专注APT攻击与防御
https://micropoor.blogspot.com/

这次继续围绕第一篇，第一季关于后门：https://micropoor.blogspot.hk/2017/12/php.html 做整理与补充。在深入一步细化demo notepad++。

后门是渗透测试的分水岭，它分别体现了攻击者对目标机器的熟知程度，环境，编程语言，了解对方客户，以及安全公司的本质概念。这样的后门才能更隐蔽，更长久。

而对于防御者需要掌握后门的基本查杀，与高难度查杀，了解被入侵环境，目标机器。以及后门或者病毒可隐藏角落，或样本取证，内存取证。.

所以说后门的安装与反安装是一场考试，一场实战考试。

这里要引用几个概念，只有概念清晰，才能把后门加入概念化，使其更隐蔽。

1：攻击方与防御方的本质是什么？

增加对方的时间成本，人力成本，资源成本（不限制于服务器资源），金钱成本。

2：安全公司的本质是什么？

盈利，最小投入，最大产出。

3：安全公司产品的本质是什么？

能适应大部分客户，适应市场化，并且适应大部分机器。（包括不限制于资源紧张，宽带不足等问题的客户）

4：安全人员的本质是什么？

赚钱，养家。买房，还房贷。导致，快速解决客户问题（无论暂时还是永久性解决），以免投诉。

5：对接客户的本质是什么？

对接客户也是某公司内安全工作的一员，与概念4相同。

清晰了以上5个概念，作为攻击者，要首先考虑到对抗成本，什么样的对抗成本，能满足概念1-5。影响或阻碍对手方的核心利益。把概念加入到后门，更隐蔽，更长久。

文章的标题既然为php安全新闻早八点，那么文章的本质只做技术研究，Demo本身不具备攻击或者持续控制权限功能。

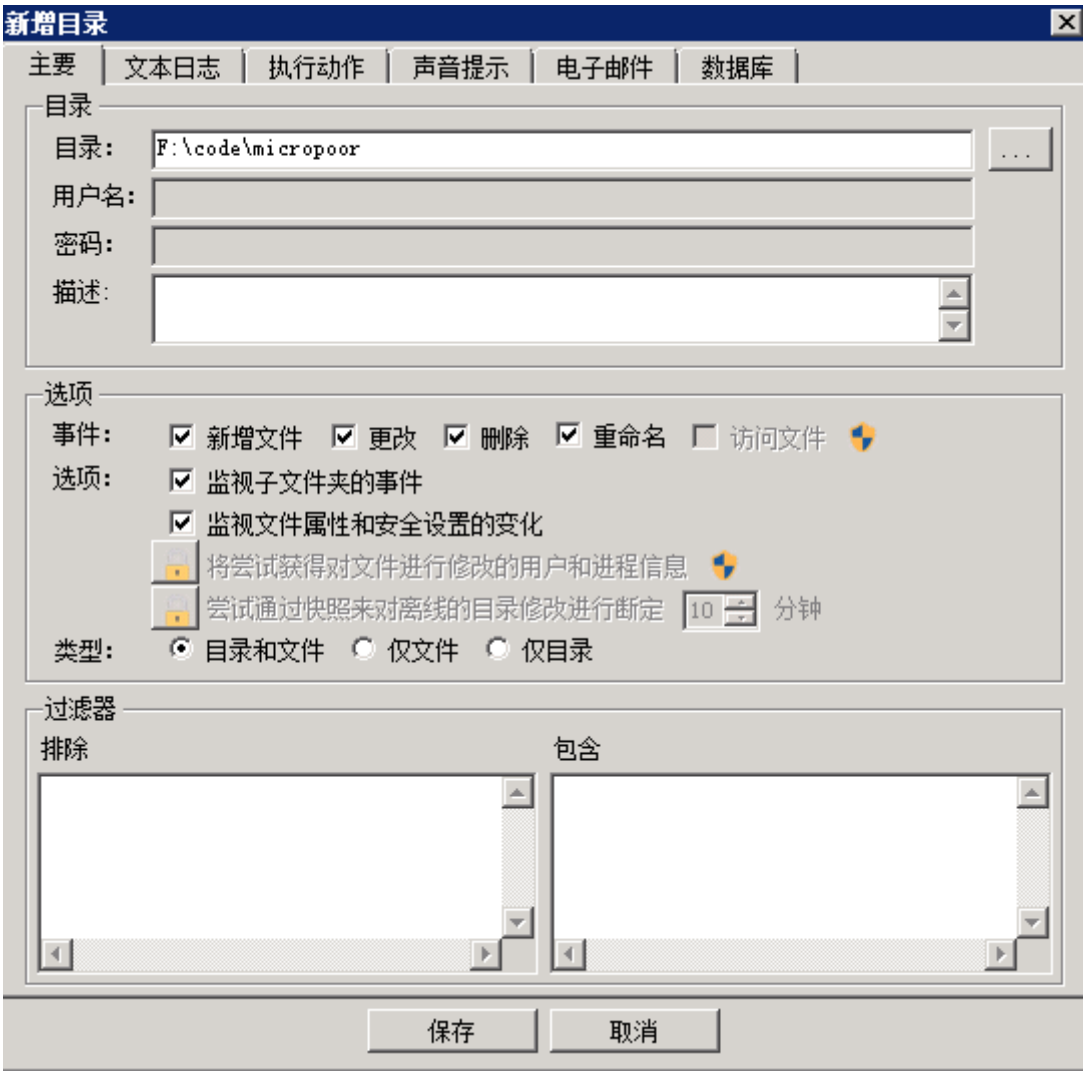
Demo连载第二季：

Demo 环境：windows 7 x64，notepad++(x64)

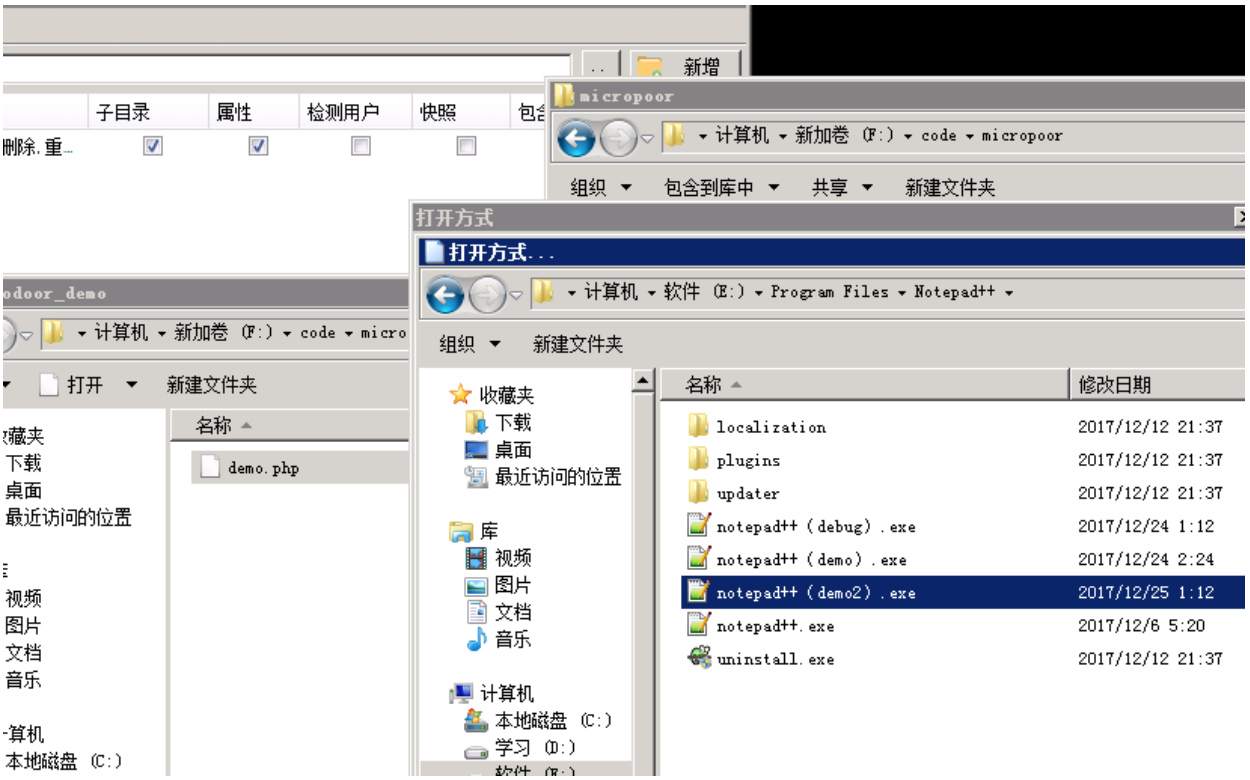
Demo IDE：vs2017

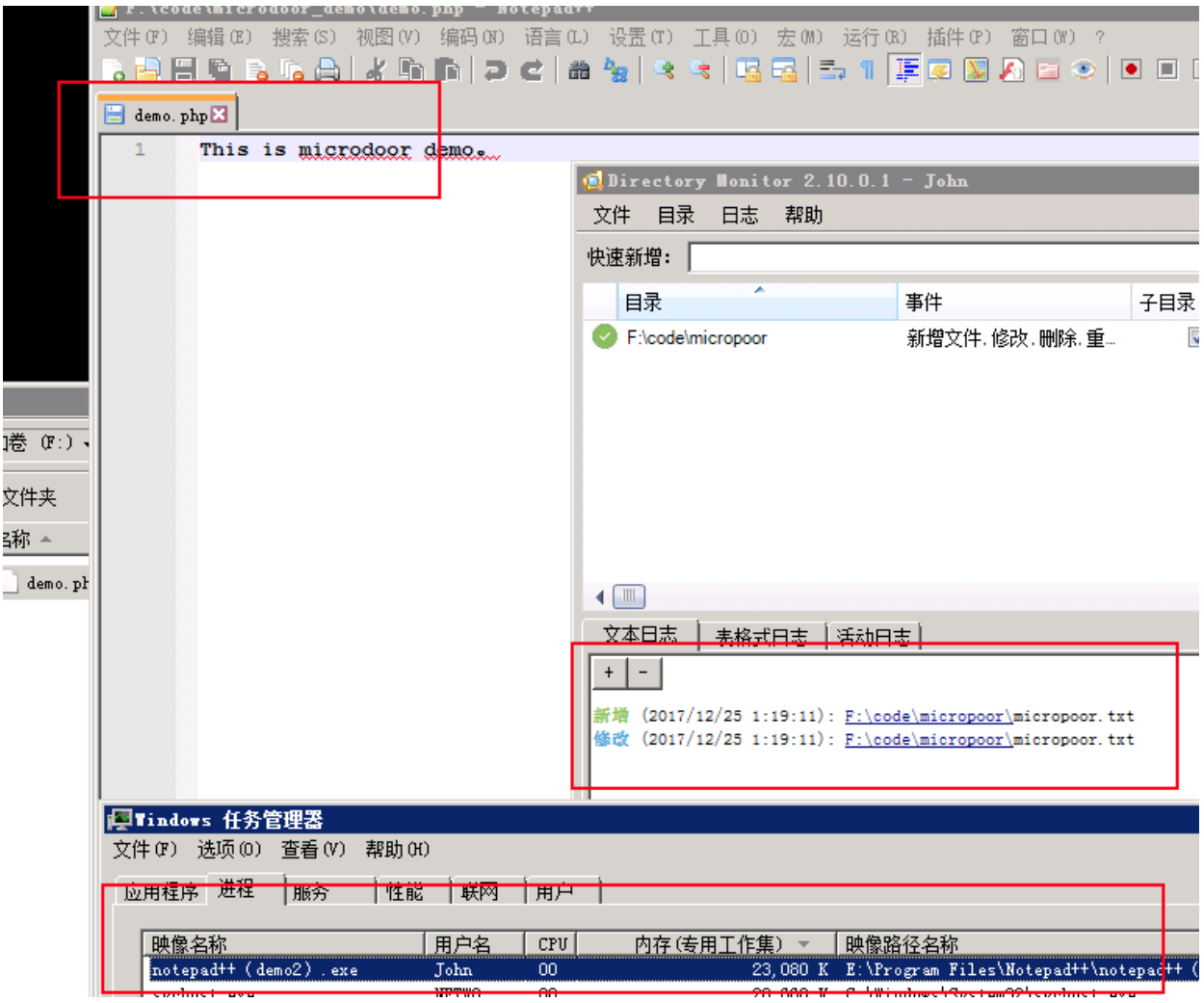
在源码中，我们依然修改每次打开以php结尾的文件，先触发后门，在打开文件。其他文件跳过触发后门。但是这次代码中加入了生成**micropoor.txt**功能。并且使用php来加载运行它，是的，生成一个txt。demo中，为了更好的演示，取消自动php加载运行该txt。

而txt的内容如图所示，并且为了更好的了解，开启文件监控。

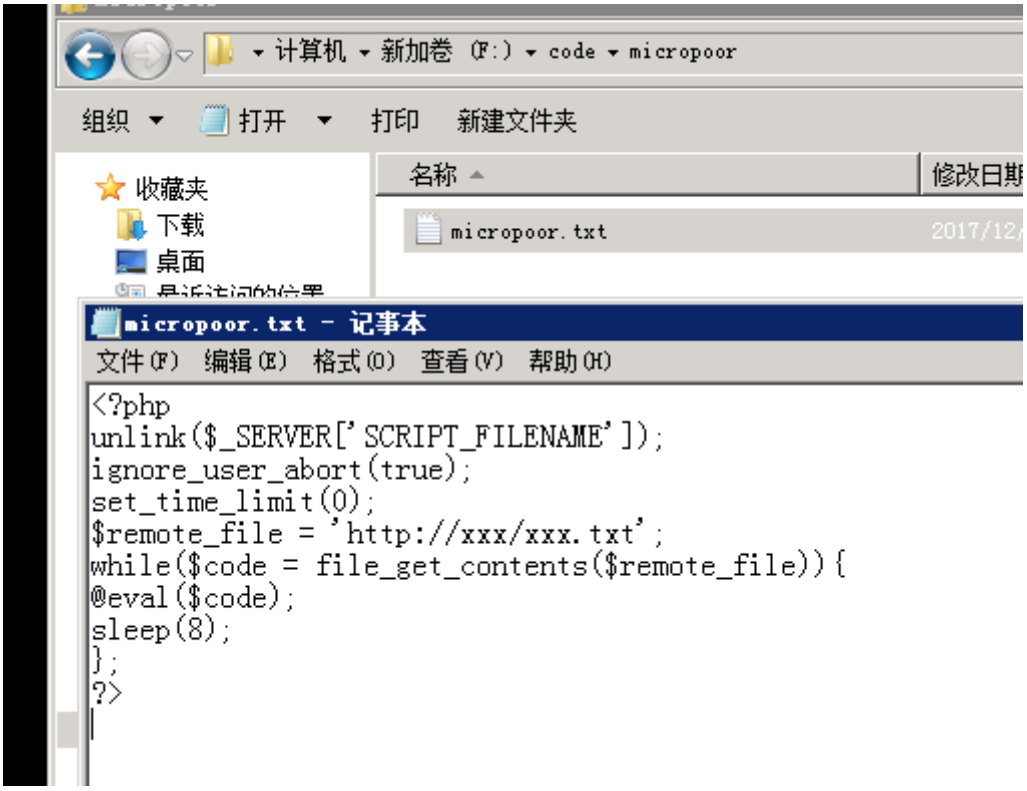


使用notepad++(demo2).exe 打开以php结尾的demo.php，来触发microdoor。并且生成了micropoor.txt


新增
子目录
属性
检测用户
快照
micropoor
计算机 ▸ 新加卷 (F:) ▸ code ▸ micropoor
组织
包含到库中
共享
新建文件夹
打开方式
打开方式...
计算机 ▸ 软件 (E:) ▸ Program Files ▸ Notepad++
组织
新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
本地磁盘 (C:)
学习 (D:)
名称
修改日期
localization 2017/12/12 21:37
plugins 2017/12/12 21:37
updater 2017/12/12 21:37
notepad++ (debug).exe 2017/12/24 1:12
notepad++ (demo).exe 2017/12/24 2:24
notepad++ (demo2).exe 2017/12/25 1:12
notepad++.exe 2017/12/6 5:20
uninstall.exe 2017/12/12 21:37
demo.php


文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
demo.php
1 This is microdoor demo.
Directory Monitor 2.10.0.1 - John
文件 目录 日志 帮助
快速新增:
目录 事件 子目录
F:\code\micropoor 新增文件,修改,删除,重...
文本日志 表格式日志 活动日志
新增 (2017/12/25 1:19:11): F:\code\micropoor\micropoor.txt
修改 (2017/12/25 1:19:11): F:\code\micropoor\micropoor.txt
Windows 任务管理器
文件(F) 选项(O) 查看(V) 帮助(H)
应用程序 进程 服务 性能 联网 用户
映像名称 用户名 CPU 内存(专用工作集) 映像路径名称
notepad++ (demo2).exe John 00 23,080 K E:\Program Files\Notepad++\notepad++

而micropoor.txt内容：



配合micropoor.txt的内容，这次的Demo将会变得更有趣。

那么这次demo 做到了，无服务，无进程，无端口，无自启。

根据上面的5条概念，加入到了demo中，增加对手成本。使其更隐蔽。

如果demo不是notepad++，而是mysql呢?用它的端口，它的进程，它的服务，它的一切，来重新编译microdoor。

例如：重新编译mysql.so,mysql.dll，替换目标主机。

无文件，无进程，无端口，无服务，无语言码。因为一切附属于它。

这应该是一个攻击者值得思考的问题。

正如第一季所说：在后门的进化中，rootkit也发生了变化，最大的改变是它的系统层次结构发生了变化。

- Micropoor