通元网页防篡改系统

产品白皮书

http://www.gpowersoft.com

目录

1. 概述

1.1. 背景

随着网络与信息技术的飞速发展，尤其是在互连网飞速发展的今天，网络已经逐渐改变了人们的生活方式 ，成了生活中不可缺少的一部分。庞大的网民数量和网站群为互联网应用的快速发展奠定了良好的基础。网页的地位也得到了空前的提高，对一个企业对一个政府机构网页无异于自己的门面。虽然目前已有防火墙、入侵检测等安全防范手段，但各类 WEB 应用系统的复杂性和多样性导致系统漏洞层出不穷、防不胜防，黑客入侵和篡改页面的事件时有发生。据中国被黑站点统计系统数据分析发现：2007 年全国共有 24516 个一级域名网站被篡改，这仅仅还是以知的不包括所有的二级或二级域名以下的网站数据，其中包括：

.gov.cn 域名 的政府网站仅 2007 年就有 708 个网站被篡改

.cn 域名被黑站点统计 为 6186 个

.com.cn 域名被黑站点统计 共计 1403 个

.com 域名 被黑站点统计共计 13664 个

.net.cn 域名 被黑站点共计 203 个

.net 域名 被黑站点统计共计 1586 个

.org 域名 被黑站点统计 共计 393 个

.org.cn 域名 被黑站点统计 102 个

。。。。。。

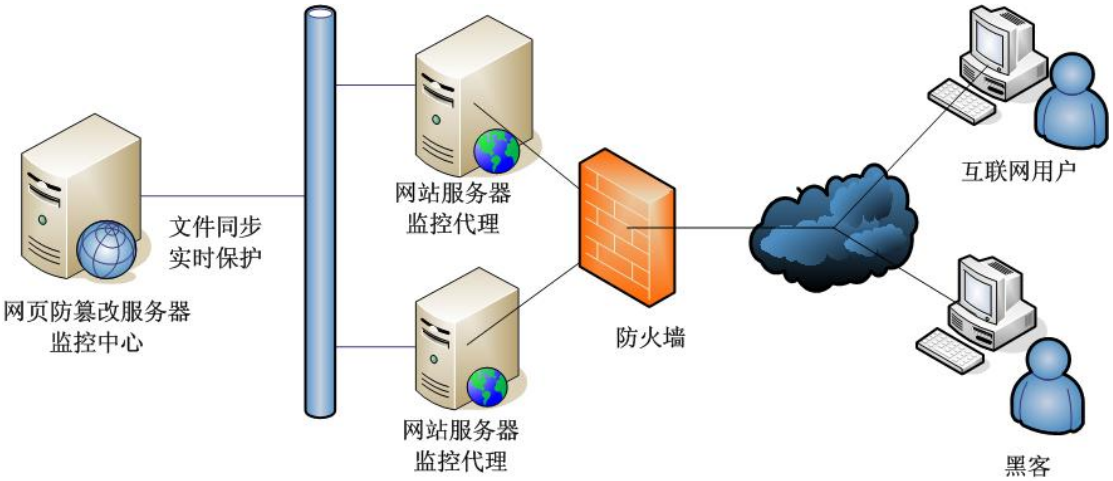
针对这些情况，通元网页防篡改系统应运而生。通元公司通过多年的技术积累，并详细分析了网页被篡改的原因与特点：黑客强烈的表现欲望，国内外非法组织的不法企图，商业竞争对手的恶意攻击，不满情绪离职员工的发泄等等都将导致网页被“变脸”。网页篡改攻击事件具有以下特点：篡改网站页面传播速度快、阅读人群多；复制容易，事后消除影响难；预先检查和实时防范较难；网络环境复杂难以追查责任，攻击工具简单且向智能化趋势发展。。。。。。

1.2. 通元网页防篡改系统简介

通元网页防篡改系统（Gpower WebGuard），是通元软件公司结合多年互联网网站安全的实施经验，采用目前最为先进的文件过滤驱动技术＋事件触发技术，并结合安全传输技术，

且遵循 Internet 相关标准协议的网页防篡改系统。产品主要提供文件监控保护、文件同步传输功能，确保文件系统的内容及权限不被篡改。

2. 系统总体结构



通元网页防篡改系统实时监测网站的各个页面，当网页被黑客非法修改时，系统能及时发出各种警报，同时自动恢复原来的页面。

通元网页防篡改系统在逻辑上分为三个子系统：监控代理 Monitor Agent （简称 MA）、监控中心 Monitor Center（简称 MC）、监控终端 Monitor Terminal（MT）。

- MA – Monitor Agent / 监控代理端

如果要监控多台网站服务器，必须在每台服务器上都部署一个 MA，但是，这些 MA 可以被同一个 MC 管理。MA 是一个后台运行的进程，系统启动后它自动运行，运行期间不需要人为干预。

MA 安装在 WEB SERVER 服务器上，利用操作系统事件触发技术监视 Web 应用的相关文件/目录的变化事件（增加/修改/删除/改名等），一旦有变化时间发生，向 MC 报告该变化

- MC – Monitor Controller/监控中心

MC 部署在管理服务器上，负责统一管理所有监控代理和集群。它提供标准的 Windows 管理界面，使用者可以轻松掌握。

MC 安装在 WEB-GUARD 服务器上，对各个要监控的 Web 应用，均在 MC 上保留一份完整的备份。一旦接收到 MA 的变化报告，将变化与备份中的文件进行对比，如果不一致，说明发生了非法篡改，利用备份文件恢复 Web 应用中的非法篡改。

- MT – Monitor Terminal/监控终端

安装在 WEB-GUARD 服务器上的一个 Web 应用，与 MC 通信，为管理员提供操作及监控界面，当有管理员关系的时间发生时按照指定的方式报警。管理员通过浏览器可以访问 MT，主要实现：监视各个 MA 的状态、配置 MC 及各个 MA、修改 MA 上 WEB 应用的内容、查看 MC,MA 的日志等。

3. 防篡改核心技术

通元网页防篡改系统的核心技术为文件过滤驱动技术＋事件触发技术，其显著特点为效率高、占用资源少、实施方便。

网页防篡改包括以下几种技术：

时间轮巡技术：时间轮询技术是利用一个网页检测程序，以轮询方式读出要监控的网页，与真实网页相比较，来判断网页内容的完整性，对于被篡改的网页进行报警和恢复。但是，采用时间轮询式的网页防篡改系统，对每个网页来说，轮询扫描存在着时间间隔，一般为数十分钟，在这数十分钟的间隔中，黑客可以攻击系统并使访问者访问到被篡改的网页。此类应用在过去网页访问量较少，具体网页应用较少的情况下适用，而对于政府或大型企业门户，网站页面通常少则几百页，多则数万页，检测轮巡时间更长，且占用系统资源较大，该技术逐渐被淘汰。

核心内嵌技术：最初先将网页内容采取非对称加密存放，在外来访问请求时将经过加密验证过的，进行解密对外发布，若未经过验证，则拒绝对外发布，调用备份网站文件进行验证解密后对外发布。此种技术通常要结合事件触发机制对文件的部分属性进行对比，如大小，页面生成时间等做判断，无法更准确的进行其它属性的判断。其最大的特点就是安全性相对外挂轮巡技术安全性大大提高，但不足是加密计算会占用大量服务器资源，系统反映较慢。

Gpower 网页防篡改系统采用目前最为先进的文件过滤驱动技术＋事件触发技术。其原理是：将篡改监测的核心程序通过文件底层驱动技术应用到 Web 服务器中，通过事件触发方式进行自动监测，对文件夹的所有文件内容，对照其底层文件属性，经过内置散列快速算法，实时进行监测，若发现属性变更，通过非协议方式，纯文件安全拷贝方式将备份路径文件夹内容拷贝到监测文件夹相应文件位置，通过底层文件驱动技术，整个文件复制过程毫秒级，使得公众无法看到被篡改页面，其运行性能和检测实时性都达到最高的水准。

Gpower 页面防篡改模块采用 Web 服务器底层文件过滤驱动级保护技术，与操作系统紧密结合，所监测的文件类型不限，执行准确率高。这样做不仅完全杜绝了轮询扫描式页面防篡改软件的扫描间隔中被篡改内容被用户访问的可能，其所消耗的内存和 CPU 占用率也远远低于文件轮询扫描式或核心内嵌式的同类软件。是一种简单、高效、安全性极高的一种防篡改技术。

4. 系统功能

4.1. 文件保护

通元网页防篡改系统采用独特的实时监控技术，实现对监控文件的实时保护，防止篡改。

4.2. 自动分发

网站采用内容管理系统，会自动生成大量网页文件，而同时系统必须保证网站内容和备份端保持一致。通元网页防篡改系统提供了热部署功能。保证用户只需经过简单配置，就可以实现对网站的完全监管。通元网页防篡改系统可与通元内容管理系统完美结合，实现网站的内容管理和网站安全。

4.3. 增量备份及更新

网站的内容时刻变化和更新，如果因为某些特殊操作，导致网站内容和备份端不一致，这时候，就需要进行备份或者更新操作。为了兼顾效率和准确性，系统提供了增量备份和同步（增量更新）功能。在进行网站备份和更新前，会首先比较监控端的文件和备份端的文件，然后仅将增量变化的文件传给另一端。

4.4. 支持多虚拟主机

通元网页防篡改系统能自动、实时监控多个网站。只要在待监控的 Web 服务器上安装并启动监控代理，每个监控网站在监控中心以虚拟主机的形式存在。管理员可以通过监控中心控制平台对监控网站对应的虚拟主机进行添加、管理、监控及删除等各种操作。

4.5. 支持动态网页

支持监控保护动态网页文件，如符合 JSP、ASP、PHP、Servlet 等技术规范的文件。

4.6. 支持自动报警

检测到非法篡改时系统自动向管理员报警，可支持多种报警方式，如：声音、邮件、短信等。

4.7. 查询审计

支持对网站维护工作的查询与审计功能。为了便于用户及时了解管理员及操作员所做的

日常维护工作。系统提供了日志审计工具，方便用户查询和统计。

4.8. 代替 CMS 的 FTP 同步功能

系统可与 CMS（内容管理系统）结合，代替 CMS 的 FTP 同步功能
支持手工进行特定内容的强制刷新
对于 CMS 多次发布相同的内容，不会多次同步，减少网络流量

5. 系统环境要求

监控中心：Linux、Windows2000 及以上等平台
监控代理：Windows2000、Linux、Unix 等各种平台

6. 部分客户列表

国家旅游局

国防科工委

国家奥林匹克文献中心

国家统计局

国家宗教事务局

国家质检总局进出口检验检疫协会

财政部资产评估协会

首钢集团

德邦证券

北京房山区政府

北京大兴区政府

国防大学

空军飞行学院

北京语言大学

北京大学

北京理工大学

。。。。。。