Jonathan Roeseler

Reflection Paper 5

Date: 10/2/205 - 10/9/2025

ODU Fall 2025

Professor Teresa Duvall

Internship Reflection Paper

250 Hours

Working as a Helpdesk Technician for 250 hours has given me a lot of working knowledge regarding incident response and working across Microsoft and Android operating systems. The incident started over the weekend, as we had a SOC alert from our third-party cyber service alerting that Entra had found a risky sign-in for a particular user. I went through the logs and found the sign-in not only anomalous but malicious. I came to this conclusion as the time between logins versus location was impossible (travel time), and sign-ins came from different countries and states. Furthermore, I looked up some of the IPs and went to abuseipdb.com and found they were malicious. After I determined it was malicious, I employed some mitigation techniques before investigating what, if any, data was accessed. To mitigate what looked like a session compromise, likely from visiting a malicious site or site infected with malicious ads (I had previously had to block a particular site for this user, as the user had scareware from it), I blocked sign-in, reset the password, and revoked sessions. Furthermore, I made a conditional access policy in Entra to block those malicious IPs tenant-wide.

Unfortunately, as my organization only had a P1 Entra license, I could not employ stricter or better measures, such as having Entra block sign-ins where it determines there is risk. Then, I went to determine the scope of the damage and utilized Microsoft's Purview to determine what was accessed by the malicious IPs. I ran some searches and saw that, luckily, the actor(s) only accessed Outlook on the web and accessed some mail. At this point, we engaged our SOC/third-party cyber team to run their tools to get the subject lines of these messages and determine the final scope of the breach. From our findings, no messages were sent out from the malicious IPs. However, we did determine that the actor tried to maintain persistence and access by using the messages they accessed and registering similar domains to the domains our user interacted with to then send phishing emails to the compromised user. Our team also spoke with our user to go over safe browsing and email practices. This event gave me tremendous experience in incident response, specifically responding to account compromise(s).

The value of team engagement is the most important thing I've learned during the first 250 hours. Without a properly structured team, a response to security incidents will likely be unsatisfactory or allow an attacker to maintain persistence, or the same attack may keep working without mitigations or training. To be successful in cybersecurity, people and organizations must recognize that the only way to really be secure is by engaging their user(s) and the proper individuals in the organization to resolve incidents best.

Overall, the first 250 hours have been a great introduction to incident response, particularly concerning account compromise/takeover(s) and learning a bit more about troubleshooting common Microsoft and Android app and operating system issues.