Светлината в края на тунела е влак

Васил Колев
vasil@ludost.net

Други заглавия

- We're fucked
- What's wrong with you, people?
- Толкова ли сме тъпи?
- Спасението на давещите се е в ръцете на самите давещи се
- Защо на нас?
- Denial is not a river in egypt
- Не сме депресирани, наистина е толкова зле

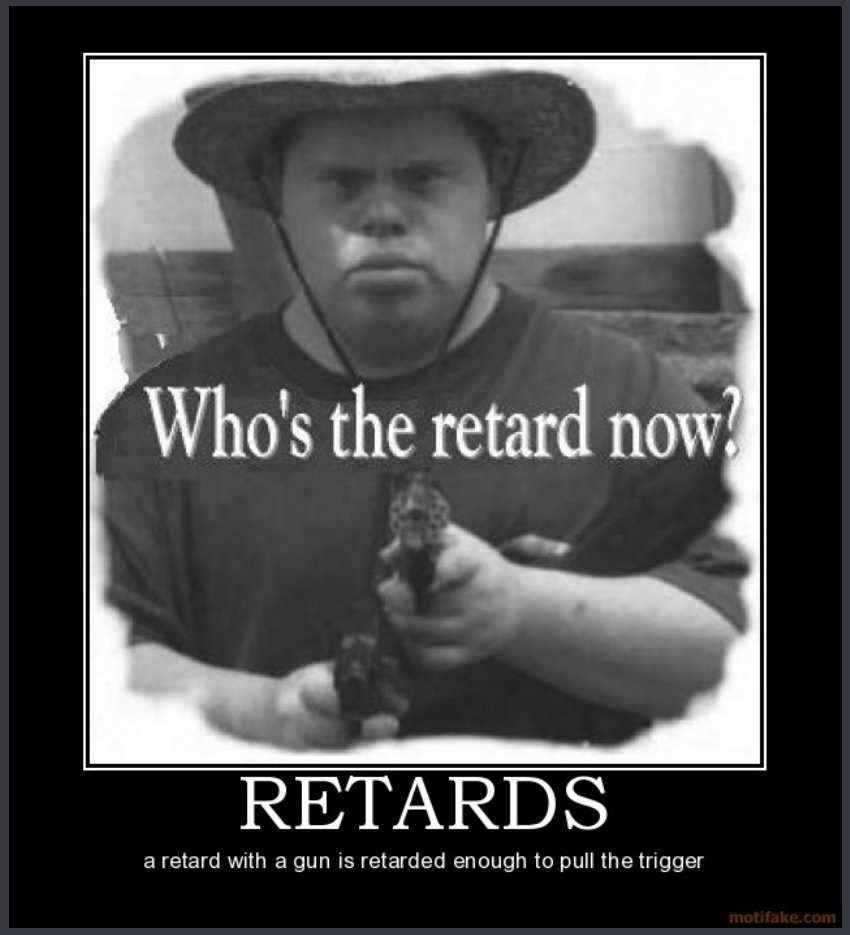
Колко вярвате?

- На софтуера?
- На хардуера?
- На „праворазраващите“ органи?
- На управляващите?
- На „облака“?

Текуща ситуация 1/X

- Целият internet се слуша
  - По тривиален начин
- Edward Snowden и NSA
- ... и как 5м човека имат допуск близо до тая информация
- http://getprsm.com/

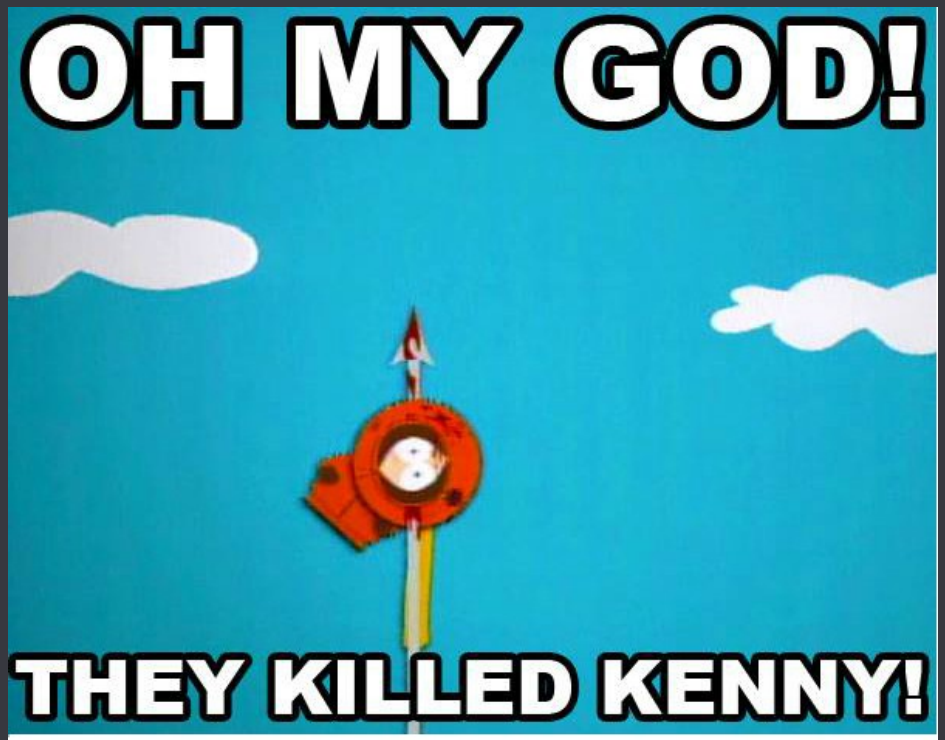
„Органите“

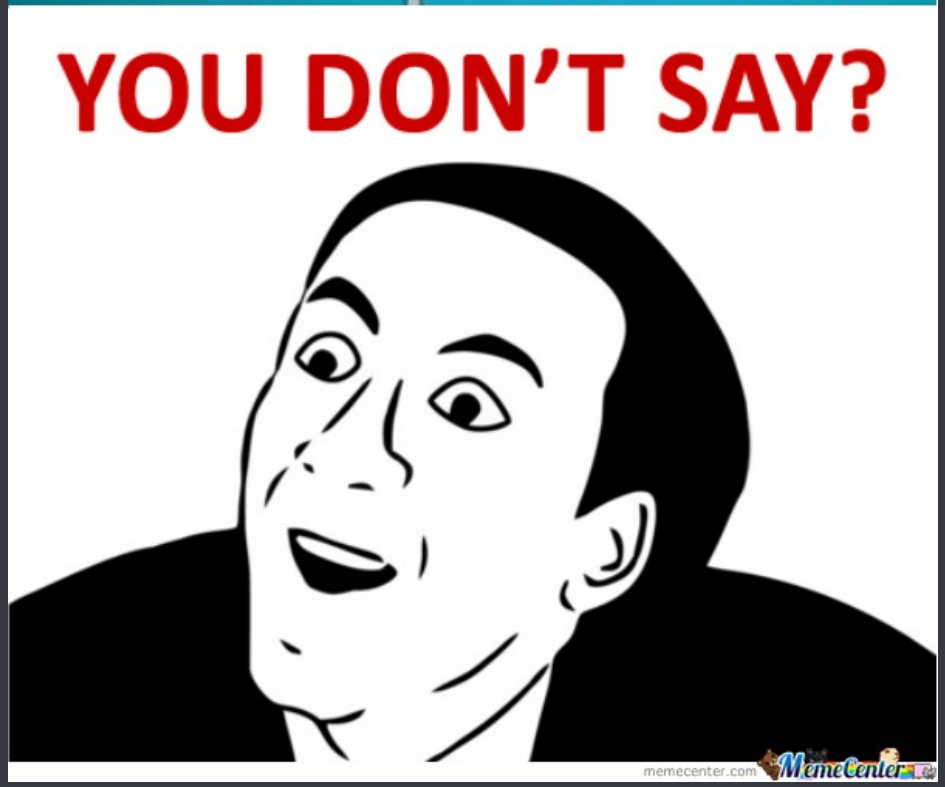


- Които борят leak-овете с уволняване на 90% от системните си администратори
- Които не си пускат криптографията за радиостанциите
- И т.н...

Текуща ситуация - облаци

- Хората, които направиха PRISM възможен
- Постоянно им се чупи нещо
- Постоянно затварят използвана услуга
- ... а ние сме като болни от Алцхаймер в публичен дом
- Google: reader, code search, talk, sms, wave cloud connect
  - http://www.wordstream.com/articles/retired-google-proje
- Реакцията винаги е същата:


OH MY GOD!
THEY KILLED KENNY!


YOU DON'T SAY?
memecenter.com
MemeCenter

Текуща ситуация - gsm

- Плащаме луди пари, за да разнасяме със себе си по няколко проследяващи устройства
- GSM-ът е счупен:
  - A5/1 е лесен, A5/0 и A5/2 са счупени отдавна, за A5/3 е известен начинът
  - Атаката в/у SIM картите
  - Brick-ване/забиване на телефони
  - Разни exploit-и
- Затворена, стара, недомислена система

Текуща ситуация - CA

- Знаете ли на кого вярва browser-ът ви?
- Редовно чупене на CA-та
  - Diginotar, startssl, comodo, verisign, ...
- CA-та, притежавани от кофти правителства
- Атаката в Иран за MITM на gmail
- Няма разлика в тежестта на CA-тата
- Https everywhere/SSL observatory се опитват да решат проблема
  - Колко от вас ги имат инсталирани?

Ето така почвам да звуча...

Текуща ситуация - OS-ове

- Windows и „NSAKEY“
- Практически невъзможно да се провери closed-source операционна система
- Случайно да вярвате на macosx?
  - Защо?

Текуща ситуация - хардуер

- Скоро ще почна да звуча като луд, но:
  - http://www.cl.cam.ac.uk/~sps32/sec_news.html#Assura
- Няма начин да проверим хардуера
- Повечето се прави в Китай
- Колко точно вярваме на китайците?

Текуща ситуация - математика

- Квантовите компютри чукат на вратата
- Освен ECC и RSA нямаме други използвани public-key алгоритми
- Атаките бавно и спокойно стават по-добри
- Все още е много трудно да се пише правилно криптография
  - Side-channel атаки, диференциален криптоанализ, related-keys атаки, ...

И какво да направим?

- Да си запушим ушите и да викаме „ляляляляляля“?
  - Ако ви харесва идеята, моля правете го някъде отвън

Неща за правене - hosting

- Всеки може да инсталира ubuntu server
- Colocation-а не е скъп
- SMTP/IMAP в/у SSL
- Jabber, IRC
- Всякакъв web
- Storage
- Каквото си искате

HTTPS до дупка

- Вече имаме достатъчно процесорна мощност
- Има начин да го подкараме както трябва
  - PFS, TLS1.2
  - SSL observatory
- DANE/DNSSEC

Лична криптография

- PGP
- OTR
- Full disk encryption
- It's about sending a message

... и леко политическо

- Можем много
- Правим малко
- Таксиметровите шофьори са по-голяма сила от нас

Проекти за мислене

- Слушане на GSM-и (тривиално е)
- 3d печат на интересни неща
  - Ключове за белезници
  - Оръжия
- Системи за изтичане на документи
- Образоване на хора
- Историята на Митьо

Вашата работа

- В България има огромен глад за IT хора
- Никой не ви кара да работите за
  - Идиоти
  - Мафиоти
  - Телекоми
  - Държавната администрация
  - Продажни медии

Финални думи

- Четете
- Мислете
- Не е ясно дали имаме шанс, но е ясно, че да се предадем сега би било тъпо.

Въпроси?

Благодаря за вниманието!