How scammers are hiding their phishing trips in public clouds

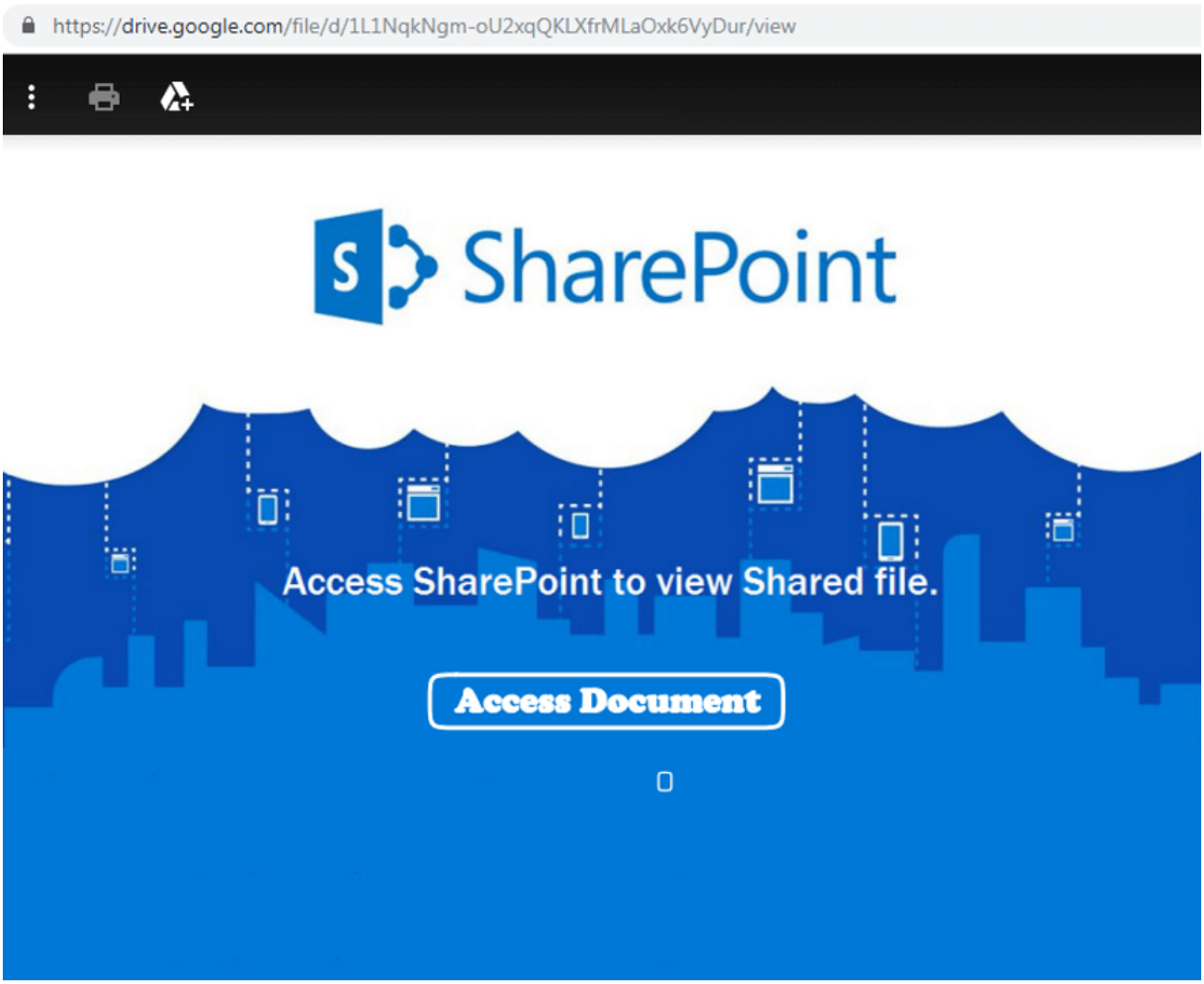
blog.checkpoint.com/2020/07/21/how-scammers-are-hiding-their-phishing-trips-in-public-clouds/

July 21, 2020

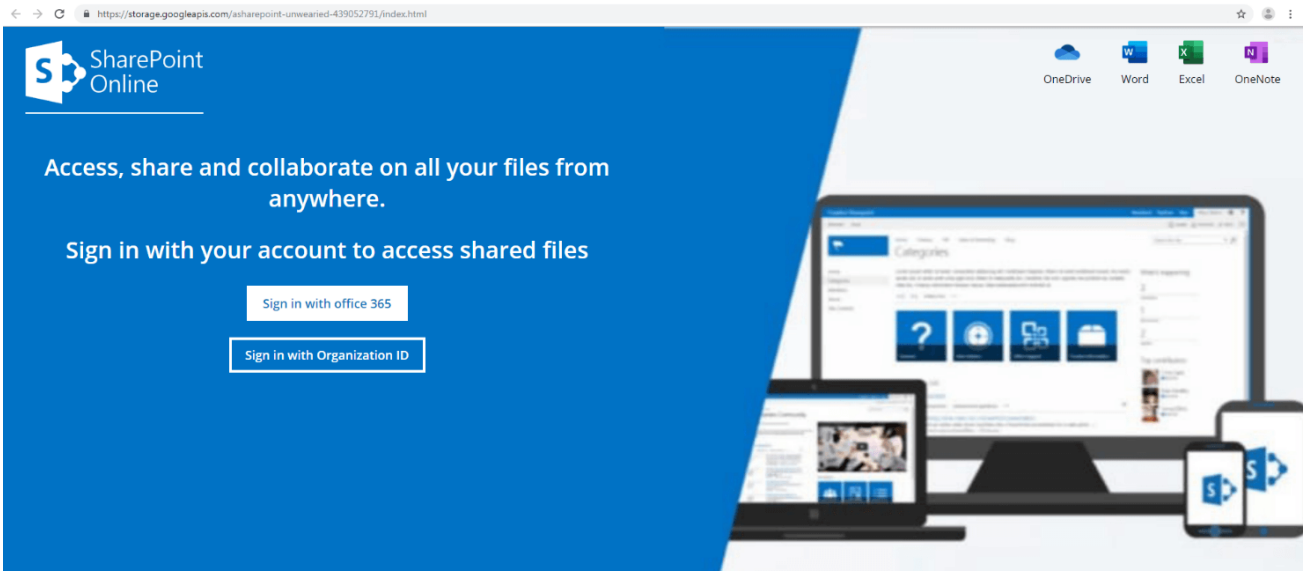
Recently, we published our research on how threat actors are taking advantage of well-known cloud services to download malicious payloads. This technique has also been observed in phishing attacks, where cloud storage services are used to host phishing pages.

Some of the warning signs that users generally look out for in a phishing attack include suspicious-looking domains, or websites without a HTTPS certificate. However, by using well-known public cloud services such as Google Cloud or Microsoft Azure to host their phishing pages, the attackers can overcome this obstacle and disguise their malicious intent, improving their chances of ensnaring even security-savvy victims.

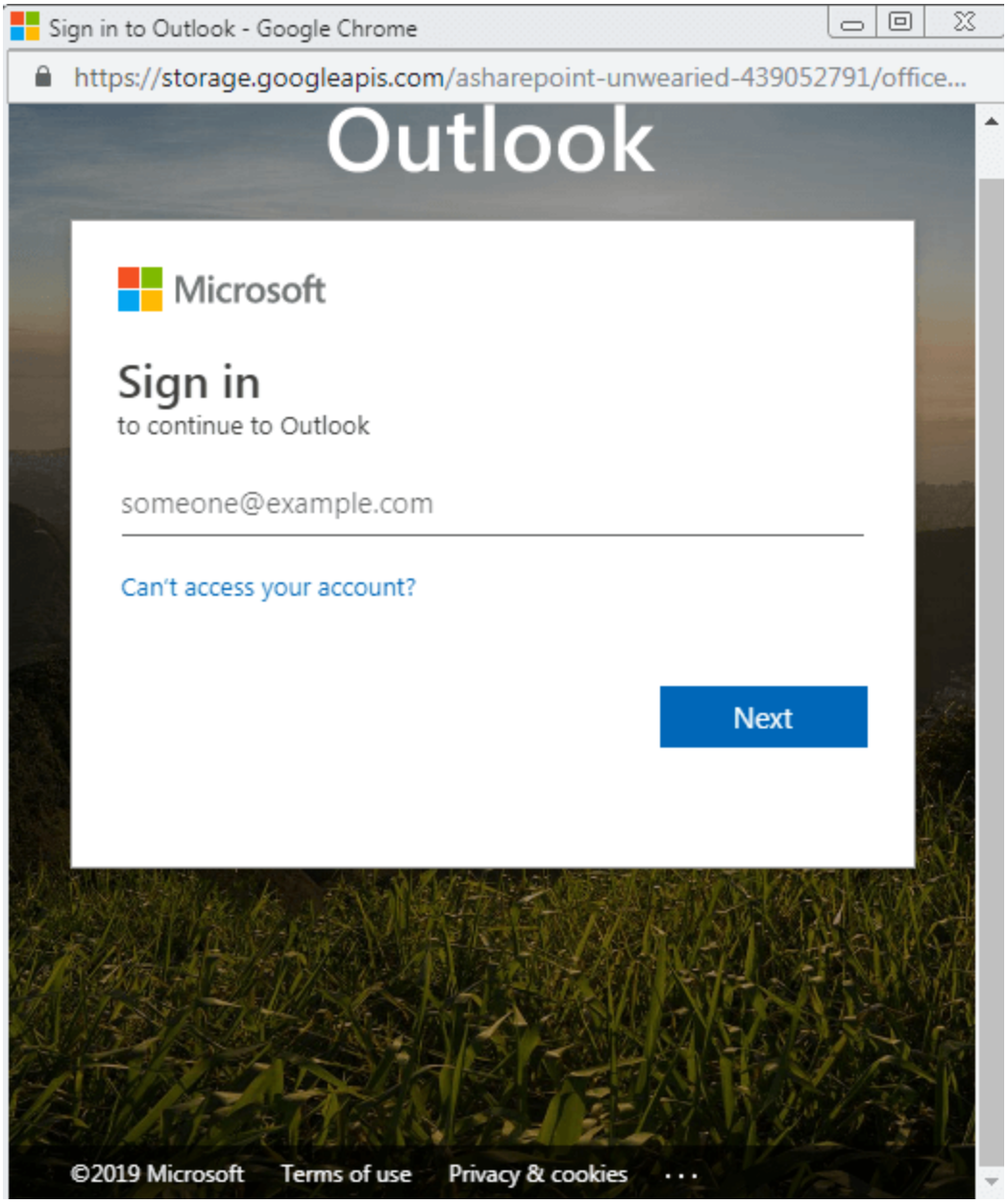
This was the case with a phishing attack we came across in January. The attack started with a PDF document that was uploaded to Google Drive, and included a link to a phishing page:



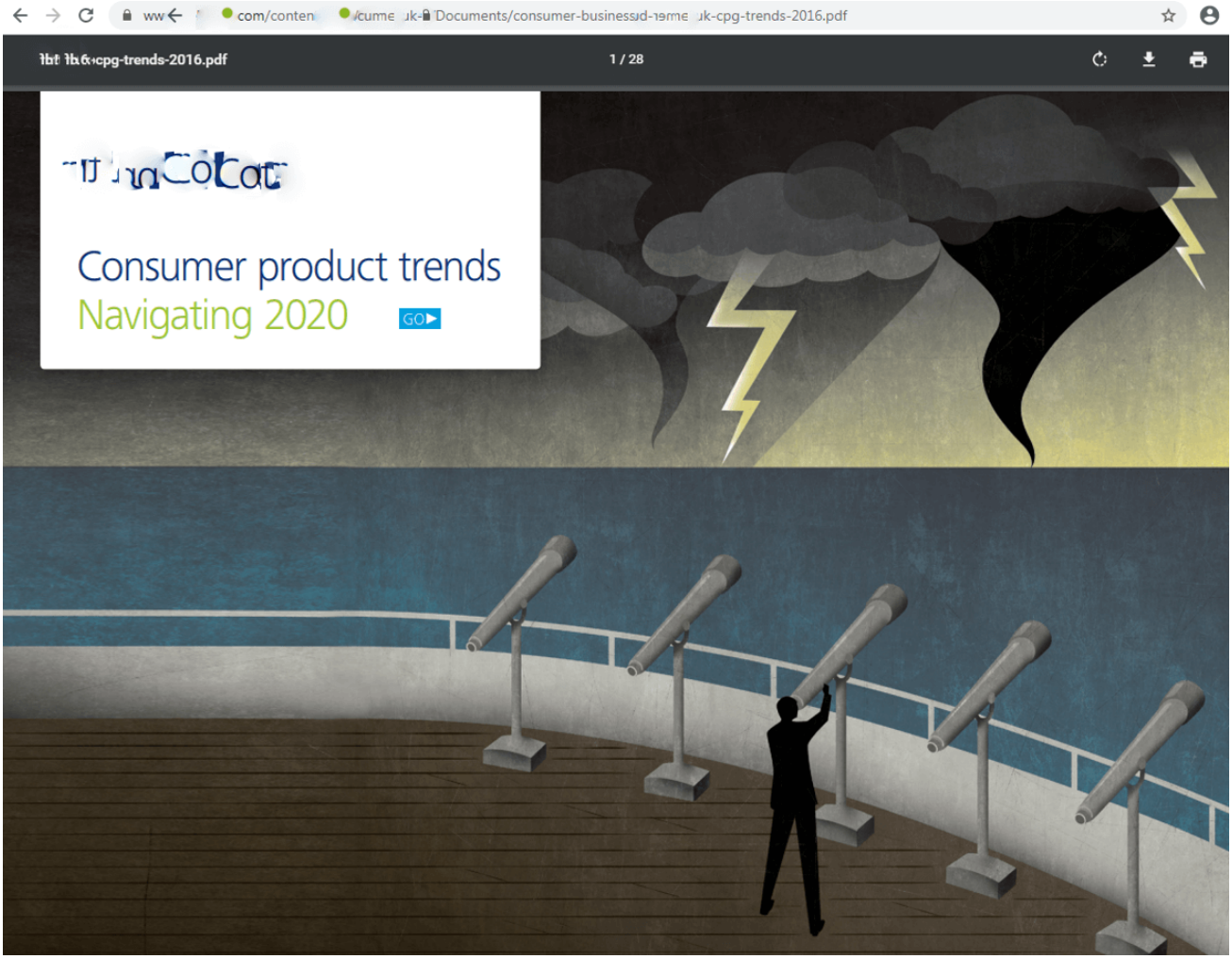
The phishing page, hosted on storage.googleapis[.]com/asharepoint-unwearied-439052791/index.html, asked the user to login with their Office 365 or organization e-mail:



When choosing one of the options, a pop-up window with the Outlook login page appears:



After the credentials were entered, the user is led to a real PDF report published by a renowned global consulting firm:



During all of these stages, the user never gets suspicious since the phishing page is hosted on Google Cloud Storage. However, viewing the phishing page's source code has revealed that most of the resources are loaded from a website that belongs to the attackers, prvtsmtp[.]com:

```
<div class="outer">
    <div class="app middle">
      <div class="background-logo-holder">
        <img id="banner_image" class="background-logo" src="
        https://prvtsmtp.com/email-list/office_bg/lib/img/logo3.png">
      </div>
      <div class="app fade-in-lightbox inner">
        <div>
          <img id="logo_image" class="banner-logo" src="
          https://prvtsmtp.com/email-list/office_bg/lib/img/logo2.svg">
        </div>
        <div>
```

In more recent attacks, even a sharp-eyed, savvy user might miss this, as the attackers started using Google Cloud Functions, a service that allows the running of code in the cloud. In this case, the resources in the phishing page were loaded from a Google Cloud Functions instance without exposing the attackers' own malicious domains:

```
<link rel="stylesheet" href=
"https://us-east1-firm-processor-264717.cloudfunctions.net/c4/6d6578736d74702e636f6d/
-/email-list/box/css/css_whE_FIKmCdJjmQukMY5DBbmkss9qZjXENYcyIcR-90c.css" media=
"all">
<link rel="stylesheet" href=
"https://us-east1-firm-processor-264717.cloudfunctions.net/c4/6d6578736d74702e636f6d/
-/email-list/box/css/css.css" media="all">
<link rel="stylesheet" href=
"https://us-east1-firm-processor-264717.cloudfunctions.net/c4/6d6578736d74702e636f6d/
-/email-list/box/css/css_7jDhC7Vm4-oxtUbtZMHwD8LA2Gp2KNpvOzvod9283FA.css" media=
"all">
```

Investigating prvtsmtp[.]com showed that it resolved to a Ukrainian IP address (31.28.168[.]4). Many other domains related to this phishing attack resolved to the same IP address, or to different ones on the same netblock.

RESOLUTIONS

1 - 25 of 77 ▾ ▸ Sort : Last Seen Descending ▾ 25 / Page ▾

Resolve	First
webpicture.cc	2019-10-17
prvtsmtp.com	2019-11-30
www.prvtsmtp.com	2019-12-02
apiserverdata1.com	2019-10-17
mainsmtp.com	2020-01-31
www.apiserverdata1.com	2019-10-17
apidatacss.com	2020-01-03
ns1.shareitoffice.xyz	2019-02-23
ns1.shareitonedrive.xyz	2019-02-23

This gave us an insight into the attackers' malicious activity over the years and allowed us to see how they have been developing their campaigns and introducing new techniques.

For example, we saw that back in 2018, the attackers used to host the phishing pages on the malicious websites directly. Later on, and before switching to Google Cloud Storage, the attackers took advantage of Azure Storage to host the phishing pages:

The attackers in this case seem to be taking advantage of different cloud storage services, a technique that has been gaining popularity due to the difficulties involved in detecting it. Because such services usually have legitimate uses and do not appear suspicious, both victims and network administrators have more difficulty identifying and fending off such attacks.

Google suspended this particular hacker project in January 2020 for phishing abuse, which subsequently suspended the URL as well as all URLs associated with that project since that time. Google investigates and suspends phishing pages when we become aware of them through Safe Browsing data feeds and other direct reports.

This incident highlights the efforts that scammers and criminals will make to conceal their malicious intentions, and to trick even security-savvy users. As we've noted in many previous blogs, practical steps we can all take to stay protected against these opportunistic attacks are:

1. Beware of lookalike domains, spelling errors in emails or websites, and unfamiliar email senders.
2. Be cautious with files received via email from unknown senders, especially if they prompt for a certain action you would not usually do.
3. Ensure you are ordering goods from an authentic source. One way to do this is NOT to click on promotional links in emails, and instead, Google your desired retailer and click the link from the Google results page.
4. Beware of “special” offers. “An exclusive cure for coronavirus for $150” is usually not a reliable or trustworthy purchase opportunity.
5. Make sure you do not reuse passwords between different applications and accounts.

Organizations should prevent zero-day attacks with end-to-end cyber architectures, to block deceptive phishing sites and provide alerts on password reuse in real time. And remember that your users’ mailboxes are the front door into your organization. Targeted phishing schemes steal $300B from businesses every month, so considers using email security measures too.