Phishing emails caught exploiting DocuSign and COVID-19

By **Lance Whitney** in **Security** on May 8, 2020, 1:07 PM PST

A new attack discovered by Abnormal Security aims to steal account credentials from people who use the online document signing platform.

Phishing emails typically try to ensnare their victims by impersonating well-known companies, brands, products, and other items used by a lot of people. If the emails can reference a topic of interest or concern to the recipients, so much the better. DocuSign is a secure electronic signature tool used by many organizations to ease and expedite the process of getting signatures on important business documents. The coronavirus quarantine has forced more people to work remotely, so a service like DocuSign is likely in much higher demand than usual.

The phishing email itself tries to look legitimate by copying the content and images of real emails from DocuSign. The attacker taps into the current anxiety over the coronavirus by referring to the sender and subject of the message as "CU #COVID19 Electronic Documents." The button in the message simply says: "Review Documents" with indications that these documents are for member agreements, health applications, and health pay authorizations.

The URL for the phishing site is hidden in the body text of the email through a SendGrid link. With the URL concealed, the recipient of the message must click on the actual button to find out where the link goes. The email actually contains several embedded links, some of which lead to authentic DocuSign web pages to give it greater legitimacy.

DocuSign

CU #COVID19 Electronic Documents sent you a document to review and sign.

REVIEW DOCUMENTS

CU #COVID19 Electronic Documents
electronic_documents@coronavirus-ctrl.org

OWEN G KELLERMAN,

Please DocuSign CE Note Disclosure Agreement (14013), DP Consumer Member Agreement (CAD611), Forms H1 and H2 for Officer 1, Health Application (14012), Health Pay Authorization

Thank You, CU #COVID19 Electronic Documents

Clicking on the button to review the documents redirects the user several times, first through the SendGrid link and then through two compromised websites. These redirects are created specifically to confuse the user and to get past URL detection security. In the end, the page that comes up is a malicious one trying to capture DocuSign credentials as well as business email addresses. People who falls for the ploy and provide the necessary information will see their account credentials compromised and stolen.

"Interestingly, the fake login page provides users a dropdown menu to select their email provider when logging in," Ken Liao, vice president of cybersecurity strategy for Abnormal Security, said, "implying that attackers are far more interested in stealing that login information as it allows them to further compromise the victim's accounts through Single Sign-On or email access.

Since the coronavirus has spread, cybercriminals have been keen to exploit the pandemic for their own purposes. They simply modify and update their malicious emails with current events to keep them relevant to their victims, according to Liao. This specific DocuSign phishing campaign was first noticed at the beginning of May. So far, Abnormal Security has discovered this attack directed at only one of its customers, specifically a healthcare company. But Liao said he expects to see more credential theft attacks using both DocuSign and COVID-19.

How can organizations and individuals protect themselves against these types of phishing attacks?
"The number one piece of advice we have for businesses and employees is to always be vigilant," Liao said. "Attacks are becoming increasingly sophisticated in their attempts to steal user credentials and access sensitive information."

Users should always scrutinize these types of emails to look for signs that something is off.
"In this particular case, the attacker disguises the malicious links through SendGrid, an email marketing service that allows businesses and individuals to send out emails en masse," Liao said. "We wouldn't expect a company like DocuSign to use SendGrid links instead of directly linking their own site when asking a user to sign documents. Furthermore, always check the website name before logging on. Again, in this case we can easily notice that the login page this attack directed the user to is clearly not a legitimate page."