附件2:Windows服务器、终端安全加固及染毒终端定位措施

**一、安全加固措施**

1. 更新所有Windows服务器及个人终端电脑的系统补丁，尤其是MS17-010漏洞补丁务必进行更新。
2. 确认所有Windows服务器及个人终端电脑中的360防病毒软件已升级天擎6的最新版本，并进行病毒查杀，病毒名称：mssecsvc.exe。
3. 管理员需对本公司DNS服务器进行日志分析，定位解析“指定域名”（见下方表格）的终端或服务器，并对其进行上述病毒处理，禁止对“指定域名”进行“禁止解析”处理，有条件的单位可将该域名指向本地网络中可能长期稳定运行的服务器。
4. 在所管理的网络设备中，禁止双向139、445端口访问，如业务需要，可针对性开放端口。
5. 开展应用系统数据备份工作。
6. 不要点击可疑邮件内的链接或附件。
7. 请二级单位管理员及时开展应急措施并通知下属单位，避免遭到病毒的侵害。
8. 如发现服务器或办公终端出现中毒情况，请及时与集团防病毒管理员联系，邮箱：

|  |  |
| --- | --- |
| **说明及要求** | |
| “指定域名” |  |
| 服务器版360下载地址 | http:// /server.html |
| PC版360下载地址 | http://10108/sd.html |
| 服务器版360版本要求 | 不低Build 2.2701 |
| 服务器版360病毒库版本要求 | 不低于Build 2.2701 |
| PC版360版本要求 | 不低于6.0 Build 22410 |
| PC版360病毒库版本要求 | 不早于2017-09-25 |

**二、通过DNS查找染毒服务器、终端的操作方法**

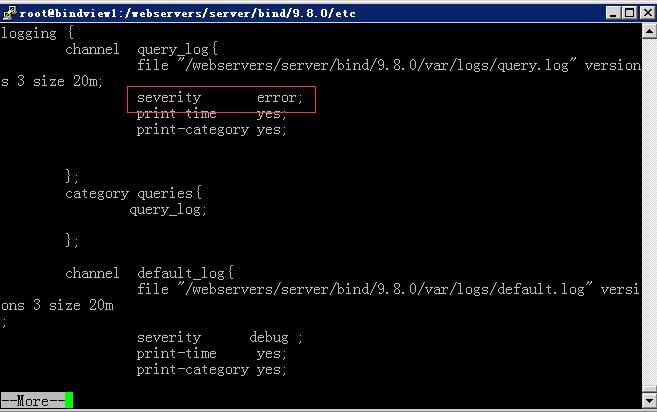
DNS分析过程参考：

1. 开启DNS解析日志；
2. 在日志中查询解析指定域名的终端IP；
3. 定位终端。

其他说明：

部分DNS服务器由于日志配置不当，导致无法查看具体请求域名解析的客户端IP地址，通过修改DNS配置，调整DNS请求日志级别，记录客户端IP地址。

具体配置参考如下：

修改bind日志配置文件，修改query\_log分类severity属性的error为info，修改保存后重启bind服务。

通过查看域名解析日志文件(query.log)筛选出访问恶意域名的客户端IP，命令如下：

Cat query.log |grep

执行完毕后，可查看所有该DNS解析该域名的终端IP。