

Sysadmin Roundtable December 2009



Topics

- Uptick in RDP blocks
- Open DNS resolver detection
- Keygen tool findings
- Copyright violations
- CST system and software moves
- CO2 phishing

RDP blocks

- Due to remote assistance
 - ◊ SCCM tool used for remote assistance
 - ◊ Remote assist opens firewall to everything
 - ◊ After assistance, firewall is not restored
- Detector changed to be informational instead of blocking for 2 weeks while this is sorted out

Open DNS resolver detection

Swept the site

- Looking for machines that would resolve names on site
- Notified sysadmins of machines that responded
- Right now the detector is just a P.O.C. but in the future could be attached to Tissue

Keygen tool findings and copyright violations

- AV detector detects more than just virus badware
 - EVEREST_Ultimate_Edition_v4[1].00.978_Beta.exe>>keygen.exe
 - Downloads\SRProTrialsetup.exe
 - everestus\keygen.exe
 - Misc Software\FlashGet_v1[1].3_by_MP2K.zip>>crack.exe
 - ToxicDualLayerPatcher-v1.0.zip>>DLPatcher.exe
- Please remind your colleagues that until further notification

Copyright violation is not allowed, per computing policy

CST system and software moves

- CST is moving to a new rackspace area in FCC
- You may see some downtime of services while this takes place
- A number of services are also being moved to different servers. We will update links on the security page as necessary.

CO2 phishing

Dear all,

Washington, D.C. - Drilling nears completion for the first large-scale carbon
CO2 sequestration.

This project will be used to demonstrate that CO2 emitted from industrial sources
deep geologic formations
to mitigate large quantities of greenhouse gas emissions.
Please refer to the details of the attachment.

Contact Us:

*By E-mail: You can send an email to the Secretary of Energy
at The.Secretary@hq.doe.gov

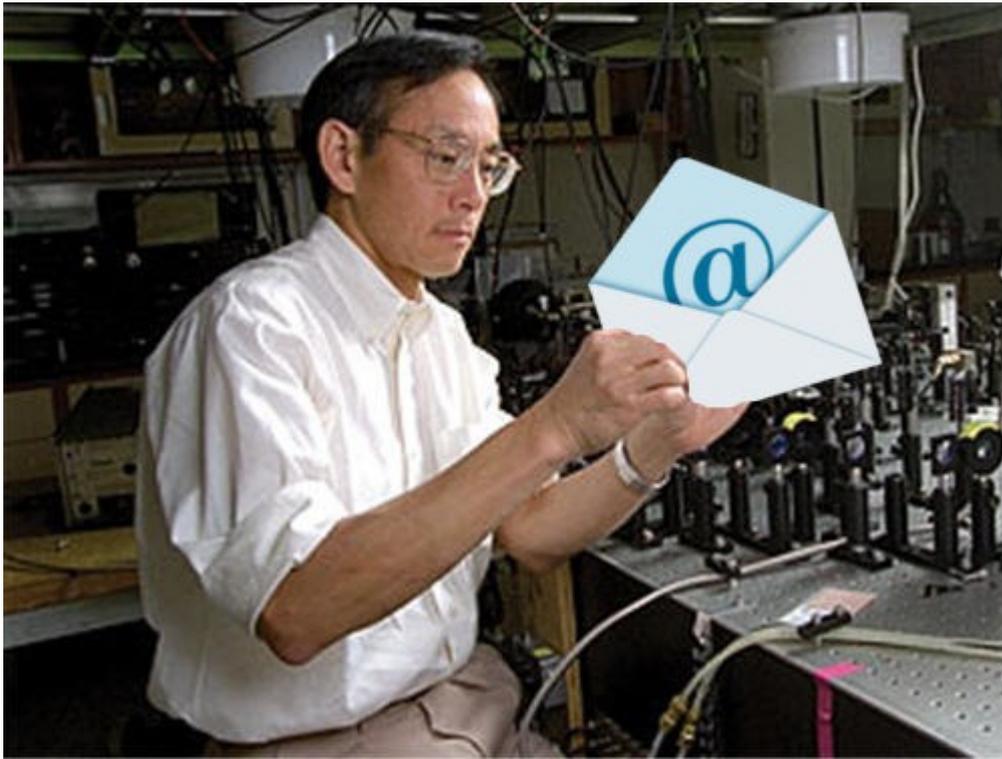
*By Phone: 1-202-586-5000 (Main Switchboard)
National Phone Directory

*By Fax: 202-586-4403

*By Mail: U.S. Department of Energy
1000 Independence Ave., SW
Washington, DC 20585

But how to tell if it's spam?





The Secretary sending me email?

Really?



Vague content

Dear all,

Washington, D.C. - Drilling nears completion for the first large-scale carbon
CO₂ sequestration.
This project will be used to demonstrate that CO₂ emitted from industrial sources

Sometimes the spammers can be pretty creative

Othertimes they appear to be writing just to fill space

```
tarupp@catbot:~$ whois 117.11.115.217
% APNIC found the following authoritative answer from: whois.apnic.net

% [whois.apnic.net node-1]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:      117.8.0.0 - 117.15.255.255
```

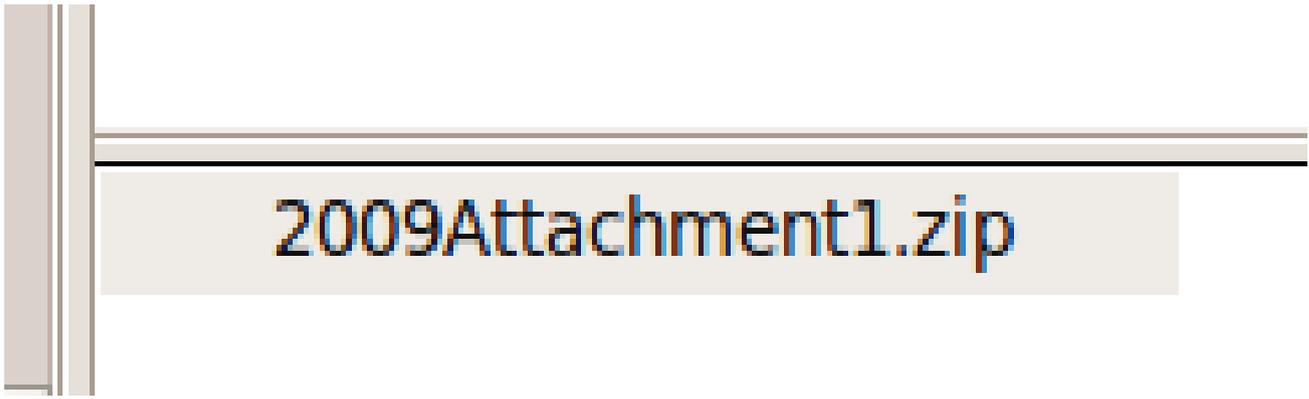
Sent from Chinese address space

```
person:      ChinaUnicom Hostmaster
nic-hdl:     CH1302-AP
e-mail:      abuse@chinaunicom.cn
address:     No.21,Jin-Rong Street
address:     Beijing,100140
address:     P.R.China
phone:       +86-10-66259940
fax-no:      +86-10-66259764
country:     CN
changed:     abuse@chinaunicom.cn 20090408
mnt-by:      MAINT-CNCGROUP
source:      APNIC
```

I must have missed the
announcement that the DOE
moved it's headquarters
to Tianjin Province

```
person:      huang zheng
nic-hdl:     HZ19-AP
e-mail:      ipaddr@ywb.online.tj.cn
address:     76 NO, ShiZiLin Street ,HeBei district of Tianjin,China
phone:       +86-22-24459190
fax-no:      +86-22-24454499
country:     CN
changed:     ipaddr@ywb.online.tj.cn 20050721
mnt-by:      MAINT-CNCGROUP-TJ
source:      APNIC
```

Attachments, while not necessarily evil
should be approached with suspicion if they're from
people you are not regularly in contact with



2009Attachment1.zip

Spammers toying with your assumptions

X-Mailer: FoxMail 3.11 Release [cn]

Anyone care to venture a guess at what **[cn]** stands for?

[cn] = China

.cn is the top-level domain for china

But he sure looks chinese, doesn't he?

He looks chinese

therefore

he uses chinese email clients



mmm....not quite

I'm sure you're all familiar with what they say about people who “assume”

This is what separates the cerebral from the non

- Current Sec. Of Energy is Chinese American
- Born and raised in St. Louis Missouri
- And never learned to speak Chinese

“ Chu said he never learned to speak Chinese because his parents always talked to him and his brothers in English, although he said (in 1997) that he was trying to learn Mandarin, believing that if he could stay in China for "at least six months", he would become fluent.[7] ”

http://en.wikipedia.org/wiki/Steven_Ch

I don't know about you, but based on what I read

I'm not ready to conclude that the real secretary sent me this email

What was in the Zip?



- 2 executable files
 - CO2_EOR_Fact.exe
 - Louisiana_CO2-EOR_Report.exe
- Both are conveniently packed with aPACK from ibsensoft
- Upon running the exe, some files are created
 - ~TX2.tmp
 - .bat
 - .pdf

 CO2_EOR_Fact.exe	148.0 KB	DOS/Windo...	16 November 2009, 14:58
 Louisiana_CO2-EOR_Report.exe	768.0 KB	DOS/Windo...	16 November 2009, 14:59

How did I know it was packed?

By using the 'strings' command

```
tarupp@catbot:~$ strings Desktop/Louisiana_CO2-EOR_Report.exe | less
tarupp@catbot:~$ █
```

```

j      X0
u.h`
tAVW
aPLib v1.00 - the smaller the better :)
Copyright (c) 1998-2009 by Joergen Ibsen, All Rights Reserved.
More information: http://www.ibsensoftware.com/
[t_ "t
n;^
Qkkbal
```

Interesting tidbits. Padding at the end of the packed file

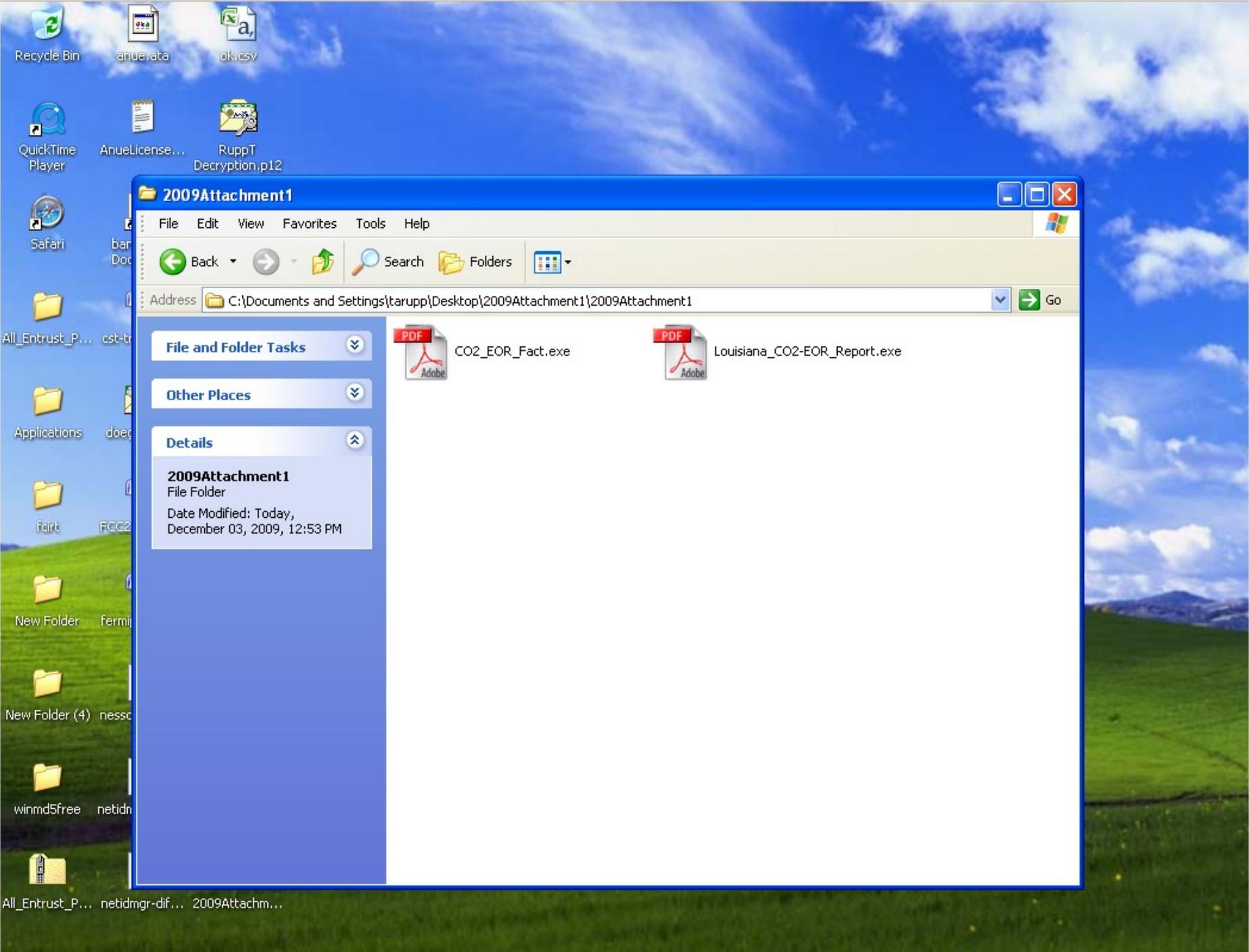
INOL

PAPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADI
DDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGGI
XPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADD:
NGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXP/
DDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGG)
GPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADD:
DINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGP/
PADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDII
GXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPAI
DINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGX
PADDINGGXXPADDINGPADDINGGXXPADDINGPADDINGGXXPADDINGPADDII
INGPADDINGGXXPADDINGPADDINGGX

(END)

Running the malware

Don't do this at home. We're professionals (or claim to be)



Recycle Bin

anue.vata

ok.csv

QuickTime Player

AnueLicense...

RuppT Decryption.p12

Safari

bar Doc

All_Entrust_P...

cst-b

Applications

doec

fcrt

FCC2

New Folder

fermi

New Folder (4)

nessc

winmd5free

netidn

All_Entrust_P... netidmgr-dif... 2009Attachm...

2009Attachment1

File Edit View Favorites Tools Help

Back Search Folders

Address C:\Documents and Settings\tarupp\Desktop\2009Attachment1\2009Attachment1

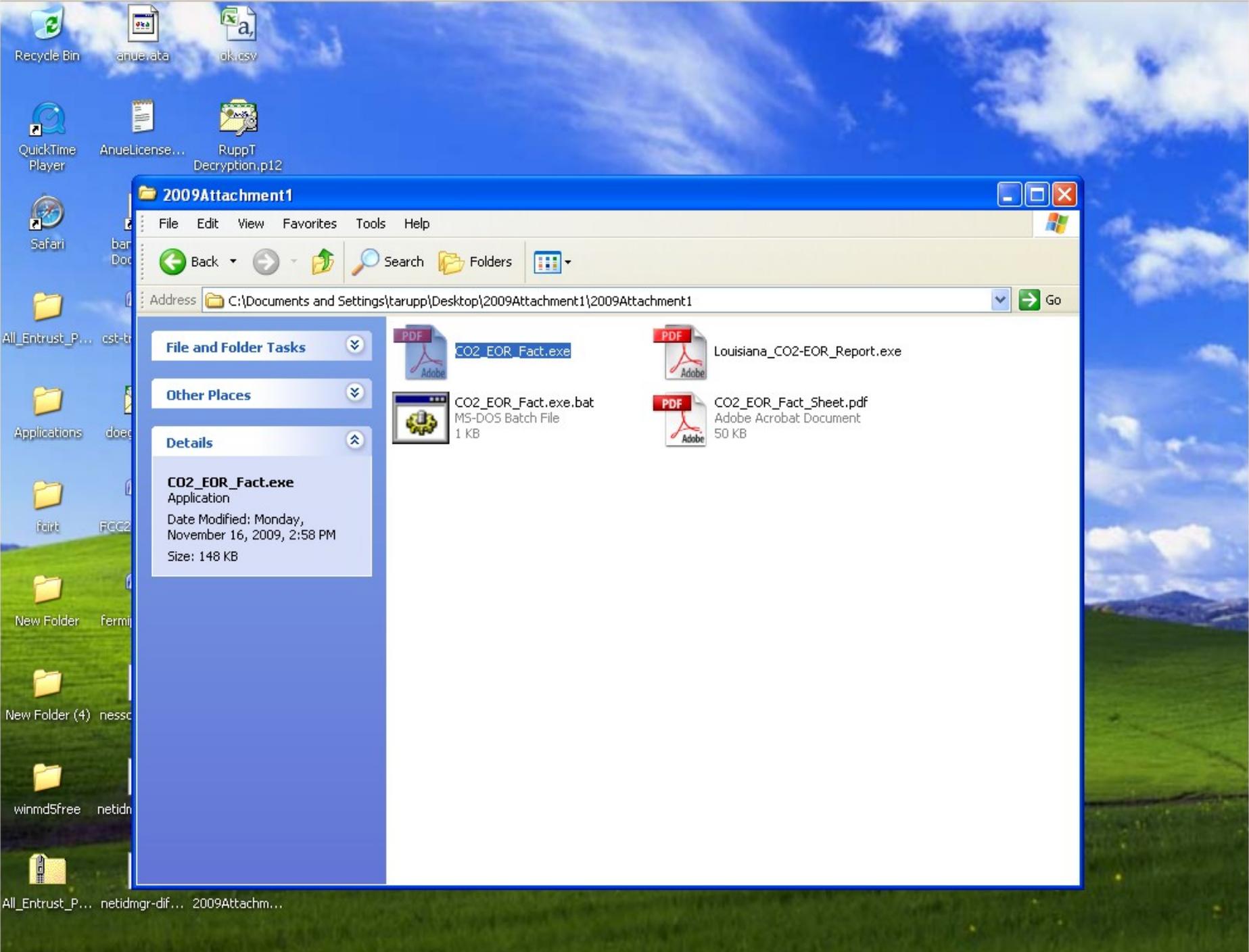
File and Folder Tasks

Other Places

Details

2009Attachment1
File Folder
Date Modified: Today, December 03, 2009, 12:53 PM

CO2_EOR_Fact.exe Louisiana_CO2-EOR_Report.exe



Recycle Bin
anue.ata
ok.csv

QuickTime Player
AnueLicense...
RuppT Decryption.p12

Safari

All_Entrust_P...

Applications

fcrit

New Folder

New Folder (4)

winmd5free

netidm...

2009Attachment1

File Edit View Favorites Tools Help

Back Search Folders

Address C:\Documents and Settings\tarupp\Desktop\2009Attachment1\2009Attachment1

File and Folder Tasks

Other Places

Details

CO2_EOR_Fact.exe
Application
Date Modified: Monday, November 16, 2009, 2:58 PM
Size: 148 KB

- CO2_EOR_Fact.exe
- Louisiana_CO2-EOR_Report.exe
- CO2_EOR_Fact.exe.bat
MS-DOS Batch File
1 KB
- CO2_EOR_Fact_Sheet.pdf
Adobe Acrobat Document
50 KB

DOE Office of Petroleum Reserves – Strategic Unconventional Fuels Fact Sheet: CO₂ Enhanced Oil Recovery

Background

- Significant volumes of conventional oil remaining in known U.S. oil reservoirs could be produced by injection of carbon dioxide (CO₂).
- CO₂ enhanced oil recovery (CO₂ EOR) has been constrained by economics, technology, CO₂ supply, and pipeline infrastructure.
- Use of CO₂ EOR in additional basins and reservoirs could increase domestic oil supply and provide effective storage of CO₂ produced from unconventional fuels production.
- Current (2005) oil production from CO₂ EOR is approximately 237,000 Bbls/day.¹ (Figure 1)

Figure 1 - U.S. CO₂-EOR Production is growing
Most Production Comes from the Permian Basin

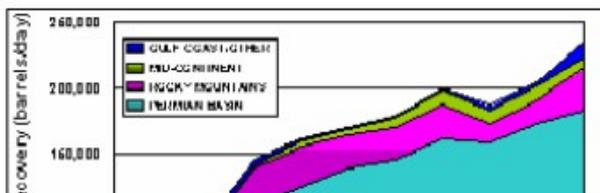
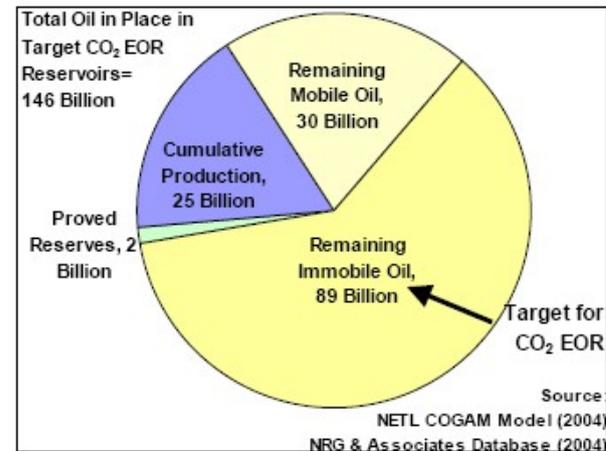


Figure 2 – Potential Target for CO₂ EOR



CO₂ EOR Economics

- Construction of new pipelines from CO₂ sources to target basins requires significant capital investments that must be supported by the long-term oil production potential of the target basin and by expectations of future oil prices.
- Oil price volatility is a significant deterrent to CO₂



Rec Louisiana_CO2-EOR_Report_web.pdf - Adobe Reader

File Edit View Document Tools Window Help

Print Search 1 / 57 95.1% Find

BASIN ORIENTED STRATEGIES FOR CO₂ ENHANCED OIL RECOVERY:

OFFSHORE LOUISIANA



All_Entrust_P... netidmgr-dif... 2009Attachm...



2009Attachment1 Louisiana_CO2-EOR_...

12:55 PM



- Be skeptical of this stuff
- Report it to Comp Sec so that we can
 - ♦ Block it where possible
 - ♦ Be on the lookout for less seasoned sysadmins who may click on the stuff and turf their machines

For up-to-date news

Visit the CST blog

<https://currency.fnal.gov/cstblog/>