



SecureBrain

製品概要

SecureBrain Zero-Hour Response System

(セキュアブレイン ゼロアワーレスポンスシステム)

1 製品紹介

新しい手法のウイルスやワーム、スパイウェア、ボット、また、特定の企業や組織を狙ったスパイア(標的)型攻撃が次々に出現し、インターネット社会を脅かしています。これらのマルウェアによる被害を最小限にいとめるためには、1分、1秒でも早く、コンピュータの管理者と利用者の双方に、信頼できる情報と確実な対策を提供しなければなりません。

「SecureBrain Zero-Hour Response System」(以下「ZHR システム」)は、従来人手に頼っていたマルウェアの解析からレポートの生成、さらには駆除ツールの生成までを、全自動かつ高速に行うことができます。

「ZHR システム」を導入することにより、企業や組織は新種のマルウェア発生時に的確な情報を迅速に入手し、被害の拡大を防止することができます。

2 機能概要

「ZHR システム」は、特許出願中(特許出願番号:2006-164285)の独自技術で、マルウェアの解析を行う検体解析システムを中心に構成されます。

1. マルウェア(検体)の情報収集・解析機能

- ▶ 検体を隔離した環境で実行し、情報収集や解析作業を全自動かつ高速に行います。
- ▶ マルウェア全般(ウイルス、ウイルス以外の悪意を持ったプログラム(ボット、スパイウェアなど)、その他通常のプログラムを含めた全ての Win32 プログラム)が解析可能です。
- ▶ 各種サーバや実行 PC などの擬似的なネットワーク環境を構築し、その中で隔離して安全に検体を実行させる独自の動的解析手法により、安全領域で検体のふるまいを自動解析します。

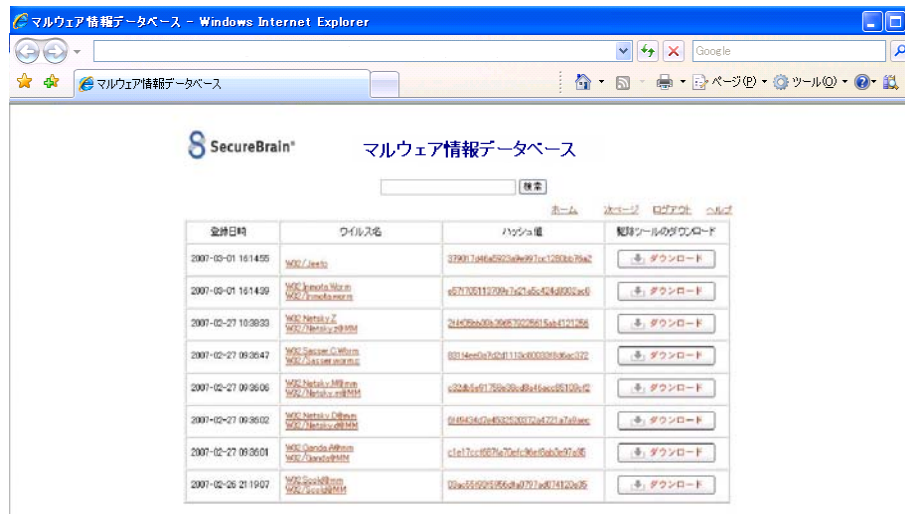
2. 解析結果を XML で出力

- ▶ 拡張性の高い XML で解析結果を出力するため、それを基に様々なフォーマットで結果表示を行うことが可能です。
- ▶ 解析レポートは、セキュリティベンダーが公開しているウイルス情報と同等レベル、またはそれ以上の内容を網羅します。

3. 検体の受付から解析結果の出力までお客様の用途に合わせた機能を実現
 - ▶ 解析等の工程管理
 - ▶ データベースの構築・管理
 - ▶ 解析結果を基に自動的に駆除ツールを生成・検証
 - ▶ 複数検体の同時解析

画面例

[結果出力画面]




SecureBrain® マルウェア情報データベース

検索

登録日時	ウイルス名	ハッシュ値	駆除ツールのダウンロード
2007-05-01 16:14:55	WG2/Fujacks	3790174464920a9971ca1202ba79a2	ダウンロード
2007-05-01 16:14:59	WG2/Smofa.Norm WG2/Smofa.Norm	e62170111220b71c7a5c4246902e0	ダウンロード
2007-05-27 10:39:23	WG2/Netshy.Z WG2/Netshy.Z	21439a20a30e83026d15a4171266	ダウンロード
2007-05-27 09:30:47	WG2/Secur.Catworm WG2/Secur.Catworm	02144e0a7d2f111e400020195cc172	ダウンロード
2007-05-27 09:36:06	WG2/Netshy.MF.mrm WG2/Netshy.MF.mrm	e2846a71720a20c494f6cc02102a2	ダウンロード
2007-05-27 09:36:02	WG2/Netshy.Catworm WG2/Netshy.Catworm	618434c7a43252027a771a7d18e6	ダウンロード
2007-05-27 09:36:01	WG2/Secur.Catworm WG2/Secur.Catworm	c1e17c4027a7ed18e6c0a3e37a06	ダウンロード
2007-05-26 21:19:07	WG2/Secur.Catworm WG2/Secur.Catworm	02a55221856a0771a071120a26	ダウンロード

[マルウェア解析レポート]



SecureBrain® マルウェア情報データベース

戻る

マルウェア名: [WG2.Fujacks.L]

ファイル情報

- ▶ 名前: arcldr.exe
- ▶ プログラムの種類:
 - ▶ WORM
 - ▶ NETWORK AWARE MALWARE
- ▶ サイズ: 189980 バイト
- ▶ MD5: 85eea3f81ed64f82d136af4920576276

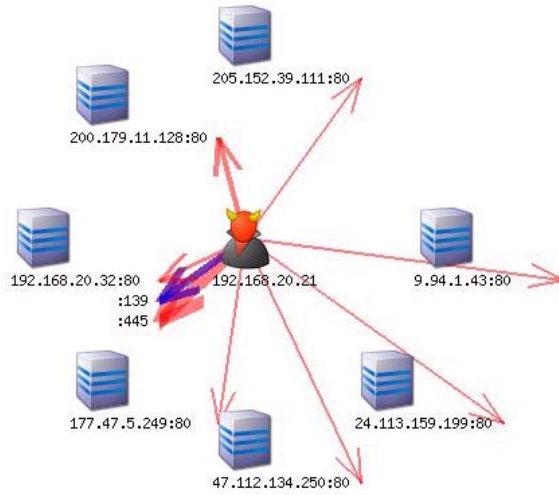
詳細情報

1. 次のファイルを作成します。
 - ▶ File: arcldr.exe.exe
 - ▶ File: C:\DOCUMENT1\<ユーザ名>\LOCALS1\Temp\10\$bat
 - ▶ File: <システムディレクトリ>\drivers\#ppoolsrv.exe

Microsoft RPCサービスに名前付きパイプで接続します。

- ▶ File: %PIPE%\svcc1
- ▶ File: %PIPE%\sarp

[マルウェアのネットワーク通信図]



[管理コンソール画面]

ID	ウイルス名	ステータス	ファイル詳細	ウイルス情報
600146756	WS2/HLW/Lovafate/C@mm WS2/Lovafate.c@MM	終了	ファイル詳細	ウイルス情報
2010790514	WS2/Mydoom.F@mm WS2/Mydoom.F@MM	終了	ファイル詳細	ウイルス情報
820202096	WS2/Netsky.F@mm WS2/Netsky.F@MM	終了	ファイル詳細	ウイルス情報
803105006	WS2/Netsky.D@mm WS2/Netsky.D@MM	終了	ファイル詳細	ウイルス情報
330773274	WS2/Netsky.C@mm WS2/Netsky.C@MM	終了	ファイル詳細	ウイルス情報
1541327849	WS2/Mydoom.F@mm WS2/Mydoom.F@MM	終了	ファイル詳細	ウイルス情報
545445918	WS2/Netsky.F@mm WS2/Netsky.F@MM	終了	ファイル詳細	ウイルス情報
2030476996	WS2/Netsky.D@mm WS2/Netsky.D@MM	終了	ファイル詳細	ウイルス情報
13309163603	WS2/Netsky.C@mm WS2/Netsky.C@MM	終了	ファイル詳細	ウイルス情報
808768446	WS2/Mydoom.F@mm WS2/Mydoom.F@MM	終了	ファイル詳細	ウイルス情報

[メニュー](#) [ログアウト](#)

ページが表示されました



3 用語について

・マルウェア

malicious software (悪意のあるソフトウェア) の短縮された語で、「悪意のある」ソフトウェアの総称。単一のコンピュータ、サーバ、コンピュータネットワークに被害を起こすように設計されたソフトウェア全般(ウイルス、またはスパイウェアなど)を示す言葉として一般的に使用される。また「悪」を意味する接頭詞の“mal-”とソフトウェアを意味する“ware”との造語という説もある。

・スパイ(標的)型攻撃

特定の企業・組織・個人を狙ってウイルスやフィッシングを仕掛ける攻撃。攻撃方法やフィッシングメールの内容は、攻撃相手に合わせ巧みにカスタマイズされている。

スパイ(spear)は「槍」を意味する。一点を狙って攻撃することからこう呼ばれるようになった。海外では Targeted attack とも呼ばれる。