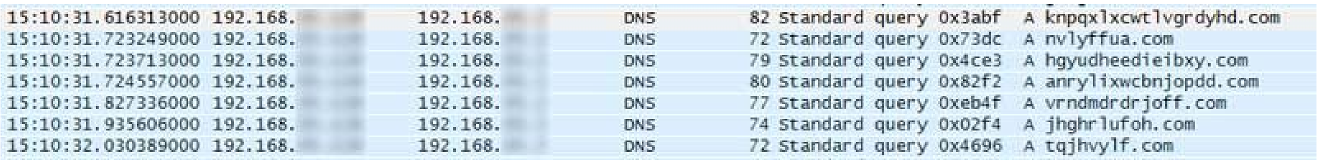
The DGA of Ramnit

bin.re/blog/the-dga-of-ramnit/

Ramnit is a Zeus-like malware from 2010 used to spy on infected users. Although the malware isn't as prevalent as it used to be, there are many recent submissions still. Ramnit uses a Domain Generation Algorithm (DGA) to contact its C2-server. Upon infection, the sample starts to make DNS queries for many different domains in rapid succession:



```
15:10:31.616313000 192.168.[redacted]   192.168.[redacted]   DNS   82 Standard query 0x3abf  A knpqxlxcwtlvgrdyhd.com
15:10:31.723249000 192.168.[redacted]   192.168.[redacted]   DNS   72 Standard query 0x73dc  A nvlyffua.com
15:10:31.723713000 192.168.[redacted]   192.168.[redacted]   DNS   79 Standard query 0x4ce3  A hgyudheedieibxy.com
15:10:31.724557000 192.168.[redacted]   192.168.[redacted]   DNS   80 Standard query 0x82f2  A anrylixwcbnjopdd.com
15:10:31.827336000 192.168.[redacted]   192.168.[redacted]   DNS   77 Standard query 0xeb4f  A vrndmdrdrjoff.com
15:10:31.935606000 192.168.[redacted]   192.168.[redacted]   DNS   74 Standard query 0x02f4  A jhghrlufoh.com
15:10:32.030389000 192.168.[redacted]   192.168.[redacted]   DNS   72 Standard query 0x4696  A tqjhvylf.com
```

I reverse engineered the underlying DGA as a sunday afternoon RCE exercise. I used a fairly recent Ramnit sample from Malware-Traffic-Analysis.

DGA Disassembly

The DGA is very simple. Here is the disassembly of the routine that generates the domains:

```
seg074:2001A91C create_next_domain proc near            ; CODE XREF: thread_start+36p
seg074:2001A91C
seg074:2001A91C seed            = dword ptr -4
seg074:2001A91C initial_seed    = dword ptr  8
seg074:2001A91C hostname        = dword ptr  0Ch
seg074:2001A91C
seg074:2001A91C                 push    ebp
seg074:2001A91D                 mov     ebp, esp
seg074:2001A91F                 add     esp, 0FFFFFFFCh
seg074:2001A922                 push    ebx
seg074:2001A923                 push    ecx
seg074:2001A924                 push    edx
seg074:2001A925                 push    esi
seg074:2001A926                 push    edi
seg074:2001A927                 push    12              ; modulus
seg074:2001A929                 push    [ebp+initial_seed] ; seed
seg074:2001A92C                 call    rand_int_modulus
seg074:2001A931                 mov     [ebp+seed], edx
seg074:2001A934                 add     eax, 8
seg074:2001A937                 mov     ecx, eax        ; ecx = = length of 2nd level
domain
seg074:2001A939                 mov     esi, [ebp+hostname]
seg074:2001A93C
seg074:2001A93C loc_2001A93C:                           ; CODE XREF:
create_next_domain+2Dj
seg074:2001A93C                 push    25              ; modulus
seg074:2001A93E                 push    edx             ; seed
seg074:2001A93F                 call    rand_int_modulus
seg074:2001A944                 add     al, 'a'         ; -> random letter (one of
25)
seg074:2001A946                 mov     [esi], al
seg074:2001A948                 inc     esi
seg074:2001A949                 loop    loc_2001A93C    ; modulus
seg074:2001A94B                 mov     byte ptr [esi], 0 ; null terminate
seg074:2001A94E                 push    offset tld_com  ; ".com"
seg074:2001A953                 push    [ebp+hostname]  ; lpString1
seg074:2001A956                 call    j_lstrcatA
seg074:2001A95B                 xor     edx, edx
seg074:2001A95D                 mov     eax, [ebp+initial_seed]
seg074:2001A960                 mov     ebx, [ebp+seed]
seg074:2001A963                 mul     ebx             ; multiply seeds
seg074:2001A965                 add     eax, edx        ; add higher dword
seg074:2001A967                 pop     edi
seg074:2001A968                 pop     esi
seg074:2001A969                 pop     edx
seg074:2001A96A                 pop     ecx
seg074:2001A96B                 pop     ebx
seg074:2001A96C                 leave
seg074:2001A96D                 retn    8
seg074:2001A96D create_next_domain end
```

The subroutine `rand_int_modulus` is:

```
seg074:2001331C ; =============== S U B R O U T I N E
=======================================
seg074:2001331C
seg074:2001331C ; Attributes: bp-based frame
seg074:2001331C
seg074:2001331C rand_int_modulus proc near              ; CODE XREF: seg074:2001303Fp
seg074:2001331C                                         ; seg074:20013089p ...
seg074:2001331C
seg074:2001331C rnd_seed        = dword ptr  8
seg074:2001331C modulus         = dword ptr  0Ch
seg074:2001331C
seg074:2001331C                 push    ebp
seg074:2001331D                 mov     ebp, esp
seg074:2001331F                 push    ebx
seg074:20013320                 push    ecx
seg074:20013321                 mov     eax, [ebp+rnd_seed]
seg074:20013324                 xor     edx, edx
seg074:20013326                 mov     ecx, 127773
seg074:2001332B                 div     ecx             ; eax = k1
seg074:2001332D                 mov     ecx, eax        ; ecx = k1
seg074:2001332F                 mov     eax, 16807
seg074:20013334                 mul     edx
seg074:20013336                 mov     edx, ecx
seg074:20013338                 mov     ecx, eax
seg074:2001333A                 mov     eax, 2836
seg074:2001333F                 mul     edx
seg074:20013341                 sub     ecx, eax        ; ix
seg074:20013343                 xor     edx, edx
seg074:20013345                 mov     eax, ecx        ; eax =ebx = ix
seg074:20013347                 mov     ebx, ecx
seg074:20013349                 div     [ebp+modulus]
seg074:2001334C                 mov     eax, edx        ; eax = rand_int(seed) %
modulus
seg074:2001334E                 mov     edx, ebx        ; edx = seed
seg074:20013350                 pop     ecx
seg074:20013351                 pop     ebx
seg074:20013352                 leave
seg074:20013353                 retn    8
seg074:20013353 rand_int_modulus endp
```

This is a Linear Congurential Generator (LCG) that produces random numbers. The parameters and implementation match this article. The subroutine gets the seed as the first argument, and the modulus as the second parameter.

The DGA uses this random number generator to first determine the length of the second level domain by uniformly picking a length between 8 and 19 characters. Next, the DGA determine the second level domain by uniformly picking letters from “a” to “x” (note: letter “z” can’t be picked, this also helps to spot Ramnit domains).

The DGA then appends the static top level domain “.com”. Finally, the seed for the next domain is determined. The first seed is hardcoded:

```
seg076:20029004 initial_seed    dd 79159C10h
```

DGA in Python

The following Python script generates Ramnit domains for a provided seed (**Edit January 18, 2015**: fixed a bug in `rand_int_modulus`, some of the generated domains were wrong before).:

```
import argparse

class RandInt:

    def __init__(self, seed):
        self.seed = seed

    def rand_int_modulus(self, modulus):
        ix = self.seed
        ix = 16807*(ix % 127773) - 2836*(ix / 127773) & 0xFFFFFFFF
        self.seed = ix
        return ix % modulus

def get_domains(seed, nr):
    r = RandInt(seed)

    for i in range(nr):
        seed_a = r.seed
        domain_len = r.rand_int_modulus(12) + 8
        seed_b = r.seed
        domain = ""
        for i in range(domain_len):
            char = chr(ord('a') + r.rand_int_modulus(25))
            domain += char
        domain += ".com"
        m = seed_a*seed_b
        r.seed = (m + m//(2**32)) % 2**32
        yield domain

if __name__=="__main__":
    parser = argparse.ArgumentParser(description="generate Ramnit domains")
    parser.add_argument("seed", help="seed as hex")
    parser.add_argument("nr", help="nr of domains", type=int)
    args = parser.parse_args()
    for domain in get_domains(int(args.seed, 16), args.nr):
        print(domain)
```

For example

```
$ python dga.py 79159C10 10
knpqxlxcwtlvgrdyhd.com
nvlyffua.com
hgyudheedieibxy.com
anrylixwcbnjopdd.com
vrndmdrdrjoff.com
jhghrlufoh.com
tqjhvylf.com
hufqifjq.com
itktxexjghvvxa.com
ppyblaohb.com
```

DGA Characteristics

```
<td>
  static
</td>

<td>
  unlimited
</td>

<td>
  unlimited
</td>

<td>
  none
</td>

<td>
  .com
</td>

<td>
  all letters except &#8220;z&#8221;</br>(picked uniformly at random)
</td>

<td>
  between 8 and 19 characters</br>(picked uniformly at random)
</td>
```

seed
domains per seed
tested domains
wait time between domains
top level domain

second level characters
second level domain length

Observed Seeds in the Wild

Even without access to the binary one can determine the seed that lead to a given domain: The seed is only 32 bit which makes it possible to enumerate all possible domains and match them with known network traffic. Using this script I analysed three different sets of DGA domains to find the underlying seeds. (**Edit January 18, 2015**: some domains were wrong before). (**Edit September 14, 2015**: found a fourth seed).

Seed: 0xEF214BBF

I found this seed by analysing a malware from malware-traffic-analysis.net. The sample can be downloaded from malwr.com. The first 30 domains for this seed are:

1. mtsoexdphaqliva.com
2. uulwwmawqjujuuprpp.com
3. twuybywnrlqcf.com
4. wcqqjiixqutt.com
5. ubgjsqkad.com
6. iihsmkek.com
7. tlmmcvqvearpxq.com
8. flkheyxtcedehipox.com
9. edirhtuawurxlobk.com
10. tfjcwlxcjoviuvtr.com
11. bfmbrrihwsfkqy.com
12. fyodimwialsoobu.com
13. crudcqgf.com
14. toixqdmkicnrdhseduj.com
15. ssofasuafn.com
16. edaqpyrppopwldv.com
17. qbuyqrogyglljk.com
18. hpmnvvbhnoomnkj.com
19. rgggwpfcwueytjoxfb.com
20. cslbnrypemnx.com
21. hycrotqqubvplffbk.com
22. ytxtdhjlme.com
23. pxgmtqfoluw.com
24. lqenouffubcjpvtmf.com
25. eqhpcqjxpeqhjravy.com
26. iqlibdbawapeb.com

27. opfgjnhe.com
28. xlrcqwuyehrsqu.com
29. arnsjlbjaqsswum.com
30. neqkjkopo.com

Seed: 0x28488EEA

This seed was used first in March 2012. Some of the samples are Malwr, Sonicwall, Sophos, another Sophos, Lavasoft. The first 30 domains for this seed are:

1. htmthgurhtchwlhwklf.com
2. jiwucjyxjibyd.com
3. khddwukkbwhfdiufhaj.com
4. snoknwlgcwgaafbtqkt.com
5. tfgyaoingy.com
6. ukiixagdbdkd.com
7. swbadolov.com
8. ouljuvkvn.com
9. tiqfgpaxvmhsxtk.com
10. cxatodxefolgkokdqy.com
11. ubkfgwqslhqyy.com
12. caytmlnlrou.com
13. qbsqnpyyooh.com
14. vrguyjjxorlyen.com
15. nvepdnpx.com
16. vwaeloyyutodtr.com
17. gokbwlivwvgqlretxd.com
18. mukevipvxvrq.com
19. empsqyowjuvvsvrwj.com
20. duomyvwabkuappgqxhp.com
21. voohnyqdinl.com
22. ncxphtrpiawmchfylsy.com
23. xwrmquiqjdsxk.com
24. ldiogjdyyxacm.com
25. kuetvxnntsk.com
26. lsawmyxqxvmogvxifm.com
27. ppdbeidwufrb.com
28. tfipmwkcgigiey.com
29. pgahbyurf.com
30. yaesbfejdxs.com

Seed: 0x4BFCBC6A

This seed probably first appeared early 2013. There are a couple of Sophos reports that correspond to this seed: Ramnit-B, Ramnit-FS, Ramnit-DD, Ramnit-DA, Ramnit-DB.

The first 30 generated domains are:

1. rkjtwjwmesvwhpc.com
2. axigleyldgeq.com
3. wxsssfvmqi.com
4. nhedwmmg.com
5. axswdqnjgrnryt.com
6. roiornfvclppad.com
7. sqhofbxqksckbfrs.com
8. rwtxpiehuiiucxkfckw.com
9. pmyadxuvmfmcajv.com
10. uejgdopjiyxnnvws.com
11. nbfplqkemrpedccrcyp.com
12. ywyqjdqktqxsxkt.com
13. gveejaqxpyrb.com
14. vuxrkjrewjwl.com
15. mgnodqfisg.com
16. dhlpcscshdrvpcpp.com
17. xygkltvhkvbje.com
18. ijxahlsdiw.com
19. jhchibrcyo.com
20. sdcepuelyqary.com
21. nqbvanrafsi.com
22. txnhnwwxfam.com
23. jpdvnajhhv.com
24. kkiykxbsc.com
25. hxlsxpmmtdqqvo.com
26. cnlbabnssw.com
27. dthjrnnicjkdetclt.com
28. eewbwvjommryy.com
29. vjckfodjtbobafxmc.com
30. yswkdrulyic.com

Seed: 0x79159C10

This seed was used first in April 2014. Here are some of the samples that use this seed: Malwr, Sophos Ramnit-BZ, many samples on Virustotal. The first 30 domains for this seed are:

1. knpqxlxcwtlvgrdyhd.com

2. nvlyffua.com
3. hgyudheedieibxy.com
4. anrylixwcbnjopdd.com
5. vrndmdrdrjoff.com
6. jhghrlufoh.com
7. tqjhvylf.com
8. hufqifjq.com
9. itktxexjghvvxa.com
10. ppyblaohb.com
11. ectdsitvvoydawmfni.com
12. vbvqbnwyurqem.com
13. jetuergatod.com
14. anxsmqyfy.com
15. ckyioylutybvcxv.com
16. khllpmpmare.com
17. riaaiysk.com
18. vfrpojablskkqrx.com
19. egopuefrdsefc.com
20. fycecyuksgjfxy.com
21. qyuylvjwh.com
22. wldlrwlygck.com
23. lcqavndroo.com
24. acuhjbadvnmhthwnlxv.com
25. qvberjspofqsxdnr.com
26. euvyalbkwahxxjn.com
27. typmyloijdcxtdxd.com
28. hjahmduyebf.com
29. ebrfoyrs.com
30. uvenqtbfbeyvebqeb.com