west

protect^{SM}

SAFE Alert!

New malicious hacking tool impersonating DocuSign®

April 2021

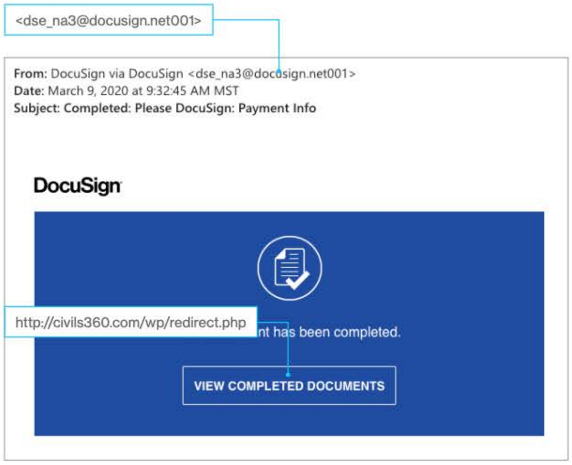
DocuSign has been made aware of a new malicious document builder used to impersonate DocuSign to deliver malware to victims. The document builder creates Microsoft Office documents containing malicious macros or attempts to exploit a known Microsoft Office vulnerability (CVE-2017-8570) to download malware onto the victim's computer. This activity is from malicious third-party sources and is not coming from the DocuSign platform.

To date, the malicious documents have been observed to deliver many different malware families such as Trickbot, QBot, Bazar, IcedID, and Ursnif. These types of malicious documents are typically delivered to victims via phishing attacks. The attackers send their emails and spoof the real DocuSign envelopes and emails, but if you check the email address or the links, they are false and don't go where you think they are going. Some examples are below:

You can learn more about this DocuSign Alert on their website https://www.docusign.com/trust/alerts/alert-new-malicious-hacking-tool-impersonating-docusign-observed, as well as view their white paper on Combating Phishing.

Fake DocuSign examples

In the examples below, the URLs don't start with "https" nor do they include "docusign.net."



<dse_na3@docusign.net001>

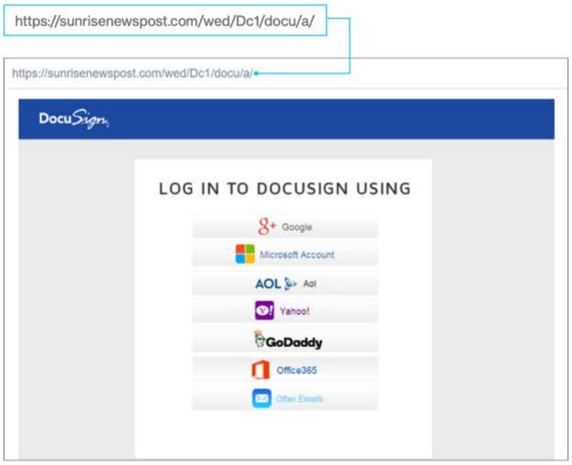
From: DocuSign via DocuSign <dse_na3@docusign.net001>
Date: March 9, 2020 at 9:32:45 AM MST
Subject: Completed: Please DocuSign: Payment Info

DocuSign

http://civils360.com/wp/redirect.php

nt has been completed.

Fake email



https://sunrisenewspost.com/wed/Dc1/docu/a/

https://sunrisenewspost.com/wed/Dc1/docu/a/

Fake login page