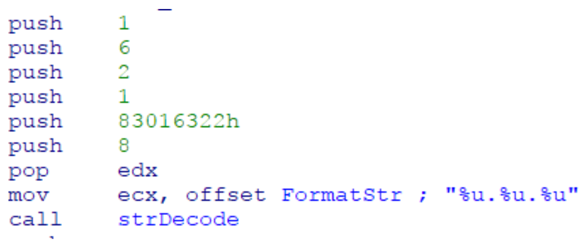
Change in the Encryption scheme

spamhaus.org/news/article/771/

Spamhaus Malware Labs - Spamhaus's malware research unit - recently observed a wave of new PandaZeuS malware samples being distributed during the Christmas season. PandaZeuS, also known as Panda Banker, is an ebanking Trojan that evolved from the notorious ZeuS trojan and is being used by different threat actors to compromise ebanking credentials, used by cybercriminals to commit ebanking fraud.

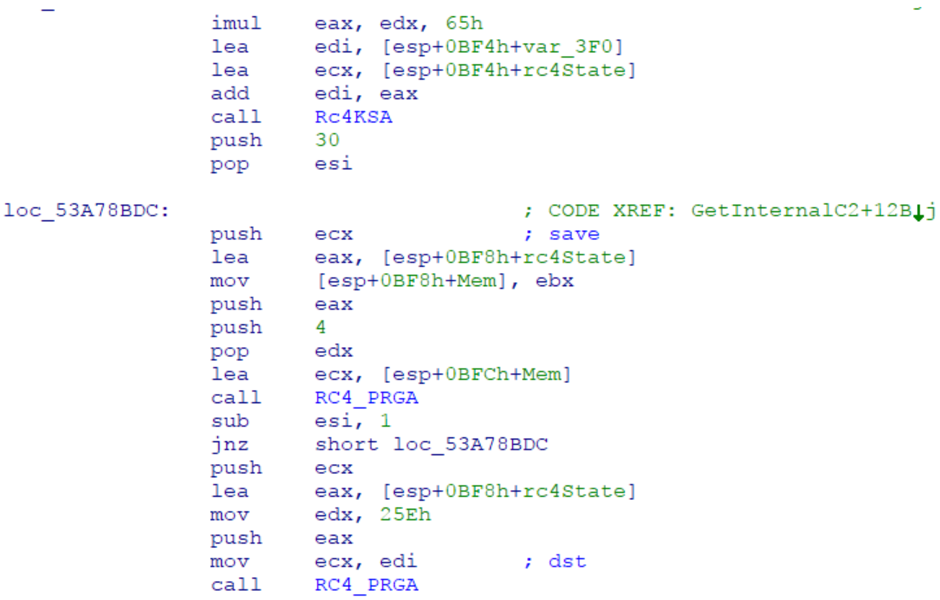
Looking into two recent PandaZeuS campaigns that have just been spread before Christmas revealed that the most recent version of PandaZeuS comes with a few minor changes. An important one is the change in the encryption scheme of PandaZeuS's Base Config. While PandaZeuS is still using the RC4 binary encryption scheme, it comes with some tiny modifications. First of all, the versioning of PandaZeuS got updated to 2.6.1:



```
push    1
push    6
push    2
push    1
push    83016322h
push    8
pop     edx
mov     ecx, offset FormatStr ; "%u.%u.%u"
call    strDecode
```

New version 2.6.1

In the previous version, the base config was AES-265-CBC and RC4 encrypted . While this is still the case of the most recent version of PandaZeuS too, a slight modification in RC4 has been done:



```
                imul    eax, edx, 65h
                lea     edi, [esp+0BF4h+var_3F0]
                lea     ecx, [esp+0BF4h+rc4State]
                add     edi, eax
                call    Rc4KSA
                push    30
                pop     esi

loc_53A78BDC:                           ; CODE XREF: GetInternalC2+12B↓j
                push    ecx             ; save
                lea     eax, [esp+0BF8h+rc4State]
                mov     [esp+0BF8h+Mem], ebx
                push    eax
                push    4
                pop     edx
                lea     ecx, [esp+0BFCh+Mem]
                call    RC4_PRGA
                sub     esi, 1
                jnz     short loc_53A78BDC
                push    ecx
                lea     eax, [esp+0BF8h+rc4State]
                mov     edx, 25Eh
                push    eax
                mov     ecx, edi        ; dst
                call    RC4_PRGA
```

PandaZeuS code snipped

The screenshot above documented the changes made to by the developers of PandaZeuS to the code:

1. Initial Key Stream Array is initialized
2. The State Array is modified 4 * 30 times and the keystream value is omitted
3. Reusing the previous indexes, State Array is modified and keystream values obtained is XORed with encrypted byte.

This can be represented in Python code as:

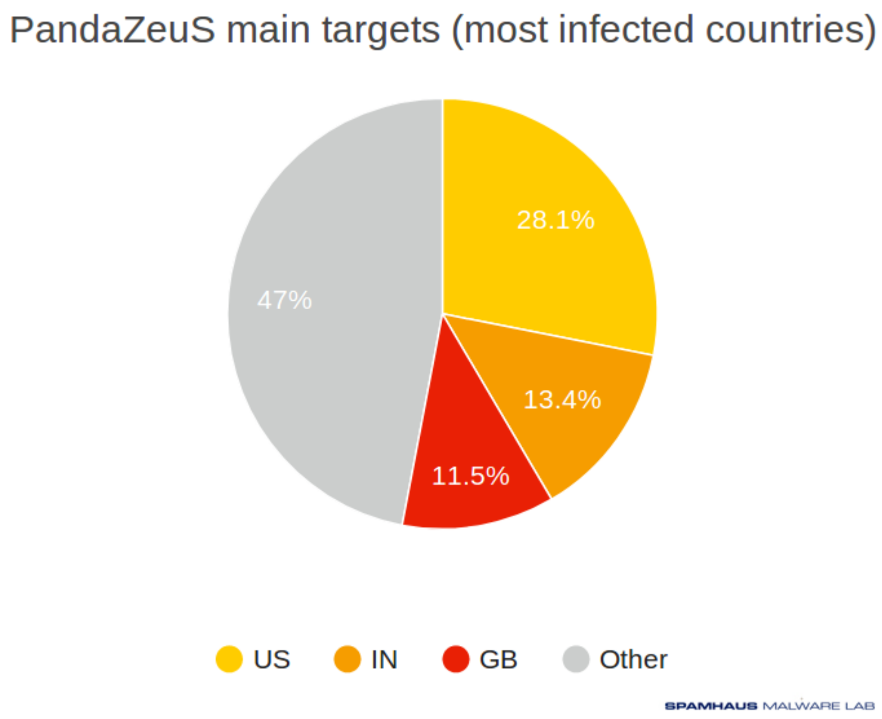
```
for i in range(256):
       j = (j + S[i] + ord(key[i % len(key)])) % 256
       S[i], S[j] = S[j], S[i]

   i = j = 0
   for x in range(0, 30 * 4):
        i = (i + 1) % 256
        j = (j + S[i]) % 256
        S[i], S[j] = S[j], S[i]

   for p in data:
       i = (i + 1) % 256
       j = (j + S[i]) % 256
       S[i], S[j] = S[j], S[i]
```

While we can only speculate about the reason of this minor change in the encryption scheme of PandaZeuS, we suspect the intent behind this code change is to break malware extractors used by malware researchers to extract botnet controllers from PandaZeuS malware samples.

Looking into sinkhole data of one of these PandaZeuS campaigns shows that the botnet is mainly targeting English-speaking internet users:



In addition, the associated botnet domain names are poorly detected:

- 262d65fc7f47.tk VT detection rate: 2/66
- 922b031aac47.tk VT detection rate: 3/66

Indicators of Compromise (IOC)

Campaign #1

PandaZeuS botnet controller URLs:

```
hxxps://922B031AAC47.tk/2egublocatolaubhaqiec.dat
hxxps://262D65FC7F47.tk/3fefavyamzaosanocheyt.dat
hxxps://262D65FC7F98.ml/4uryctexaesleikbosoil.dat
hxxps://262D65FC7F10.ga/5texyiwkuoffokirefeub.dat
hxxps://262D65FC7F98.cf/6huqefeaplefoucvyudow.dat
```

PandaZeuS botnet controller domain names (blocked by Spamhaus RPZ):

```
262D65FC7F10.ga
262D65FC7F47.tk
262D65FC7F98.cf
262D65FC7F98.ml
922B031AAC47.tk
```

PandaZeuS botnet controllers (blocked by Spamhaus BCL):

```
89.18.27.155
94.156.128.207
155.94.67.27
```

Related malware samples (MD5):

```
0d1150d89f94701b54c7feb81d83a8fd
3e7632e36c96a5be6721f57828dbc7f5
```

Campaign #2

PandaZeuS botnet controller URLs:

```
hxxps://gromnes.top/1iqrozoymydfykiabloyx.dat
hxxps://aklexim.top/2pugyomxixiusqoxuvein.dat
hxxps://kichamyn.top/3efqykyfeetraygyhytuz.dat
hxxps://myrasno.top/4tieseqpaowosputoezyl.dat
hxxps://brumnoka.top/5ybveogaqydriumytzaun.dat
hxxps://bqwernod.top/6efudpigoreudtygoedco.dat
```

PandaZeuS botnet controller domain names (blocked by Spamhaus RPZ):

```
aklexim.top
bqwernod.top
brumnoka.top
gromnes.top
kichamyn.top
myrasno.top
```

PandaZeuS botnet controllers (blocked by Spamhaus BCL):

```
27.102.67.144
5.8.88.133
```

Related malware samples (MD5):

```
02ac00fe985091b78eaeb64ee697d57f
9be7c5e014c560db231518a13b18dfea
a3a4ef76764c9e3e9c91698b7adbd795
b42d194091de01d9645b323cd8ac425f
48e4f66aeb6dcb991ae57ac8294d2911
9ff828a80d8408a1e5533ecc304c7e9e
```

Related Spamhaus Products

- Spamhaus Response Policy Zone (RPZ)
- Spamhaus Botnet + Malware Domain List (BDL)
- Spamhaus Botnet Controller List (BCL)

Spamhaus Malware Labs is Spamhaus's malware research unit run in conjunction with Deteque, a subsidiary of Spamhaus Technology Ltd.