HC3: Sector Alert

November 19, 2024 TLP:CLEAR Report: 202411191200

E-Signature Platform Abused in Phishing Campaigns

Executive Summary

Security researchers recently published details of a widespread phishing campaign abusing e-signature software to impersonate well-known brands, with the goal of luring recipients to e-sign documents and enable authorization of payments from the victim company's billing departments. While HC3 has not received reports from health sector organizations related to this campaign, the threat activity has the potential to impact the health sector. This alert includes tips for detecting and reporting related activity.

Report

On November 5, 2024, researchers published a blog post regarding attackers abusing the electronic signature (e-signature) platform DocuSign's Envelopes API to create and mass-distribute fake invoices that appear genuine, impersonating well-known brands like Norton and PayPal. Unlike traditional phishing scams that rely on deceptively crafted emails and malicious links, these incidents use legitimate DocuSign accounts and templates to impersonate reputable companies, making detection for end users and security tools more difficult. According to the report, the attackers bypass email security protections by using a legitimate service, as the phishing emails originate from an actual DocuSign domain, docusign[.]net. The goal of this campaign is to entice targeted recipients to e-sign the documents, which the attackers can then use to authorize payments independently from the impersonated company's billing departments. Over the past five months, user reports of such malicious campaigns have noticeably increased, and DocuSign's community forums have seen a surge in discussions about fraudulent activities, indicating that the attackers may be leveraging automation for these phishing campaigns.

Analysis

While the researchers did not indicate any specific industry targeting in this recent campaign, it is likely that this threat activity has the potential to impact all industries, including the Healthcare and Public Health (HPH) sector. HC3 has previously observed similar scams opportunistically targeting users in the health sector. For example, medical bill fake invoice scams have historically involved a fraudulent practice where a threat actor creates a fake medical bill, often resembling a legitimate invoice from a healthcare provider, and attempts to deceive individuals into paying for services they never received, usually by inflating costs, adding unnecessary procedures, or billing for completely phantom treatments, which is a form of healthcare fraud.

Patches, Mitigations, and Workarounds

To mitigate DocuSign invoice phishing, key strategies include: thoroughly verifying sender details, educating employees to carefully examine suspicious emails, requiring additional approvals for financial transactions, monitoring for unusual invoice requests, reporting suspicious activity to DocuSign, and implementing robust email filtering to catch potential phishing attempts. Always double-check the sender's email address and the content of the invoice before taking any action. If you think that you have received a fraudulent email purporting to come from Docusign, DocuSign recommends forwarding the entire email as an attachment to spam@docusign.com and deleting it immediately. Additionally, if you do not recognize the sender of a Docusign envelope and are uncertain of the email's authenticity, look for the unique security code in the the bottom portion of the Docusign envelope notification email. If you do not see the security code, do not click on any links or open any attachments. Additional guidance for identifying imiation emails and websites leveraging DocuSign are detailed here.

HC3: Sector Alert

November 19, 2024 TLP:CLEAR Report: 202411191200

References

Novikov, Ivan. “Attackers Abuse DocuSign API to Send Authentic-Looking Invoices At Scale.” Wallarm. November 5, 2024. https://lab.wallarm.com/attackers-abuse-docusign-api-to-send-authentic-looking-invoices-at-scale/

FBI. “Health Care Fraud.” https://www.fbi.gov/investigate/white-collar-crime/health-care-fraud

LarryAZ. “Phishing Emails from Docusign.net Domain.” DocuSign Community Forum. May 7, 2024. https://community.docusign.com/esignature-111/phishing-emails-from-docusign-net-domain-4174

DocuSign. “How Docusign Users Can Spot, Avoid and Report Fraud.” August 26, 2022. https://www.docusign.com/blog/how-docusign-users-can-spot-avoid-and-report-fraud

DocuSign. “Incident Reporting - Security Concerns.” https://www.docusign.com/trust/security/incident-reporting

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback