All Your Macs Are Belong To Us

Christopher Elisan
@Tophs
About Me

• Principal Malware Scientist / Sr. Manager MIT

• Past Adventures
  – Damballa (2009-2012)
  – F-Secure (2006-2009)

• @Tophs
Author of

MALWARE, ROOTKITS & BOTNETS
Christopher C. Elisan

Advanced Malware Analysis
Christopher Elisan

Lab Setup and Top Tier Tools for Analysis & Reporting

2013

2015
Co-Author of

2nd Edition

2015
Let the Fun Stuff Begins...
Targeting Mac
The Culprit

The image shows a webpage with a message stating that the browser has been locked due to violating copyright and related rights laws. It warns that all activities of the computer have been recorded and that the browser has been blocked due to at least one of the reasons specified below.

The webpage contains text explaining that the user has been found to be violating copyright laws by distributing copyrighted content, which includes music, video, and software. It also mentions the violation of viewing or distributing prohibited content such as child pornography.

Further details include the possibility of a release fee of $300 being required to unlock the computer, payable through Green Dot MoneyPak. The user is instructed on how to find a MoneyPak location, pick up the card, and enter the code to unlock the PC.

The URL to unlock the computer is provided:

http://fbi.gov.id657546456-3999456674.k8381.com
Weapon of Mass Deception

- Targets Mac-specific browsers
- Fake FBI website
- "Locks" browsers
- Asks for $300 as ransom
Timeline

- **July 14, 2013**
  - Discovered the link
  - Analysis done
  - Informed customers
  - Informed LEO’s

- **July 15, 2013**
  - Reports from different outfits started coming out
Lock Mechanism

http://fbi.gov.id657546456-3999456674.k8381.com

Are you sure you want to leave this page?

YOUR BROWSER HAS BEEN LOCKED.

ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.

Stay on Page  Leave Page
<script type="text/javascript">
    show_count = 150;
    for (i = 0; i < show_count; i++) {
        frame = document.createElement("iframe");
        frame.setAttribute("class", "frame");
        frame.setAttribute("width", "0px");
        frame.setAttribute("height", "0px");
        frame.setAttribute("src", "close.html");
        document.body.appendChild(frame);
    }
</script>
MoneyPak Format

http://fbi.gov.id657546456-3999456674.k8381.com

YOUR PAYMENT INFORMATION IS NOT CORRECT.

ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.

OK
If an application doesn't respond for a while, select its name and click Force Quit.

You can open this window by pressing Command-Option-Escape.
It Keeps Coming Back
It Keeps Coming Back

```html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>

<script type="text/javascript" language="javascript">
var areYouReallySure = false;
var internalLink = false;
function areYouSure() {
    if (!areYouReallySure && !internalLink) {
        areYouReallySure = true;
        str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.\n';
        alert(str);
        return str;
    }
}
window.onbeforeunload = areYouSure;
```
Kill it for Good
Reset Safari

Are you sure you want to reset Safari?
Select the items you want to reset, and then click Reset. You can’t undo this operation.

- Clear history
- Reset Top Sites
- Remove all webpage preview images
- Reset all location warnings
- Reset all website notification warnings
- Remove all website data
- Remove saved names and passwords
- Remove other AutoFill form text
- Clear the Downloads list
- Close all Safari windows

[Cancel] [Reset]
Clear Firefox
Restore from Crash

- Default web browser: Google Chrome.app
- Default search engine: Google
- Safari opens with: All windows from last session
- New windows open with: Homepage
- New tabs open with: Top Sites
- Homepage: http://www.apple.com/startpage/
- Remove history items: After one year
- Save downloaded files to: Downloads
- Remove download list items: Manually

Open “safe” files after downloading
“Safe” files include movies, pictures, sounds, PDF and text documents, and archives.
Restore from Crash
Solutions

• Force Quit
• Clear History / Reset
• Restore from Crash Settings
• Update Browsers
Karma

• Jay Riley, 21, From Virginia
• http://bit.ly/1fUD3K1
Thank You!!!

*Images are copied from the Internet and are owned by their respective authors*
*Images are copied from the Internet and are owned by their respective authors