Measures for prevention of Web intrusion attacks/Web Defacement

- SOC Team to be kept on alert to monitor all web facing interface for any suspicious activity.
- Use latest version of Web server, Database Server, Hypertext Processor (PHP).
- Apply appropriate updates/patches on the OS and Application software.
- Conduct complete security audit of web application, web server, database server periodically and after every major configuration change and plug the vulnerabilities found.
- Validate and sanitize all user input, and present error messages that reveal little or no useful information to the user to prevent SQL injection attacks.
- Enable and maintain logs of different devices and servers and maintain the same for all the levels.
- Use Web Application Firewall (WAF), Security Information and Event Management (SIEM) and/or Database Activity Monitoring (DAM) solutions.
- Search all the websites hosted on the web server or sharing the same DB server for the malicious web shells or any other artefact.
- Periodically check the web server directories for any malicious/unknown web shell files and remove them as and when noticed. In order to identify Web shells, scan the server with Yara rules.
- Change database passwords of all the accounts available in the compromised database Server. Also change the passwords/credentials stored in the databases present on the database server.
- Use an application firewall to control input, output and/or access to the web application.
- Limit the file types allowed to be uploaded to the web server by using a list of predetermined file types. Define permissions on the directory the files are uploaded into, to prevent attackers from executing the files after upload.
- Consider using File Integrity Monitoring (FIM) solution on web servers to identify unauthorized changes to files on the server.