CIRT Playbook Battle Card: GSPBC-1018 - Collection - Email Collection - Cloud Email Compromise

(P) Preparation

1. Ensure client software is fully patched
2. Perform routine inspections of controls/weapons
3. Verify that logging and alerting are enabled and configured
4. Make use of risk based conditional access policies
5. Perform routine phishing education and testing
6. Familiarize yourself with the available security features of your service
7. Generate and review reports of logins on a regular basis
8. Ban the use of passwords that include your company's name or product names, if possible
9. Make use of a third party service to monitor for data breaches that include company email addresses

(I) Identification

1. Monitor for:
   a. Unusual login activity
   b. Changes to email forwarding rules
   c. Security features being disabled
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Review logs to determine if the attacker successfully accessed any other accounts
5. Lock any compromised accounts
6. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Reset the credentials of any compromised accounts
3. Inspect the workstations of compromised users

(R) Recovery

1. Restore to the RPO within the RTO
2. Resolve any related security incidents
3. Address collateral damage

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Notes:

1. Report cybercrime: https://www.ic3.gov/default.aspx