

Spyware vs. Spyware

James Grimmelmann

Ohio State Technology Law Journal Distinguished Lecture

The Ohio State University

Moritz College of Law

September 20, 2019



zoom

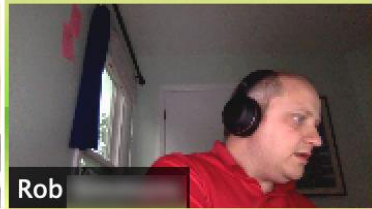
Matt Haughey



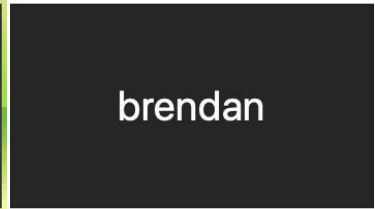
Jonathan



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





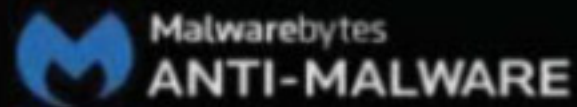
Teq's wowhacks: debug console

```

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)

```





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.

<input type="checkbox"/>	Vendor	Date	Type	Location
<input type="checkbox"/>	...yHunter	...16 8:15 AM	File	...ftware Group\SpyHunter\SH4Service.exe
<input type="checkbox"/>	...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



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

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)

[Click Here to Claim Your FREE* Desktop Computer!](#)

by ExclusiveRewards



*with participation in our program

Microsoft Internet Explorer



Click OK to download our free software while browsing the site

OK

Cancel

POKER ON-NET

[Download](#) [Getting Started](#) [Features](#) [Contact Us](#) [Help](#) [In...](#)

> **Current Events**

[Finale](#)
\$5,000



[GAMES](#) [WHITE PAGES](#)

☐ Blackjack
☐ Roulette
☒ Slot Machine

**Click
Here!**

seconds)

games live, for Fun or Real Money. Chat with Others. 25% Deposit Bonus. 24/7 Support.

Internet



"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)



User



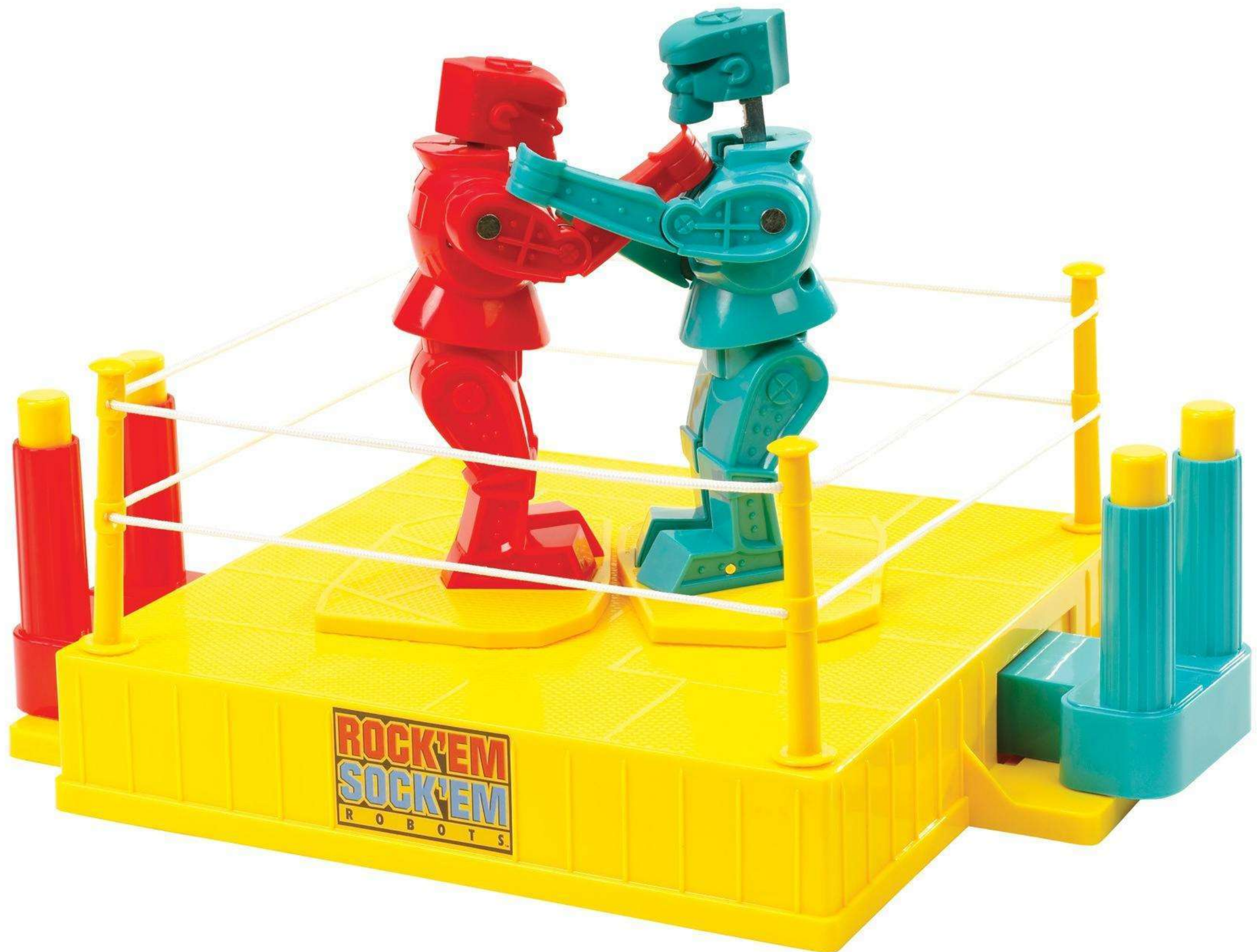
Program A

Program B

A close-up shot of a man in a dark military uniform, wearing a peaked cap with a silver emblem. He is looking off-camera to the left with a slight, knowing smile. The background is dark and out of focus.

Are we the baddies?

Theory 1: Deregulate





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 matter where you are.**

Theory 2: Good vs. Bad



Norris Hall 1977





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

[About bitcoin](#)[How to buy bitcoins?](#)[Contact Us](#)

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

GMT from Monday to Friday



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

[Check Payment](#)[Decrypt](#)



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 

9:22 AM Connecting...

9:22 AM Connected. A support representative will be with you shortly.

9:23 AM Support session established with 


9:23 AM  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 

9:23 AM You have granted full permission to . To revoke, click the red X on the toolbar or press Pause/Break on the keyboard.

9:23 AM Remote Control started by .

Type here and press Enter to send



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.



Theory 3: Click to Agree





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

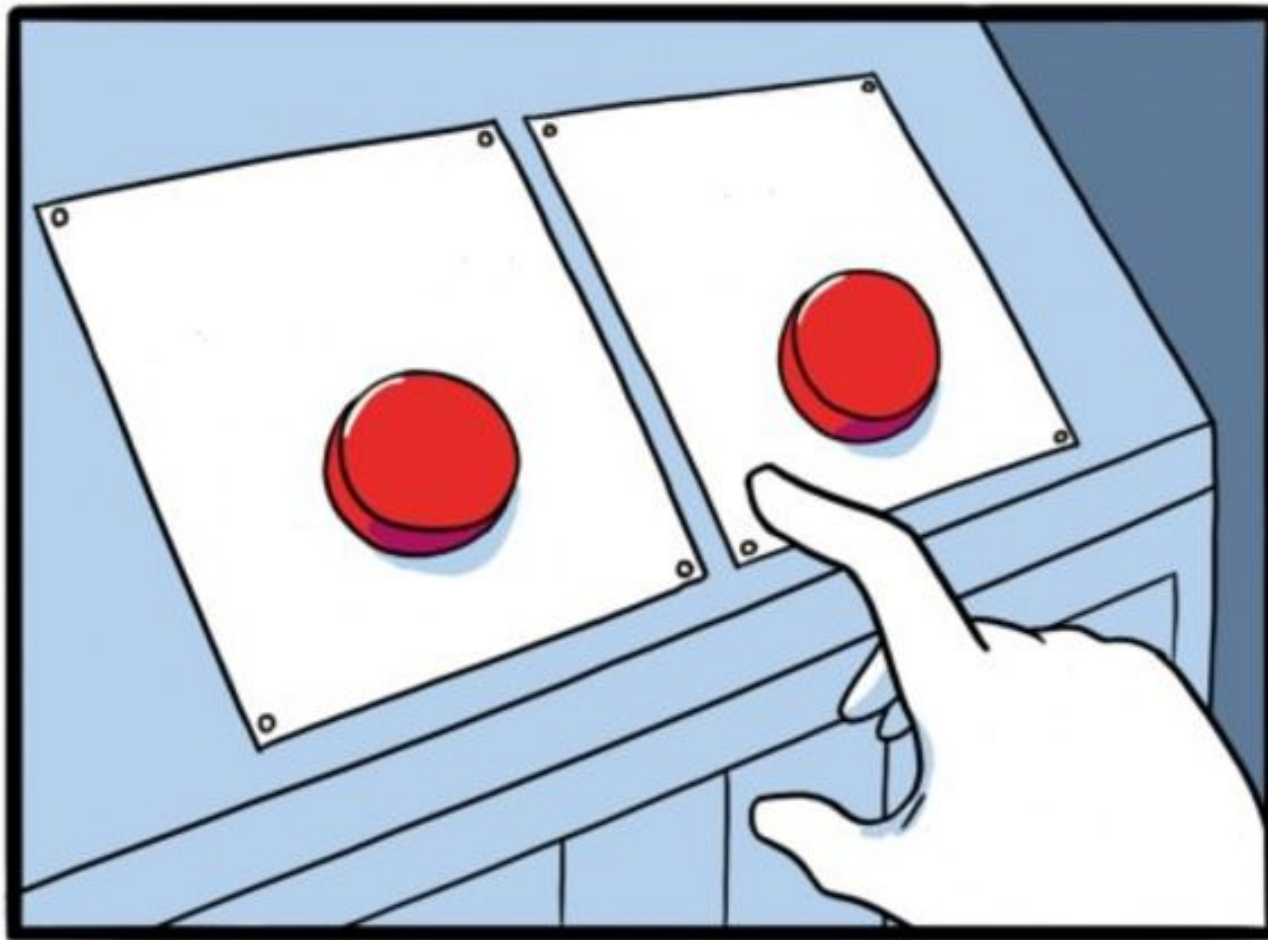
A copy of the License will be saved on your system and can be found through About This Mac after installation. It is also posted at <http://www.apple.com/legal/sla>



Disagree



Agree



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.

< Back

Yes

No

Theory 4: Freedom to Tinker





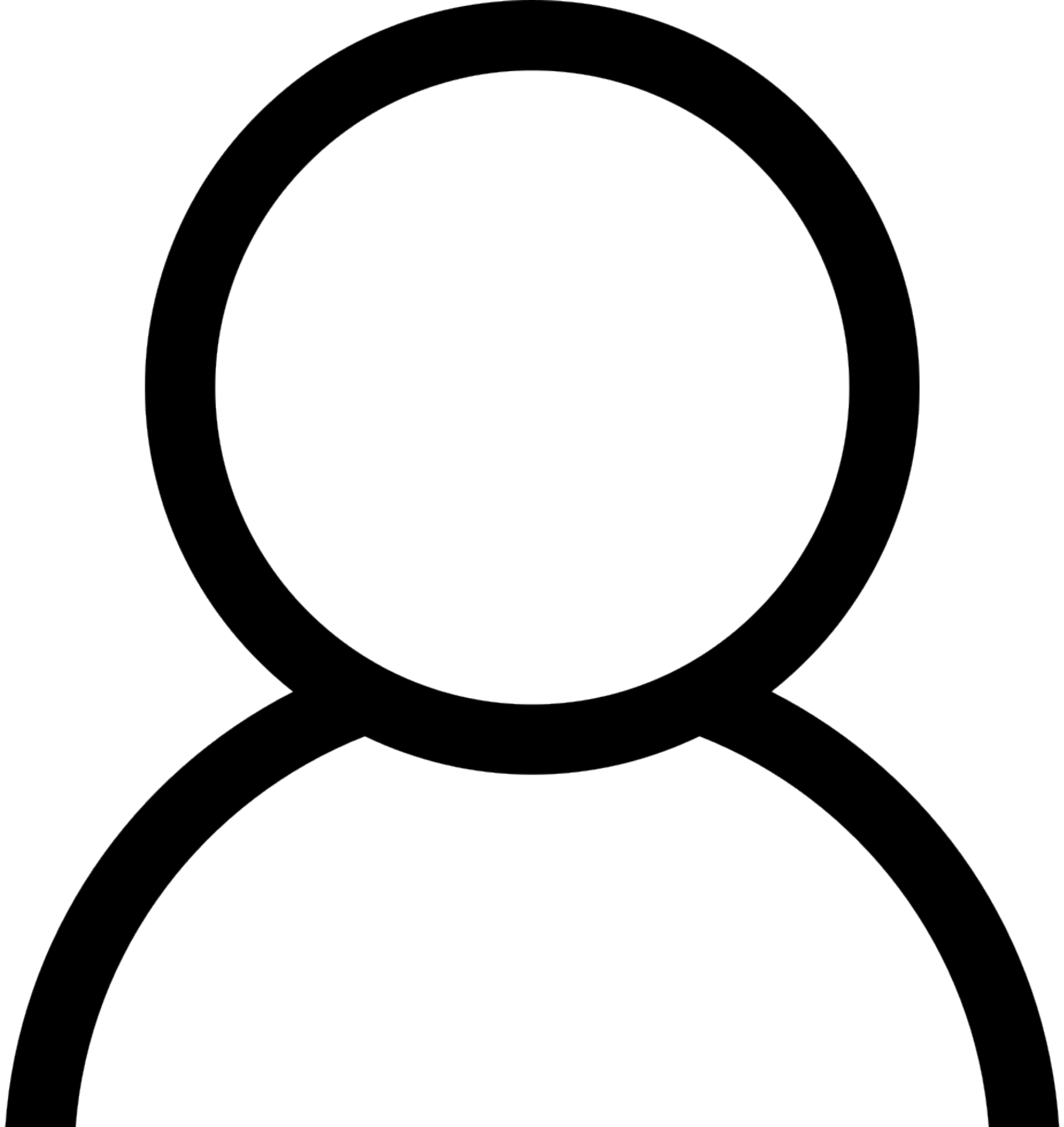




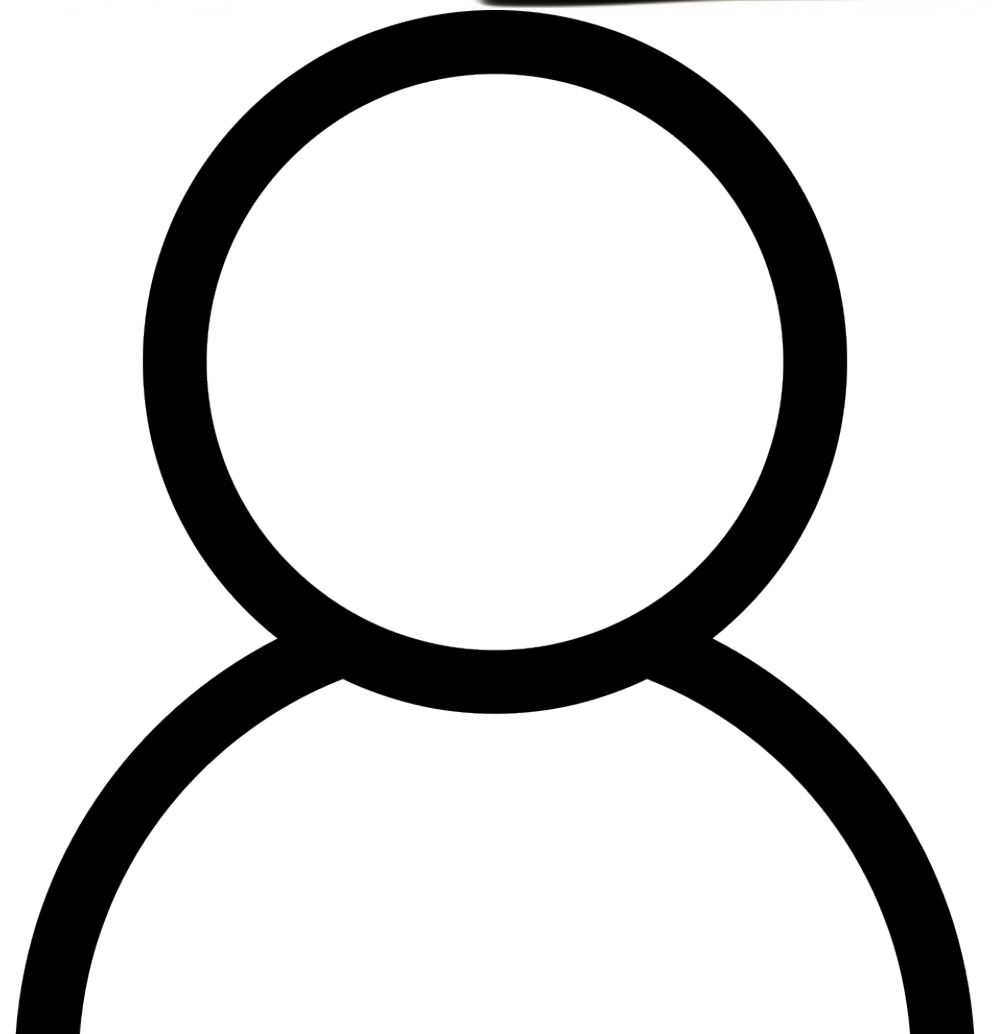












Silent Mac update nukes dangerous webserver installed by Zoom

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

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



"NO" DOES
NOT MEAN
"CONVINCE
ME"