A Big Catch: Cloud Phishing from Google App Engine and Azure App Service

By Ashwin Vamshi

Published: 2020-08-12 · Archived: 2026-04-05 16:11:03 UTC

Threat actors are leveraging top tier cloud apps to host phishing baits. Netskope Threat Labs has identified an ongoing O365 phishing campaign hosted in Google App Engine with the credential harvester mostly hosted in Azure App Service. This phishing campaign typically targets O365 users via phishing emails with a direct link or attachment.

The campaign started in late June 2020 and is still active today. Based on similarities in the phishing pages, we believe the same threat actor is responsible for generating more than 100 phishing pages and continues to add more daily. These phishing pages and attack elements were hosted in different App Engine and Azure websites. At the time of writing, more than 60% of the URLs we observed were active and not detected or blocked by security scanning services in popular browsers like Chrome and Firefox.

Our earlier posts Phishing in the public cloud: You've been served and Amazon themed Phish hosted in Azure Sites detailed phishing attacks that used Azure Websites to serve up parts of the attack. This ongoing campaign indicates that threat actors are continuing to use cloud services to launch phishing attacks at scale from widely used cloud services, making it harder for users to recognize and vendors to detect, block, or take down.

This blog post details our analysis of this campaign and provides recommendations to help protect you and your organization from falling victim to similar phishing campaigns.

Appspot.com – Phishing baits

Google App Engine is a Google Cloud Platform (GCP) service for developing and hosting web applications. App Engine allows you to serve SSL (HTTPS) traffic through your appspot.com domain, https://<app>.r.appspot.com. Users tend to place trust in websites that are hosted by top-tier vendors like Google. Threat actors are exploiting this trust by hosting phishing baits in Google services as shown in Figure 1.

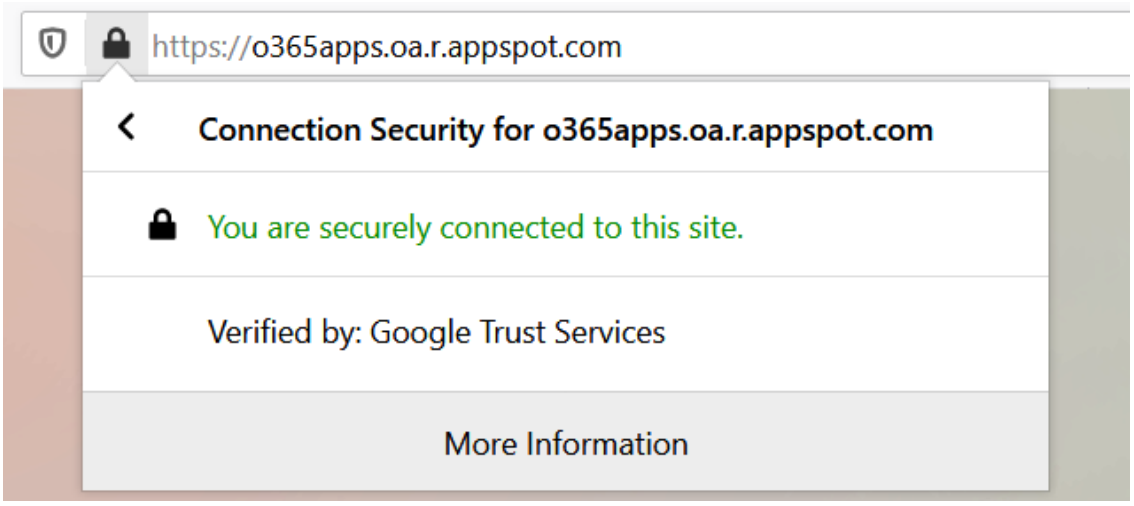

Figure 1: Phishing page hosted in appspot.com

Analysis of the phishing campaign

The attack starts with a bitly link shortener link, https://bitly[.]com/33nMLkZ, generally distributed via phishing emails that redirect to https://o365apps[.]oa.r.appspot.com as shown in Figure 2.

Figure 2: bitly URL shortener

When visiting the bait, the victim is presented with a phished page hosted in appspot.com to enter the credentials as shown in Figure 3.

Figure 3: Phished page hosted in appspot.com

Upon entering the email and password, the victim is presented with a fake message that the account and password are incorrect as shown in Figure 4.

Figure 4: Phished page displaying a fake message that the account or password is incorrect

The victim's credentials are then sent to the page, 'handler.php' hosted in july-28[.].azurewebsites[.]net as shown in Figure 5.

Figure 5: Snippet of the victim’s credentials hosted in july-28[.].azurewebsites[.]net

The packet capture illustrating this credential theft action is shown in Figure 6.

Figure 6: Packet capture of the credential theft

Phishing campaign

Using NSIQ, Netskope's in-house threat intelligence hub, we were able to identify multiple O365-themed phishing pages using appspot.com. Starting in late June, we observed 110 unique bait URLs and 72 credential hosting URLs related to this campaign. We identified that the threat actor tried using several domains to host the credentials as shown in Figure 7.

Figure 7: Credential hosted domains

The above figure clearly shows that the threat actor has mostly used Azure App Service to host the credential harvester at azurewebistes.net. It appears the attacker tried out multiple different options to serve the credential harvester and chose to use Azure App Service on an ongoing basis, likely because of its ease of use and Microsoft-issued SSL certs. That we continue to see new subdomains appear daily on both Azure App Service and Google App engine indicates that the attacker is having success on both of these platforms.

Conclusion

This post described a phishing campaign that used appspot.com and azurewebsites.net for hosting the phishing baits and attack elements. We would recommend users to not enter their credentials from unknown websites and hyperlinks even if the website is from a trusted domain. Users can recognize a phishing site based on the domain, which indicates that it is in App Engine appspot.com, and not an official Microsoft website. Enterprises should educate their users to recognize AWS, Azure, and GCP object store URLs, so they can discern phishing sites from official sites. Netskope reported the phishing sites to Google and Microsoft Security teams on August 10, 2020.

IOCs

p3lll0plprd.el.r.appspot.com

xxddfete.nw.r.appspot.com

eyettrttr.wn.r.appspot.com

login-microsoft-office365.df.r.appspot.com

sodium-ceremony-277916.dt.r.appspot.com

vp35yvpvyup.el.r.appspot.com

officeeev2.ew.r.appspot.com

tlook-off365-signin.el.r.appspot.com

microsoft-account-security.oa.r.appspot.com

userpodium.et.r.appspot.com

golden-pointer-281517.nw.r.appspot.com

civic-depth-281113.oa.r.appspot.com

user7770001255.el.r.appspot.com

vbf9iuherwiu.wl.r.appspot.com

userc9fo9ffzo.el.r.appspot.com

account-security-6581a.el.r.appspot.com

esoteric-mote-284316.uc.r.appspot.com

officecloudapps.ey.r.appspot.com

outlook-office365-signin.el.r.appspot.com

e710z0ear.du.r.appspot.com

user7383493930.et.r.appspot.com

xh36954689734987348098.el.r.appspot.com

cp0c7pc.du.r.appspot.com

ppypcc11crp.appspot.com

user67509874097802.el.r.appspot.com

sharepoint-secure-online.df.r.appspot.com

key-acronym-281808.et.r.appspot.com

keen-sight-280309.nw.r.appspot.com

login-microsoft-online-secure.nw.r.appspot.com

login-microsoft-outlook.el.r.appspot.com

x394uirjomokf30.wm.r.appspot.com

d48dkduy4mnnxh.du.r.appspot.com

riqri733r.ts.r.appspot.com

microsoftaccountsecurityportal.wl.r.appspot.com

mlcrosoft-0nedrive-portal.el.r.appspot.com

secure-login-microsoftonline.oa.r.appspot.com

arched-elixir-280012.nw.r.appspot.com

outlook-0ffice365-0nline.nw.r.appspot.com

user7774398409.el.r.appspot.com

microsoft-secure-online.oa.r.appspot.com

d91ddd0c.el.r.appspot.com

c0lbltclsp.el.r.appspot.com

sapient-flare-279107.df.r.appspot.com

r444r0r0uuser.du.r.appspot.com

user1238090.el.r.appspot.com

login-microsoft-0nline.ts.r.appspot.com

logln-office365-0nline.wm.r.appspot.com

microsov.oa.r.appspot.com

useryxijxui99.an.r.appspot.com

secureduser.du.r.appspot.com

my-project-1-6316.ue.r.appspot.com

officecloudapp.ey.r.appspot.com

micro-app-284821.appspot.com

compact-pier-280012.nw.r.appspot.com

user12746463989284.el.r.appspot.com

cbu4397422nj.oa.r.appspot.com

mm9pnpnjj.an.r.appspot.com

datasec.du.r.appspot.com

user379834709348-0.oa.r.appspot.com

userzixmessage.du.r.appspot.com

secure-microsoft-online.oa.r.appspot.com

jalonf129431.uc.r.appspot.com

officecloudweb.oa.r.appspot.com

login-office365-microsoft.el.r.appspot.com

y80yyxccn.df.r.appspot.com

xh1643879264863098023.el.r.appspot.com

offmenow20249.uc.r.appspot.com

qnaqaaa08cowa.et.r.appspot.com

outlook-webapp-portal.el.r.appspot.com

logln-micr0s0ft-0nline.ts.r.appspot.com

user983270932.oa.r.appspot.com

civil-campaign-279715.el.r.appspot.com

eliduhjner.dt.r.appspot.com

qu10hh1qh.ts.r.appspot.com

corporate-onlinecloudfiles.df.r.appspot.com

user849494949.el.r.appspot.com

login-outlook-office365.el.r.appspot.com

user9765656787.et.r.appspot.com

office365-login-outlook.el.r.appspot.com

sharedpont77wwjxjx.df.r.appspot.com

xh1oiuej.oa.r.appspot.com

sharepntonline.oa.r.appspot.com

pro645r.uk.r.appspot.com

office365-0nedrive-portal.el.r.appspot.com

user1246578909.el.r.appspot.com

ddccc-a8448.appspot.com

smartcloudfiles-2020.nw.r.appspot.com

nn0p00n0.ts.r.appspot.com

office365-portal-verify.el.r.appspot.com

login-offlce365-0utl00k.nn.r.appspot.com

fbproject4df3409fkl342ef043.el.r.appspot.com

xxxfoxwew.wn.r.appspot.com

o365apps.oa.r.appspot.com

securemssgs.du.r.appspot.com

crsupp0p011ypp.appspot.com

uuuiquiuroff.du.r.appspot.com

online-career-projects.ew.r.appspot.com

b60xbxvsharedpoint.an.r.appspot.com

f3jsffd3fosowa.ts.r.appspot.com

intense-reason-280011.nw.r.appspot.com

secureuser00403034.du.r.appspot.com

fy1i0cipn.et.r.appspot.com

secure-login-portal-outlook.el.r.appspot.com

user4567890.oa.r.appspot.com

idfudupp.du.r.appspot.com

gs68798094387.nw.r.appspot.com

office-mail-d-eliverys.el.r.appspot.com

v550vcc5ishare-onlieporit.et.r.appspot.com

hmmmchm8husers.du.r.appspot.co

tluyc30tc.an.r.appspot.com

user23546576879809ip.dt.r.appspot.com

sonarqberb.azurewebsites.net/handler3/handler.php

h088n00hq.azurewebsites.net/handler.php

ffddfdd00cp.azurewebsites.net/handler.php

officecallapp.azurewebsites.net/res/handler.php

just-storage.jp/7863473827382/handler.php

newonejj.azurewebsites.net/handler.php

bambangherlandi.web.id/backup/handler.php

ncloudset.com/themes.php

sonarquberb.azurewebsites.net/ceo/handler.php

sonarqberb.azurewebsites.net/handler1/handler.php

0977r90rz.azurewebsites.net/handler.php

00q0h8hqaph.azurewebsites.net/handler.php

pwwebtraffic.com/themes.php

p720j70al2cp.azurewebsites.net/handler.php

fud.azurewebsites.net/white/handler.php

col36543.azurewebsites.net/handler.php

dfdgfgfggr.azurewebsites.net/handler.php

9r9cz7r9rwa.azurewebsites.net/handler.php

co2y552p2cp.azurewebsites.net/handler.php

capitandescargas.com/urus/handler.php

sonarqberb.azurewebsites.net/newallusers/handler.php

slepeghed.azurewebsites.net/handler.php

c1oudhq.com/cryptome/themes.php

701r10010ye.azurewebsites.net/handler.php

sonarquberb.azurewebsites.net/1900/handler.php

c1oudhq.com/onos/themes.php

sdeedfr.azurewebsites.net/handler.php

fud.azurewebsites.net/gs/handler.php

sonarqberb.azurewebsites.net/ceolist/handler.php

hddhvvfh0chp.azurewebsites.net/handler.php

9hxs99qsq90.azurewebsites.net/handler.php

47w4j4jx4c.azurewebsites.net/handler.php

900h9fyy0.azurewebsites.net/handler.php

zrae1110rcpff.azurewebsites.net/handler.php

fud.azurewebsites.net/fud/handler.php

sonarquberb.azurewebsites.net/ley/handler.php

www.imai-zei.net/22323231210/handler.php

c1oudhq.com/wire/themes.php

3q302n022ppc.azurewebsites.net/handler.php

lecoless.azurewebsites.net/handler.php

sp0drsphhcf.azurewebsites.net/handler.php

www.imai-zei.net/only1/handler.php

sonarqberb.azurewebsites.net/handler2/handler.php

www.imai-zei.net/test/handler.php

fud.azurewebsites.net/snow/handler.php

sonarqberb.azurewebsites.net/allusersd1/handler.php

jlredes.com.br/well-known/handler.php

just-storage.jp/0191919191919/handler.php

just-storage.jp/83839839292/handler.php

btopensworld.com/page1/login.php

www.camperlife.jp/wp-includes/js/jcrop/handler.php

oticapenha.com.br/lord/handler.php

c1oudhq.com/crypt/themes.php

sonarqberb.azurewebsites.net/ausinew/handler.php

syeuijfy.azurewebsites.net/handler.php

c1oudhq.com/kel/themes.php

p2npnpn00.azurewebsites.net/handler.php

yinnyyn00p.azurewebsites.net/handler.php

sonarqberb.azurewebsites.net/7262020/handler.php

july-28.azurewebsites.net/handler.php

r7077hh1hc.azurewebsites.net/handler.php

steemneddone.azurewebsites.net/handler.php

cgfsfdgffdfgedg.azurewebsites.net/handler.php

accrocoroservices.azurewebsites.net/handler.php

c1oudhq.com/aol/login.php

90ddpp5rhub.azurewebsites.net/handler.php

sonarqberb.azurewebsites.net/allusersd2/handler.php

deepakrajgiri.com/well-known/handler.php

sonarqberb.azurewebsites.net/linkers4/handler.php

n0n0iitiiphl.azurewebsites.net/handler.php

ff02fefifiop.azurewebsites.net/handler.php

sdsfsfef.azurewebsites.net/handler.php
