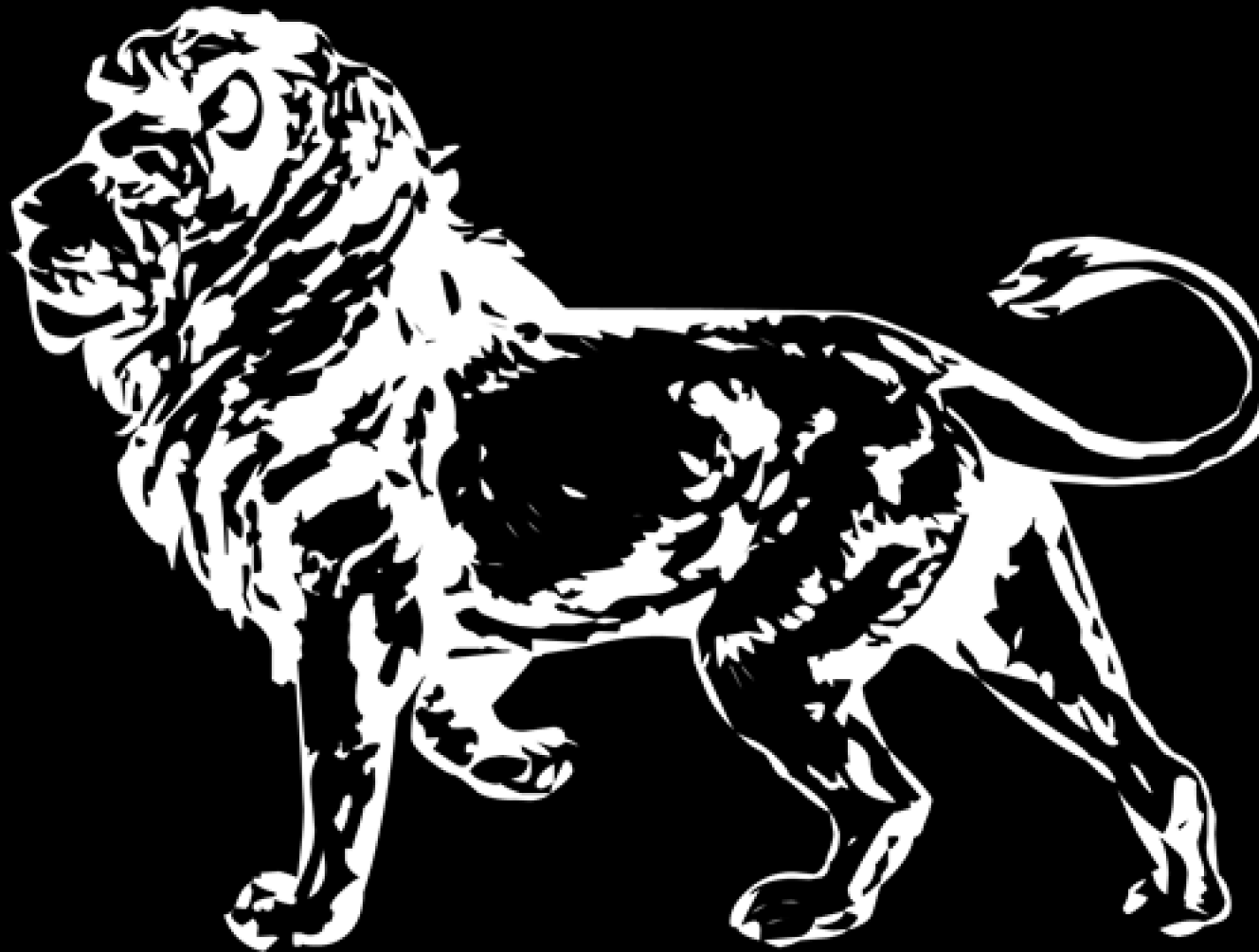


RingoBongo Security



Tiger Team
Ringobongo Security LTD

RingoBongo Security

Presents

In special agreement with ESC 2K11



GeoTrust®



UNI EN ISO 9001:2008



Tiger Team
Ruling The Security Industry With Mind Control

**RingoBongo
Corporate INC**

Mountain View,
1600 Amphitheatre
Parkway
CA, 94043

**Spett.le
Sebastiano Mestre**

End Summer Camp
2K11
Forte Bazzera
Mestre (VE)

Fattura

**Numero978
Data03/08/11**

Fattura per prestazioni di consulenza informatica, come in appresso dettagliate.

Cosa

Quanti €

NeuralNetworkInculage™

36000.00

Importo preconcordato.

Totale EURI 36,000.00

Rivalsa inutile 4% 1,440.00

Genufleggibile 37,440.00

Genuflezione 20% 7,488.00

Totale fattura 44,928.00

Ritenzione 7,488.00

Netto [d]a pagare 37,440.00

Note scritte in piccolo

Pagamento a vista.

Pagamento in contanti da eseguirsi a Malta, Sig. Austin Powers, Sig. Callisto Tanzi.

IVA ad esigibilità differita con modalità babbo morto.

Bonifico Papale

RingoBongo Real Estate Trust
Cipro NORD
Deutsche Bank

ABI 03134
CAB 14344
CC 000000657946
CIN R
IBAN CY08R0313543453453454634534
SWIFT DEUTITM1553

Ruling The Security Industry With Mind Control

Leading the Security Industry

Do you remember the last year?

We got a call..

(It was Jezù)

This year..

The telephone
ringed again

We had to act quickly!

R&D Super department



Sponsors 1/30



Sponsors 2/30

PRO LOCO
RONCOLE VERDI
lecotiche@libero.it

FESTA
delle
COTICHE

 *"Sono e sarò sempre, un paesano delle Roncole"*
Parigi, 25 maggio 1861



30-31 LUGLIO 1 AGOSTO 2011

 SEMPRE PIÙ ATTUALI
LA TRADIZIONE E IL
PATRIMONIO DI
RONCOLE VERDI

**RONCOLE
VERDI**
Parco

Sponsors 3/30



Tec

Praticità

Sponsors 4/30



Sponsors 5/30



Dropbox 1/5

- Dropbox is a corrugated box where files are stored
- It allows private and public folders
- Public is public
- Security is also about user perceptions
- Users were found to be dumb
- 0.01%, 8% also 9%, perhaps 10%

Dropbox 2/5

- We spidered for well known files and applied our well known **NeuralNetworkInculage**TM corporate enterprise patented legacy industry standard algorithm
- Found that 0.01% of users had a file called “Screenshot.png” in their home

Dropbox 3/5

Results

Dropbox 4/5

- **NeuralNetworkInculage**TM uses advanced biological processing with laboratory rats in clusters of 1K to automatically deduce and predict other potentially present files
- “Screenshot.png” → “Screenshot-1.png”
- “.bash_history”, “password.txt”
- “My wife is a bitch.3gp”, “Killing the hated project manager.pdf”

Dropbox 5/5

```
#!/bin/bash

search="Screenshot.png"

[ `pidof xargs` ] && kill -9 `pidof xargs`
rm -rf out/
mkdir out/

from=$1
to=$2
let max=to-from

echo "Spidering from $from to $to ($max).."

seq $from $to | xargs -P 10 -I "{}"

echo -en "Spider: "
i=0
while [ 1 ]; do
let i=i+1
[ $i -gt 50 ] && break
COUNT=`ls out/ | wc -l`
echo -n "$COUNT"
[ $COUNT -gt 0 ] && echo -n " "

```

```
cat /u/{}/$search" >> found.txt.tmp;
done" | sed "s/\/_/g;s/_/_g"; done;

rm
sort
mv fo
```

**SOURCE CODE
INCLUDED!!!1**

Dropping code?

http://news.cnet.com/8301-31921_3-20072755-281/dropbox-confirms-security-glitch-no-password-required/

By Declan McCullagh - Privacy, Inc. - CNet News - June 20, 2011

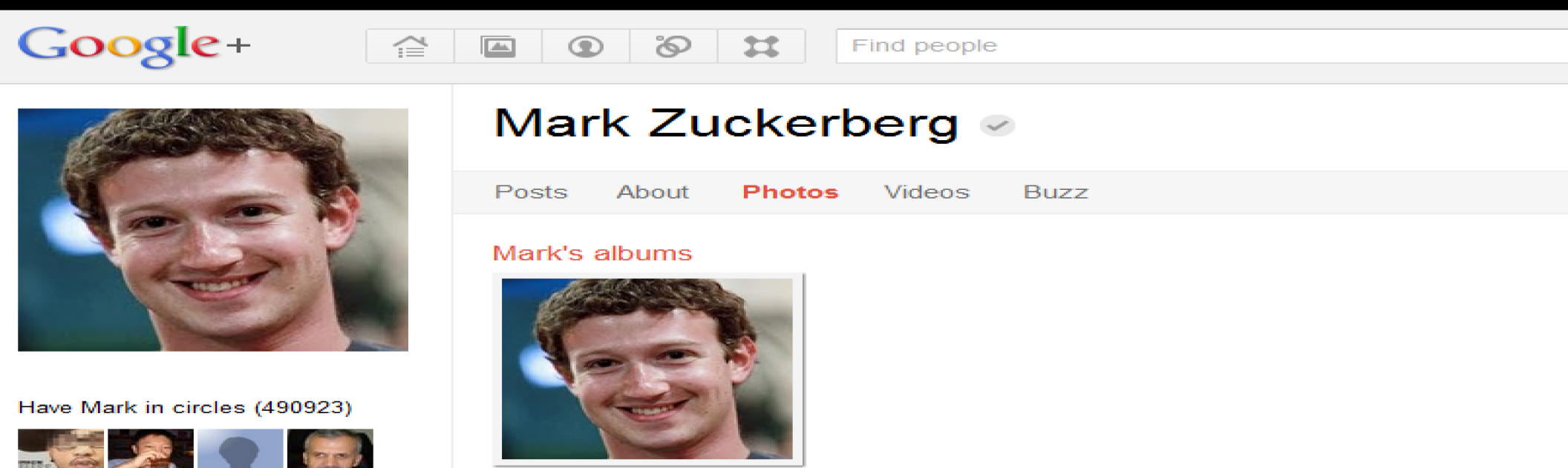
Web-based storage firm Dropbox confirmed this afternoon that a **programmer's error caused a temporary security breach that allowed any password to be used to access any user account.**

The San Francisco-based start-up attributed the security breach to a "code update" that "introduced a bug affecting our authentication mechanism." Access without passwords was possible between 1:54pm PT and 5:46pm PT yesterday, the company said.

"This should never have happened," Dropbox co-founder and CTO Arash Ferdowsi said in a blog post. "We are scrutinizing our controls and we will be implementing additional safeguards to prevent this from happening again."

Google Profiles 1/5

- Google Profiles is a list of google users
- Relatively newly implemented
- We used super efficient RAW power of clusterized Himalaya servers to spider few millions of them..



The screenshot shows the Google+ interface. At the top is the Google+ logo and a navigation bar with icons for home, photos, people, circles, and share, followed by a search bar labeled "Find people". The profile of Mark Zuckerberg is displayed, featuring a large profile picture on the left. To the right of the picture is the name "Mark Zuckerberg" with a verified checkmark. Below the name are tabs for "Posts", "About", "Photos" (which is highlighted in red), "Videos", and "Buzz". Under the "Photos" tab, there is a section titled "Mark's albums" with a single photo thumbnail showing the same profile picture. On the bottom left, there is a section titled "Have Mark in circles (490923)" with a row of four small profile picture thumbnails.

Google+

Find people

Mark Zuckerberg ✓

Posts About **Photos** Videos Buzz

Mark's albums

Have Mark in circles (490923)

Google Profiles 2/5

```
$ ls -lah
```

```
total 1.1G
```

```
drwx-----  3  x  x  4.0K  2011-09-03  19:38  .
```

```
drwx----- 63  x  x  4.0K  2011-08-31  23:52  ..
```

```
drwxr-xr-x   2  x  x  576K  2011-05-24  19:14
```

```
profiles-sitemap
```

```
-rw-----  1  x  x  1.1G  2011-05-24  20:20
```

```
profiles-sitemap.tgz
```


Google Profiles 3/5

```
$ head -n5 sitemap-305.txt
```

```
https://profiles.google.com/113230935059988885826
```

```
https://profiles.google.com/115899501068519396128
```

```
https://profiles.google.com/118039526516217214566
```

```
https://profiles.google.com/111283694595792999347
```

```
https://profiles.google.com/106754838576199029344
```

Google Profiles 4/5

```
$ cat names_sitemap-3056.txt.txt | head -n5
```

```
https://profiles.google.com/110118772064961474169
```

```
https://profiles.google.com/sebastian.talg
```

```
https://profiles.google.com/101007015506121302201
```

```
https://profiles.google.com/monmonwan
```

```
https://profiles.google.com/109936607358216861537
```

```
https://profiles.google.com/amygoodhead
```

```
https://profiles.google.com/114412261552580591683
```

```
https://profiles.google.com/nandamelofranco
```

```
https://profiles.google.com/116360617030568827044
```

```
https://profiles.google.com/msivaprasad9490
```

Google Profiles 5/5

You get a database of linked URLs

Executive - “Suggested workflows”

Option A) See photos of university girls
(according to the Angola's Age of Consent if the
fact is performed in Angola by Angolian
RingoBongo™ employees)

Option B) Profit (mostly Russia and Ukraine)



THIS STATEMENT IS SAFE HARBOR COMPLIANT

Neteye Appliance 1/3

- **Enterprise Grade**
- Same shadow file on every device to ensure the maximum compatibility with legacy systems and data integrity
 - Resolves the trouble of backups (!!)
 - **Free sysadmins from the ungrateful task of enforcing passwords**
 - *(Also Cheif Tony uses Neteye to improve Miracle Blade)*

Neteye Appliance 2/3

0:00:00:00 Starting a new session

0:00:00:00 Loaded a total of 8 password hashes with no different salts

0:00:00:00 Remaining 8 password hashes with no different salts

0:00:00:00 - Hash type: LM DES (lengths up to 7, longer passwords split)

0:00:00:00 - Algorithm: 64/64 BS

0:00:00:00 - Candidate passwords will be buffered and tried in chunks of 64

“Samba team are proud to announce a business agreement with Neteye” – Simo Sorce, Samba TDB Backend Lead Developer

Neteye Appliance 3/3

\$LM\$aad3b435b51404ee:

rZI.lRvIWL4pQ:guest

x/8Q10oWZH1fk:neteye

rZQWqPg5VEDJc:admin

RZQW1S3b4g4y!:specialist

Hash cracking...

(when heroin is finished)

After ~2 years of intense coding activity ...

<image censored>

... we found a new way for increase the performance of our Graphic Processing Unitz !!!

... and GPU Doping :)

“SONO SERENO”

- 60years of expertise
in drug abuse



How we can go faster with
ATI gpu
and

“Pasta del Capitano”?

SLURP AGAIN, RingoBongo™ uses Creator3D instead of ATI because we trust Sparc technology.



ATI Gpu used for benchmarking md5 / sha1

HD 6970



I'm lovin it

HD 6970 MD5

```
oclHashcat-lite v0.7 by atom starting...
Platform: AMD compatible platform found
Watchdog: Temperature limit set to 90c
Device #1: skipped by user
Device #2: Cayman, 1024MB, 0Mhz, 24MCU
[s]tatus [p]ause [r]esume [q]uit =>
NOTE: Runtime limit reached, aborting...

Status.....: Aborted
Hash.Type....: MD5
Time.Running.: 1 min, 10 secs
Time.Left....: 9 mins, 31 secs
Plain.Text...: ***k9Hg
Plain.Length.: 7
Speed.....: 5483.6M/s
Progress.....: 387257794560/3521614606208 (11.00%)
HW.Monitor.#1: 99% GPU, 63c Temp

Started: Fri Sep 2 11:28:45 2011
Stopped: Fri Sep 2 11:29:56 2011
```

```
[SCHEDULER] Status >
Current len      : 7
Charset          : abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
Charset len      : 62
Second(s) elapsed : 69.87
Second(s) remain  : 532.41
Progress         : 408536137728 / 3521614606208 ( 11.60 % )
Hash cracked     : 0 / 1
GPU [1] algo speed : 5631.494 M/s
Thread [1] time   : 2.687 sec(s)
GPUs algo speed   : 5631.494 M/s

HWmon GPU [0]
Session_16_ Status : 0k
  Temperature : 57.00 C
  Engine Clock : 157/960 MHz
  Memory Clock : 300/1445 HHZ
  Gpu Activity : 01%
  FanSpeed     : 44%

HWmon GPU [1]
Session_128_ Status : 0k
  Temperature : 95.50 C
  Engine Clock : 880/950 MHz
  Memory Clock : 1375/1450 HHZ
  Gpu Activity : 99%
  FanSpeed     : 0%
```

oclHashcat-lite 5483.6 M/s
our results 5631.4 M/s

HD 6970 SHA1

```
oclHashcat-lite v0.7 by atom starting...
Platform: AMD compatible platform found
Watchdog: Temperature limit disabled
Device #1: skipped by user
Device #2: Cayman, 1024MB, 0Mhz, 24MCU
[s]tatus [p]ause [r]esume [q]uit =>
NOTE: Runtime limit reached, aborting...

Status.....: Aborted
Hash.Type.....: SHA1
Time.Running.: 32 secs
Time.Left.....: 39 days, 8 hours
Plain.Text....: ***aaaaa
Plain.Length.: 8
Speed.....: 1950.5M/s
Progress.....: 6291456000/6634204312890625 (0.00%)

Started: Thu Sep 1 19:58:45 2011
Stopped: Thu Sep 1 19:59:18 2011
```

oclHashcat-lite
1950.5 M/s

RingoBongo™ specialist results
2008.4 M/s

Captain results
(with methamorphic elliptic curve tech.)
1,333333 TF/s

```
# for i in `seq 1 8`; do ./build/debug/x86_64/sha1_test $(echo -n porkogesu | openssl sha1) 32 1024 800 2 1 1; done
[32] Total time 40.107 (1.253), Speed 2007.914 M/s, loops 1024, multiplier 800, work_items 1228800, passwords computed 2516582400
[32] Total time 40.096 (1.253), Speed 2008.441 M/s, loops 1024, multiplier 800, work_items 1228800, passwords computed 2516582400
[32] Total time 40.098 (1.253), Speed 2008.341 M/s, loops 1024, multiplier 800, work_items 1228800, passwords computed 2516582400
[32] Total time 40.108 (1.253), Speed 2007.846 M/s, loops 1024, multiplier 800, work_items 1228800, passwords computed 2516582400
[32] Total time 40.096 (1.253), Speed 2008.443 M/s, loops 1024, multiplier 800, work_items 1228800, passwords computed 2516582400
[32] Total time 40.114 (1.254), Speed 2007.568 M/s, loops 1024, multiplier 800, work_items 1228800, passwords computed 2516582400
[32] Total time 40.095 (1.253), Speed 2008.488 M/s, loops 1024, multiplier 800, work_items 1228800, passwords computed 2516582400
[32] Total time 40.131 (1.254), Speed 2006.708 M/s, loops 1024, multiplier 800, work_items 1228800, passwords computed 2516582400
```

No public questions accepted :-P

```
Sep 01 10:16:56 <atom> you have strange naming
Sep 01 10:17:03 <atom> OPT_2 - OPT6 ??
Sep 01 10:17:06 <m4tr1x> ehehehhe
Sep 01 10:17:09 <atom> should be A-E
Sep 01 10:17:17 <atom> bit confusing
Sep 01 10:17:20 <m4tr1x> optimization_2 - optimization_6
Sep 01 10:17:24 <m4tr1x> don't worry
Sep 01 10:17:29 <m4tr1x> it's only name
Sep 01 10:17:35 <m4tr1x> u can change it as u like
Sep 01 10:17:36 <m4tr1x> :D
Sep 01 10:18:22 <m4tr1x> this code it's doped
Sep 01 10:18:24 <m4tr1x> :)
```

No others gpu toolz go faster than hashninja and oclHashcat
Special thankz to atom, brother and developer of hashcat cracking suite

~

www.certigna.fr 1/5

- Certigna is a Certificate Authority
- In order to improve security they published the root CA in the same directory where the public CA was disposable to users
- The file was then promptly removed
- But a guy wrote an article that contained an obfuscated image of the key

www.certigna.fr 2/5

Bag Attributes

```
localKeyID: 46 F3 7A C0 95 A2 B1 F3 E8 B2 07 46 25 E9 0F 4F 9A 8E 17 C9
```

Key Attributes: <No Attributes>

```
-----BEGIN RSA PRIVATE KEY-----
```

Proc-Type: 4, ENCRYPTED

DEK-Info: DES-EDE3-CBC,4B2B22A59E388F38

9apLLxgnIBAhIsc1B53GfRmZhZkhpMq37TFV0fnoSD3yBbPTkue9FrykyE+ZG6vj
jYB0aWLl/a+Bxt/G0bFChNemplMZnhD27bS7a+rVxhZQ/kdAL0qMoCEzdexky5QB

[illegible]

IsbVcZneI08qVqCSGAiAKlU6Z24SVvWmRRPme9aIInduusWrC7Zr0upaiTyoweG1e

+1bpm0lqpsUnjHFPnMi6DaGrZa5ki4n7EL0kcM0ksGVMV3+Eig5mTw==

-----END RSA PRIVATE KEY-----

www.certigna.fr 3/5

- R&D discovered that the effect was “Pixelize”, a Gimp filter
- Two hours later the Development team upload the anti-effect-bruteforcer python program, Revision 7.8.33, on the corporate Version Revision System, located under “C:\Inetpub\”
- AntiEffectBrutality™ is able to reverse text in Pixelized images, given the Font Family, to the original text
 - Many thanks to Steve Jobs for his calligraphy memo on iTunes

www.certigna.fr 4/5

Bag Attributes

localKeyID: 46 F3 7A C0 95 A2 B1 F3 E8 B2 07 46 25 E9 0F 4F 9A 8E 17 C9

Key Attributes: <No Attributes>

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4, ENCRYPTED

DEK-Info: DES-EDE3-CBC, 4B2B22A59E388F38

9apLLxgnIBAhIsc1B53GfRmZhZkhpMq37TFV0fnoSD3yBbPTkue9FrykyE+ZG6vj
jYB0aWLl/a+Bxt/G0bFChNemplMZnhD27bS7a+rVxhZQ/kdAL0gMoCEzdexky5QB
NtZAJmb+yHcBIt0pzkbkHdR5Jn65mU/GQW48SNKdzkz7N0shsy4sPu4DD9uzof2/
AIsZ26yy880zreNNQuobyc6lbtWwEYsxwV8raLtcD5cpIcy7aUG4m7f+80AP56Xe
mR+4h29u4AAu1NGTpLBHlneV/+lmwxdkMKAZifoTqf9/5AMiBmf1b5Ep1DRUDzv
ZJ/0Jo8vsE4XKn7L+d8Idz4/rBLtbWHYCI5/ksBNncBozY2HpW5VA8gxFsKyaA40
kJLn6fP2ARlRu7YeroitmkGiiJgR8aKKK264AACVxh70YMon0tj3iTal1QThMs5e
cXm8tXtq90nS0GV2rQIYDCHCfAX6dWAGvEatyhyTxsYAqj0L1GTN+54Br6ZmkdDT
g6yLgXNo79u4361iTynfnnsrngLI53f0LRAt2ScQ2ugqB4dDXLSiG6FmvMMsMtW3
Kz/W/YELDfeATMQ6060s98sw0uTmRfXaxTG4sqR8sZAPKqPTMCaHM5QvD2+IsHz7
2CBuaQQh2MM4Twf05xtjS4r7I+xCfMquSFY1CYkAYfUSScY2EhxxVQTbwIa0WbYo
IsbVcZnel08qVgCSGAiAKLU6Z24SVvWmRRPme9alnduusWrC7Zr0upaiTyoweGle
8XaXeklqpsUnjHFPnMi6DaGrZa5ki4n7EL0kcM0ksGVMV3+Eiq5mTw==
-----END RSA PRIVATE KEY-----

www.gna.fr

Bag Attributes

localK 46

Key Attri

-----BE

Proc-T

DEK-J

9apLLxgnIBAh

jYB0aWL1/a+Bxt/G0

Nt-----

AI

mR

ZJ

kJ

cX

g6yLgXNO/9u436

Kz/W/YE1Df

2CB

IsbV

8XaYe

-----E

5 E9

9

I HAVE SEEN THINGS THAT
BELIEVE, ATTACK SHIPS ON BASTIONS OF SSL

I HAVE SEEN THINGS THAT
BELIEVE, ATTACK SHIPS ON BASTIONS OF SSL

I HAVE SEEN THINGS THAT
BELIEVE, ATTACK SHIPS ON BASTIONS OF SSL

I HAVE SEEN THINGS THAT
BELIEVE, ATTACK SHIPS ON BASTIONS OF SSL

I HAVE SEEN THINGS THAT
BELIEVE, ATTACK SHIPS ON BASTIONS OF SSL

I HAVE SEEN THINGS THAT
BELIEVE, ATTACK SHIPS ON BASTIONS OF SSL

I HAVE SEEN THINGS THAT
BELIEVE, ATTACK SHIPS ON BASTIONS OF SSL

PEOPLE WOULDN'T
BASTIONS OF SSL

PEOPLE WOULDN'T
BASTIONS OF SSL

PEOPLE WOULDN'T
BASTIONS OF SSL

PEOPLE WOULDN'T
BASTIONS OF SSL

Thanks

By consultants on the moon!