Spyware vs. Spyware

James Grimmelmann

Ohio State Technology Law Journal Distinguished Lecture
The Ohio State University
Moritz College of Law
September 20, 2019
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:

<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>...tware Group\SpyHunter\SHService.exe</td>
</tr>
<tr>
<td>...yHunter</td>
<td>16:8:15 AM</td>
<td>File</td>
<td>...tware 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.
“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)
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

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.
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:

12tYDPgwueZ9NyMgw519p7AA8isjr6SMw

Contact Us
WARNING!

COMPUTER MAY BE AT RISK:

855-486-1800

Emergency Tech Support call immediately

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
Theory 3: Click to Agree
I have read and agree to the terms of the software license agreement.

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
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.
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"