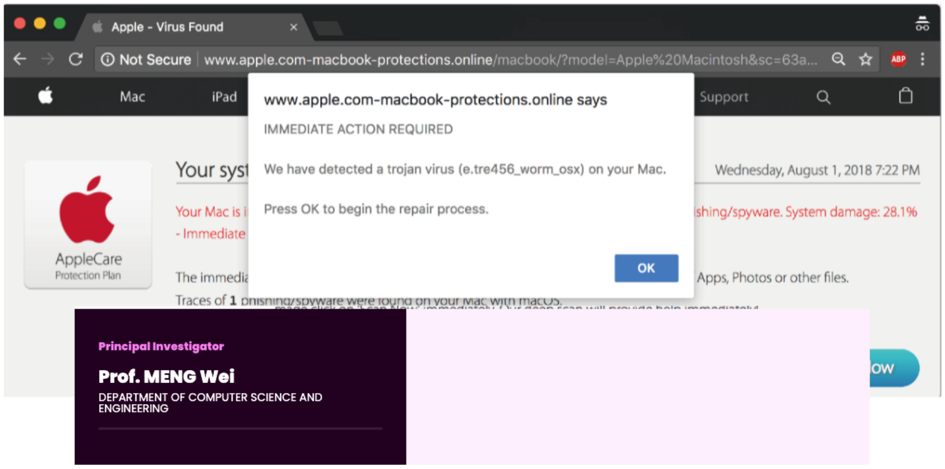
Novel Browser-based Analysis Framework Observer

#2020 #Network #Security


Apple - Virus Found
Not Secure www.apple.com-macbook-protections.online/macbook/?model=Apple%20Macintosh&sc=63a...
Mac
iPad
Support
AppleCare
Protection Plan
Your syst
Wednesday, August 1, 2018 7:22 PM
Your Mac is i
- Immediate
shing/spyware. System damage: 28.1%
The immedia
Apps, Photos or other files.
Traces of 1 phishing/spyware were found on your Mac with macOS.
ow

www.apple.com-macbook-protections.online says

IMMEDIATE ACTION REQUIRED

We have detected a trojan virus (e.tre456_worm_osx) on your Mac.

Press OK to begin the repair process.

OK

Principal Investigator

Prof. MENG Wei

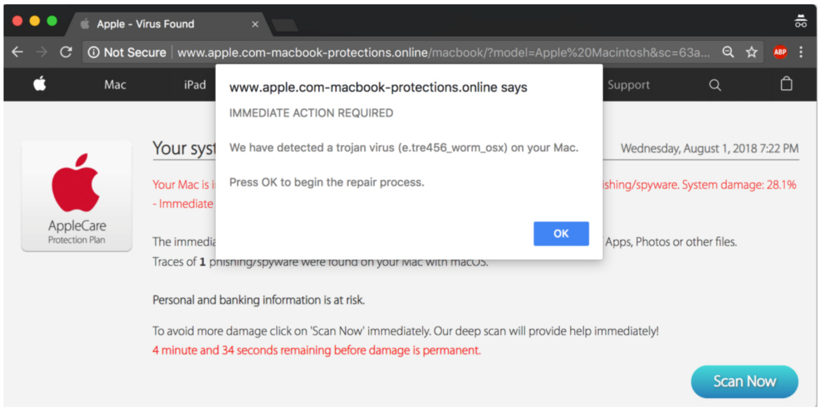
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

A click is the prominent way that users interact with content on the World Wide Web (WWW). Malicious third-party advertisers or hackers expose web users to a security threat by injecting malicious JavaScript code to intercept user clicks and trick them into visiting untrusted web content. Attackers aim to intercept genuine user clicks to either launch ad click frauds by fabricating ad click traffic, or to send malicious commands to another website on behalf of the user (e.g., to force the user to download malwares). This project developed a browser-based analysis framework – Observer, which is able to detect three different techniques for intercepting web user clicks. Different from previous researches that mainly considered the type of click interceptions launched by malicious first-party websites, Observer addresses this research gap, in which it considers the various click interceptions launched by third-party JavaScript code.

It is acknowledged that web behaviour caused by third-party JavaScript code is difficult to record and analyse. Observer detects third-party click interceptions by extending the browser to collect the behaviour at runtime and thoroughly analysing the click-related behaviour. Using Observer, we analysed Alexa top 250K websites, and detected 437 third-party scripts that intercept user clicks on 613 popular websites, which in total receive around 43 million visits on a daily basis. In particular, though click interception, these scripts could trick users into visiting 3,251 untrusted unique uniform resource locators (URLs) controlled by third parties. Over 36% of them were related to online advertising. Further, some click interception URLs led users to malicious content such as scamwares. This demonstrates that click interception has become an emerging threat to web users. Our research team has released the source code of the framework publicly to help web browsers detect malicious click interceptions and alert users about the malicious behaviour to protect them from being exposed to malicious content.

The research identified three categories of click interception techniques:

1. Modifying the destination URL of hyperlinks to lead users to malicious websites upon clicks.
2. Adding click event listeners to manipulate user clicks.
3. Visual deception, for example, by creating web content that is visually similar to first-party content, or displaying transparent elements on top of the web page. The former will trick users into clicking third-party element, and the latter enables the transparent elements to capture all user clicks on first-party content. Consequently, the users can be led to a page controlled by the attackers.


Apple - Virus Found
Not Secure www.apple.com-macbook-protections.online/macbook/?model=Apple%20Macintosh&sc=63a...
Mac
iPad
Support
AppleCare
Protection Plan
Scan Now

www.apple.com-macbook-protections.online says

IMMEDIATE ACTION REQUIRED

We have detected a trojan virus (e.tre456_worm_osx) on your Mac.

Press OK to begin the repair process.

OK

Your syst

Wednesday, August 1, 2018 7:22 PM

Your Mac is i

- Immediate

shing/spyware. System damage: 28.1%

The immedia

Apps, Photos or other files.

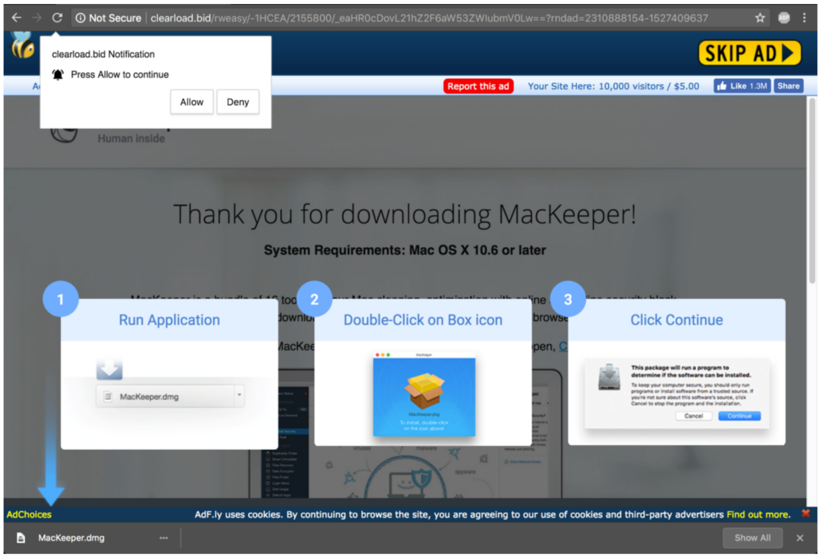
Traces of 1 phishing/spyware were found on your Mac with macOS.

Personal and banking information is at risk.

To avoid more damage click on 'Scan Now' immediately. Our deep scan will provide help immediately!

4 minute and 34 seconds remaining before damage is permanent.

Victim users can be directed to fake antivirus pages.



Not Secure | clearload.bid/rweasy/-1HCEA/2155800/_eaHR0cDovL21hZ2F6aW53ZWlubmV0Lw==?rndad=2310888154-1527409637

clearload.bid Notification

Press Allow to continue

Thank you for downloading MacKeeper!

System Requirements: Mac OS X 10.6 or later

1 Run Application

2 Double-Click on Box icon

3 Click Continue

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.

AdF.ly uses cookies. By continuing to browse the site, you are agreeing to our use of cookies and third-party advertisers Find out more.

Victim users can be directed to drive-by download pages.

DO YOU LIKE OUR PROJECT?

Contact us

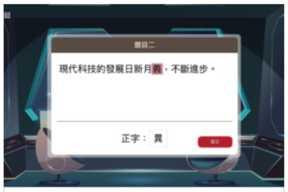
MORE TO EXPLORE

All projects ›

Information and Communication Technologies

Jockey Club Community Care and STEM in Action Project

Read more ›



Information and Communication Technologies

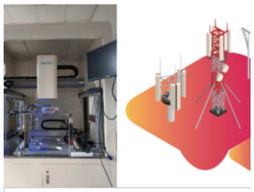
Drill-Easy – An AI-based Language Learning System

Read more ›

Information and Communication Technologies

A Breakthrough in Photonic Integration Facilitating High-...

Read more ›



Information and Communication Technologies

An Intelligent Robot System for Adaptive tuning of 5G Microwa

Read mo