南京邮电大学网络攻防平台逆向writeup之[WxyVM2]

原创

巫师54 于 2017-08-02 01:23:09 发布

1#

先找到最后判断的地方，2.5万行啊，2.4万行无效运算，2400多有效运算，坑死人不偿命。

```
25008  dword_6941A0 ^= dword_69419C;
25009  dword_6941A4 ^= dword_6941A0;
25010  dword_6941A8 ^= dword_6941A4;
25011  dword_6941AC ^= dword_6941A8;
25012  dword_6941B0 ^= dword_6941AC;
25013  dword_694150 = -1304438312;
25014  dword_694154 = -1859898891;
25015  dword_694158 = 871339566;
25016  dword_6941CC ^= dword_6941C8;
25017  dword_6941D0 ^= dword_6941CC;
25018  dword_6941D4 ^= dword_6941D0;
25019  dword_6941D8 ^= dword_6941D4;
25020  dword_6941DC ^= dword_6941D8;
25021  dword_6941E0 ^= dword_6941DC;
25022  byte_694102 ^= 0xBu;
25023  byte_694100 ^= 0x5Eu;
25024  byte_694111 += 69;
25025  byte_694109 += 7;
25026  for ( i = 0; i <= 24; ++i )
25027  {
25028    if ( *(&byte_694100 + i) != dword_694060[i] )
25029      v4 = 0;
25030  }
25031  if ( v4 )
25032    puts("correct");
25033  else
25034    puts("wrong");
25035  return 0LL;
25036}
```

2#

复制出来吧，还好，变量名称里面带得有地址，input的字符串只有25个字节，也就694100－694117吧，大神最善良的地方就是，把所有无效计算的过程都是dword变量，有效计算的部分变量全是byte。用python截出来，再反序，保存为一个文件再利用，code3.txt 。

3#

逆运算的原理，就是把 + - 互换，如果用C语言来编写应该很简单吧，苦B的我没环境，我是用php来运算的，还要注意运算后的溢出，比如小于0，或者大于255.总之，身心疲惫。

给出逆运算的php源码。调试过程没删干净，比较乱，大家忍耐一下。代码中 code3.txt 就是上面得出来的。

```
<?php
$a=array(0xC0 ,0x85 ,0xF9 ,0x6C ,0xE2 ,0x14 ,0xBB ,0xE4  ,0x0D ,0x59 ,0x1C ,0x23 ,0x88 ,0x6E ,0x9B ,0xCA ,0
$b="abcdefghijklmn";

#echo $b[ss];
#die;
#echo "aaa\n";
```

```
$f=file_get_contents('code3.txt');

#echo count($f);

#var_dump($f);

$line=split("\n",$f);

#echo count($line)."\n";
#echo $line[1]."\n";

#echo count($a);

for($i=6897920;$i<6897920+24;$i++)
{
 eval('$byte_'.strtoupper(dechex($i))."=".$a[$i-6897920].";");
 echo '$byte_'.strtoupper(dechex($i)).'=';
 eval('echo dechex($byte_'.strtoupper(dechex($i)).');');
 echo "\n";
}
#echo('test $byte_694112 = '.$byte_694112."\n");
#die;
#eval('$byte_694111 ^= 0x30;');
#echo('test $byte_694111 = '.$byte_694111."\n");
#$tmp='++byte_694114;';
#echo substr($tmp,2);
#die;
#$byte_694109+=7;byte_694111 ^= 0x30u;
#echo('test $byte_694109 + 7 = '.$byte_694109."\n");

#$tmp='byte_694106 ^= 0x70;';


#$num=substr($tmp,strpos($tmp,"^=")+2);
#echo $num;
#die;

echo "\n初始化好了\n";
$i=0;
$j=0;
foreach($line as $value)
{
 #echo '$'.$value."\n";
 #echo 'counting : '.$i.' ';
 $i++;
 #echo substr($value,0,strpos($value,"+="))."\n";
 #echo strstr($value,"+=")."\n";
 /*
 if (strstr($value,'byte_694111'))
 {
  $j++;
  echo '*****$byte_694111 = '.$byte_694111;
  #if($byte_69410F<244)die;
  echo " source :";
  echo $value."\n";
 }
 */

 if(strstr($value,"+="))
```

```
{
 $tmpstr='$'.substr($value,0,strpos($value,"+="));
 $act="+=";
 $act2="-=";
 $num=substr($value,strpos($value,"+=")+2);
 #echo "doing ".$tmpstr.$act2.$num."\n";
 eval($tmpstr.$act2.$num);

 eval('if('.$tmpstr.'<0)'.$tmpstr.'+=256;');
 eval('if('.$tmpstr.'>255)'.$tmpstr.'-=256;');

}
elseif(strstr($value,'-='))
{
 $tmpstr='$'.substr($value,0,strpos($value,'-='));
 $act="-=";
 $act2="+=";
 $num=substr($value,strpos($value,"-=")+2);
 #echo "doing ".$tmpstr.$act2.$num."\n";
 eval($tmpstr.$act2.$num);
 eval('if('.$tmpstr.'>255)'.$tmpstr.'-=256;');
 eval('if('.$tmpstr.'<0)'.$tmpstr.'+=256;');
}
elseif(strstr($value,"--"))
{
 $tmpstr='$'.substr($value,2); #++byte_694114;
 $act="--";
 $act2="++";
 #$num=substr($value,strpos($value,"-=")+2);
 #echo "doing ".$act2.$tmpstr."\n";
 eval($act2.$tmpstr);


 $tmpstr = substr($tmpstr,0,strlen($tmpstr)-2);
 #echo 'if('.$tmpstr.'>255)'.$tmpstr.'-=256;';die;

 eval('if('.$tmpstr.'>255)'.$tmpstr.'-=256;');
}
elseif(strstr($value,"++"))
{
 $tmpstr='$'.substr($value,2); #++byte_694114;
 $act="++";
 $act2="--";
 #$num=substr($value,strpos($value,"-=")+2);
 #echo "doing ".$act2.$tmpstr."\n";
 eval($act2.$tmpstr);
 $tmpstr = substr($tmpstr,0,strlen($tmpstr)-2);
 eval('if('.$tmpstr.'<0)'.$tmpstr.'+=256;');
}
elseif(strstr($value,'^='))
{
 $tmpstr='$'.substr($value,0,strpos($value,"^="));
 $act="^=";
 $act2="^=";
 $num=substr($value,strpos($value,"^=")+2);
 #echo "doing ".$tmpstr.$act2.$num."\n";
 eval($tmpstr.$act2.$num);
 #eval('if('.$tmpstr.'>255)'.$tmpstr.'-=256;');
}
else
```

```
 else

 die('something wrong! '.$value);
 /*
 if (strstr($value,'byte_694111'))
 {
  echo '---$byte_694111 = '.$byte_694111."\n";
  #die;
 }
 */
}

for($i=6897920;$i<6897920+24;$i++)
{
 #echo '$byte_'.strtoupper(dechex($i)).'=';
 eval('echo chr($byte_'.strtoupper(dechex($i)).');');
 #echo ' | ';
 #eval('echo $byte_'.strtoupper(dechex($i)).';');
 #echo "\n";
}
echo "\n===============\n";echo 'j is '.$j."\n";
$a=10;
echo $a^10;
echo "\n";
echo $a^0xa;
```

逆向

Hello,RE!	ReadAsm2	Py交易	WxyVM	maze	WxyVM 2
80	150	150	300	300	500