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
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
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.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Date</th>
<th>Type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>...yHunter</td>
<td>16:8:15 AM</td>
<td>File</td>
<td>...ftware Group\SpyHunter\SHHService.exe</td>
</tr>
<tr>
<td>...yHunter</td>
<td>16:8:15 AM</td>
<td>File</td>
<td>...ftware Group\SpyHunter\SpyHunter4.exe</td>
</tr>
</tbody>
</table>

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.
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
“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.
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)
Қазақстандағы пайдаланушыларымызды қорғай

Маусым айында Firefox пайдаланушысы Mozilla ұйымына Қазақстандағы Firefox пайдаланушыларына асер етіп жатқан қауіпсіздік мәселесі туралы хабарлады: Оның мәлімдедеуінше, Қазақстандағы интернет провайдерлері (ISP) тұтынуышыларына ұқімет берген тұбір сертификатты өз құрылғыларына өрнітті керектігін айта бастады. Интернет провайдерлері өз тұтынуышыларына сертификат желілік байланысқа араласу ушін пайдаланылатындығы туралы айтпады. Басқа пайдаланушылар мен зерттеушілер бұл жағдайлды растады және оның отыз танымал елеуметтік желі мен байланыс сайтына ықпалы тиді.

Firefox және басқа браузерлердегі HTTPS шифрланған байланыстарының қауіпсіздігі мен құпиялығы бойынша сенімді сертификаттау органдары (СО) домен немесе веб-сайттың кәсіпорының жаңы сертификатты пайдалану қажетті.
Why the thing matters
Relevant laws

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

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
Ooops, your files have been encrypted!

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:

![bitcoin](https://example.com/bitcoin.png)

About bitcoin
How to buy bitcoins?
Contact Us

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
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.
Your desktop is being remotely controlled by [user].

9:22 AM Connecting...
9:22 AM Connected. A support representative will be with you shortly.
9:23 AM Support session established with [user].
9:23 AM Application running as Windows system service
9:23 AM Connecting. 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 [user]. To revoke, click the red X on the toolbar or press Pause/Break on the keyboard.
9:23 AM Remote Control started by [user].

Your 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
Switchfoot
Nothing Is Sound

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
WinX DVD Ripper Platinum

Level-3 Hardware Acceleration

5 Minutes Only! Digitize Any DVDs with Intact Videos

DVD Movies
TV Series
99-title DVDs
Old DVDs

32x Real-time speed
Welcome to CleanMyMac X

Start with a nice and thorough scan of your Mac.
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 LICENSE, RETURN THE ENTIRE PICTURED PRODUCT IN ACCORDANCE WITH THE REFUND POLICY.

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
"No" Does Not Mean "Convince Me".
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.

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.
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.
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?