securing a client

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

hardening a host

Hardening a host

- Differs per operating system
  - Windows: users can not be trusted to make security related decisions in almost all cases
  - OS X : make things work magically for users. Try to handle security issues in the background
  - Linux: varies by distribution:
    - Ubuntu: try like OS X to make things just work.
    - RedHat: include very useful tools but turned off by default
  - BSD: users will figure it out
- Changes with time

General consideration

- Define a personal usage profile and policy.
  - What hardware do you use?
  - What software tasks do you do on your computer?
  - Do the first two change when you travel?
  - What habits from the above two do you need to change to be more secure?
  - Decide if you *really* need VPN access to your network while travelling.

General practices

- Install only the services and software you actually need.
  - Uninstall or disable all software and services you do not use or need.
  - Periodically actively scan your machine for vulnerabilities.
  - Have as few user accounts on your systems as possible
- Protect your administrative account. Have a strong password, do not permit remote password based logins and do not log in as an administrator unless you need to do an administrative task.

Hardware

- Rule 1: all bets are off with physical access to your devices.
- Consider removing hardware you never use – say bluetooth.
- Disable in BIOS or EFI or your operating system the hardware or features you can not remove physically.
  - wake on lan
  - Bluetooth discoverability
  - USB ports?
- BIOS passwords not that useful
- BIOS level encryp8on/locking of hard disks may not be portable

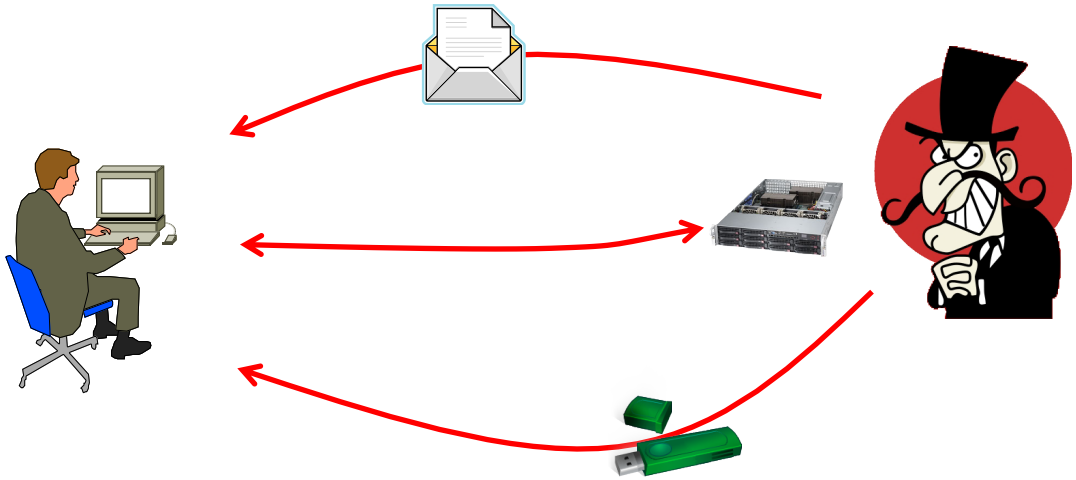
anti virus

Malware

- The generic term for computer virus, worms, spyware and other malicious software
- Skilled attacker can make it, fun attacker can use it.
  - even there are malware build tools with GUI ☹

Infection

- attackers try to make your devices infected in many ways
  - security holes, e-mail, web
  - USB memory, file servers



Causes

- vulnerability
  - 0-day security holes
  - old security holes are still used to infect
- auto-execution for removal media
  - USB memory, CD loading
- users’ careless open
  - infected files
  - sometimes happen to execute malwares

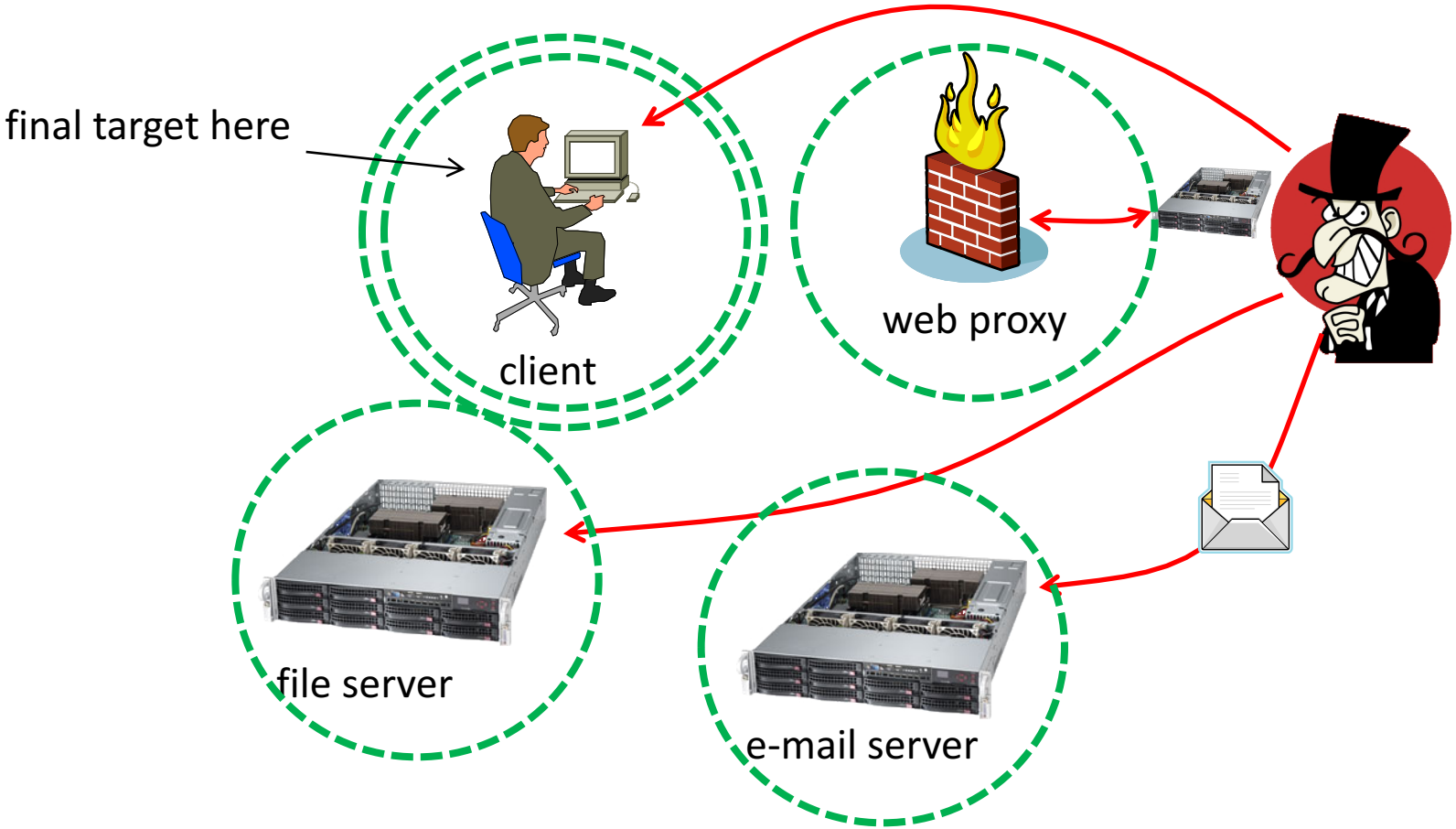
Detection

- signature-based detection
  - blacklist of malwares
  - check a file with the signatures
  - update needed to detect newer malware
- heuristics detection
  - behavior, characteristic code

When?

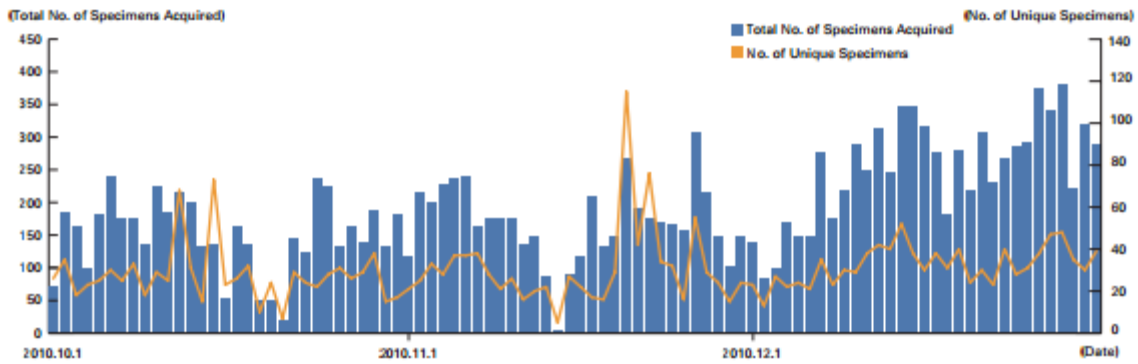
- write operations take place
  - creating a new file, modifying an existing file
- new media is inserted
  - USB memory, CD
- periodic or manually
  - scan all or important files

Where?


final target here
client
web proxy
file server
e-mail server

Hiding

- attackers modify malwares
  - not to be detected by anti-virus detectors
  - they can check this locally

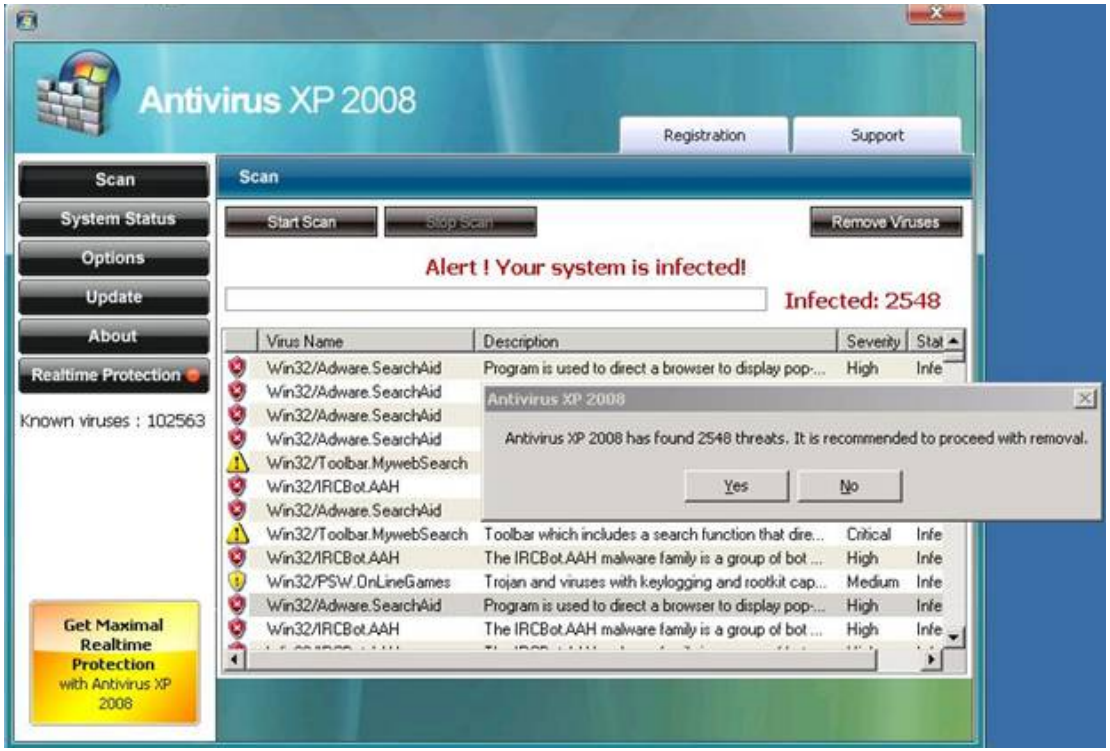


Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

- updating your signature DB is needed

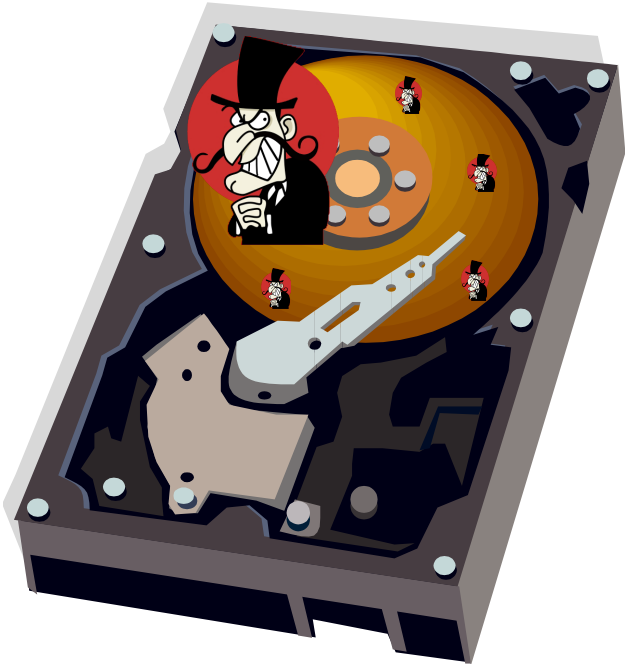
Fake security software

- Do nothing, or is just a malware
  - also known as ‘scareware’



Compromised system

- Any file on the system is already suspicious
  - You may be able to remove a malware
  - there could be another one that you can not detect



Wipe

- Don’t use files in the compromised system
  - programs
  - documents
  - images
- Clean up the storages that was connected to the system
  - HDD
  - SSD
  - flash memory

How can we rescue information from suspicious data files

- convert it into another format
  - png -> jpg, jpg -> png
  - doc -> txt
  - excel -> csv
  - pdf -> png/jpg

- infected code can not survive such a drastic modification

Wipe to give away

- data is still there even if it’s formatted
  - experts can read the data by using special tools
  - an electric microscope can read more
  - leakage of secret data
- you need to make sure the data is erased
  - # dd if=/dev/urandom of=/dev/<disk> bs=16M

Recover

- ‘clean install’ from a scratch
  - format the disk, use a proper OS image
- apply latest OS patches to be up-to-date
  - it could be vulnerable before patched
  - do update in a secure network
- install needed applications
  - check upgrades, of course

Recover (cont.)

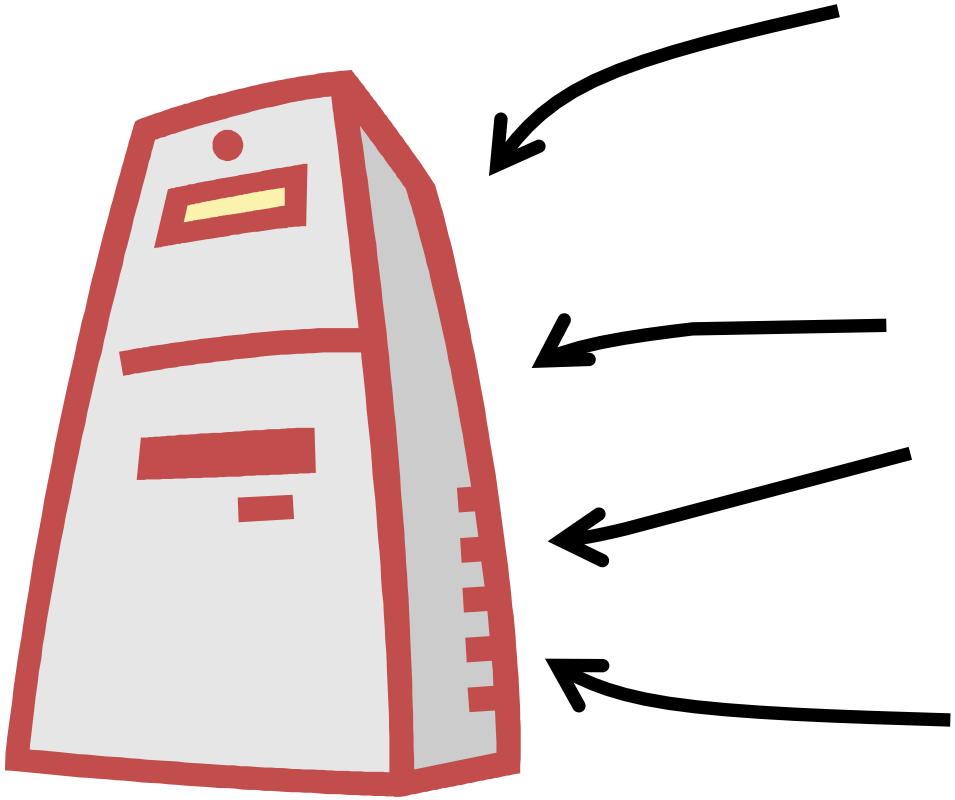
- disable unnecessary services
  - the same as hardening procedure
- check configurations
  - if any weakness
- change all password on the system
  - any password might be stolen

Replacing might be your choice

- securing the compromised system as is
  - for further investigation
  - malware that stays in the memory only
- just replace the compromised system
  - spare hardware

Backups

- Encryption
- Automation
- Generations



Encryption

- Assume theft and lost
- Your backups must have at minimum the same encryption level as the source data

Automation

- We are lazy!
  - easy to forget
- automated backup will help you
  - most systems have scheduled backup

Generations

- you shoud have a ‘good’ version of backup there
  - if a system is compromised, malware might be also backup in the archive, you won’t want to restore that though
  - if something goes wrong by change, you may restore the previous version
- find a ‘good’ version from your archives

Off-site archives

- 2011 Tohoku earthquake and tsunami
  - flushed buildings, data centers
  - 4 local governments lost whole data on the family registration system
- They have off-site backups ☺
  - took about 1 month to recover though
  - wanted to make sure nothing is missed

e-mails

The key points

- Authenticity of Servers
- Encrypted Transport

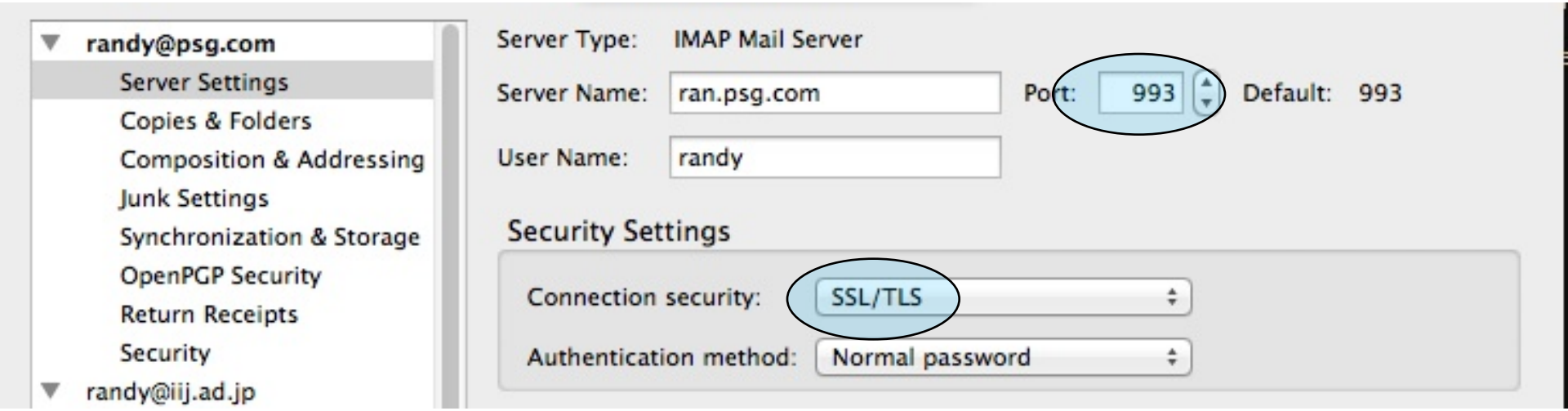
It’s easy

- Do not use pop, it is in the clear
- Use pop3s, port 995 over TLS

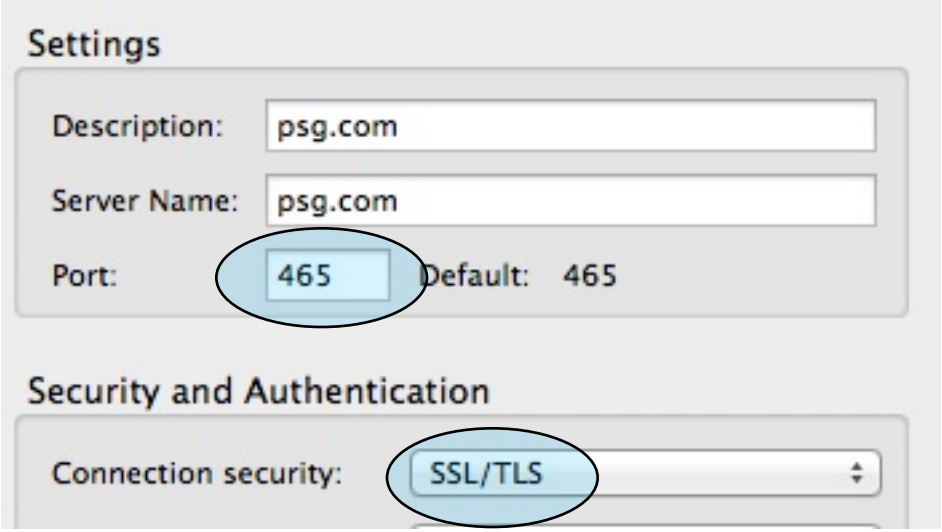
- Do not use imap, it is in the clear
- Use imap4s, port 993 over TLS

- And they Authenticate the Servers using X.509 Certificates. CHECK IT!

fetch using IMAP4S



SMTP over TLS



Authenticate Servers

- Assume the Wire is Tapped
- Assume Someone will Spoof Servers
- Know Your Servers' Root Certificates
- Confirm Certificates on Configuration
- Choose Good Passphrases

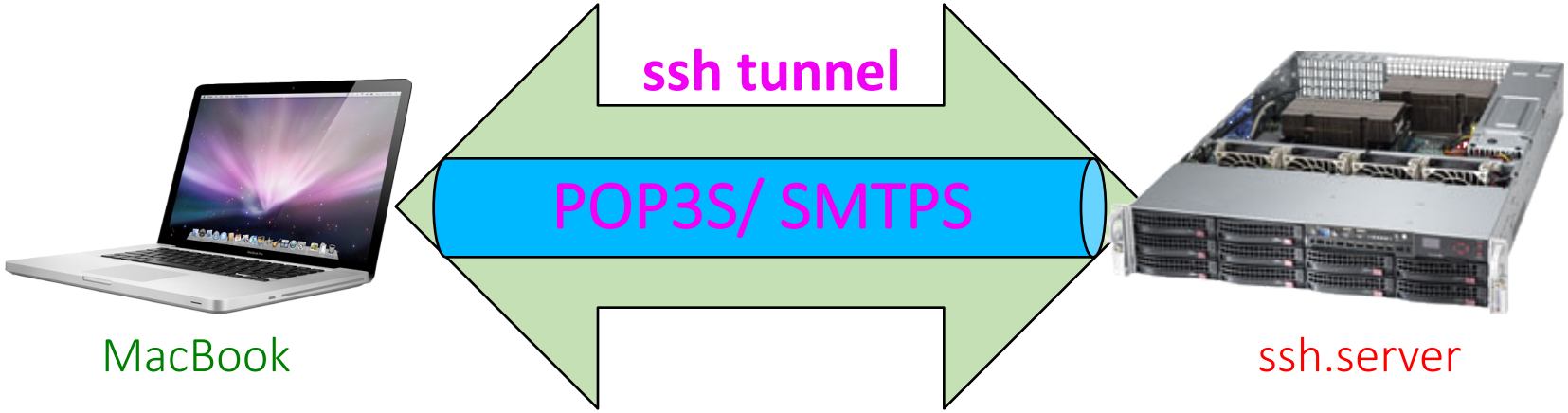
Encrypt Critical E-Mail

- Assume the Wire is Tapped
- Use a Personal X.509 PKCS#12 User Certificate with SMIME – T’Bird etc.
- Use a PGP key with Enigma – T’Bird

I tunnel & email

smtp.server

pops.server




```
$ ssh <ssh.server> -L 9955:<pops.server>:995
$ ssh <ssh.server> -L 4465:<smtp.server>:465
```

Step Host

Port on MacBook

Tunnel EndPoint

example: LocalForward

.ssh/config

```
Host mail
    HostName        <step.host>
    LocalForward    4465 <smtp.server>:465
    LocalForward    9995 <pops.server>:995
```

$ ssh mail

example: stephost

.ssh/config

```
Host stephost
    HostName        <step.host>
Host internal
    HostName        <internal.ssh.server>
    ProxyCommand    ssh -W %h:%p stephost
```

$ ssh internal

web browsing

Microsoft Internet Explore

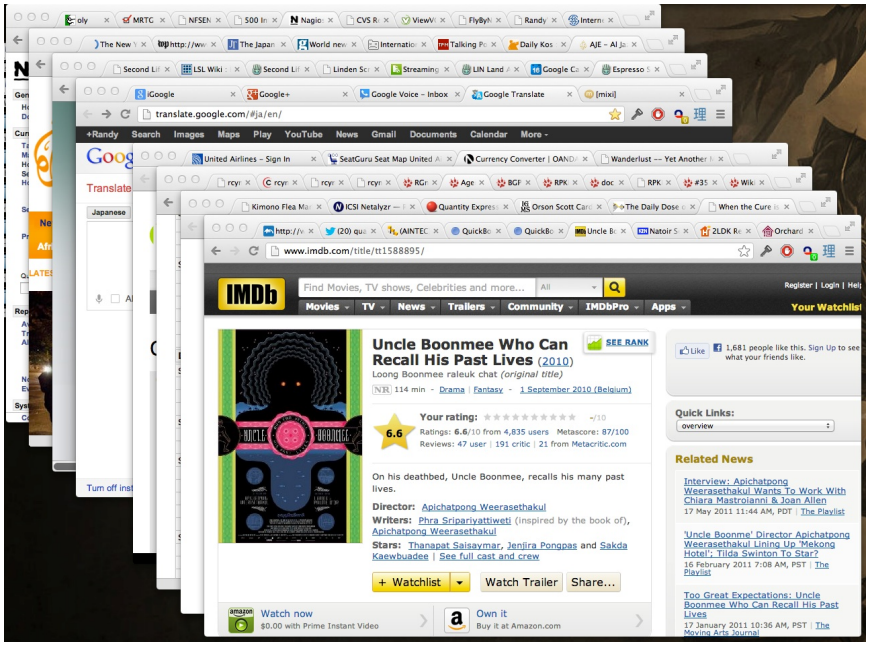
- Long History of Vulnerabilities
- First Target because of Popularity
- Microsoft is Not Always Concerned with Your Privacy
- Closed Source, No One Inspects it

Microsoft Edge

- brand-new web browser
- shipped with Windows10
- does SandBoxing, so reasonably safe

I use Google Chrome

- Process Isolation per Tab, so scales well



- But I worry about Leaking Data to Google

I also use FireFox

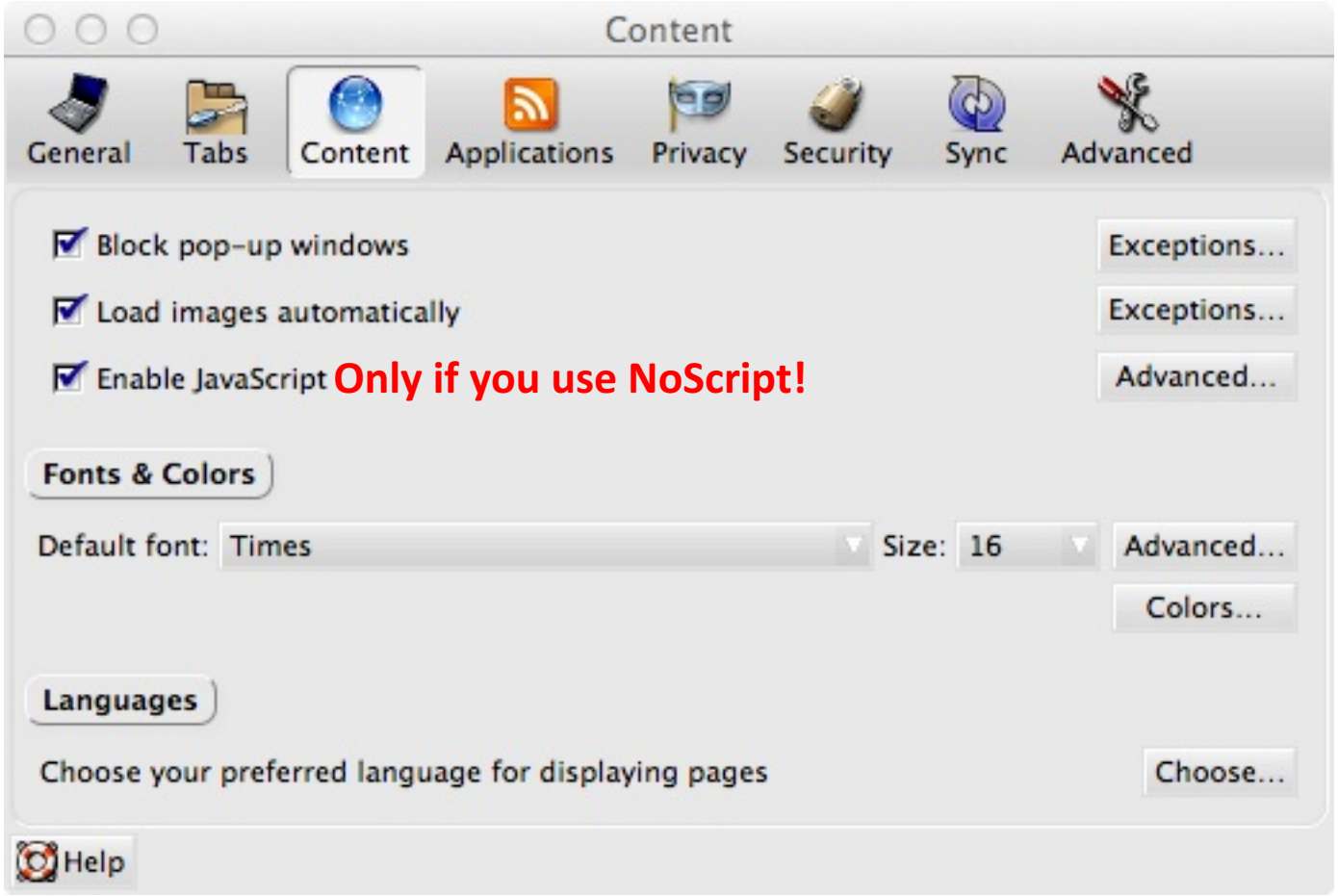
- Free and Open Source (i.e. inspected)
- Standards Compliant, no Proprietary Tricks to Lock You In
- Popular, so has Rich Extension Catalog
- Runs on All Significant Platforms

Do Not Let Browser Remember Passwords

- Lose Laptop and Lose your Bank Account
- Password Database Encryption is Weak

- recommendations
  - encrypted text file (pgp)
  - 1Password

Prefs


Content
General
Tabs
Content
Applications
Privacy
Security
Sync
Advanced
Block pop-up windows
Exceptions...
Load images automatically
Exceptions...
Enable JavaScript
Only if you use NoScript!
Advanced...
Fonts & Colors
Default font:
Times
Size:
16
Advanced...
Colors...
Languages
Choose your preferred language for displaying pages
Choose...
Help

Privacy

General | Tabs | Content | Applications | Privacy | Security | Sync | Advanced

Tracking

☑ Tell websites I do not want to be tracked **New Feature**

History

Firefox will: Remember history

Firefox will remember your browsing, download, form and search history, and keep cookies from websites you visit.

You may want to clear your recent history , or remove individual cookies .

Location Bar

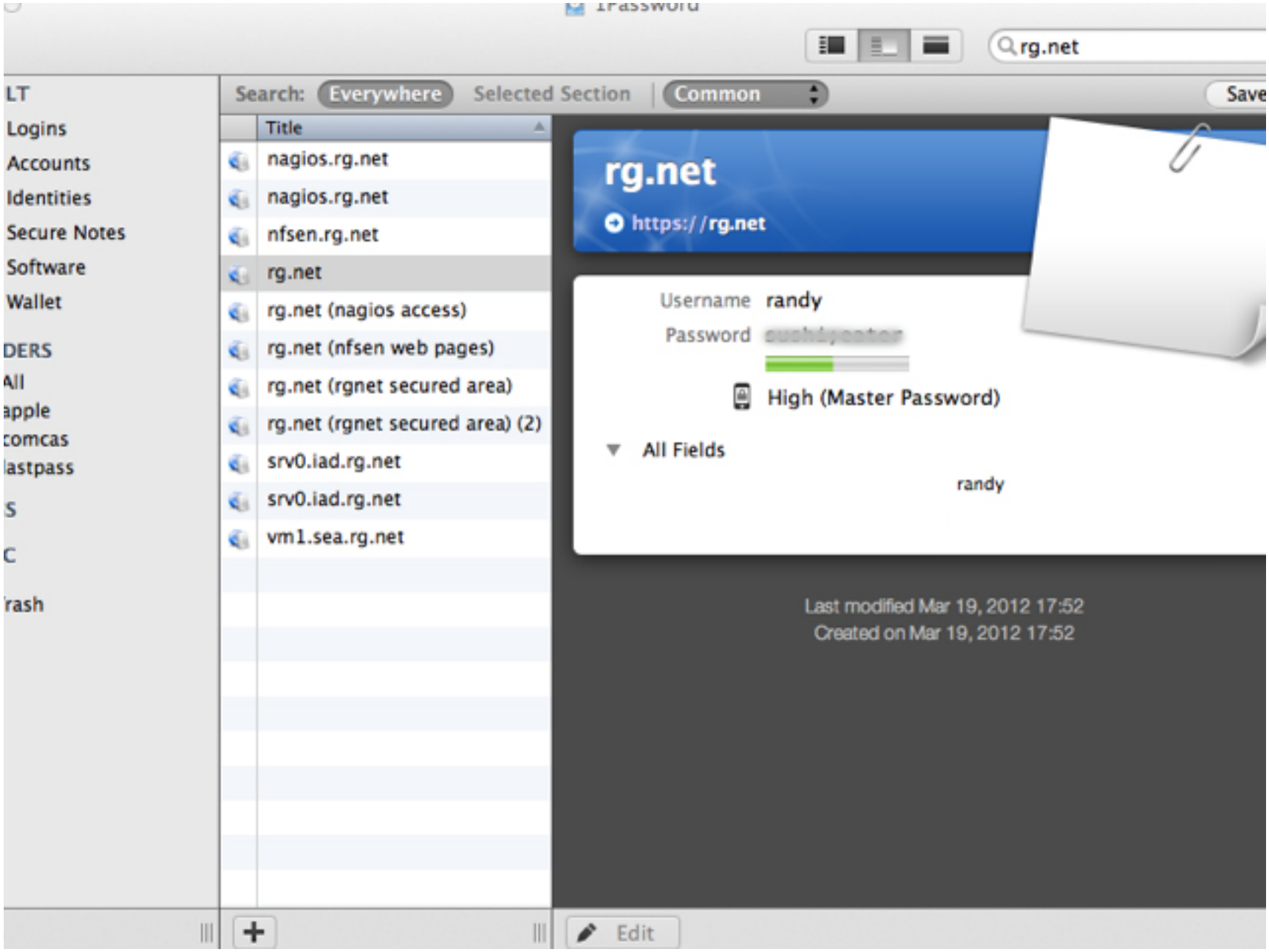
When using the location bar, suggest: History and Bookmarks

Help


Security
General
Tabs
Content
Applications
Privacy
Security
Sync
Advanced
Warn me when sites try to install add-ons
Exceptions...
Block reported attack sites
Block reported web forgeries
Passwords
Remember passwords for sites
Exceptions...
Use a master password
Change Master Password...
Saved Passwords...
Help

Plug-Ins


1Password 3.9.9
Password and identity manager for Mac, Windows, iOS and Android.
Adblock Plus 2.1.2
Ads were yesterday!
DoNotTrackPlus 2.2.1.829
Stops web tracking to protect your privacy
NoScript 2.6.1
Extra protection for your Firefox: NoScript allows JavaScript, Java (and other plugins) only...
HTTPS-Everywhere 3.0.4
Encrypt the Web! Automatically use HTTPS security on many sites.

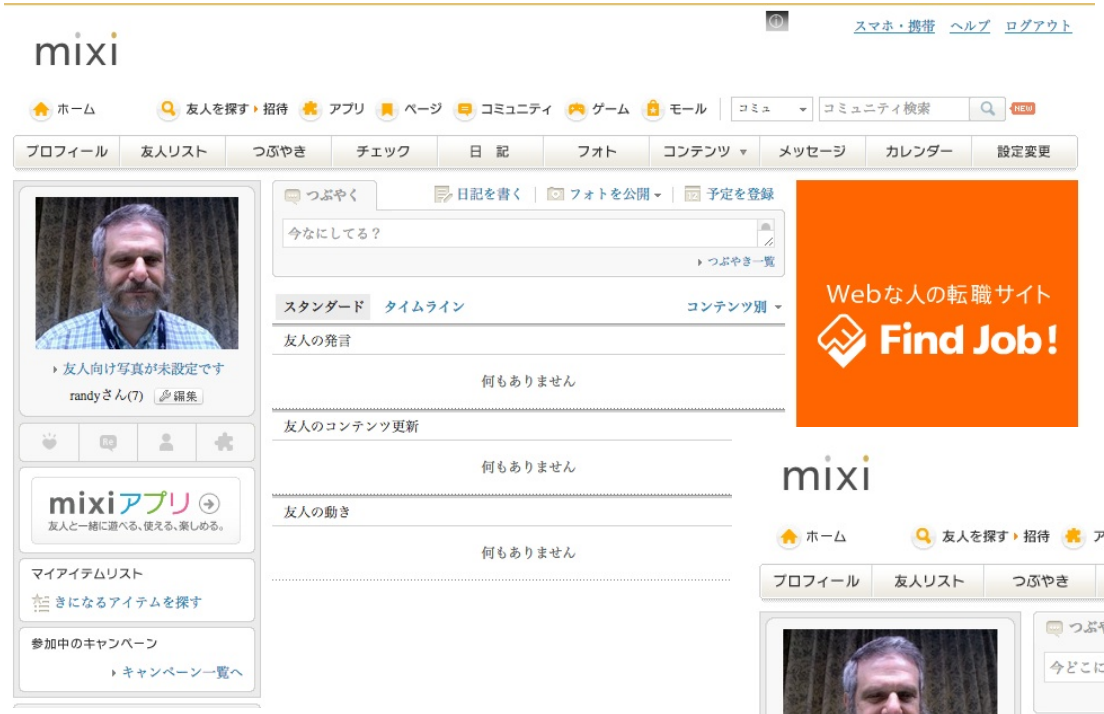

1Password
rg.net
LT
Logins
Accounts
Identities
Secure Notes
Software
Wallet
DERS
All
apple
comcas
astpass
S
C
rash
Search: Everywhere Selected Section
Common
Save
Title
nagios.rg.net
nagios.rg.net
nfsen.rg.net
rg.net
rg.net (nagios access)
rg.net (nfsen web pages)
rg.net (rgnet secured area)
rg.net (rgnet secured area) (2)
srv0.iad.rg.net
srv0.iad.rg.net
vm1.sea.rg.net
rg.net
https://rg.net
Username randy
Password
High (Master Password)
All Fields
randy
Last modified Mar 19, 2012 17:52
Created on Mar 19, 2012 17:52
Edit

1Password

- Runs on Most Platforms
- Plug-Ins for Most Browsers
- Passwords, Credit Cards, Addresses, …
- Keep DataBase in DropBox/iCloud and you have Data on Phone, Laptop, Tablet, …

- It Does Cost Money ☹

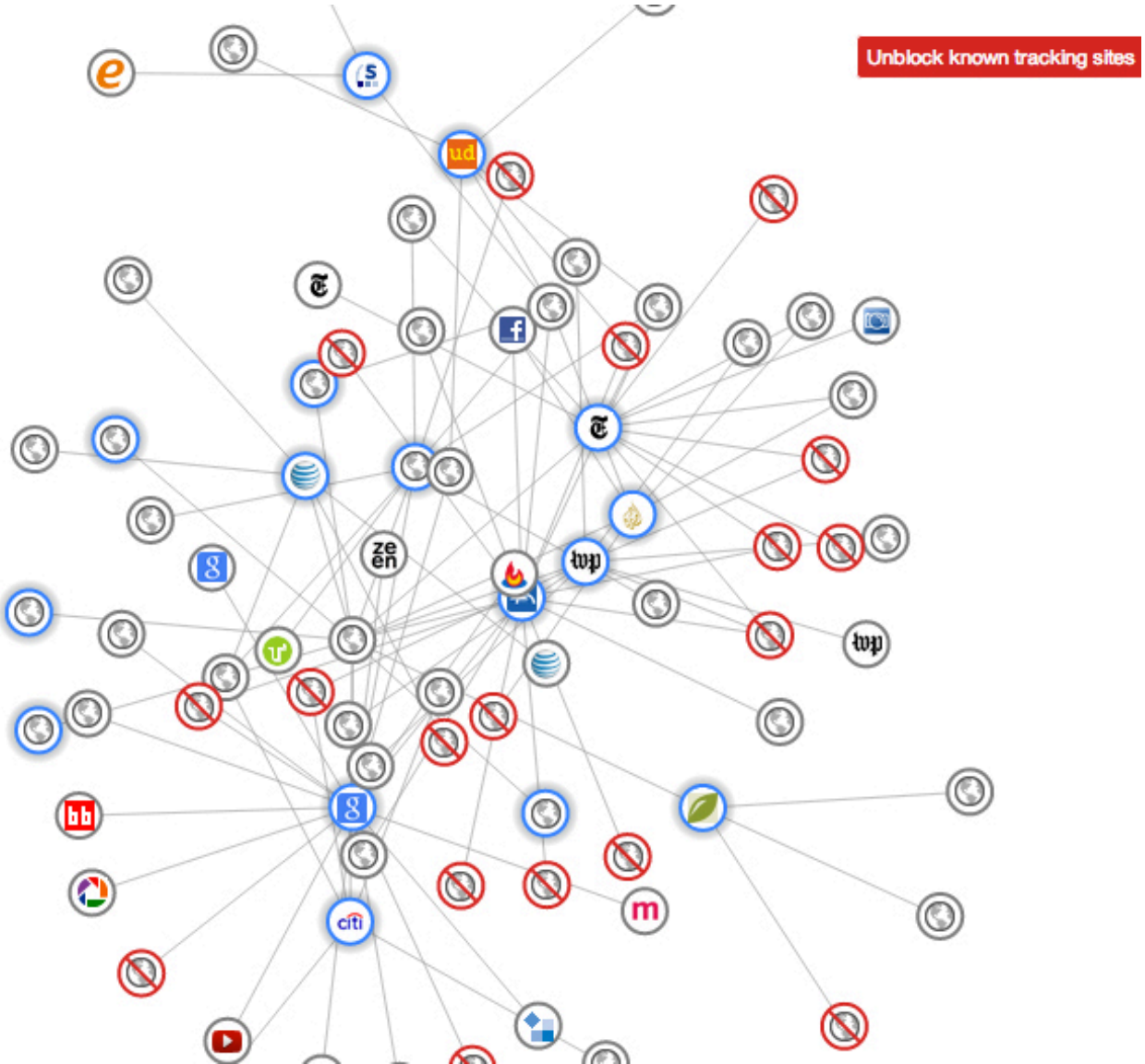
AddBlock Plus



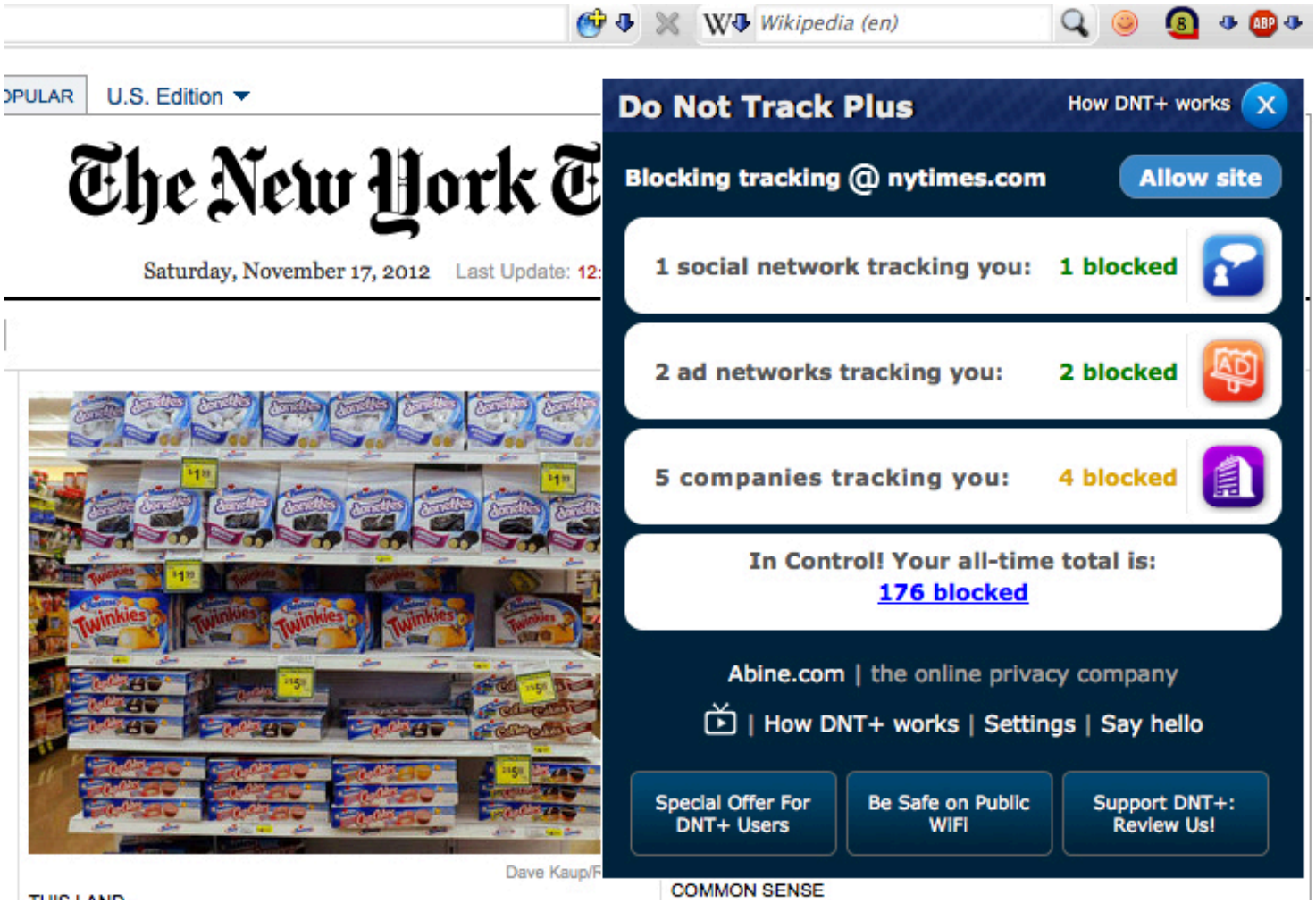
Without AddBlock

With AddBlock

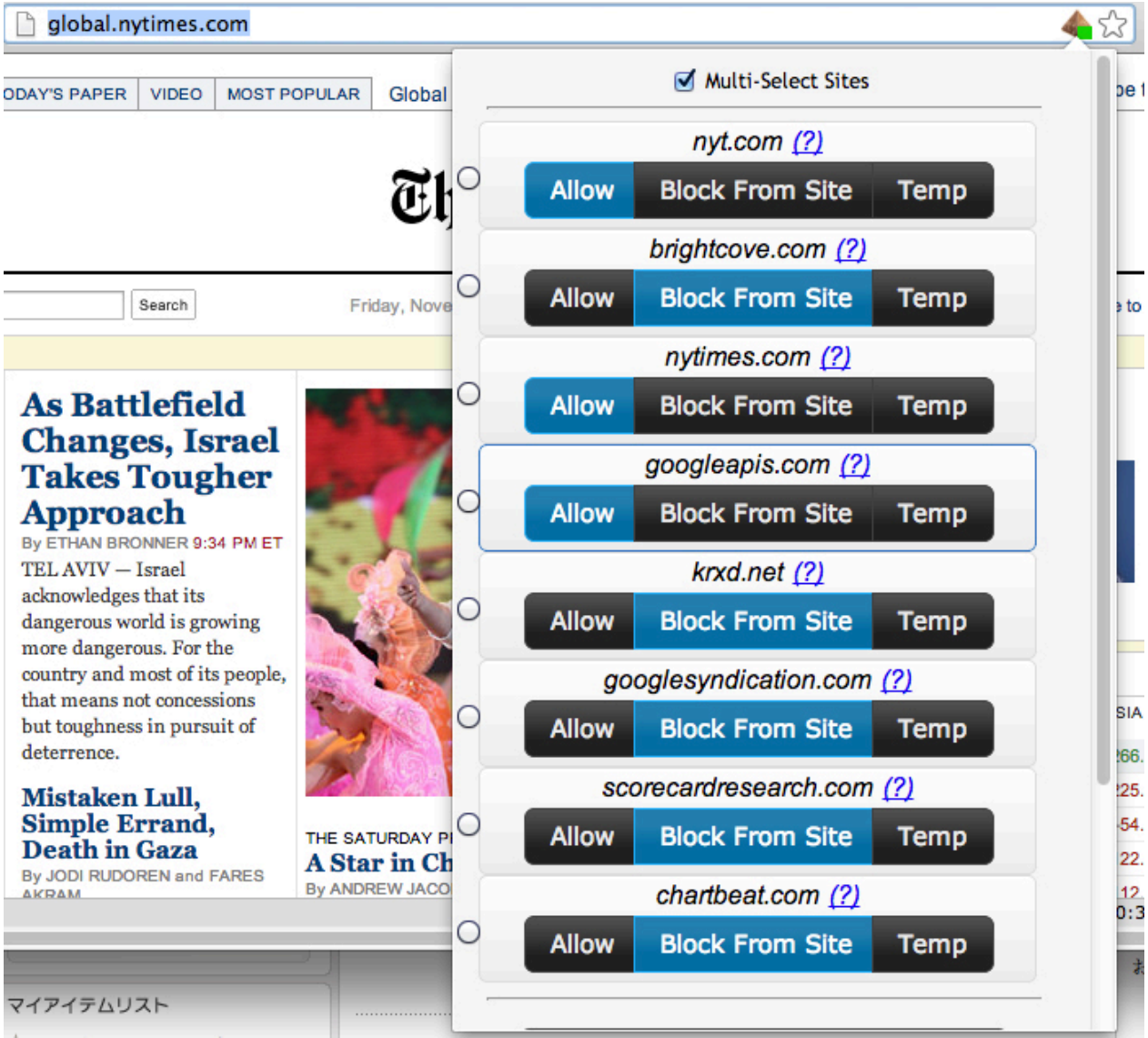
Collusion – Who Tracks



Do Not Track Plus



NoScript – JavaScript



HTTPS Everywhere

- If a Site has HTTP and HTTPS, it Forces Use of HTTPS
- I.e. You get Authentication of Site
- Your Traffic is Encrypted

Let’s do it

Root CA certificates

- Your system has root CAs by default
  - Some applications use own Certificate Store
  - Any certificates issued by these CAs are trusted

- Check it out
  - Execute ‘certmgr.msc’ on windows
  - open ’about:preferences#advanced’ on FireFox

Windows10

- Execute “compmgmt.msc” and have a look
  - disable Guest account
  - disable unused system services
- Verify the Local Security Setting
- Check the Windows Firewall Setting
- Disable hiding of file extensions
  - Start -> File Explorer -> “Change folder and search options” of “View tab” -> uncheck the “Hide extensions for known file types”