

非法入侵网站案件的电子取证分析

庄建儿

(浙江省湖州市公安局网络警察支队, 浙江 湖州 313000)

摘要: 为有效打击入侵网站的行为, 以 Windows 系统为例, 对一般网站服务器常见的电子取证内容和方法进行了总结和分析. 重点就易变数据、事件日志、网站日志、异常帐户和文件、特殊目录下的文件记录等证据的取证进行了分析和阐述, 提出了一些有用的对策.

关键词: 网站; 入侵; 电子证据

中图分类号: TP393.08

文献标识码: A

文章编号: 1001-5132 (2012) 04-0055-04

随着计算机与网络技术的迅猛发展, 互联网已经广泛应用于社会的各个领域, 网络犯罪也一直呈上升趋势. 近年来, 怀有各种目的的黑客行为大量出现, 很多网站包括一些政府门户网站相继被黑客入侵, 严重危害信息网络安全. 加强对网站入侵案件电子数据证据的提取和分析, 已成为网络警察的重要工作内容之一. 最近新修改的《刑事诉讼法》顺应时代潮流, 将电子数据纳入刑事诉讼的法定证据种类之一, 也说明了电子数据勘查取证的重要性. 笔者以 Windows 系统为例, 对一般网站服务器常见的电子取证内容和方法进行了总结和分析.

1 电子证据取证注意事项

根据公安部《计算机犯罪现场勘验与电子证据检查规则》之规定^[1], 电子证据的采集应遵循合法性、及时性、全面性和严格管理过程等原则, 严格按规范进行, 以确保证据的真实性和完整性. 整个取证过程中, 每个环节都必须检查真实性和完整性, 尽量拍照或摄像, 制作详细的笔录, 由行为人共同签名^[2].

取证人员要注意发掘电子证据各种信息: 一是主要信息, 即文件的内容, 如文字、图像、声音、录像等或实现特定功能的数据代码; 二是附属信息, 即关于这些数据内容的来源、创建日期、修改日期、作者等附属信息; 三是环境信息, 即这些数

据内容的逻辑存储地址、物理存储地址等环境信息. 例如 1 个数码照片文件, 除内含的图像信息外, 还包括拍摄这张照片的相机品牌、型号、拍摄日期、光圈值、曝光时间等附属信息^[3].

网络数据的勘查取证除了前面的内容外, 还需要重点关注各种日志、入侵者与受害者的计算机的连接. 网络数据量非常大, 勘查取证需要确定恰当的策略, 如可从报警数据等方面入手.

2 提取易变数据

通常情况下, 取证人员拔掉可疑计算机的电源线, 以防止该机上的数据被破坏, 但这在服务器上实行并不妥当, 而是应该及时拔掉网线, 并马上提取各种易变数据: 系统时间、当前登录用户、打开的文件、网络信息、网络连接、进程信息、进程到端口的映射、进程内存、网络状态、剪贴板内容、服务/驱动信息、命令行历史、映射的驱动器、共享等. 取证时, 先获取内存数据, 使取证过程对内存的影响最小, 然后获取其他易变数据^[4].

取证人员应自带相关工具(如 cmd.exe 等命令解释程序), 尽可能少地对原始证据造成更改. 检查前, 注意查看服务器时间与标准时间间的误差.

对可能通过 ARP 欺骗和 DNS 欺骗实现网络钓鱼案件, 则分别通过“arp-a”、“ipconfig/displaydns”等命令查看 ARP 缓存表和 DNS 缓存表.

远程控制木马一般使用反弹端口的连接方式,

肉鸡开机后主动与黑客主机建立联接。一般可使用“netstat-ano”查看TCP/UDP网络连接、侦听端口和使用网络连接的进程标识信息,找到攻击者主机的IP地址。比如,如果本机系统中的高端口的客户进程连接到远程的80端口就可能存在问题。

如果服务器出现了超过正常数倍的连接数,会大量出现SYN_RECEIVED、TIME_WAIT等状态,如:TCP 192.168.0.2:80, 61.175.*.*:2203 SYN_RECEIVED,说明Web服务器出现80端口对外关闭现象,因为这个端口已经被大量的垃圾数据堵塞,正常的连接被中止。其中,“61.175.*.*”就是被用来代理攻击主机的IP,“SYN_RECEIVED”是TCP连接状态标志,意思是“正在处于连接的初始同步状态”,三次握手无法完成。

3 提取事件日志

网站入侵案件的取证,除了获取静态文件外,还要特别注意各类日志记录。服务器事件日志记录服务器软件、硬件、系统和安全问题,可以帮助取证人员了解服务器运行过程中发生的事件、找寻黑客入侵时留下的蛛丝马迹。Windows系统事件日志共三类:系统日志、安全日志和应用程序日志。系统日志记录Vista之前的操作系统事件日志存储位置为“%Systemroot%\System32\config”,Vista及之后的操作系统事件日志存储位置为“%Systemroot%\System32\winevt\Logs”。查看日志除系统自带的“事件查看器”外,还可使用MyEventViewer、LogParser等工具软件。

我们重点可以查看ID号为528(成功登录)、529(试图使用未知的用户名或已知用户名但错误密码进行登录)、624(用户创建)、517(事件日志被清除后在系统日志中出现的记录)、520(系统时间修改)等。其中,事件528还要查看登录类型。Windows为了让用户从日志中获得更多有价值的信息,它细分了9种登录类型,以便区分登录者到底是从本地登录、网络登录还是其他登录方式。

了解这些登录方式,将有助于从事件日志中发现可疑的黑客行为,并能够判断其攻击方式。

需要重点关注类型是登录类型10,其为远程交互,通过终端服务、远程桌面或远程协助访问计算机时,因此Windows将其记为类型10,以便与真

正的控制台登录相区别,XP之前的版本不支持这种登录类型,比如Windows 2000仍然会把终端服务登录记为类型2。

Windows 2000引入事件编号540(网络登录),用来代替528登录类型3(成功从网络登录,例如通过net use、访问网络共享或者从网络中使用net view查看共享)。在Vista以后版本(.evtx)中,又被合并到事件编号4624中。在evtx中,一般情况下,原有的ID+4096=新的事件ID,但并不总是一对一的映射关系,除了528和540合并为4624外,登录失败的529至537及539统一合并为4625。

4 提取网站日志

网站日志记录Web服务器接收处理请求以及运行错误等各种原始信息,包括用户访问的IP地址、访问的具体页面、访问方法或发生的请求提交事件、访问时间、端口、http状态、浏览器、操作系统等项目。分析网站服务器生成的日志是找到攻击尝试和入侵细节的最好方法之一。在电子数据勘查取证中,分析网站日志重点查看错误和非正常访问信息,如ShowFile(显示文件)、UpFile(上传文件)、EditFile(修改文件)等信息^[5]。还有特殊关键字请求,如select*、delete、update、insert into、drop from、exec、master、cmd等,以及异常参数请求,如“or 1=1”等。

IIS日志的名称格式是exYYMMDD.log(YY代表年份的后两位,MM代表月份,DD代表日期)。IIS5和IIS6(Windows 2000、Windows XP、Windows Server 2003)日志存储位置为“%Systemroot%\System32\LogFiles\”,IIS7和IIS7.5(Windows Server 2008、Windows Vista、Windows 7)日志存储位置为“%SystemDrive%\InetPub\LogFiles\”。需要注意的IIS日志记录时间是格林尼治时间,需要加8小时得到的才是北京时间。

2012-02-28 00:00:01 W3SVC1 202.96.*.* GET /admin/news.asp id=51%20And%20(Select%20Count (name)%20from%20[master]..[sysobjects])>0 80 - 60.190.*.* Mozilla/4.0.....200 0 0

这是1个简单的入侵案例,入侵者(60.190.*.*)通过80端口以GET方式在网站admin文件夹下的news.asp文件上构造Sql语句,猜解网站表段及字

段, 以得到网站的管理员账号密码。GET 是客户端试图执行的操作, 另外还有 POST 方法。后面的 200 是操作状态代码, 常见的有 200 表示成功, 403 表示没有权限, 404 表示找不到该页面, 500 表示程序有错。

一个较复杂的利用 SQL 注入漏洞入侵的日志记录如下^[6]。

```
..... GET /news/shownews.asp newsid=166;  
DROP TABLE kill_kk; CREATE TABLE kill_kk  
(subdirectory VARCHAR(100),
```

```
depth VARCHAR(100), [file]VARCHAR(100))  
Insert kill_kk exec master..xp_dirtree "E:\WEB", 1,1  
80 - 116.52.144.* Mozilla/4.0+.....200 .....
```

该日志中, 入侵者建立 1 个临时表 kill_kk, 用于存放执行 master..xp_dirtree 生成的目录树, 表中的 subdirectory 字段表示目录或文件的名称, depth 字段表示深度, file 表示是否为文件(1 表示文件, 2 表示目录), 然后执行扩展存储过程 xp_dirtree 获得 E:\WEB\下的目录树及文件。E:\WEB 是网站的根目录, 说明入侵者已经找到了 WEB 根目录。

xp_dirtree 存储过程功能是查看文件夹树状结构或 1 个文件夹下的文件列表。为防止黑客再次入侵, 网站管理员应该删除存储过程 xp_dirtree 或去掉 public 角色对 xp_dirtree 的 exec(执行)权限。

5 识别未授权用户的帐户和异常文件

入侵者常用的方法是在系统中将用户权限提升或者启用一个欺骗性帐户, 以访问到未经授权许可的数据。在活动系统中, 有几种审核用户帐户、用户组的方法^[7]。

(1) 查看本机用户, 寻找未授权的用户帐户。

(2) 查看事件日志, 重点关注 ID 为 624(用户创建)、626(用户启用)、636(成员已添加至本地组)、642(用户帐户已更改)等。

网站被入侵后, 黑客一般会上传木马文件。由于木马文件和网站文件不是同一时间上传的, 因此可以通过文件的创建时间、修改时间等属性进行查找, 也可通过相应的辅助软件帮助定位。

异常文件查看过程中, sethc.exe 值得特别关注。该文件本是为不方便按组合键的人设计的, 按 5 下 shift 键后, windows 就执行了 system32 下的

sethc.exe。很多黑客用 cmd.exe 替换这个文件来给自己留后门, 这样在登录界面连按 5 下 shift 键就可以调出 cmd 命令窗口, 从而获得系统权限。

6 察看入侵者其他痕迹

入侵者留下的其他痕迹有网络通信数据、最近使用过的文件、预读文件、回收站、注册表等。IDS、防火墙等网络安全设备的日志当然也很有用, 在常见的网站攻击案件中, 管理员大都因为不重视这些而遭到黑客入侵, 系统根本没有这些日志。

一些木马在记录到使用的信息之后, 会通过电子邮件送到控制者的邮箱里。目前我们使用的以太网采用带冲突检测的载波侦听多路访问协议(CSMA/CD)作为介质控制协议。该协议使用广播机制, 传输的数据包能被共享信道的所有主机接收。因此, 只要设置网卡为混杂工作模式, 在理论上就能抓到局域网的所有数据包。我们可使用 Wireshark 等软件获取网络封包信息, 一般用明文传送的邮箱等信息均能提取。

最近使用过的文件记录(.lnk 文件)对调查工作也很有用。用户访问文件、硬盘、移动存储设备都会在用户目录的 Recent 目录下创建一个快捷方式。

从 Windows XP 开始, 微软操作系统开始使用预读技术来改进系统性能。Windows 2003 默认执行启动预读, XP、Vista 等则默认程序和启动预读都启用。应用程序预读时, 预读文件被写到 Windows\Prefetch 目录下, 生成.pf 文件。预读文件可以告诉们程序运行的痕迹包括最后一次运行时间信息。

Windows 删除文件机制中, 如果用常规办法删除 1 个文件, 文件本身并未被真正清除, Windows 会把文件放入回收站, 即使清空了回收站, 操作系统也不会真正清除文件的数据。Windows 所谓的删除实际上只是把文件名称的第一个字母改成一个特殊字符, 然后把该文件占用的簇标记为空闲状态, 但文件包含的数据仍在磁盘上。只有在下次有新的文件要保存到磁盘时, 这些簇才可能被新的文件使用, 从而覆盖原来的数据。只要不被新的文件覆盖, 被删除文件的数据实际上仍旧完整无缺地保存在磁盘上。恢复被删除文件的工具软件很多, 如常见的 EasyRecovery。如果被删除文件在硬盘上的位置已被覆盖, 则可使用 EnCase、取证大师、

SafeAnalyzer 等专业软件根据关键词进行搜索。

7 非法入侵网站案件对安全防范工作的启示

网站安全防御是一个长期持续的工作,只能运用最新技术成果不断改进安全措施,及时调整防护策略,而不能一劳永逸。从网站入侵案件来看,很多网站服务器存在着诸如未及时安装补丁程序、未关闭不必要的系统服务和端口、未启用登录失败处理功能、未对外部开发与维护人员的行为进行审计、未对远程管理终端地址范围和远程管理方式进行有效限制等情况。这些问题反映了网站安全技术策略配置不规范,安全管理制度有漏洞。当前,信息安全等级保护已被确立为国家信息安全保障工作的基本制度。为此,信息网络安全应树立整体理念,以“对信息系统分等级保护与监管”与“适度安全、重点保护”为指导思想,坚持以管理为龙头、技术为基础、运维为保障,建立以防火墙、入侵检测、漏洞扫描、身份认证、安全审计等为主要策略的安全防护体系,严格落实信息安全等级保护的一系列标准和等级测评等方法,保障信息网络“长治久安”。

8 结语

网站电子数据勘查取证实际上是一个全面检

查网站计算机系统、重建入侵事件并固定电子证据的过程,从而发现线索、抓获嫌疑人。实际勘查过程中,调查人员往往得不到完美的数字犯罪现场。越来越多的人包括违法犯罪分子开始使用工具软件擦除和隐藏数据,掩盖消除入侵痕迹。大容量存储介质和虚拟存储技术的发展,也大大增加了取证工作的难度。因此,电子数据勘查取证工作人员需要不断总结工作方法,与时俱进,以适应信息时代打击计算机网络犯罪的要求。

参考文献:

- [1] 公信安(2005)161号. 计算机犯罪现场勘验与电子证据检查规则[S].
- [2] 陈龙, 麦永浩, 黄传河. 计算机取证技术[M]. 武汉: 武汉大学出版社, 2007:7-8.
- [3] 高峰, 邹积超. 试论刑事诉讼中电子证据的审查[J]. 信息网络安全, 2011(9):167-170.
- [4] Harlan Carvery. Windows 取证分析[M]. 王智慧, 崔孝晨, 陆道宏, 译. 北京: 科学出版社, 2009:7.
- [5] 刘建军, 黄政. 网站入侵案件中的电子证据研究[J]. 信息网络安全, 2011(11):93-96.
- [6] 范春荣, 张战勇, 肖新华. 充分利用 WEB 日志分析检测黑客入侵[J]. 石家庄铁路职业技术学院学报, 2009(1):90-94.
- [7] 陈龙, 麦永浩, 黄传河. 计算机取证技术[M]. 武汉: 武汉大学出版社, 2007:119-120.

Electronic Evidence Gathering for Illegal Network Intrusion

ZHUANG Jian-er

(The Internet Police Detachment of the Huzhou Public Security Bureau, Huzhou 313000, China)

Abstract: Illegal Network Intrusion is one of the main threats that we are facing in the field of network security. In order to crack down the illegal network intrusion, in this work, taking the Windows system as the platform, the author makes some efforts on summarizing the methods and analyzing the contents of the electronic evidence obtained from the common website servers in illegal network intrusion activities. The focal point of this article is set on the analysis and statement of the evidence gathering, which involves using the mutable figures, event logs, website logs, unusual accounts and documents, the documents record in some particular contents. Some useful countermeasures are also presented in the end of this paper.

Key words: website; illegal intrusion; electronic evidence

(责任编辑 章践立)