Spyware vs. Spyware

James Grimmelmann

Digital Life Seminar
November 7, 2019

In this talk

- Here is a thing
- Why the thing matters
- How to think about the thing
- What to do about the thing

Here is a thing

zoom

Zoom Meeting ID: [redacted]

Matt Haughey

Jonathan

Rob

brendan

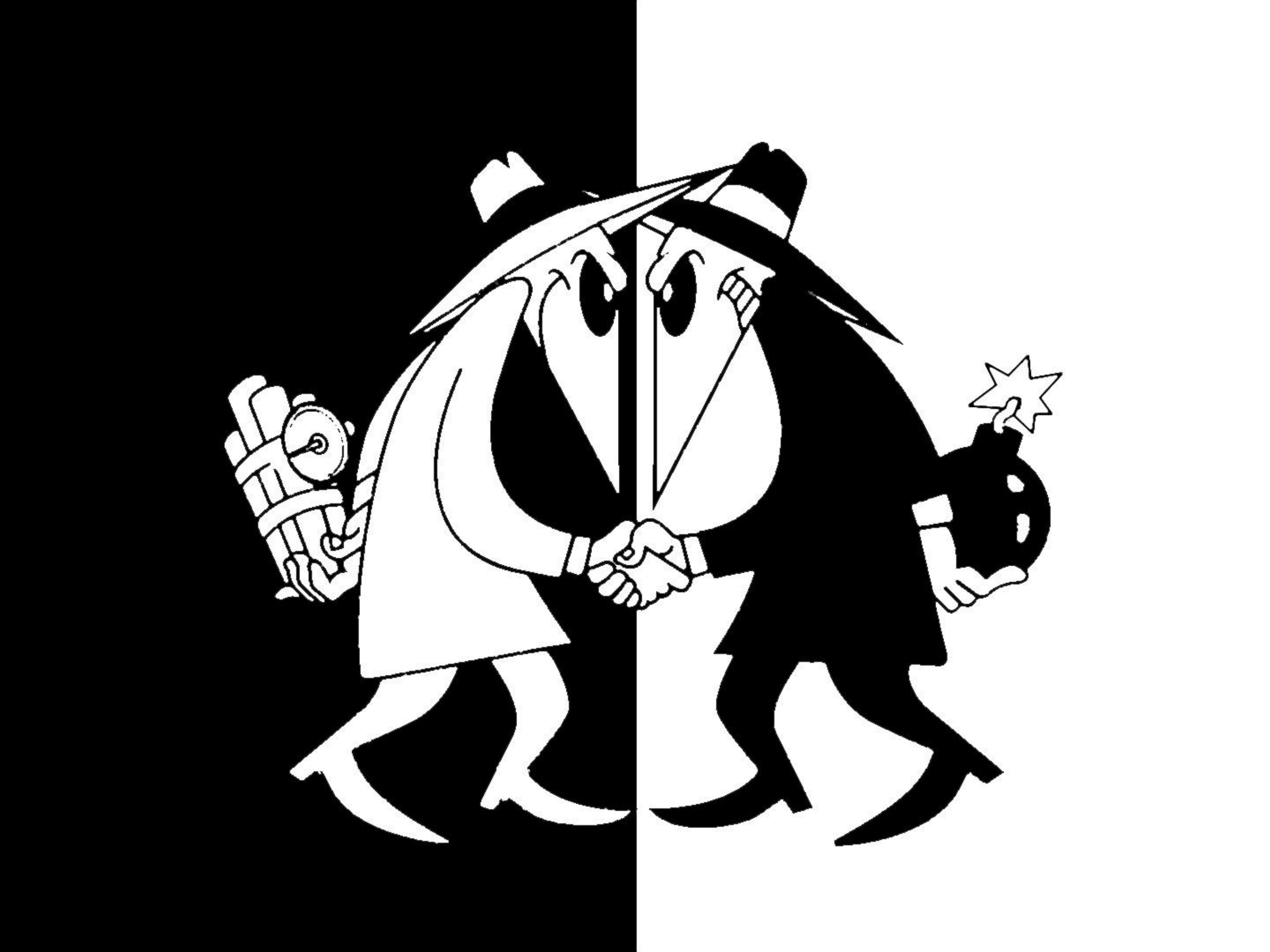
Gallery View

Unmute | Start Video | Invite | Participants 4 | Share | Chat | Record | Leave Meeting

Silent Mac update nukes dangerous webserver installed by Zoom

Fix also requires users to confirm they want to join a Zoom conference.

DAN GOODIN - 7/10/2019, 7:50 PM



Malwarebytes Anti-Malware Home (Trial) 2.2.1.1043

Malwarebytes ANTI-MALWARE

DASHBOARD | SCAN | SETTINGS | HISTORY | ACTIVATE | UPGRADE NOW

- Quarantine
- Application Logs

Quarantine

These threats have been quarantined by your Malwarebytes Anti-Malware. They do not pose a threat when quarantined. You may restore or delete these threats. Threats deleted from quarantine will be permanently removed from your computer.

Vendor	Date	Type	Location
...yHunter	...16 8:15 AM	File	...ftware Group\SpyHunter\SHHService.exe
...yHunter	...16 8:15 AM	File	...ftware Group\SpyHunter\SpyHunter4.exe

Restore

Malwarebytes Anti-Malware

Non-Malware Detected

Malwarebytes has blocked a potentially unwanted program.

Vendor: PUP.Optional.SpyHunter

Path: C:\Program Files\Enig...Hunter\SpyHunter4.exe

Teq's wowhacks: debug console

```
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x01080384 (8 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x012E9E72 (11 bytes)
RDEN: Scan at: 0x1C7A5EAA (4 bytes)
RDEN: Scan at: 0x0346B1F0 (4 bytes)
RDEN: Scan at: 0x1C7A5EAF (10 bytes)
RDEN: Scan at: 0x0346B1F0 (10 bytes)
RDEN: Scan at: 0x1C7A5EBA (0 bytes)
RDEN: Scan at: 0x0346B1F0 (0 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x01080484 (5 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x00A8FD53 (3 bytes)
RDEN: Scan at: 0x0C2CF0F5 (10 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x012EA73A (5 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x012EB0CE (12 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x01080361 (10 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x00E09745 (10 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x0131E56E (9 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x00E5FA94 (10 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x0131E1FC (12 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x00B1CCAD (10 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x01309A3E (5 bytes)
RDEN: PREVENTED Scan at: 0x01309A3E (5 bytes) with Patch at 0x01309A3E
RDEN: Scan at: 0x1882B542 (4 bytes)
RDEN: Scan at: 0x0346B1F0 (4 bytes)
RDEN: Scan at: 0x1882B547 (12 bytes)
RDEN: Scan at: 0x0346B1F0 (12 bytes)
RDEN: Scan at: 0x1882B554 (17 bytes)
RDEN: Scan at: 0x0346B1F0 (17 bytes)
RDEN: Scan at: 0x1882B566 (7 bytes)
RDEN: Scan at: 0x0346B1F0 (7 bytes)
RDEN: Scan at: 0x1882B56E (0 bytes)
RDEN: Scan at: 0x0346B1F0 (0 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x00EBB1EB (7 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x012E9E72 (11 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x0131E56E (9 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x0157D138 (4 bytes)
RDEN: Scan at: 0x0C2CF0F5 (12 bytes)
RDEN: Scan at: 0x0C2CF102 (17 bytes)
RDEN: Scan at: 0x0C2CF0F0 (4 bytes)
RDEN: Scan at: 0x0108043C (5 bytes)
RDEN: Scan at: 0x0C2CF114 (7 bytes)
```

Uh oh. Looks like you're using an ad blocker.

We charge advertisers instead of our audience. Please whitelist our site to show your support for CNN.com

whitelist us

http://ads1.revenue.net - ExclusiveRewards - Microsoft Internet Explorer

CONGRATULATIONS!

You've been chosen to receive a
FREE* Gateway Desktop Computer!

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

FREE!

Click Here to Claim Your FREE* Desktop Computer!

by ExclusiveRewards

*with participation in our program

WELCOME TO CASINO DEL RIO - Micr

File Edit View Favorites Tools Help

Back

Address http://www.casinodelrio.com/

SEARCH

SideFind

sideFind powered by IST

casino Find

www.888.com CASINO ON NET Click

Address http://www.poker-on-net.com/index.htm?SR=916066

SEARCH TopSearches

SideFind

sideFind powered by IST

casino Find

www.888.com CASINO ON NET Click

Casino On Net - Up to 200$ Welcome Bonus
Since 1996, over 8,000,000 people have experienced Casino On...
www.casinoonnet.com

50 Best Online Casinos-Ranked by Quality
Top 50 online casinos ranked by quality and payout rate -...

POKER ON-NET

Download | Getting Started | Features | Contact Us | Help | In

> Current Events

Finale
$5,000

Done

Internet

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

OK Cancel

Go Links

Travel Practical

GAMES WHITE PAGES

Blackjack
Roulette
Slot Machine

Click Here!

econds)

oker events. Play all the popular poker games live, for Fun or Real Money. Chat with Others. 25% Deposit Bonus. 24/7 Support.

Online Dating

Internet

Recycle Bin

start

SLOTCH.COM - Find ...

WELCOME TO CASIN...

Online Poker Room T...

http://ads1.revenue....

6:09 PM

“HandBrake” can’t be opened because it is from an unidentified developer.

Your security preferences allow installation of only apps from the Mac App Store and identified developers.

Safari downloaded this file today at 6:44 PM from download.handbrake.fr.

?

OK

Chimera

Your device, your way.

All devices, iOS 12 — 12.2

Download Chimera 1.2.7
iOS 12 — 12.2

Download ChimeraTV 1.2.6
tvOS 12 — 12.2

Note: A7 - A11 devices only supported on 12.1.3 - 12.2. All devices supported on 12.0 - 12.1.2
Note: Some 12.3 betas are compatible with Chimera. (Beta 6 is not compatible)

Mozilla Security Blog

Қазақстандағы пайдаланушыларымызды қорғау

Маусым айында Firefox пайдаланушысы Mozilla ұйымына Қазақстандағы Firefox пайдаланушыларына әсер етіп жатқан қауіпсіздік мәселесі туралы хабарлады: Оның мәлімдеуінше, Қазақстандағы интернет провайдерлері (ISP) тұтынушыларына үкімет берген түбір сертификатты өз құрылғыларына орнату керектігін айта бастады. Интернет провайдерлері өз тұтынушыларына сертификат желілік байланысқа араласу үшін пайдаланылатындығы туралы айтпады. Басқа пайдаланушылар мен зерттеушілер бұл жағдайды растады және оның отыз танымал әлеуметтік желі мен байланыс сайтына ықпалы тиді.

Firefox және басқа браузерлердегі HTTPS шифрланған байланыстарының қауіпсіздігі мен құпиялығы бойынша сенімді сертификаттау органдары (CO) домен немесе веб-

Why the thing matters

Relevant laws

- Unauthorized use
- Breach of contract
- Copyright infringement
- Defamation
- Antitrust
- Deceptive trade practices
- &c.

Program A — Program B

Program

User

Program A

Program B

User

How to think about the thing

Three heuristics

- Bad Programs Are Bad
- Freedom to Tinker
- Click to Agree

Theory 1: Bad Programs are Bad

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

About bitcoin

How to buy bitcoins?

Contact Us

Check Payment

Decrypt

The World's Most Powerful Monitoring Software for Computers, Mobile Phones and Tablets

Know Everything That Happens on A Computer or Smartphone, No Matter Where You Are

- Monitor all Android and iPhone digital and audio communications
- Monitor everything that happens on a PC or Mac
- More monitoring features than any other product
- No Hassle Remote Installation Service
- FREE Mobile Viewer App for Android and iPhone
- Used for Parental Control and Employee Monitoring

View Demo | Buy Now

FlexiSPY is monitoring software that you install on your computer or mobile device. It takes complete control of the device, letting you ***know everything, no***

http://www.error711971669.com/

error711971669.com

LogMeIn123.com – Remote Su...

WARNING!

COMPUTER MAY BE AT RISK:

855-486-1800

Emergency Tech Support call immediately

System may have found (2) viruses that pose a serious threat
Rootkit.Sirefef.Spy ./ Trojan.FakeAV-Download

Your personal and financial information
may not be secured.

Call us now for support

855-486-1800

TECH SUPPORT

LogMeIn Rescue

Your desktop is being remote controlled by [redacted]

Powered by LogMeIn

AAA

9:22 AM Connecting...
9:22 AM Connected. A support representative will be with you shortly.
9:23 AM Support session established with [redacted]
9:23 AM [redacted] restarting application as Windows system service
9:23 AM Connecting...
9:23 AM Connected. A support representative will be with you shortly.
9:23 AM Connection closed. Attempting reconnection...
9:23 AM Application running as Windows system service
9:23 AM Support session established with [redacted]
9:23 AM You have granted full permission to [redacted]. To revoke, click the red X on the toolbar or press Pause/Break on the keyboard.
9:23 AM Remote Control started by [redacted].

Type here and press Enter to send

9:23 AM
5/28/2014

PLAYLR

Switchfoot

Nothing Is Sound

MUSIC

Lonely Nation	03:45
Stars	04:20
Happy Is A Yuppie Word	04:51
The Shadow Proves The Sunshine	05:04
Easier Than Love	04:29
The Blues	05:17
The Setting Sun	04:24
Politicians	03:28
Golden	03:36
The Fatal Wound	02:44
We Are One Tonight	04:42

Lonely Nation 00:00

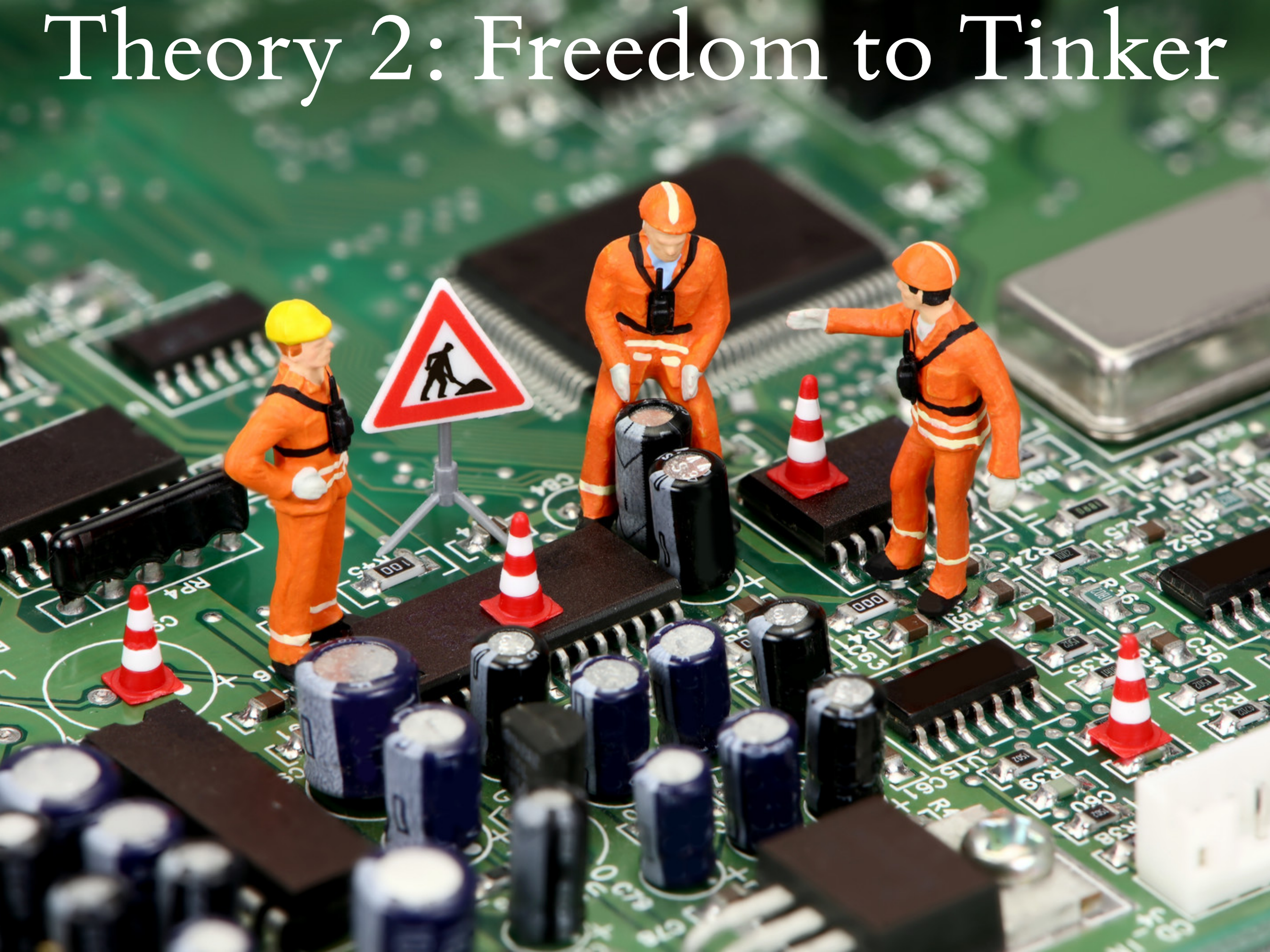
CONSUMER ALERT

Please disregard this message if you have already updated the XCP software on this computer.

This CD contains XCP content protection technology. Installing XCP software on your computer may make it vulnerable to certain computer viruses. Click here for a security update to eliminate this vulnerability and for more information about XCP software.


Are we the baddies?

Theory 2: Freedom to Tinker



Level-3 Hardware Acceleration

WinX DVD Ripper Platinum

5 Minutes Only! Digitize Any DVDs with Intact Videos

CleanMyMac X

- Smart Scan

Cleanup
- System Junk
- Mail Attachments
- Trash Bins

Protection
- Malware Removal
- Privacy

Speed
- Optimization
- Maintenance

Applications
- Uninstaller
- Updater
- Extensions

Files
- Space Lens
- Large & Old Files
- Shredder

Welcome to CleanMyMac X

Start with a nice and thorough scan of your Mac.

Scan

Name
- Cooperation
- DataViews
- DebugClients
- Debugger
- DocumentationTools
- E5Graphics
- E5Gui
- E5Network
- E5XML
- Examples
- Globals
- Graphics
- Helpviewer
- IconEditor
- MultiProject
- Network
- PluginManager
- Plugins
  - AboutPlugin
  - CheckerPlugins
  - DocumentationPlugins
  - VcsPlugins
  - ViewManagerPlugins
  - WizardPlugins
  - __init__.py
  - PluginAbout.py
  - PluginCodeStyleChecker.py
  - PluginEricapi.py
  - PluginEricdoc.py
  - PluginSyntaxChecker.py
    - Coding: utf-8
    - Globals
    - SyntaxCheckerPlugin(QObject)
      - Attributes
      - __init__(self, ui)
      - __editorClosed(self, editor)
      - __editorOpened(self, editor)
      - __editorShowMenu(self, menuName, mer
      - __editorSyntaxCheck(self)
      - __initialize(self)
      - __projectBrowserShowMenu(self, menuN
      - __projectBrowserSyntaxCheck(self)
      - __projectShowMenu(self, menuName, me
      - __projectSyntaxCheck(self)
      - activate(self)
      - deactivate(self)
  - PluginTabnanny.py
  - PluginVcsMercurial.py
  - PluginVcsPySvn.py
  - PluginVcsSubversion.py
  - PluginVmListspace.py
  - PluginVmTabview.py
  - PluginWizardE5MessageBox.py
  - PluginWizardPyRegExp.py
  - PluginWizardQColorDialog.py
  - PluginWizardQFileDialog.py
  - PluginWizardQFontDialog.py
  - PluginWizardQInputDialog.py
  - PluginWizardQMessageBox.py
  - PluginWizardQRegExp.py
  - PluginWizardQRegularExpression.py
- Preferences
- Project
- PyUnit
- QScintilla
- Snapshot
- SqlBrowser
- Tasks
- Templates
- ThirdParty

eric5.py | ...csPlugins/vcsMercurial/HgStatusDialog.py

HgStatusDialog | __commit

```
588         """
589         self.__restoreMissing()
590
591     ###################################################################
592     ## Context menu handling methods
593     ###################################################################
594
595     def __showContextMenu(self, coord):
596         """
597         Protected slot to show the context menu of the status list.
598
599         @param coord the position of the mouse pointer (QPoint)
600         """
601         # TODO: set status of menu entries according to their conditions
602         if self.vcs.isExtensionActive("largefiles"):
603             enable = len(self.__getUnversionedItems()) > 0
604         else:
605             enable = False
606         for act in self.lfActions:
607             act.setEnabled(enable)
608         self.menu.popup(self.mapToGlobal(coord))
609
610     def __showAddMenu(self):
611         """
```

Plugins/PluginSyntaxChecker.py

SyntaxCheckerPlugin

```
34
35  error = ""
36
37
38  class SyntaxCheckerPlugin(QObject):
39      """
40      Class implementing the Syntax Checker plugin.
41      """
42      def __init__(self, ui):
43          """
44          Constructor
45
46          @param ui reference to the user interface object (UI.UserInterface)
47          """
48          super().__init__(ui)
49          self.__ui = ui
50          self.__initialize()
51
52      def __initialize(self):
53          """
54          Private slot to (re)initialize the plugin.
55          """
56          self.__projectAct = None
57          self.__projectSyntaxCheckerDialog = None
```

Summary	Filename
TODO: add support for hg summary --mq	Plugins/VcsPlugins/vcsMercurial/QueuesExtensi
TODO: release - reenable redirection	UI/UserInterface.py
TODO: set status of menu entries according to their conditions	Plugins/VcsPlugins/vcsMercurial/HgStatusDialog

Shell | Task-Viewer | Log-Viewer | Numbers | Time Tracker

Channels

[Arfrever]
Arfrever
ChanServ
detlev

[13:09] [-->] You have joined the channel #eric-ide (~detlev@2a02:3100:1601:3e00:d08:3175:dee2:be10).
[13:09] [***] Channel modes: no colors allowed, no messages from outside, topic protection.
[13:09] [***] This channel was created on 2012-11-15 18:36.
[13:09] [***] Channel URL: http://eric-ide.python-projects.org

Enter a message, send by pressing Return or Enter

#eric-ide (5)

Network

[13:09] [MOTD] - together with like-minded FOSS enthusiasts for talks and
[13:09] [MOTD] - real-life collaboration, if you're more keen on the outdoors why
[13:09] [MOTD] - not attend or arrange a local geeknic (http://www.geeknic.org).
[13:09] [MOTD] -
[13:09] [MOTD] - We would like to thank Private Internet Access
[13:09] [MOTD] - (https://www.privateinternetaccess.com/) and the other
[13:09] [MOTD] - organisations that help keep freenode and our other projects
[13:09] [MOTD] - running for their sustained support.
[13:09] [MOTD] -
[13:09] [MOTD] - In particular we would like to thank the sponsor
[13:09] [MOTD] - of this server, details of which can be found above.
[13:09] [MOTD] -
[13:09] [MOTD] - **********
[13:09] [MOTD] - Please read http://blog.freenode.net/2010/11/be-safe-out-there/
[13:09] [MOTD] - **********
[13:09] [MOTD] End of message of the day
[13:09] [Mode] You have set your personal modes to [+Zi].
[13:09] [Notice] -NickServ- detlev_ is not a registered nickname.
[13:09] [Notice] -ChanServ- [#eric-ide] eric the Python IDE - http://eric-ide.python-projects.org

Freenode (SSL)

detlev_ | #eric-ide

Theory 3: Click to Agree

Install OS X

I have read and agree to the terms of the software license agreement.

Disagree | Agree

OS X El Capitan

To continue installing the software, you must agree to the terms of the software license agreement.

ENGLISH

APPLE INC.
SOFTWARE LICENSE AGREEMENT FOR OS X EL CAPITAN
For use on Apple-branded Systems

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING THE APPLE SOFTWARE. BY USING THE APPLE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT INSTALL AND/OR USE THE APPLE SOFTWARE AND, IF PRESENTED WITH THE OPTION TO "AGREE" OR "DISAGREE" TO THE TERMS, CLICK "DISAGREE". IF YOU ACQUIRED THE APPLE SOFTWARE AS PART OF AN APPLE HARDWARE PURCHASE AND IF YOU DO NOT AGREE TO THE TERMS OF THIS

A copy of the License will be saved on your system and can be found through About This Mac after installation. It is also posted at http://www.apple.com/legal/sla

Disagree Agree


JAKE-CLARK.TUMBLR

"NO" DOES NOT MEAN CONVINCE ME."

Install Zoom

This package will run a program to determine if the software can be installed.

To keep your computer secure, you should only run programs or install software from a trusted source. If you're not sure about this software's source, click Cancel to stop the program and the installation.

Cancel | Continue

- Introducti
- Destinatio
- Installatior
- Installatior
- Summary

Zoom is the leader in modern video communications, with an easy, reliable platform for video and audio conferencing, messaging, and webinars across mobile, desktop, and room systems. Visit blog.zoom.us and follow @zoom_us.

Go Back | Continue

InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

1. Consent to E-Mail Your Contacts. As part of the installation process, Permissioned Media will access your MicroSoft Outlook(r) Contacts list and send an e-mail to persons on your Contacts list inviting them to download FriendGreetings or related products. By downloading, installing, accessing or using the FriendGreetings, you authorize Permissioned Media to access your MicroSoft(r) Outlook(r) Contacts list and to send a personalized e-mail message to persons on your Contact list. IF YOU DO NOT WANT US TO ACCESS YOUR CONTACT LIST AND SEND AN E-MAIL MESSAGE TO PERSONS ON THAT LIST, DO NOT DOWNLOAD, INSTALL, ACCESS OR USE FRIENDGREETINGS.

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install Friend Greetings, you must accept this agreement.

InstallShield

< Back | Yes | No

What to do about the thing

Actual users

- Software vs. software cases involve conflicting expressions of user consent
  - User consent was already problematic
  - This just makes it more obvious
- Good software help users do what they want
  - So software law should focus on users' goals

What do users need?

- Some tasks require delegation to software
- Including protection from other software!
- Users need *access* to software to do things
- Users need *loyalty* from the software they use

What do users want?

- User choice is an essential value, but …
  - Some choices are harmful to others
  - Some explicit “choices” are the result of mistake, fraud, or coercion
  - Some choices are implicit
- Click-to-agree is a bad choice architecture

Conclusion

Silent Mac update nukes dangerous webserver installed by Zoom

Fix also requires users to confirm they want to join a Zoom conference.

DAN GOODIN - 7/10/2019, 7:50 PM

What Apple got right

- Users *could* rationally choose Zoom's server
- Most users *did not* actually choose it
- Most users *would not* choose it if they knew
- Automatic security updates with a System Preference opt-out are a reasonable balance between beneficence and respect

Questions?