



***Issued 5/22/18***

## **Chrome, Firefox Browsers are Targeted by New 'Vega Stealer' Malware**

A new malware strain is targeting popular browsers and programs such as Microsoft Word. The “Vega Stealer” malware can steal credit card data and passwords stored in Chrome and Firefox and snatch sensitive data from infected computers, according to Proofpoint, a cybersecurity company based in Sunnyvale, Calif. The malware currently targets marketing, advertising, public relations, retail and manufacturing industries but “this threat may continue to evolve and grow to be a commonly observed threat,” Proofpoint said on its website. Proofpoint first spotted Vega Stealer earlier this month when it observed a “low-volume” email campaign with subject lines such as “Online store developer required.” Some of the malicious emails went to individuals while other emails went to common distribution lists used at many companies such as info@. “An approach that has the effect of amplifying the number of potential victims,” the company said. Messages contain a malicious attachment called “brief.doc.” Software – known as a “macro” – downloads the Vega Stealer malware. These macros can fool the user into clicking on buttons in programs such as Microsoft Word that “enable” the macro and download the malware. For example, a macro in Microsoft Word might say “Enable editing” or “Enable content.” The macro retrieves the payload in a two-step process which ultimately saves it to the victim’s computer in the "Music" directory with a filename of “ljoyoxu.pkzip.” Once this file is downloaded and saved, it is executed automatically, Proofpoint said. “Enterprises are very frequently targeted with malware that has credential

stealing capabilities built in,” Kowsik Guruswamy, Chief Technology Officer with Menlo Security, told Fox News in an email.