



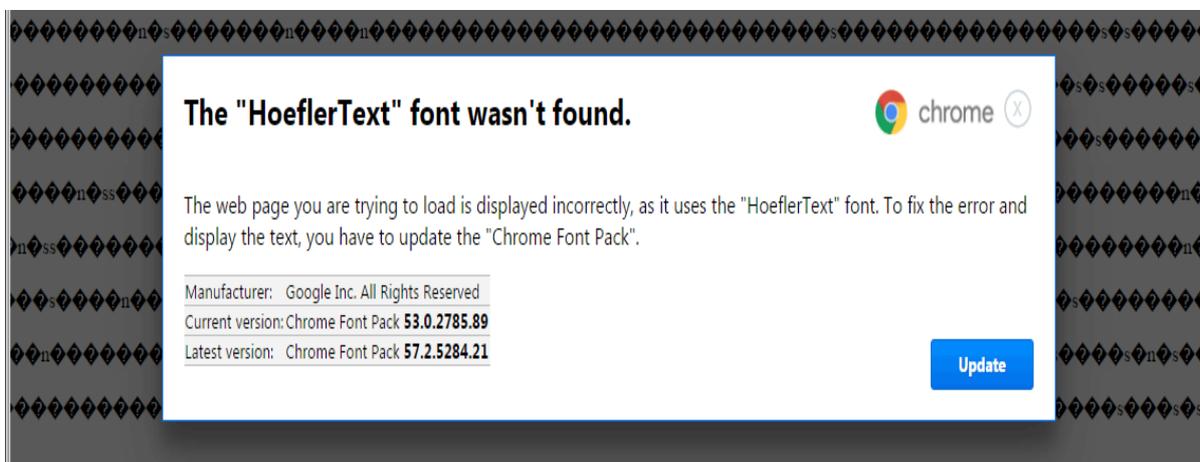
COMPUTER SECURITY BULLETIN

Risk/Impact Rating: **SERIOUS**

< Google Chrome Malware > CSB17-009

Description:

Scammers and hackers are targeting Google Chrome users with this new hacking scam that's incredibly easy to fall for, prompting users to download a fake Google Chrome font pack update just to trick them into installing malware on their systems.



This pop-up is part of an attack called EITest, which injects JavaScript into a hacked web site that you are visiting in order to display the popup.

If you visit a site that has been hacked to show the EITest attack, and come to that site through a search engine result and are using Chrome, then the JavaScript will scramble the text on the legitimate websites so it is unreadable and then display the fake Chrome alert.

Everything about the browser message looks legit, from the type of “missing font” and the dialog window to the Chrome logo and the right shade of blue on the “update” button.

Once this malicious program is installed, whenever you will browse the Internet, an ad with the same message will randomly pop-up.

The Chrome browser doesn't flag the file as malware, but the browser does block it because the file is not downloaded too often, which is a standard warning.

The malware currently targets Windows users.

Risks to PNP Computer Users:

- Hackers disrupt a computer's operations;
- Steal files and corrupt data;
- Encrypt files and ask for a ransom in return; and
- Other unwanted adware programs might get installed in the computer without the user's knowledge.

Recommendations:

- Exercise caution when downloading anything from the Internet onto computers;
- Keep antivirus software up-to-date; and
- Do not ever fall for scam asking to update the Chrome font pack.

References:

<http://thehackernews.com/2017/02/HoeflerText-font-chrome.html>

<https://www.bleepingcomputer.com/virus-removal/hoeflertext-font-wasnt-found-and-chrome-font-pack-guide>

<https://www.superantispysware.com/blog/2017/02/22/the-hoeflertext-font-wasnt-found-google-chrome-malware-scam-what-it-is-and-how-to-avoid-it/>

<http://www.wmur.com/article/warning-google-chrome-update-scam-infects-computers-with-malware/8972032>

For inquiries, please contact WSCSD thru:

- a. Telephone number: (02)723-0401 local 4225
- b. E-mail address: wcsditms@pnp.gov.ph
- c. Chat service: www.itms.pnp.gov.ph

* For dissemination to All PNP Personnel