Website information in FGXWeb

Dimitris Kamenopoulos - 2023-01-10 - Comments (0) - FGX Web

FGX-Web Alert

If log file analysis is enabled, all log files which have been included in its configuration are visited every scan. New log entries are copied to FGX-Web (in encrypted S3 storage) for analysis and retention.

If File Integrity Monitoring is enabled, with every scan interval FGX-Web lists every directory under the document root and sends back file names, modification times and checksums (the checksum is calculated locally on the webserver) for every file. The resulting data set is retained in a database and the next time FIM runs compared with the next data set to identify new/modified/deleted files and directories. The set of changes that is calculated ("changeset") is retained for at least three months and no more than six.

If the Internal Malware Scanner is enabled, a separate change detection phase similar to that run by FIM is run, followed by downloading every file listed in the changeset. The file copies are downloaded in RAM and scanned for viruses and other malware. If a file is smaller than 2MB, it is downloaded in full. Otherwise, only the first and last MB of the file are downloaded. If a file is found to contain malware, we store its location and other attributes in order to populate the resulting alert, as well as a copy of the file in encrypted S3 storage for forensic investigation.

The other internal scanners are basehunter (base 64 detector), file card data scanner, database scanner and Magento scanner. They run locally on the server hosting the website. If a credit card number is found, only the first six digits and the location (filename or logical location within the database) are sent back to the portal in order to assist the investigation that follows. Similarly, if malware is found, only the location is sent back to the portal. It is however possible for an authorised user (a forensic investigator or an incident response analyst) to view the file or download a copy on demand. If the finding is a false positive, the user will destroy the copy. Otherwise, it might be retained as evidence.

All scanners mentioned above will completely ignore files and directories that match an exclusion rule.

The External Scanner visits only public pages of your website and stores only findings (e.g. "The version of Magento that I see is 1.9.2") and their dates. The findings are stored indefinitely unless their deletion is requested.

FGX-Web Protect (WAF)

If the website implements FGX-Web WAF, our WAF becomes the mediator between every end user and the website. When a visitor requests a resource, the request is intercepted by the WAF and analysed for indicators of undesired activity (such as the presence of a known SQL injection vector in some header). If nothing is found, the request is forwarded to the website. If there is a finding but the WAF is on Alert mode, the request is still forwarded but an alert is sent to our business contact and any other notification recipients. If the WAF is on Protect mode the request is blocked and a summary can be seen in the dashboard. We also intercept response status codes for brute force attack detection. For example, repeated 401 status codes indicate the user is constantly giving the wrong password. This entire analysis happens on the fly and all information is normally destroyed after the response has been sent back to the end user.

However, in order to populate summaries/statistics, measure bandwidth usage and assist with troubleshooting (e.g. with false positives) and/or PFI cases we do log with every request :

- end user IP
- requested FQDN (host: header)
- user agent
- whether the request was secured by TLS or not (HTTPS vs HTTP)
- requested URI
- request size
- response status
- whether the response came from us or from the customer’s server
- response size
- total roundtrip time

Additionally, if a rule is triggered by a request, we log all request headers and the reason a rule was triggered (e.g. "Header user-agent contains matches XYZ"). Sensitive headers such as cookies, HTTP Auth and any text that looks like a credit card number are never written on the log.

All logs are stored for at least 6 months in live format and 12 months as backups.