Ver 1.00.14

FFRI yarai

syslog 通知機能

FFRI Security, Inc.
株式会社FFRIセキュリティ

目次

更新履歴

2013-12-03	1.00.01	パートナーサイト用
2014-3-27	1.00.02	「4 syslog メッセージフォーマット」の表を修正。 ・罫線を追加。 ・検知コードを修正。
2014-9-4	1.00.03	機械学習エンジンに対応
2015-4-23	1.00.04	FFR yarai v2.6 に対応
2015-11-5	1.00.05	FFR yarai v2.7 に対応
2016-1-7	1.00.06	OS を再起動する必要性があることを追記 「Confidential」表記を削除 HIPS で検知した場合の alert 値を追加
2016-12-16	1.00.07	FFRI yarai 2.8 に対応
2017-05-31	1.00.08	FFRI yarai 2.9 に対応
2018-07-19	1.00.09	FFRI yarai 3.2/2.12 に対応
2019-10-18	1.00.10	FFRI yarai 3.3/2.13 に対応 送信元ポート番号の説明とデフォルト値を修正。
2020-06-05	1.00.11	旧社名を新社名に変更
2021-02-26	1.00.12	FFRI yarai 3.4/2.14 に対応 HIPS で検知した場合の検知理由の追加・変更
2021-06-18	1.00.13	「syslog 通知機能設定方法」について追記
2022-04-04	1.00.14	FFRI yarai 3.5 に対応 機械学習エンジンで検知した場合のフォーマットについて注釈を追加 HIPS エンジンで検知した場合の検知理由の追加・変更

文書情報

発行元: 株式会社FFRIセキュリティ

連絡先: 株式会社FFRIセキュリティ

sales@ffri.jp

〒100-0005
東京都千代田区丸の内3丁目3－1 新東京ビル2階

1. 対象バージョン

本機能は FFRI yarai v2.4 以降でご利用頂けます。また、バージョンによって、仕様に差異があることがございます。

2. syslog 通知タイミング

Static、Sandbox、ZDP、HIPS、機械学習エンジンのいずれかで検知した際に、FFRI yarai から指定されたサーバへ syslog を送信します。プロトコルには UDP を使用し、送信に失敗した場合の再送制御は行いません。

3. syslog 通知機能設定方法

syslog 通知機能はレジストリ設定により行います。以下に設定に使用するレジストリ値の一覧を示します。また、設定を変更した後は OS を再起動する必要があります。

※キー／値が存在しない場合は、新規作成を行ってください。

キー名	値名	型	値	デフォルト値
HKEY_LOCAL_MACHINE¥SOFTWARE¥FFR¥yarai¥Syslog	enable	REG_DWORD	0：syslog 通知を行わない 1：syslog 通知を行う	0
	server	REG_SZ	①送信先 IP:送信先ポート ②送信先ホスト名：送信先ポート ①または②をカンマ切りで指定する。最大 20 個まで指定可能。	空
	facility	REG_DWORD	facility	16
	priority	REG_DWORD	priority	1

キー名	値名	型	値	デフォルト値
	localport	REG_DWORD	クライアントの送信元ポート番号を指定する。0 の場合はポート番号を指定せずシステムに任せる。	0
	tag	REG_SZ	タグ	yarai
	encode	REG_DWORD	Syslog メッセージ内に格納する検知ファイル path の Base64 エンコード機能 0:無効 1:有効	1

※x64 環境の場合、

HKEY_LOCAL_MACHINE¥SOFTWARE¥FFR¥yarai¥Syslog は

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥FFR¥yarai¥Syslog と読み替えて下さい。

4. syslog メッセージフォーマット

以下に syslog メッセージのサンプルを示します。

```
2013/11/11 17:28:50.777 192.168.0.71 <52>Nov 11 18:05:02 PC
yarai:<engine>STATIC<path>STpcdG9vbFxOZXNOIHRvb2wgc2VOXHRlc3RfbWFsd2FyZVx5YXJhaV9TdGFOaWNUZXNOLmV4ZQ==
2013/11/11 18:06:42.058 192.168.0.71 <52>Nov 11 18:42:53 PC
yarai:<engine>HIPS<alert>29<action>2<path>STpcdG9vbFxOZXNOIHRvb2wgc2VOXHRlc3RfbWFsd2FyZVx5YXJhaV9IaXBzVGVzdC5leGU=
```

以下に syslog メッセージのフォーマットを示します。

区分	項目	意味	値
PRI	facility	facility	レジストリで変更可能。デフォルトは 16（local0）
	priority	priority	レジストリで変更可能。デフォルトは 1（alert）
HEADER	timestamp	timestamp	検知時刻
	hostname	hostname	検知した PC のホスト名
MESSAGE	tag	tag	レジストリで変更可能。デフォルトは yarai。
	delimiter	tag と以降のメッセージを区切る文字	コロン 1 文字（:）
	engine	検知エンジン名	<engine>XXXX XXXX には検知したエンジン名（STATIC、SANDBOX、ZDP、HIPS、ZDP(design)、MACHINELEARNING、Defender のいずれか）が入る。
	alert	検知コード（HIPS、MACHINELEARNING のみ）	<alert>XX ■HIPS XX には検知コード（1～46）が入る。 ■MACHINELEARNING※v3.4/2.14 以前のみ XX には検知コード（1）が入る。

区分	項目	意味	値
	action	検知時のアクションコード（HIPS、ZDP、MACHINELEARNING のみ）	<action>XX XX にはアクションコードが入る ■ZDP 3：処理を許可しました。 4：プロセスを終了させました。 ■ZDP(design) 5:未使用 ■HIPS 0：処理を許可しました。 1：脅威を緩和しました。 2：処理の実行を拒否しました。 3：プロセスを終了させました。 4：処理を許可しました。 ※v2.6 以降では 3、4 のみ ■MACHINELEARNING※v3.4/2.14 以前のみ 3：プロセスを終了させました。 4：処理を許可しました。
	path	検知したプロセスの実行ファイルパス	<path>XXXX XXXX にはプロセスの実行ファイルパスが入る（文字コードは shift-jis）。Base64 エンコーディングが設定されたいた場合、エンコードされたパスが入る。

以下に HIPS で検知した場合の alert 値の一覧を示します。

検知コード	検知理由
1	プロセスがデバッグ権限を取得しようとしました。
2	プロセスが別のプロセスを不正利用しようとしました。
3	プロセスが別のプロセスのスレッドを不正利用しようとしました。
4	プロセスが自分自身の実行ファイルを操作して痕跡を消そうとしている疑いがあります。
5	プロセスが頻繁に SMTP 接続を確立していました。
6	プロセスが大量に不信な SMTP 応答を受信していました。
7	プロセスが頻繁に SMTP コマンドを送信していました。
8	他のプロセスのメモリをアンマップしようとしました。※v2.6 以降のみ
10	呼び出し元で適切に解決されていない API が呼び出されました。
11	プロセスが自分自身のコピーを実行しようとしました。
12	隠しプロセスがシステムユーティリティを実行しようとしました。
13	隠しプロセスが自身で生成したバッチファイルを実行しようとしました。
14	隠しプロセスがムービーをキャプチャーしようとしました。
15	プロセスが攻撃プログラムを起動しようとしています。
16	アプリケーションが自身(または自身のコピー)をサービスとして登録しようとしました。※ v3.4/2.14 以前 アプリケーションが不審なサービスを登録しようとしました。※v3.5 以降
17	プロセスがキーストロークを監視しようとしました。
18	隠しプロセスが Windows フックをインストールしようとしました。スパイウェアに利用される可能性があります。
19	プロセスが ZwLoadDriver を呼び出そうとしました。
20	プロセスが書き込み権限で「¥¥Device¥¥PhysicalMemory」を開こうとしました。
21	プロセスがバックドアを設置して、ドライバを読み込もうとしました。
22	アプリケーションが自身を別のプロセスに挿入しようとしました。

検知コード	検知理由
23	アプリケーションが不審な方法でファイルをコピーしようとしました。
24	アプリケーションが自分自身のプログラムファイルを消そうとして、痕跡を消そうとしています。
25	アプリケーションが自分自身のプログラムファイルを書き換えようとしています。
26	アプリケーションに異常な解析対策が施されています。
27	アプリケーションが他のプロセスに侵入しようとしています。
28	プロセスが HOSTS ファイルを不正に変更し、重要なアップデートなどを無効にしようとしました。
29	プロセスがドライブの自動再生で実行ファイルを登録しようとしました。
30	隠しプロセスがシステムのファイアウォールを無効にするよう、レジストリを変更しようとしました。
31	プロセスが他のプロセスをデバッグできるよう、レジストリを変更しようとしました。
32	隠しプロセスが Windows 起動時に自身が実行されるよう、レジストリを変更しようとしました。
33	隠しプロセスが非標準のエクスプローラが実行されるよう、レジストリを変更しようとしました。※v3.3/2.13 以前 隠しプロセスがログオンの設定に関する不審なレジストリ設定を行いました。※v3.4/2.14 以降
34	不審なファイル削除を検知しました。※v2.7 以降のみ
35	不審なファイル生成を検知しました。※v2.7 以降のみ
36	不審なプロセス生成を検知しました。※v2.7 以降のみ
37	不審なメモリ書換えを検知しました。※v2.7 以降のみ
38	物理ドライブを開こうとしました。※v2.7.7 以降のみ
39	レジストリに悪意あるコードを書き込もうとしました。※v2.7.7 以降のみ
40	プロセスが不審なファイル検索を試みました。※v2.8 以降のみ
41	マクロ（またはスクリプト）内で生成されたファイルが実行されようとしました。※v2.8 以降のみ
42	自己解凍書庫による不審なプロセス生成を検知しました。※v2.9 以降のみ

検知コード	検知理由
43	不審な挙動を検知しました。※v2.9 以降～v3.4/2.14 以前 ファイルレスマルウェアの挙動を検出しました。※v3.5 以降
44	プロセスがクレデンシャル情報への不審なアクセスを試みました。※v3.2/2.12 以降のみ
45	不審な DLL 読み込みを検知しました。※v3.3/2.13 以降のみ
46	不審な権限昇格を検知しました。※v3.4/2.14 以降のみ
47	複製された正規プログラムの悪用を検出しました。※v3.5 以降のみ
48	不審なマクロの構造を検出しました。※v3.5 以降のみ

以下に MACHINELEARNING（機械学習エンジン）で検知した場合の alert 値の一覧を示します。※v3.4/2.14 以前のみ

検知コード	検知理由
1	機械学習による判定の結果、このプロセスはマルウェアである可能性が疑われます。