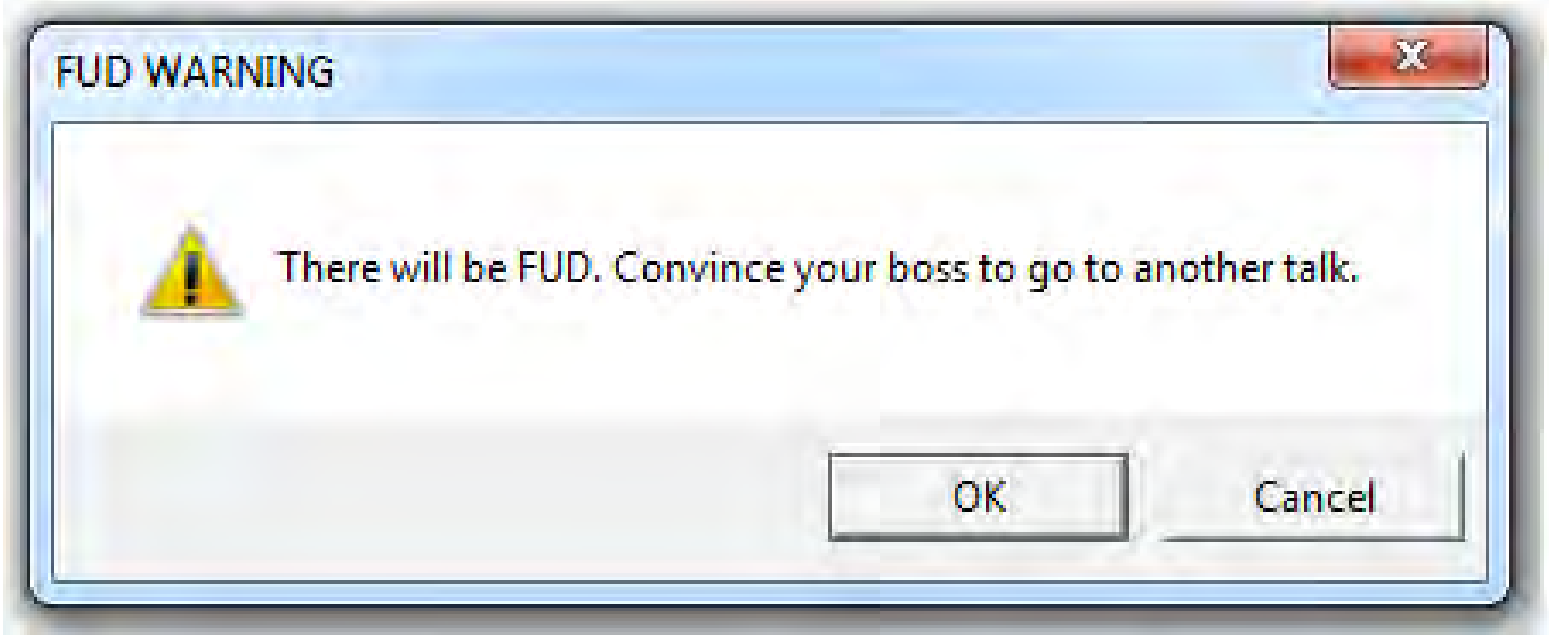
THE SECRET LIFE OF KRBTGT

DISOBEY
DEFCON

Bio

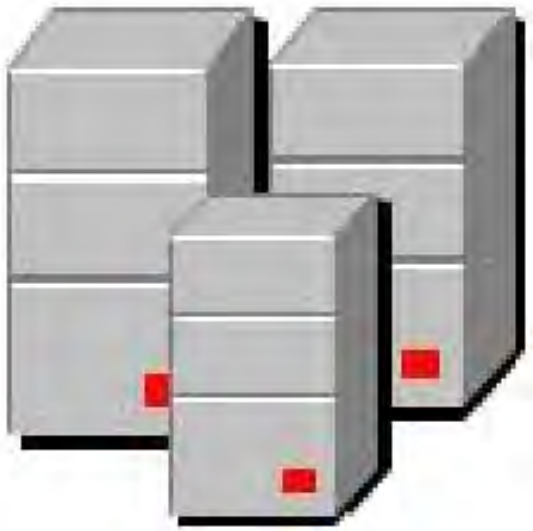
- Security Researcher/Tester (Harris Corp)
- Former Army Red Team Operator
- One of the developers of PowerSploit
- Twitter: @obscuresec
- Blog: www.obscuresec.com


FUD WARNING
There will be FUD. Convince your boss to go to another talk.
OK
Cancel

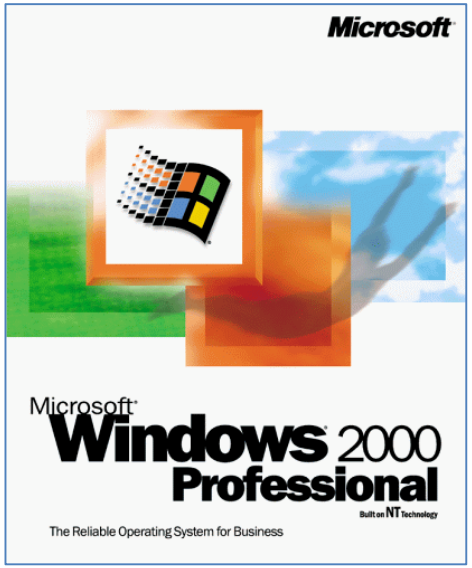

DISOBEY
DEFCON

Say hello to krbtgt

He’s been here since the beginning



The Early Years: 2001-2004




```
/*
  DCOM RPC Overflow Discovered by LSD
   -> http://www.lsd-pl.net/files/get?WINDOWS/win32_dcom

  Based on FlashSky/Benjurry's Code
   -> http://www.xfocus.org/documents/200307/2.html

  Written by H D Moore <hdm [at] metasploit.com>
   -> http://www.metasploit.com/

  - Usage: ./dcom <Target ID> <Target IP>
  - Targets:
  -          0    Windows 2000 SP0 (english)
  -          1    Windows 2000 SP1 (english)
  -          2    Windows 2000 SP2 (english)
  -          3    Windows 2000 SP3 (english)
  -          4    Windows 2000 SP4 (english)
  -          5    Windows XP SP0 (english)
  -          6    Windows XP SP1 (english)

*/
```

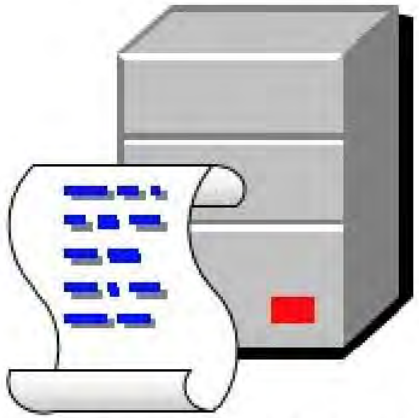
DISOBEY
DEFCON

Growing Pains: 2005-2008

DISOBEY
DEFCON

Maturity Realized: 2009-2012

Windows Server 2008



Group Policy Preferences

DISOBEY
DEFCON

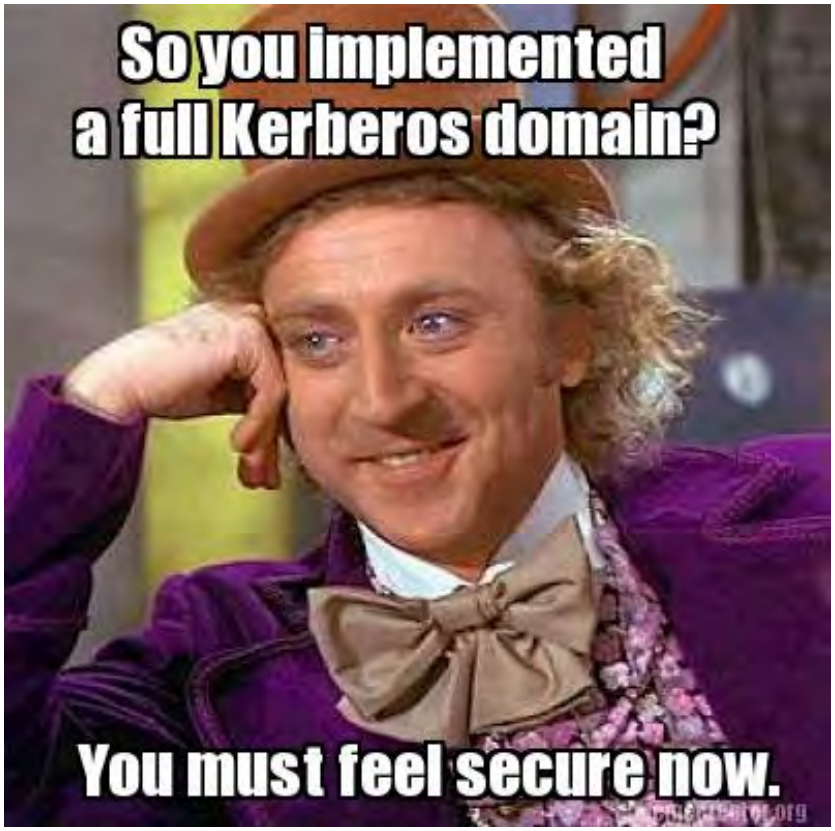
Meme Count: 1


WE PREVENT ADMIN ACCOUNT ABUSE
WITH GROUP POLICY PREFERENCES

Skeletons in the Closet: 2013-2014

Windows Server 2012

Meme Count: 2



http://blog.gentilkiwi.com/securite/mimikatz/golden-ticket-kerberos

How old is your krbtgt hash?

Know where your krbtgt hash is?

RAW Paste Data

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:67f89191aee12099ec7a754de34fc287:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:52a6a5b7d2003afedf59f8848a54ea2c:::
carrie:1105:aad3b435b51404eeaad3b435b51404ee:5053e7c659a614ce46d99dcfb8d9763a:::
brett:1106:aad3b435b51404eeaad3b435b51404ee:8fdecf063cdac5d8407c5b1a75826fad:::
niky:1107:aad3b435b51404eeaad3b435b51404ee:ef00760ac292f0e8da9ca1850ee5be2f:::
kevin:1108:aad3b435b51404eeaad3b435b51404ee:5052340fe27eb55317e38a7876480b18:::
sean:1109:aad3b435b51404eeaad3b435b51404ee:ad0c54ced11a55168eef0429775b1f7e:::
nina:1110:aad3b435b51404eeaad3b435b51404ee:d22d7dfc2fb717d7663b47131b1e2347:::
cory:1111:aad3b435b51404eeaad3b435b51404ee:5053e7c659a614ce46d99dcfb8d9763a:::
jeff:1112:aad3b435b51404eeaad3b435b51404ee:b180be38c6c29a74431c966e57e4a7d8:::
joe:1113:aad3b435b51404eeaad3b435b51404ee:e50be861156e77e57e7247b3edc1d9b6:::
```

The point is…

If your enterprise has ever been compromised, it may still be compromised – even if you changed every password.

We scan so we are secure

Good luck with that

Meme Count: 3

XXX

DISOBEY
DEFCON

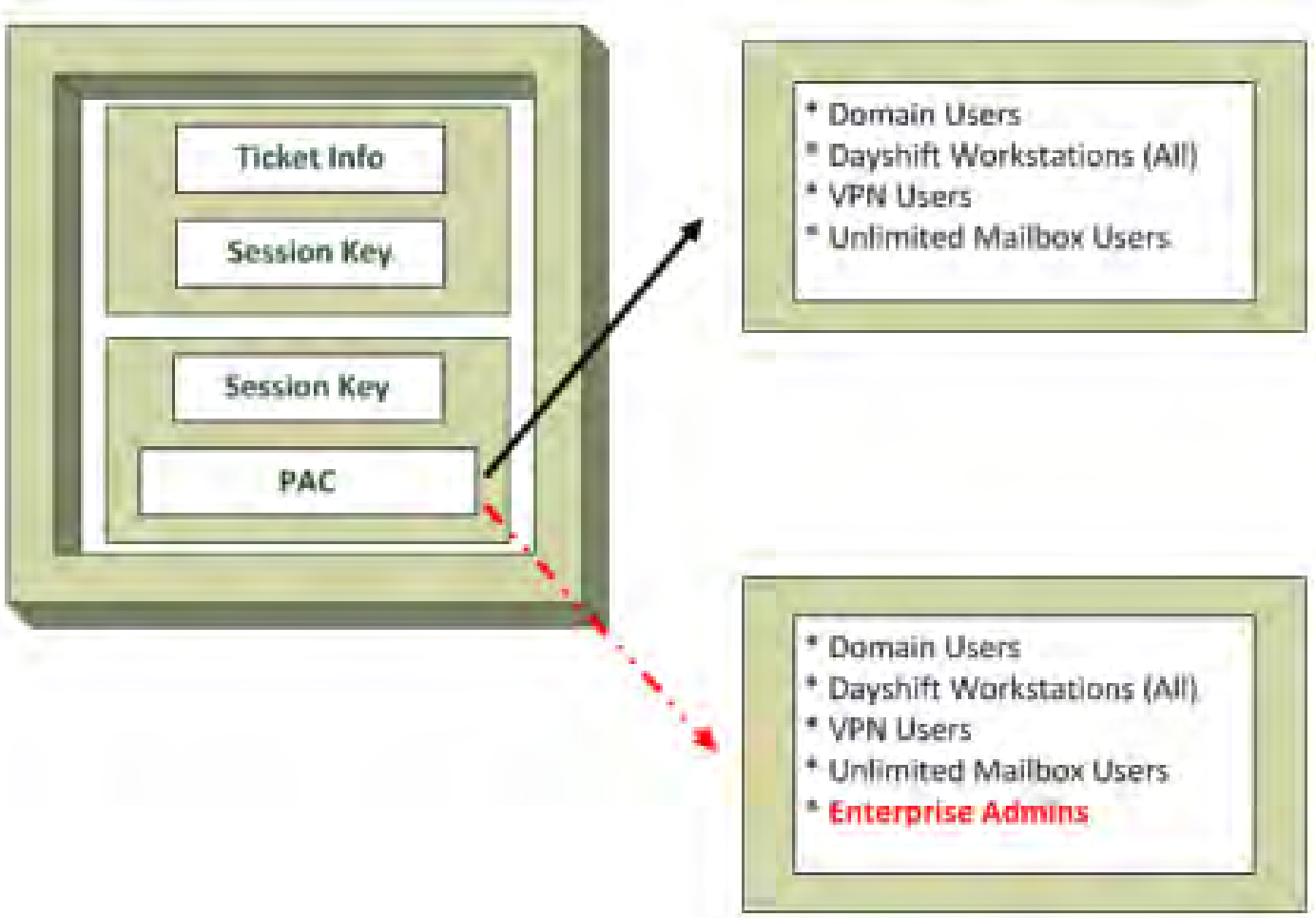
Kerberos Authentication

AS

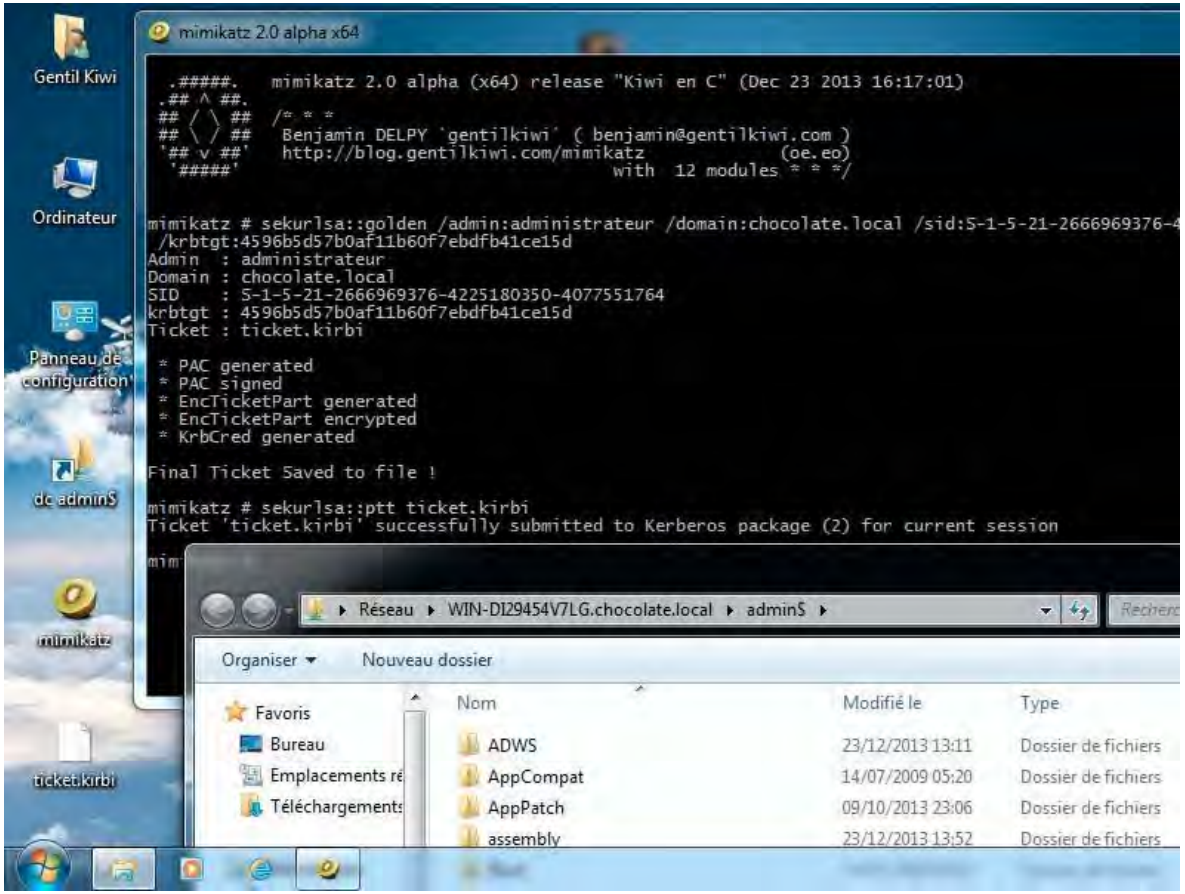
TGS

1. TGT requested by client
2. AS sends TGT and session key
3. Client requests access from TGS
4. TGS sends encrypted session key & ticket
5. Client sends service ticket to server
6. Server sends time stamp for client to verify

“Spoofed PAC” Attack



“Golden Ticket” Attack

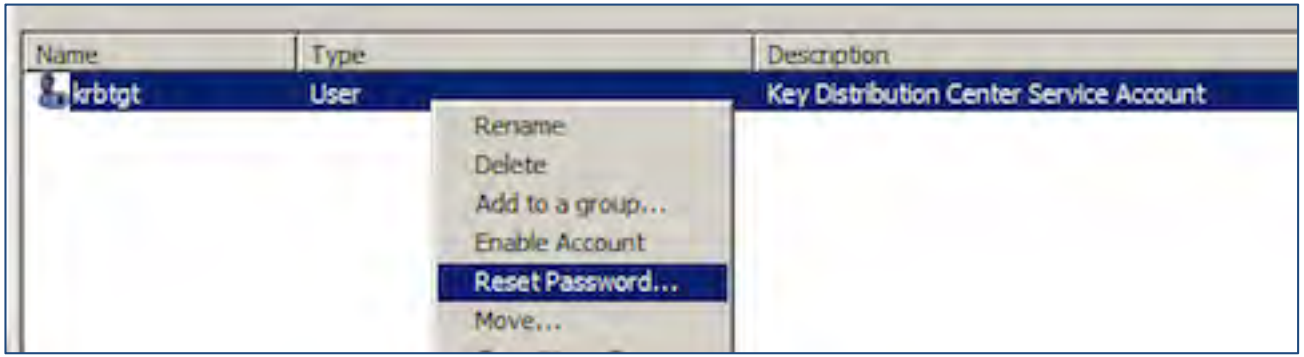


https://twitter.com/gentilkiwi/status/415147415474167808

Demo Time

Mitigation

- Don’t get owned again
- Use RODC where appropriate
- Upgrade functional level
- Reset the krbtgt account password on the PDC-emulator **TWICE**



Detection

- Needle in a hay stack
- Harder to detect than PtH
- Look for strange account activity
  - Low privileged account performing privileged actions

Thanks

- Skip Duckwall
- Benjamin Delpy
- Joe Bialek
- Will Peteroy
- Carlos Spicyweiner
- Matt Graeber
- Many others…

Questions?