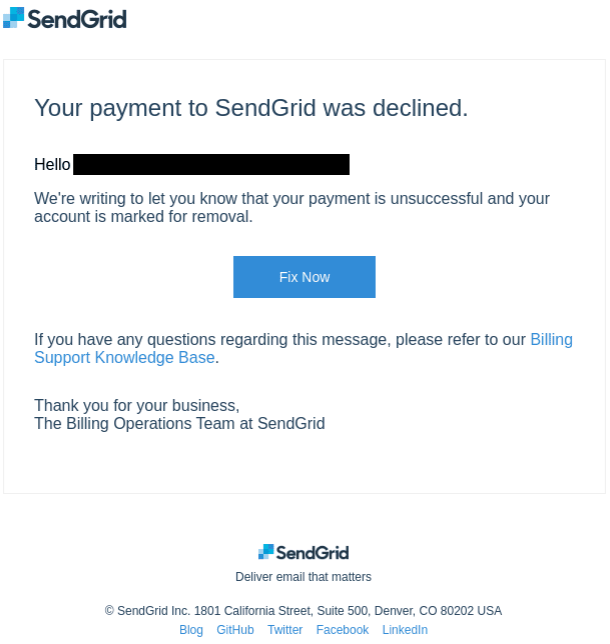
Phishception – SendGrid is abused to host phishing attacks impersonating itself

Published: 2024-02-07 · Archived: 2026-04-05 21:07:22 UTC

Netcraft has recently observed that criminals abused SendGrid's services to launch a phishing campaign impersonating SendGrid itself. The well-known provider, now owned by Twilio, makes sending emails at scale simple and flexible. In addition to scale, the promise of high deliverability and feature-rich tools make Sendgrid a sought-after service for legitimate businesses and a likely target for criminals.

The campaign observed uses a variety of complex lures, such as claiming the victim's account has been suspended while its sending practices are reviewed or that the victim's account is marked for removal due to a recent payment failure, combined with other SendGrid features to mask the actual destination of any malicious links.



Screenshot of one of the phishing emails seen by Netcraft in the campaign.

The criminals behind the campaign used SendGrid's click-tracking feature, with the malicious link masked behind a tracking link hosted by SendGrid. As the actual destination link is encoded in a URL parameter, even technically savvy recipients cannot determine its destination without following it.

Examining the email headers reveals that the phishing emails are sent using SendGrid's infrastructure:

SendGrid advertises an "industry-leading 99% delivery rate". With even legitimate companies sometimes struggling to deliver emails to users' inboxes successfully, it is easy to see how using SendGrid for phishing campaigns is attractive to criminals.

One giveaway indicates that the emails are not legitimate: while the campaign uses SendGrid's email servers, the *"From:"* addresses do not use SendGrid's domain name. Instead, the emails are sent from a variety of unrelated domain names. All the domain names appear to be other SendGrid customers, suggesting criminals use compromised SendGrid accounts rather than registering their own.

Netcraft has identified at least nine companies whose accounts have been used in the campaign. These companies span a range of industries, including cloud hosting, energy, healthcare, education, property, recruitment, and publishing.

The use of compromised SendGrid accounts explains why SendGrid is targeted by the phishing campaign: the criminals can use the compromised accounts to compromise further SendGrid accounts in a cycle, providing them with a steady supply of fresh SendGrid accounts.

A compromised SendGrid account could also be used to send phishing emails impersonating the compromised company. Companies often authorize SendGrid to send emails on their behalf from their domain name, using SPF and DKIM policies. The phishing emails would, therefore, pass the checks and appear authentic.

After clicking the tracking link in the email, victims are redirected to JSPen. This code editor allows pages to be stored entirely within the URL fragment – everything after the hash (#) character:

The attack is more challenging to detect and block as the URL fragment is not sent to the server and is only used within the victim's browser. The operator of the JSPen service might not know it is being abused for malicious purposes.

Decoding the URL fragment reveals a single

Cloud services like Azure are attractive to fraudsters due to the availability of free tiers and credits. While Azure Front Door is not included in Azure's free tier, Azure does provide new customers with a $200 credit, which can be spent on any Azure service.

The JavaScript file is heavily obfuscated, with variables and functions given meaningless names and all whitespace removed:

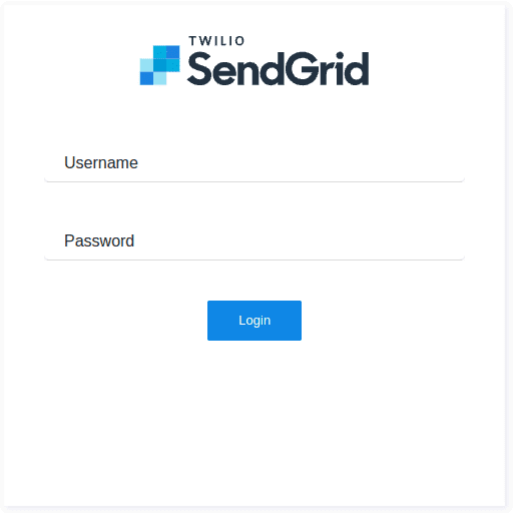
Screenshot of part of the obfuscated JavaScript file.

De-obfuscating the file reveals that the contents of the phishing site are stored within an AES-encrypted string, which is decrypted and written to the web page at runtime. Criminals employ these techniques to make it harder for human analysts and automated systems to determine whether a script is malicious.

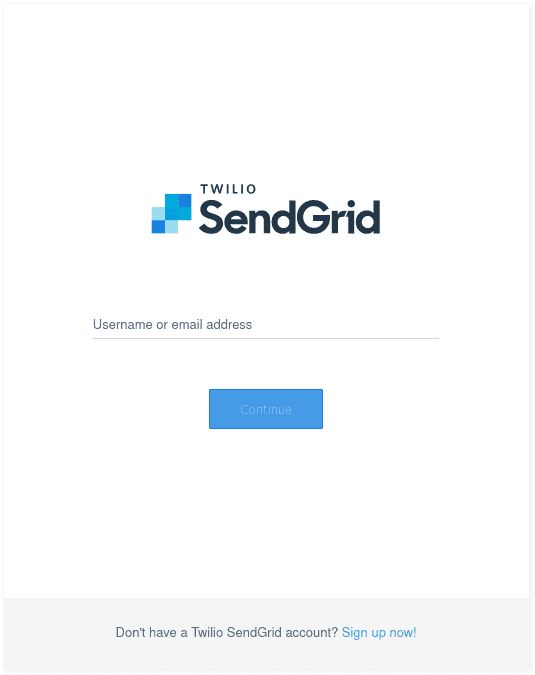
```
}(a, 0x3963a), document[z(0xc4)]('keydown', function(c) {
    var A = z;
    c[A(0xc8)] && (c[A(0xca)] === 0x55 || c[A(0xca)] === 0x49
}, ![]), (function() {
    var B = z;
    const i = B(0xc2);
    var o = [B(0xd1), B(0xdc)],
        p = B(0xcf),
        q = B(0xd8),
        r = o[0x0],
        s = o[0x1];
    for (var t = 0x0; t < 0xa; t++) {
        var u = Math[B(0xc6)]()[B(0xc0)](0x24)[B(0xd3)](0x7);
        console[B(0xdb)]('token:\x20' + u);
    }
    const v = CryptoJS['enc']['Hex'][B(0xcd)](r),
        w = CryptoJS['enc']['Hex'][B(0xcd)](s),
        x = CryptoJS[B(0xcc)][B(0xbe)](i, v, {
            'iv': w,
            'mode': CryptoJS[B(0xc5)][B(0xd4)],
            'padding': CryptoJS['pad']['Pkcs7']
        });
    document['write'](x[B(0xc0)](CryptoJS['enc'][B(0xd9)]));
}()));
```

Screenshot of the partially-deobfuscated AES decryption code. The phishing site relies on a CDN-hosted copy of the CryptoJS library to provide the AES decryption routine.

The phishing site itself is a convincing replica of the actual SendGrid login page:



Fake SendGrid login page.



Legitimate SendGrid login page.

After entering some credentials, the phishing site requests SendGrid's API to verify whether the username and password are correct or not:

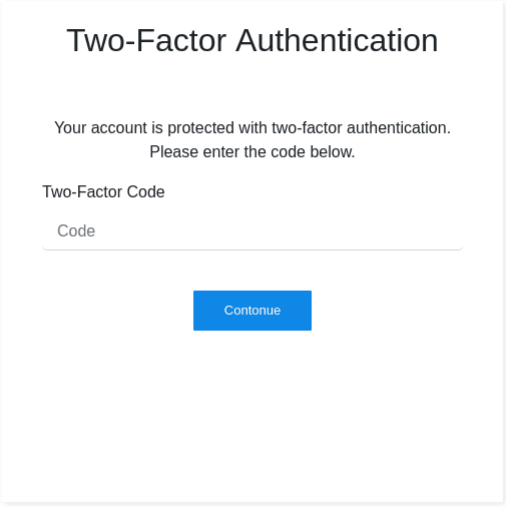
Sometimes, a trick to detect simple phishing attempts is to enter an invalid username or password. As primary phishing sites naively accept any credentials, the lack of an error message reveals the site is fake. However, cleverer phishing sites like this appear authentic, rejecting invalid login attempts and asking the user to try again.

Both JSPen and Azure Front Door only allow users to host static files. The phishing site delivers the stolen credentials to a separate drop site - pnp-api[.]com – using AJAX:

We first saw pnp-api[.]com in our November 2023 survey. Its home page is default page of the Laravel PHP framework. Its age and lack of content means it is likely that the drop site was purpose-registered by the criminals, rather than being a compromised site.

pnp-api[.]com was registered at Wild West Domains, a subsidiary of GoDaddy. Measuring ping times from various monitoring locations confirms that Aurologic hosts it in a data center in Frankfurt, Germany.

After the victim enters a valid username and password, the phishing site uses SendGrid's API to request that a two-factor authentication code be sent to the victim's phone. Then, it displays a copy of SendGrid's two-factor authentication form:



Screenshot of the phishing site's two-factor authentication form.

The phishing site also verifies the two-factor authentication code entered by the victim is correct with SendGrid's API. It continues, prompting the victim to try again if it is incorrect.

After the victim enters the correct code, the phishing site makes another request to the drop site. However, it does not send the two-factor code to the drop site. Instead, it sends the session token provided by the SendGrid API, giving the criminals more time to take over victims' accounts: while a two-factor authentication code might only be valid for a few minutes, the session token is valid for much longer.

Finally, the victim is redirected to SendGrid's official website, possibly not realizing that their account has been compromised.

At the time of writing, JSPen and the malicious JavaScript file hosted on Azure are no longer available.

Netcraft's position at the epicenter of the battle against cybercrime allows us to rapidly identify, monitor and react to new phishing campaigns. Consumers can use Netcraft's browser extension and apps to protect themselves from

phishing attacks and other threats. Organizations targeted by phishing can leverage our digital risk protection services to ensure that malicious content is blocked and removed quickly and efficiently through our disruption and takedown platform. Contact us to learn more.

Netcraft researchers contacted SendGrid on February 1 through their abuse reporting mechanisms to inform them of this attack and subsequent research.
