SAS 検体送付手順(誤検知/検知漏れ修正)

誤検知や検知漏れと思われる状況が発生した場合、検体解析システム（SAS）により、エフセキュアセキュリティラボへの確認/修正リクエストをご提出いただけます。1.対象のファイル、2.検知が発生した端末の診断情報を採取し、下記 URL からご提出ください。オフライン環境で弊社製品をご利用の場合はその旨をご記載下さい。

隔離保存フォルダからの検体ファイル復元方法
https://www.f-secure.com/content/dam/f-secure/ja/business/support-resources/windows/20210617-RecoveryQuarantneFiles.pdf

検体解析にてご提供可能な情報について

- ファイル/URL の危険性判断
- 現時点で弊社ウイルス対策ソフトが検知ができるかどうか？
- パターンファイルリリース情報
  DBtracker https://www.f-secure.com/dbtracker/

検体解析システム (SAS)

https://www.f-secure.com/en/web/labs_global/submit-a-sample

当窓口は英語対応のみとなりますが、24 時間対応の為、早急な修正対応が可能です。下記に英文対応依頼サンプルを紹介いたしますので、こちらのご利用をお願い致します。

Product name :

Internet　　:　Online / Offline (please correct in pattern file)

Detail　　:下記

(**安全なファイルの誤検知修正依頼**)Could you kindly check if this file is realy malicious? This file is detected as malicious by F-secure product.

(危険な**ファイルが** F-Secure **製品で検知されない場合**) Could you kindly check if this file is really safe? This file is not detected as malicious by F-secure product. This file is marked as malicious by other product(Product name:xxxx).

検体提出に対し、研究ラボでは誤検知/検知漏れ修正のみを行い、報告等を行いません。対応の詳細を知らいたい場合は下記のチェックを入れて提出を行ってください。

☐ I want to give more details about this sample and to be notified of the analysis results

日本語対応をご希望の場合

日本語対応をご希望の場合、以下手順を確認のうえ、指定メールアドレス宛に検体ファイルをお送りください。日本サポートチームより、日本営業時間内での順次対応を行わせていただきます。検体ファイルは通常サポート窓口では受け取ることができません。特に危険なファイルとして検知されている検体は、通常サポート窓口の受付時点でウイルス駆除が行われ、削除されます。

[手順]

検体を暗号化 ZIP で圧縮します。暗号化パスワードは「infected」
（検体取得の際には、リアルタイムスキャン機能を一時的に OFF にする必要があります。）

1. コンピュータ端末内で診断情報を採取します。
2. 「検体」「診断情報」「カテゴリ」を添付/記載したメールを以下に送信します。
   ※診断情報 -> https://www.f-secure.com/jp-ja/business/support-and-downloads/support-request#fsdiag

- カテゴリ

A. 安全なファイルの誤検知。自社開発ツール等の場合はその旨を記載ください。
B. 危険なファイルが F-Secure 製品で検知されない検知漏れ。

検体送付先 アドレス： japan-samples@file-samples.f-secure.com

※日本語対応は平日の月-金 9:30-12:00, 13:00-17:30 となります。

ジェネリック検知について

検知名: Generic.malware.[variant], Generic.[variant], gen:win32.malware.[variant], Gen:variant.

ジェネリック検知とは特定パターンファイルに登録されているウイルスの情報にファイルが一致したわけではなく、振る舞いやデータパターン等が類似している為に検知が発生します。そのため、自動解凍/自動ダウンロードアプリケーションといったファイルをシステム的に生成する場合、このジェネリック検知が継続的に発生する可能性があります。これはパターンファイル精度の問題ではなく、疑わしいファイルは検知するセキュリティー・ポリシーによるものです。同様の事象に対しては、ファイルの作成者側でデジタル証明書を埋め込み、弊社側で該当デジタル証明書の付加されたファイルについてのリスク判断を下げ

る事で、誤検知の発生頻度を低減する事が可能です。弊社サポートへファイルへ付加するデジタル証明書をご提出ください。もしくは単純にリアルタイムスキャンからの除外フォルダを作成し、そのフォルダ内での該当ファイルの作業を行うなどの対処をとって下さい。該当フォルダ内のセキュリティーは下がりますのでご留意ください。