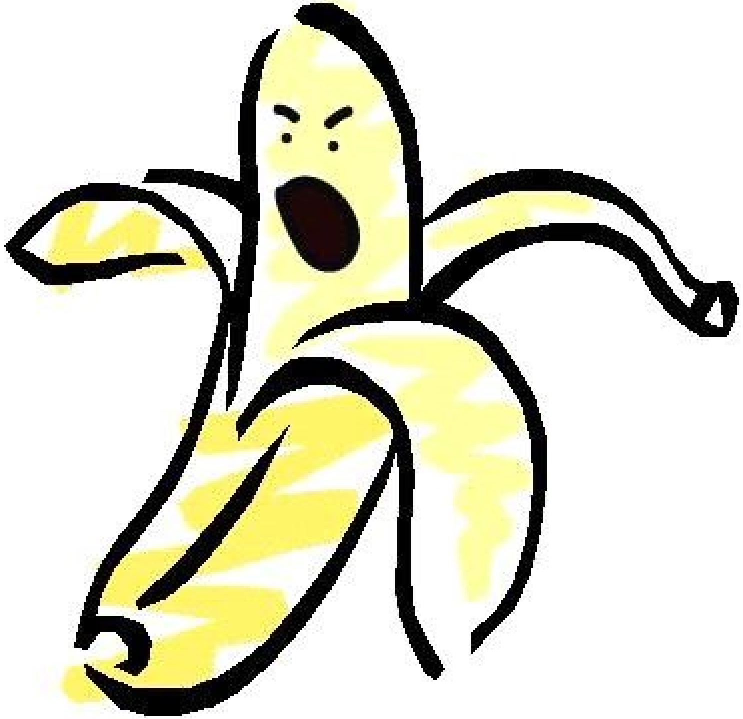
# Sysadmin Roundtable
# April 2008

Angry



Banana

# Agenda

Red Team Phishing and cached creds badness

LDAP service

Web exemptions

Remote access policy

Cool thing : andlinux

OMG!!!

Ponies!

WITH GLITTER!!!

# Phishing; no u!

- SLAC noticed this first
- Red Teaming is starting
  - hasn't been officially announced but...well...
- Level of detail in the email is really high
  - Knowledge of who to send from
  - Registered domain names are too specific
  - Asking you to run an application
- So we think it's a Red Teaming thing going on at SLAC, but in case you also see it here
- Be aware of targeted (spear phishing) emails!
  - HTML email or HTML email with view inline images

# Phishing + HTML; no u!

- You read HTML email?
- Images or links can fetch from an outside server and that server can log the fetch
- You're now a validated email address
- And an IP address is in that access log. If you marry that with GeoIP, you now have direct marketing!

# Value to vendors

- tarupp@fnal.gov

$

- #1 verified

$$

- #2 with GeoIP

$$$

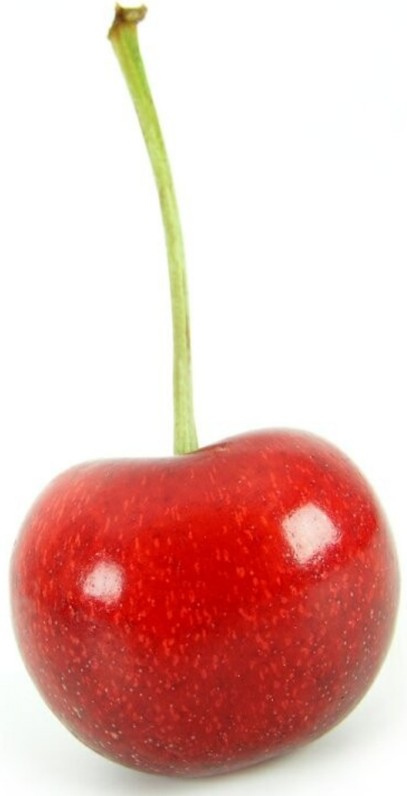
# More badware

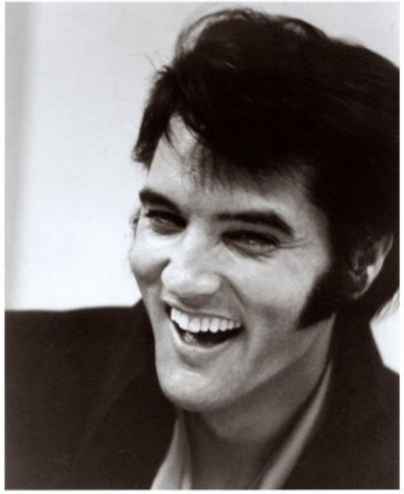
- zip file with an MDB (said MS Access) file in it.
- Clickity click click causes stack overflow
- Code execution and then “uh oh”
- ANL CST had a bad run-in with this
- Cached credentials were used by code to skip around to other machines, trying to get admin/domain admin privileges

# Response

- Cut down # of cached creds to 1
- Only perceive potential problem with laptops
- Last logged on user will be cached
- Limits the possibility that the exploit can nab admin level privileges.
- And we'll probably be saying this for the rest of eternity, but...

# ***Pretty Please***

with a  on top



Stop blindly clicking on

links in your email

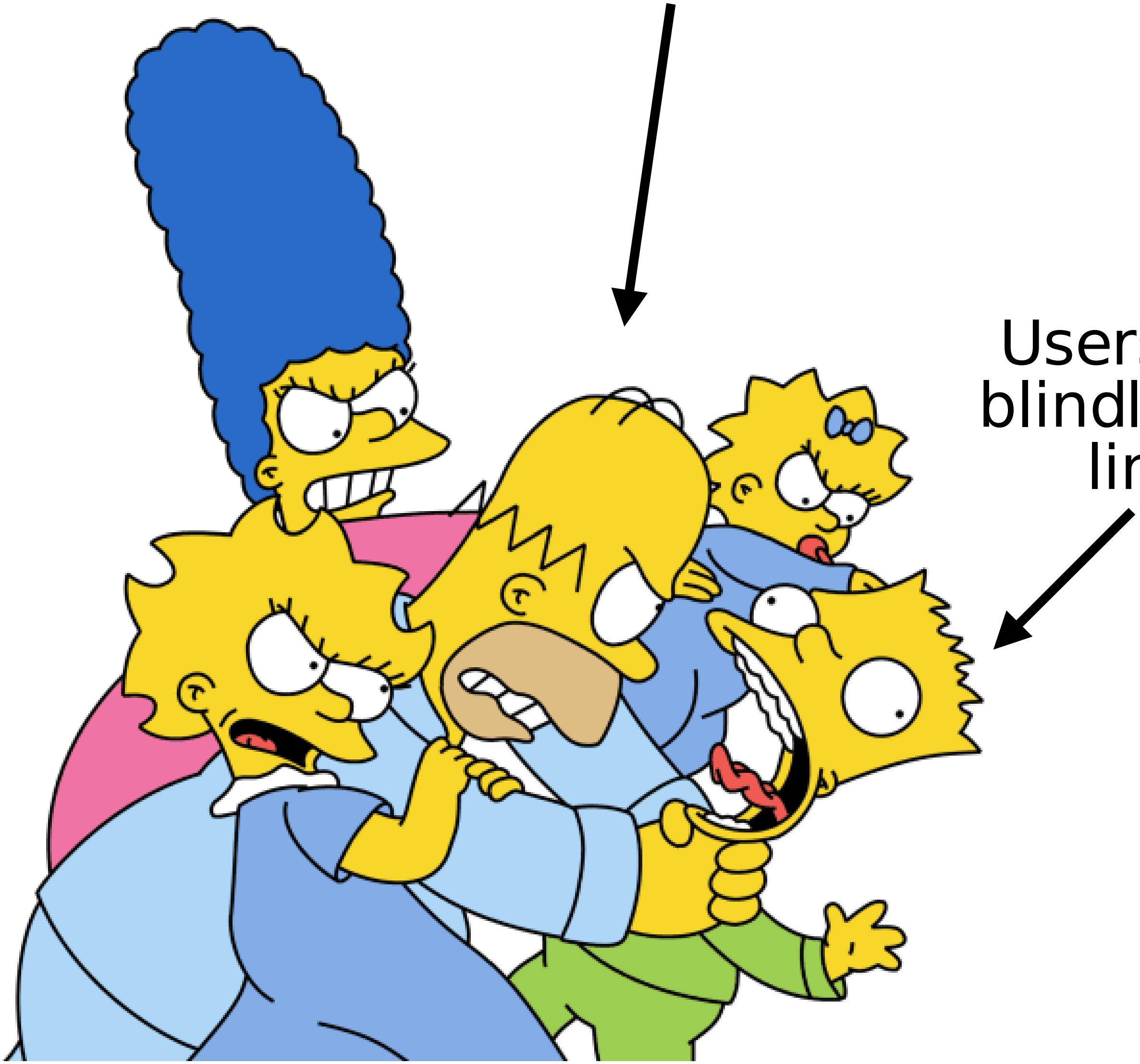
If you're not sure...don't click

O
r

Ask the person to

resend the email

Because we (CST) do love and look out for our community



Computer Security Team

Users who blindly click links

Even if they make us angry from time to time

# More

- There are AV signatures for the aforementioned MDB problem
- Next patch Tuesday (April 8th) should have patches available

CAUTION
THIS IS SPARTA!
ACHTUNG
ATTE
TION
CUIDADO
CONTINENTAL
COMMERCIAL PRODUCTS

# No, it's Central LDAP Service

- Going to be services.fnal.gov
- CST has been attempting to connect our own applications to it
- It's not ready for public use yet
- Core Services is in charge of it. When will it be production ready?

# WebEx…

- …emptions
- Cleaning up list
- Removing non-validated in April
- Soon after remainder will need to meet web baseline
  - Central logging of access, error and SSL logs
    - Marc has instructions for doing this!
  - Central means clogger.fnal.gov

# Web Server Baselines

- Apache

**cd-docdb # 1536**

- IIS

see this man

# Enforcement of Remote Access Policy

# RA Policy
## slide 1 of 1000000000

- RDP
  - On site only, using domain account
  - Via VPN or kerb auth'd session if off site
- Or things that meet the following
  - Accept centrally managed accounts and comply with Strong Auth Policy
  - Reside on OS that complies with FNAL Baseline

# RA Policy

## slide 2 of 1000000000

- Need to tunnel through Kerb auth'd session
  - Timbuktu
  - PCAnywhere
  - Back2MyMac
  - RemotelyAnywhere
  - GoToMyPC
  - ...

# RA Policy
## slide 3 of 1000000000

- Provisions for WebEx and the like
  - A badged Fermi user must negotiate with the connecting party a non-reoccurring time for the connection.
  - A badged Fermi user must be manually authorize the WebEx connection at time of initiation, and must remain present during the WebEx activites.
  - Any passwords that are created or changed by a non badged WebEx user must immediately be changed and not communicated back to the non-badged user after the WebEx session has ended.
  - Deviations from the above (such as reoccurring or unattended WebEx sessions) require an exemption.

slides 4 to 999999999 were just a bunch of pictures of Joe's house we took over Xmas

Probably irrelevant for this meeting...

# RA Policy

## slide 1000000000 of 1000000000

- RA Policy

**cd-docdb # 2336**

- RA Technical Details (meat and potatoes)

**cd-docdb # 2360**

It's not easy being green...

...and having no limbs

time for Joe

# wait, in before Joe!

- Reminders
  1. basic auth with local password store is bad
  2. basic auth over non-https is worse
  3. Please reboot your Windows boxes to clear your credential cache
  4. Please keep your hands and arms inside the cars at all times (don't be like the frogs)
  5. Please don't go opening attachments or clicking links willy-nilly

# Cool Thing : andlinux

# What is it?

- Software stack
  - coLinux
  - Xming
  - Ubuntu
  - PulseAudio
- Use linux apps in Windows
  - kate, rhythmbox, mplayer, nedit, whatever
  - Install new apps with apt

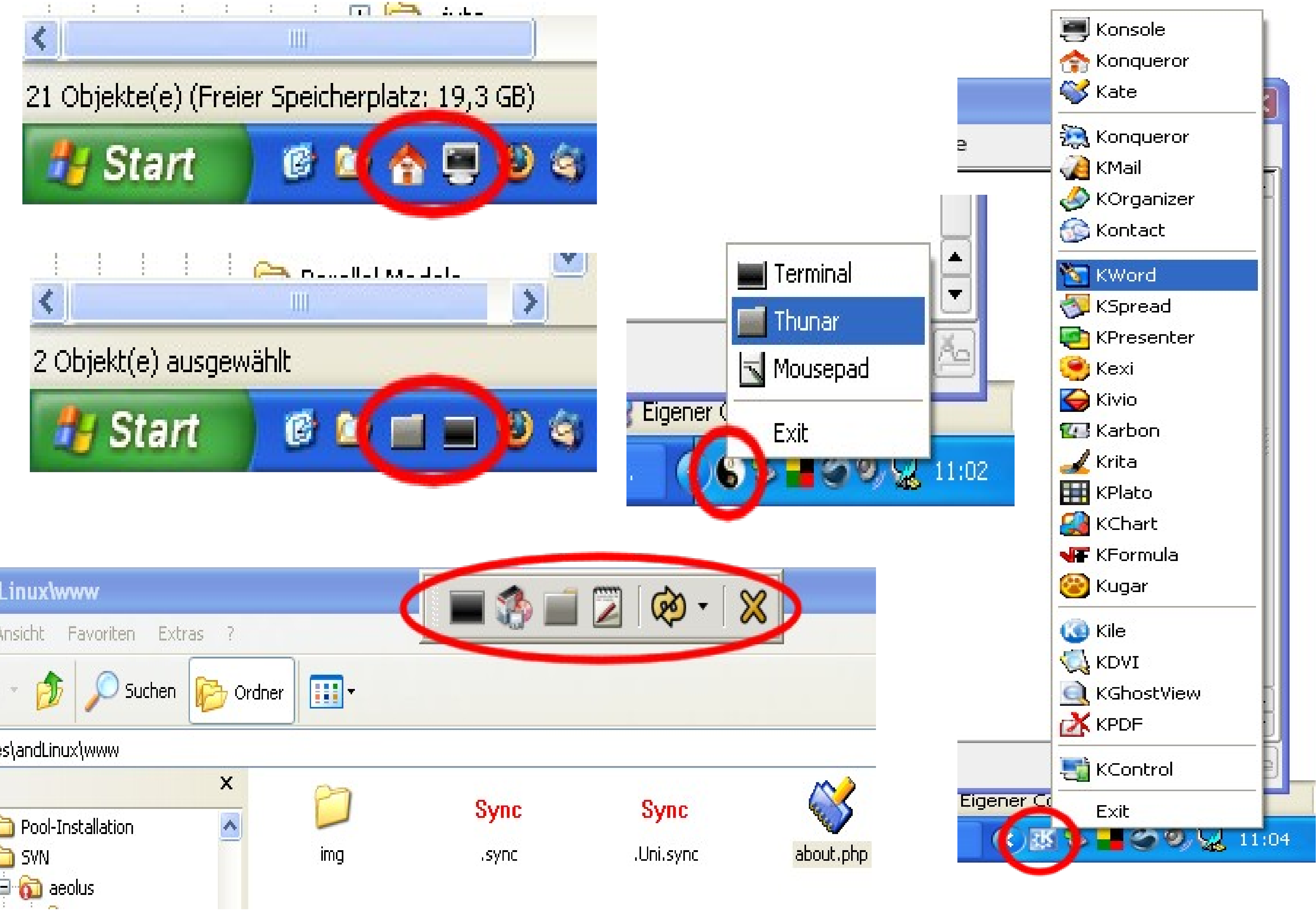
# Why use it?

- One way to skip around Reflection and cygwin but get similar (better?) functionality
- Sandbox for running applications
- Use linux apps without rebooting into linux
- Integrates apps into the Windows shell

# If you install it

- Remove '-ac' from the run shortcut
- Use X0.host file to restrict who can connect to Xming
- Firewall off port 6000 to localhost or face the wrath of the “port 6000 exposed” email generator

- In a nutshell you're restricting Xserver access to “you and only you, so help you CST”



21 Objekte(e) (Freier Speicherplatz: 19,3 GB)

2 Objekt(e) ausgewählt