BROWSER NOTIFICATION MALWARE
by Francis Chao
fchao2@yahoo.com

TuCSon Society
WINNERS WINdows usERS

apcug
An International Association of Technology & Computer User Groups
Web location for this presentation:

http://aztcs.org

Click on “Meeting Notes”
SUMMARY
Malware criminals are now using "browser notifications" to launch malware in "Windows.." computers. As of February 2019, no antivirus program is able to block these new form of malware you much manual them when they occur.
TOPICS

• Browser Notification Malware Example

• Remove "Browser Notification Malware" from Browser Settings
On February 1, 2019, the following phony "toast notification" repeatedly popped up in my "Windows 10 Home" computer whenever I was using the "Google Chrome" Web browser.
Antivirus protection is OFF

Device may be infected by viruses.
Click here to do a scan

Your PC could be hacked!
Click here to scan
Google Chrome • bouptosaive.com

Close
Antivirus protection is OFF

Device may be infected by viruses.
Click here to do a scan

Your PC could be hacked!
Click here to scan
Google Chrome ● bouptosaive.com
BROWSER NOTIFICATION
MALWARE EXAMPLE (continued)

- A "Full scan" with "Windows Security" did not remove the problem
  ("Windows Security" used to be called "Windows Defender").
BROWSER NOTIFICATION
MALWARE EXAMPLE (continued)

- A "Threat Scan" with "Malwarebytes Premium" did not remove the problem ("Malwarebytes Premium" is the not-free version of "Malwarebytes".)
The removal for this malware is described in the section on removing notifications inside the Chrome browser as described at https://www.bleepingcomputer.com/news/security/sites-trick-users-into-subscribing-to-browser-notification-spam/
Similar instructions for removing "browser notification malware" can be found in https://www.fixyourbrowser.com/removal-instructions/popups/bouptosaive-com/
ADDITIONAL REFERENCES

http://bouptosaive.com
Ask before sending (recommended)

Block

No sites added

Allow

- http://docs.google.com/*
  embedded on http://docs.google.com/*

- http://drive.google.com/*
  embedded on http://drive.google.com/*

- https://docs.google.com/*
  embedded on https://docs.google.com/*

- https://drive.google.com/*
  embedded on https://drive.google.com/*

- *://mail.google.com/mail/ca*
  embedded on *://mail.google.com/mail/ca*