专注APT攻击与防御

https://micropoor.blogspot.com/

本季是作《PHP安全新闻早八点-高级持续渗透-第六季关于后门》的补充。

https://micropoor.blogspot.com/2018/12/php.html

原本以为第六季的demo便结束了notepad++

但是demo系列的懿旨并没有按照作者的想法来表述。顾引入第七季。

在第一季关于后门中，文章提到重新编译notepad++，来引入有目标源码后门构造。

在第六季关于后门中，文章假设在不得知notepad++的源码，来引入无目标源码沟门构造。

而第七季关于后门中，让这个demo更贴合于实战。此季让这个demo成长起来。它的

成长痕迹分别为第一季，第六季，第七季。

该系列仅做后门思路。

懿旨：安全是一个链安全，攻击引入链攻击，后门引入链后门。让渗透变得更加有趣。

Demo 环境：

Windows 2003 x64 Windows 7 x64

notepad++ 7.6.1，notepad++7.5.9 vs 2017

靶机以notepad++ 7.5.9为例：

默认安装notepad++流程图，如下：一路下一步。

目标机背景：windows 2003，x64，notepad++ 7.6.1，notepad++7.5.9，iis，aspx

shell权限如下：

notepad++7.5.9

安装路径：E:\Notepad++\

插件路径：E:\Notepad++\plugins\

检查默认安装情况如下：

注：为了让本季的demo可观性，顾不打算隐藏自身。

端口如下：

shell下写入：

注：

notepad++ v7.6以下版本插件路径为：X:\Notepad++\plugins\

notepad++ v7.6以上版本插件路径为：

X:\Documents and Settings\All Users\Application Data\Notepad++\plugins

目标机管理员再次打开notepad++：

注：demo中不隐藏自身

端口变化如下：

msf 连接目标机：

后者的话：

如果此demo，增加隐身自身，并demo功能为：增加隐藏帐号呢？或者往指定邮箱发目标机帐号密码明文呢？如果当第六季依然无法把该demo加入到实战中，那么请回顾。这样实战变得更为有趣。安全是一个链安全，攻击引入链攻击，后门引入链后门。让渗透变得更加有趣。

Micropoor