer's team to investigate.

Figures 1 and 2 show the MixMode Security Events Overview dashboard for the relevant period. In figure 1 we can clearly see an AI Anomaly Indicator with a Risk Score of 10. Figure 2 shows the AI Anomaly Indicator details with the webserver's IP address surfaced. This proactive notification provided the customer's team with the identity of the compromised web server, experiencing the anomalous behavior, allowing them to target their investigation quickly.

Pivoting off the proactive AI indicator notification we are able to leverage MixMode's forensic search capability to discover the successful login via RDP (see figure 3). We could not see the attacking IP address as the attack originated on the internet coming into the DMZ. This is an example of why it is extremely important to have comprehensive coverage of both internal (East/West) and external (North/South) traffic.

Once the attacker took control of the Web Server, MixMode saw a number of SMB tree scanning events, giving evidence of the database attack (see figure 4). From here, the remediation team scanned the machine that was compromised and found a number of viruses on the machine, closed the open public ports that were used for the attack, and had the user whose credentials were used to change their password.

This use case is a great example of the need to look at behavioral analytics and anomaly detection. Had it not been for the MixMode's AI detection, the attacker could have established persistence on the web server and delivered malware to any user who visited the web server in question. MixMode's AI recognized the anomalous behavior and surfaced an AI indicator allowing the company to act swiftly to remediate. Further, the visibility provided by MixMode's platform helped the customer discovery additional gaps in their DMZ security which have since been fixed.

About MixMode

MixMode is a next-generation, AI-powered cybersecurity platform focused on solving three primary issues for the Security Operations Center: providing next-generation threat detection, surfacing zero-day attacks and improving false-positive alert fatigue. MixMode combines the functionality of tools like SIEM, XDR, NTA and UEBA and allows security teams to dramatically increase productivity and efficiency while significantly decreasing the wasted time, effort, and resources associated with legacy cybersecurity tools.

MixMode's AI intelligently creates and updates the network baseline, then provides security teams with sophisticated functionality like predictive attack detection, 95% false-positive alert reduction, and all the tools necessary to investigate a threat. SOC teams can easily integrate MixMode into their security stack to dramatically reduce the investigation time, cost, and expertise required to respond to persistent threats, malware, insider attacks, and nation-state espionage efforts. MixMode's core AI algorithm is patented and was utilized over the past 20 years on projects for DARPA and the DoD. MixMode is headquartered in Santa Barbara, CA.

Figure 1

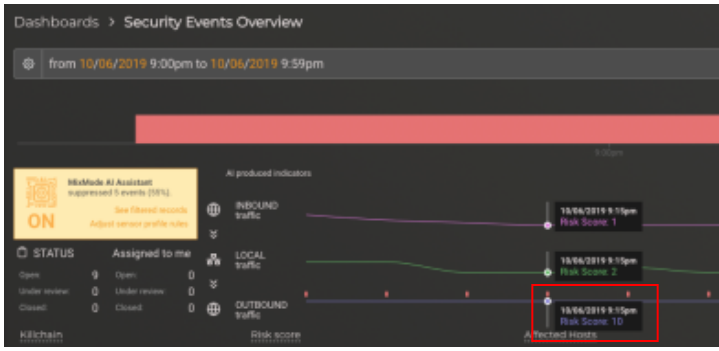


Figure 2

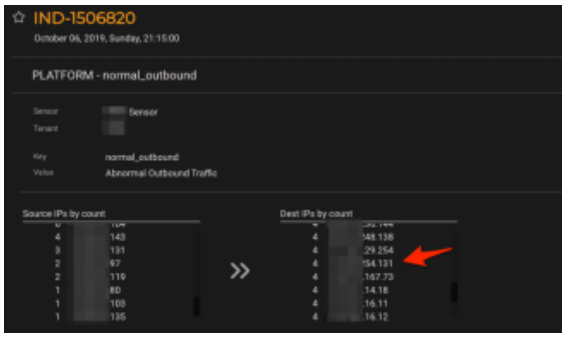


Figure 3

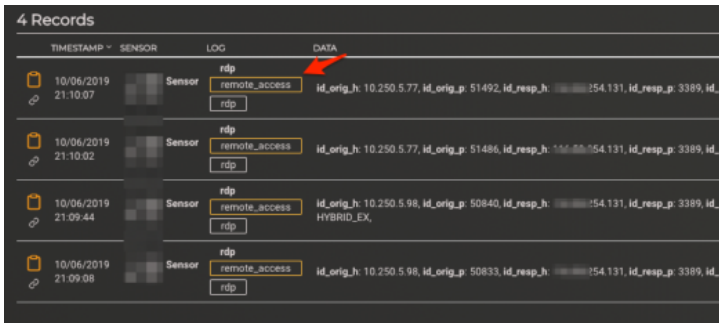


Figure 4