ultraviolet

CONFIDENTIAL

THREAT REPORT:

Sendception: SendGrid Impersonation Campaign

Services Performed By:
UltraViolet Cyber
Jacob Wyatt
(443) 351-7630
info@uvcyber.com

Published Date:
03/21/2024

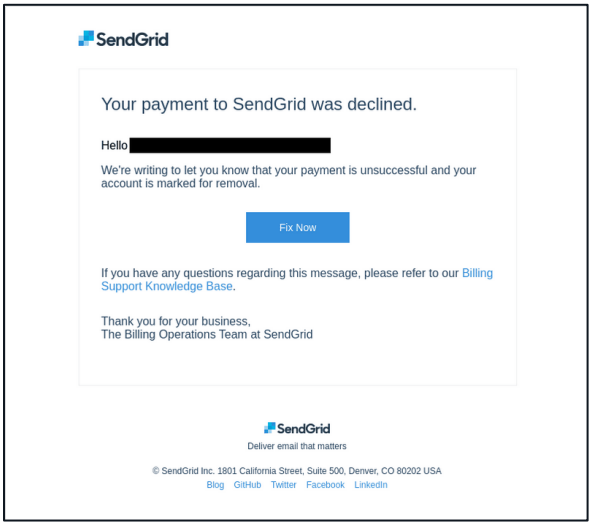
Contents

1 Executive Summary

In a recent discovery by Netcraft, a sophisticated phishing campaign has been observed exploiting the popular email service SendGrid (a subsidiary of Twilio) to impersonate the service itself. SendGrid, renowned for its scalability, high deliverability rates, and extensive feature set, has become a tool in the hands of cybercriminals targeting its users. The campaign tricks victims with a series of tactics, including false account suspension notices and payment failure alerts, skillfully using SendGrid's features to obscure malicious link destinations. The campaign also leverages SendGrid's click-tracking functionality, disguising the true endpoint of the phishing links behind SendGrid's own tracking URLs. This tactic cleverly encodes the malicious URL in a parameter, making it challenging for even IT and security professionals to identify the threat without clicking the link. In this article, we are going to breakdown how this attack works and how to readily identify the tactics used.

2 Technical Analysis

To better understand how this phishing campaign works, we begin by analyzing what a typical email looks like that is being used for the phishing campaign. Note here, the email states the user had an unsuccessful payment (Figure 1):

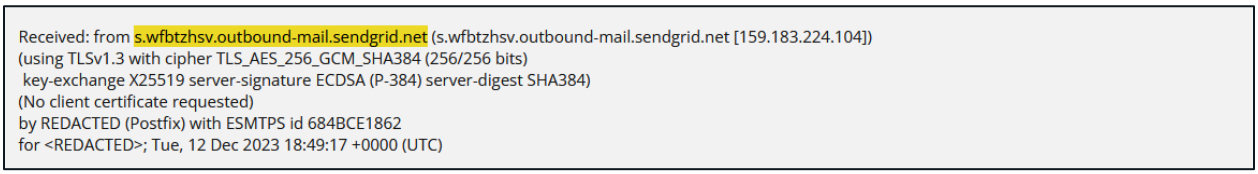


(Figure 1 – SendGrid phishing email – source: Netcraft)

The crime group behind this campaign exploited SendGrid's click-tracking functionality to conceal their phishing link behind a SendGrid-hosted tracking URL (the fix now button). This technique involves encoding the phishing URL as a parameter within the tracking link, effectively obfuscating the malicious link. This obfuscation tactic means that even recipients with technical skill are unable to determine the final URL without clicking on the link, therefore exposing themselves to potential risk. A phishing link hidden inside of the parameter of the tracking link can be seen in the below example (Figure 2):

(Figure 2 – SendGrid disguising phishing link inside of tracking link – source: Netcraft)

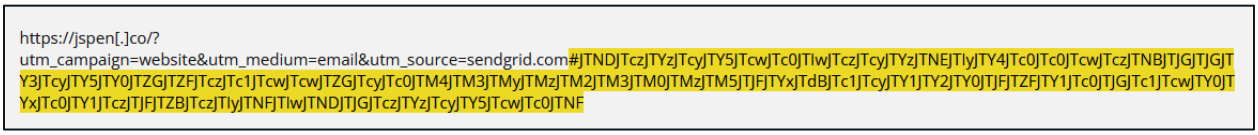
Analysis of the email headers confirms that the phishing emails originate from SendGrid's infrastructure, indicating that the emails originated from SendGrid (Figure 3):



(Figure 3 – SendGrid phishing email header– source: Netcraft)

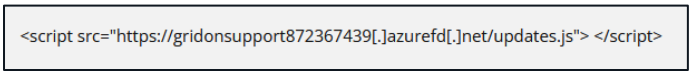
One potentially obvious sign that points to the email being phishing is the discrepancy between the "From:" addresses and SendGrid's domain, with emails originating from a range of unaffiliated domains. This implies the exploitation of SendGrid accounts belonging to companies from various sectors, including cloud hosting and healthcare, identified by Netcraft in at least nine different instances. These tactics enable attackers to exploit more SendGrid accounts, capitalizing on the established trust and authentication protocols like SPF and DKIM that these companies have implemented with SendGrid.

Once users interact with the "Fix Now" button in the email, they are then led to JSPen. This platform, a code editor, uniquely stores page content directly in the URL fragment, which is the portion following the hash (#) symbol (figure 4):



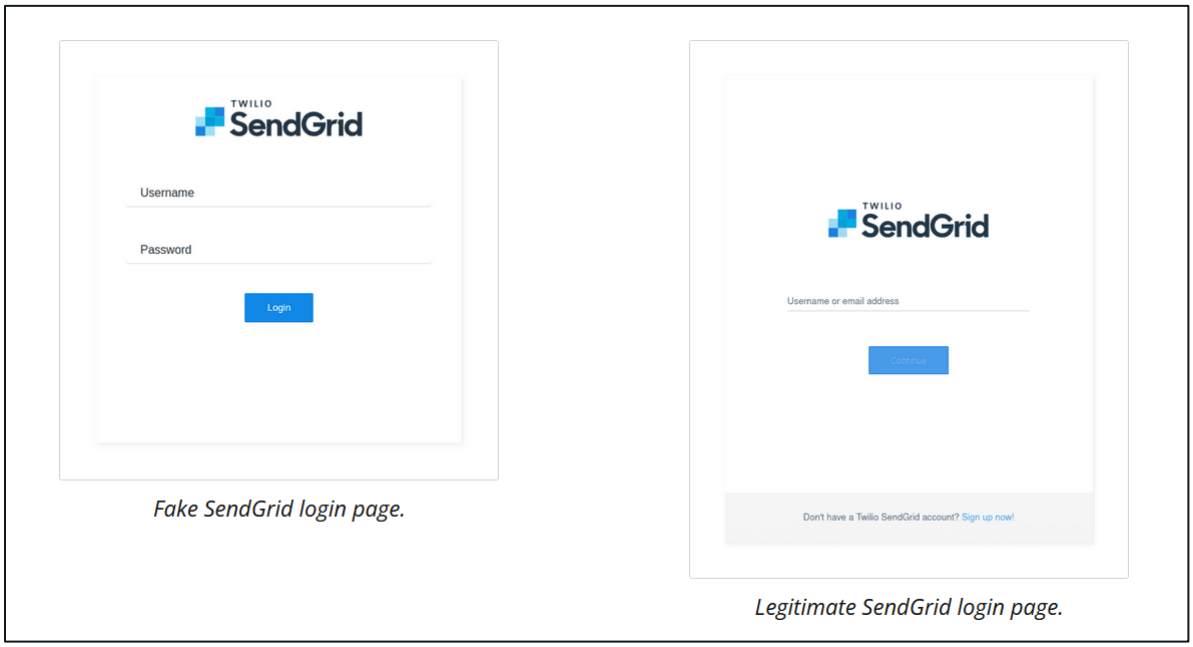
(Figure 4 –JSPen content in URL fragment– source: Netcraft)

Detecting this attack is difficult because the URL fragment, used solely within the victim's browser, is never transmitted to the server. This also means that administrators of the JSPen service may be unaware of its misuse in these phishing campaigns. Upon decrypting the URL fragment, it reveals a <script> tag that references a JavaScript file served by Azure Front Door, Microsoft's cloud-based content delivery network (Figure 5):



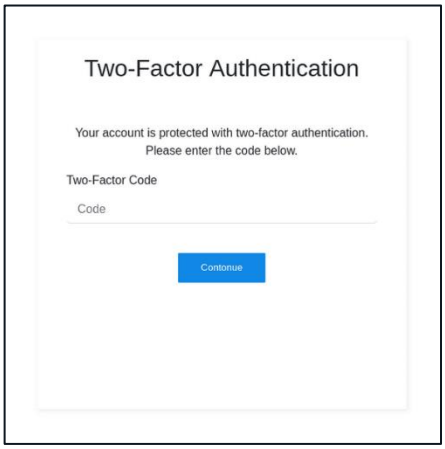
(Figure 5: Decrypted URL fragment– source: NetCraft)

The phishing site users will see looks similar to the legitimate login for SendGrid. Notice the differences between the username and password fields (Figure 6).



(Figure 6: Comparison of the real and fake login pages – source: Netcraft)

Once the victim inputs correct login credentials, the phishing website uses SendGrid's API to send a two-factor authentication code to the victim's phone. It then presents a replica of SendGrid's two-factor authentication form (Figure 7):



(Figure 7: Fake MFA prompt using API to verify code – source Netcraft)

The fraudulent site confirms the validity of the two-factor authentication (2FA) code submitted by the victim through SendGrid's API. If the code is incorrect, it requests the victim to input it again. Upon receiving the correct 2FA code, the phishing site does not transmit this code to its control server - instead, it sends the session token obtained from SendGrid's API, giving the attackers more time to access the victim's account. Unlike a 2FA code which has a short lifespan, a session token remains valid for a longer amount of time.

Once the user enters the correct MFA, victims are seamlessly redirected to the legitimate SendGrid website, often without realizing their account security has been breached.

3 What UltraViolet Cyber is Doing

- We are closely analyzing emails, especially those sent through, or claiming to be, from SendGrid. This includes verifying the authenticity of the “From:” addresses and checking for discrepancies that might indicate a phishing attempt.
- Our team is deploying techniques to analyze and decode URLs within emails, especially those employing SendGrid's click-tracking feature. By inspecting the destination of encoded URLs, we aim to prevent users from inadvertently accessing malicious sites.
- Recognizing that attackers may compromise legitimate SendGrid accounts, we are monitoring for unusual activity patterns that could indicate that an account has been hijacked.

4 What Customers Can Do

- Verify the sender's address in emails received, especially those from SendGrid or other trusted services. Be wary of any discrepancies or unfamiliar domain names.
- Conduct regular training sessions for your team on recognizing phishing emails. Highlight the tactics used by attackers, such as urgent language or requests for sensitive information, and the misuse of trusted platforms like SendGrid.
- Ensure the timely application of security updates and patches across all systems, software, and web platforms to mitigate vulnerabilities.

5 References

- "Popular Email Platform Used to Impersonate Itself." Netcraft, 7 Feb. 2024, https://www.netcraft.com/blog/popular-email-platform-used-to-impersonate-itself/.

- Constantin, Lucian. "Phishing Attack Uses Compromised SendGrid Accounts to Target Additional Users." CSO Online, 8 Feb. 2024, https://www.csoonline.com/article/1306712/phishing-attack-uses-compromised-sendgrid-accounts-to-target-additional-users.html.

- "Phishception: SendGrid Is Abused to Host Phishing Attacks Impersonating Itself." IT Security News, 7 Feb. 2024, https://www.itsecuritynews.info/phishception-sendgrid-is-abused-to-host-phishing-attacks-impersonating-itself/.