GIDEON

Linuxサーバ向けソフトウェア製品

「ギデオン リアルタイムスキャン」
ご説明資料

株式会社ギデオン

Aug, 2012

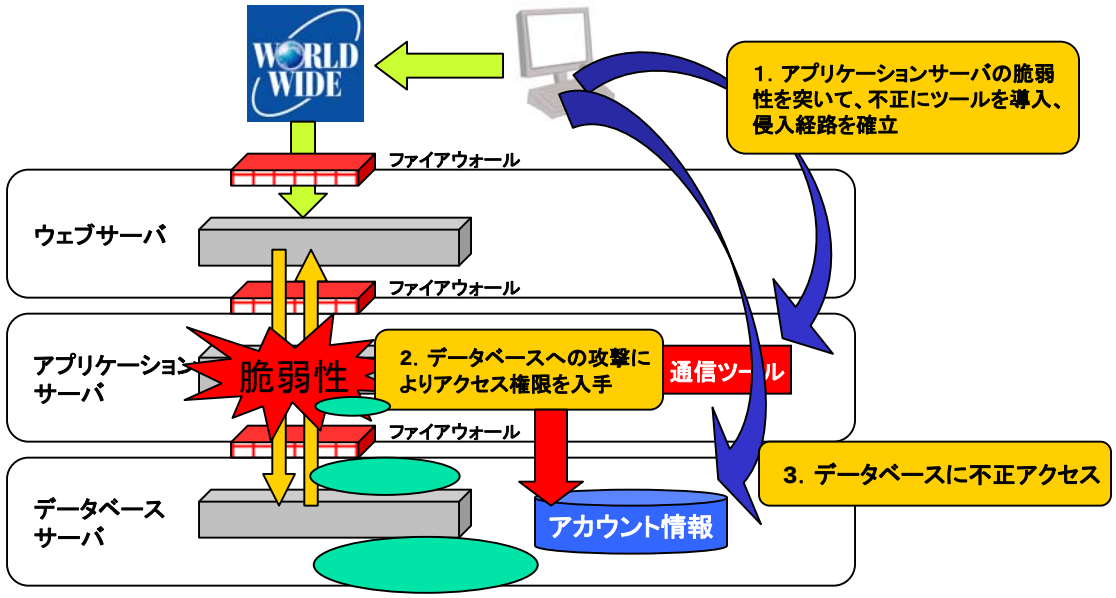
サイト改ざんに対する備え

- 今までのサイト改ざん防止対策
  - ファイアウォール(UTM)の利用
    →一般に公開しているWEBサイト(HTTP)からの改ざんの場合、アクセス制限などで改ざんを防止するのは困難
    →HTTPSサイトではウイルスチェックも不能
  - サイト改ざん検知ソフトウエアの利用
    →サイト改ざんが行われたらサイトを修復する作業が必要
  - サイト改ざん外部チェックソフト/サービスの利用
    →サイトページ数が多いと数時間に一度のチェックとなるため、発覚するまでのタイムラグがあり、その間に改ざんされたECサイトでの取引やサイト上に仕組まれたウイルスファイルが流布されてしまう可能性がある
    →費用が安くない(月額￥10,000以上)

<u>＋システムリソースの改ざんは検知困難</u>

GIDEON

最近の事例に見るサイトからの情報漏洩



もし、システムリソースの改ざん検知＆修復が
出来ていれば情報漏洩は防げていたかも…

出典：ソニー・コンピュータエンタテインメント社 2011年5月1日記者会見資料

ギデオン リアルタイムスキャンの機能

以下の処理を組み合わせて実行できます。

- リアルタイムウイルススキャン

  指定されたフォルダ下のファイルを監視し、改ざんファイルのウイルスチェックを行います。アンチウイルスにはカスペルスキー社のエンジンを利用し、Windows、Mac OSやモバイル（Androidなど）向けウイルスを検知します。
  (ウイルス定義ファイルは1時間ごとに自動更新)

- リアルタイム改ざん検知

  WEBサイトだけでなく、システムリソースも併せて、指定されたフォルダ下のファイルを監視し、GUI上のログ表示と管理者向けメールにて改ざん通知を行います。

- リアルタイム修復

  ウイルス検出、或いは改ざん検知されたファイルを外部から読み取れなくしたり、バックアップファイルからの修復を行います。

インストールするシステムの要件

- 適用できるシステム

  Kernel 2.6.13以降のLinux OSで稼動するシステム

  [例. Redhat EL 5/6、Cent OS 5/6、Debian 4/5/6、SUSE 10/11、
  Turbolinux 11(TLAS 3.0)]

- 推奨ハードウェア

  CPU: Pentium 4以上

  RAM: 1GB以上

  ハードディスク空容量: 300MB以上(バックアップ領域は除く)

ギデオン リアルタイムスキャンの特徴

- 簡単インストール

  Kernelに組み込むタイプではないため、インストールごとのコンパイルなどの手間が不要でコマンド1つでインストールできます。

- 改ざん防止対策にも有効

  改ざん検知&修復はシステムリソースにも適用可能で、システムリソースの変更→WEB改ざんという通常の改ざん手口を元からシャットアウトできます。

- コマンド連携設定で追跡調査情報の入手にも有効

  改ざん検知時に管理者に任意のLinuxコマンド実行結果を通知可能で、ps(プロセス状態表示)やnetstat(ネットワーク稼働状況表示)コマンドなどを連携させて追跡調査のための情報も入手可能です。

- お手頃な価格

  従来のLinux向けウイルススキャン＋改ざん検知のソフトウエアや改ざん監視サービスより安い価格設定となっています。

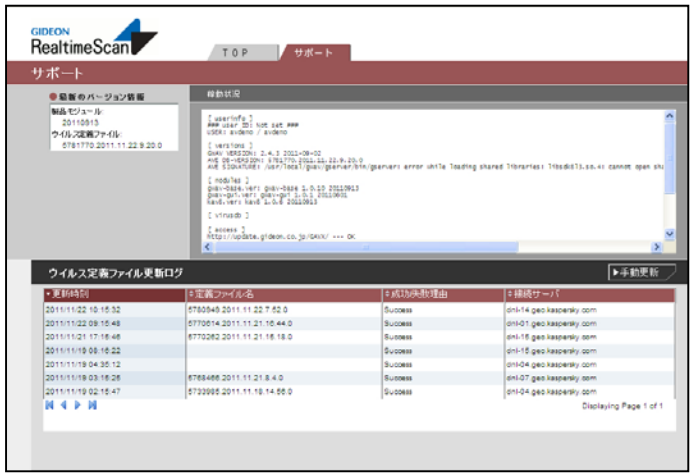
  新規定価: ￥80,000/サーバ、 次年度更新: ￥40,000/サーバ

  ※さらに5台以上一括導入の場合、ボリュームディスカウント有

GIDEON

ギデオン リアルタイムスキャンの操作

- GUIから各種操作・ログ閲覧が出来ます。



過去事例を基にした製品有効性(1)

- 攻撃ツール「MPack」による改ざん事例
  - 「MPack」とは？

MPackは商用のクラッキング・ツールであり，正規のWebサイトを改ざんしてiframeを埋め込み，そこからクライアント・アプリケーションのぜい弱性を悪用してユーザーのクライアントPCにマルウエア（不正プログラム）を導入するというものである。

  - 改ざん手順と弊社製品による検知タイミング対比

ステップ 1: 攻撃者は何らかの手段で Web サーバに侵入する
ステップ 2: 攻撃者は HTML 文書に MPack の 攻撃コードを読み込ませる ための iframe を記述する

ステップ 3: ステップ 2 で iframe が記述された HTML 文書を閲覧した被害者は、自動的に MPack の 攻撃コードを開いてしまう
ステップ 4: MPack の 攻撃コードは被害者がアクセスした際にOS やブ ラウザを判別し、被害者のコンピュータの脆弱性を攻撃する
ステップ 5: 被害者のコンピュータに MPack が対象とする脆弱性が存在する場合、攻撃者が準備した悪意のあるプログラムが実行さ れる

ステップ2で改ざん検知＆修復

ステップ3以降には進めない

出典：JPCERTコーディネーションセンター 2007年6月28日「複数の脆弱性を使用する攻撃ツール MPack に関する注意喚起 」
http://www.jpcert.or.jp/at/2007/at070016.html

過去事例を基にした製品有効性(2)

- 「SQLインジェクション」による改ざん事例
  - 「SQLインジェクション」とは？

データベースと連携したウェブアプリケーションに、問合わせ命令文の組み立て方法に問題があるとき、ウェブアプリケーションへ宛てた要求に、悪意を持って細工されたSQL文を埋め込まれて（Injection）しまうと、データベースを不正に操作されてしまうこと。ウェブサイトは個人情報などが盗まれたり、注文情報を書き換えられたりといった被害を受けてしまう。

  - 改ざん手順と弊社製品による検知タイミング対比

ステップ 1: 攻撃者はインターネットを巡回して、攻撃対象となるWEBサイトを探す

ステップ 2: 攻撃者は 攻撃対象に対して、SQLインジェクション攻撃によりWEBページを改ざんし、悪意のあるJavaScriptを挿入

ステップ2で改ざん検知＆修復

ステップ 3: 改ざんされたWEBサイトを閲覧したユーザのプラウザ上で悪意のあるJavaScriptが起動

ステップ 4: 悪意のあるJavaScriptはユーザのパソコン上の脆弱性を利用してマルウェアなどを導入

ステップ3以降には進まない

出典：日経BP社 ITpro 2008年6月30日『改ざん攻撃はこう防げ！Webサイトの正しい守り方「 第1回 急増するWebサイト改ざん事件」』
http://itpro.nikkeibp.co.jp/article/COLUMN/20080624/309301/

GIDEON

http://www.gideon.co.jp

製品に関するお問合せは弊社営業部
Tel: 045-590-1216
E-mail: sales@gideon.co.jp