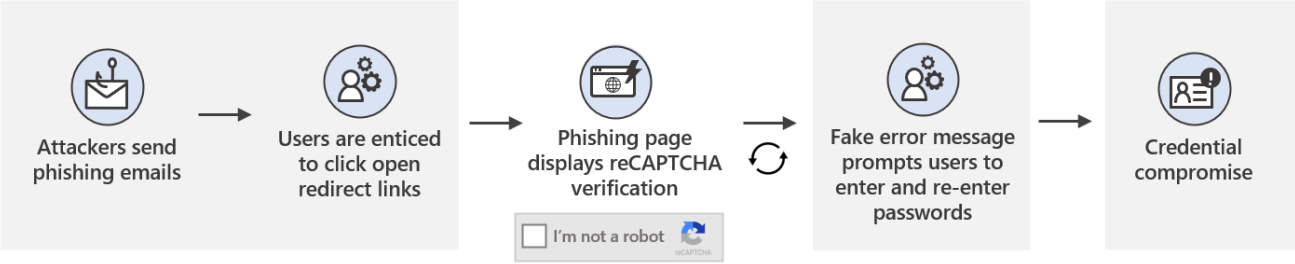
Widespread credential phishing campaign abuses open redirector links

microsoft.com/security/blog/2021/08/26/widespread-credential-phishing-campaign-abuses-open-redirector-links/

August 26, 2021



Microsoft has been actively tracking a widespread credential phishing campaign using open redirector links. Attackers combine these links with social engineering baits that impersonate well-known productivity tools and services to lure users into clicking. Doing so leads to a series of redirections—including a CAPTCHA verification page that adds a sense of legitimacy and attempts to evade some automated analysis systems—before taking the user to a fake sign-in page. This ultimately leads to credential compromise, which opens the user and their organization to other attacks.

The use of open redirects in email communications is common among organizations for various reasons. For example, sales and marketing campaigns use this feature to lead customers to a desired landing web page and track click rates and other metrics. However, attackers could abuse open redirects to link to a URL in a trusted domain and embed the eventual final malicious URL as a parameter. Such abuse may prevent users and security solutions from quickly recognizing possible malicious intent.

For instance, users trained to hover on links and inspect for malicious artifacts in emails may still see a domain they trust and thus click it. Likewise, traditional email gateway solutions may inadvertently allow emails from this campaign to pass through because their settings have been trained to recognize the primary URL without necessarily checking the malicious parameters hiding in plain sight.

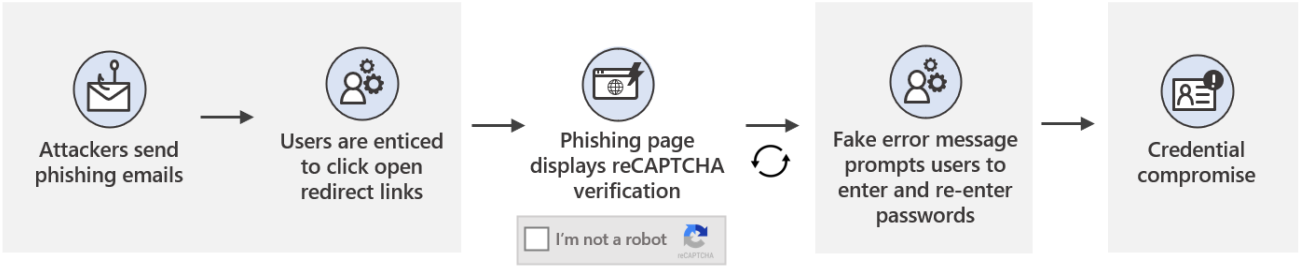


Figure 1. Attack chain for the open redirect phishing campaign

This phishing campaign is also notable for its use of a wide variety of domains for its sender infrastructure—another attempt to evade detection. These include free email domains from numerous country code top-level domains (ccTLDs), compromised legitimate domains, and attacker-owned domain generated algorithm (DGA) domains. As of this writing, we have observed at least 350 unique phishing domains used for this campaign. This not only shows the scale with which this attack is being conducted, but it also demonstrates how much the attackers are investing in it, indicating potentially significant payoffs.

Today's email threats rely on three things to be effective: a convincing social engineering lure, a well-crafted detection evasion technique, and a durable infrastructure to carry out an attack. This phishing campaign exemplifies the perfect storm of these elements in its attempt to steal credentials and ultimately infiltrate a network. And given that 91% of all cyberattacks originate with email, Organizations must therefore have a security solution that will provide them multilayered defense against these types of attacks.

Microsoft Defender for Office 365 detects these emails and prevents them from being delivered to user inboxes using multiple layers of dynamic protection technologies, including a built-in sandbox that examines and detonates all the open redirector links in the messages, even in cases where the landing page requires CAPTCHA verification. This ensures that even the embedded malicious URLs are detected and blocked. Microsoft Defender for Office 365 is backed by Microsoft experts who enrich the threat intelligence that feeds into our solutions through expert monitoring of email campaigns.

Attack analysis: Credential phishing via open redirector links

Credential phishing emails represent an extremely prevalent way for threat actors to gain a foothold in a network. The use of open redirects from legitimate domains is far from new, and actors continue to abuse its ability to overcome common precautions.

Phishing continues to grow as a dominant attack vector with the goal of harvesting user credentials. From our 2020 Digital Defense Report, we blocked over 13 billion malicious and suspicious mails in the previous year, with more than 1 billion of those emails classified as URL-based phishing threats.

In this campaign, we noticed that the emails seemed to follow a general pattern that displayed all the email content in a box with a large button that led to credential harvesting pages when clicked. The subject lines for the emails varied depending on the tool they impersonated. In general, we saw that the subject lines contained the recipient's domain and a timestamp as shown in the examples below:

- [Recipient username] 1 New Notification
- Report Status for [Recipient Domain Name] at [Date and Time]
- Zoom Meeting for [Recipient Domain Name] at [Date and Time]
- Status for [Recipient Domain Name] at [Date and Time]
- Password Notification for [Recipient Domain Name] at [Date and Time]
- [Recipient username] eNotification

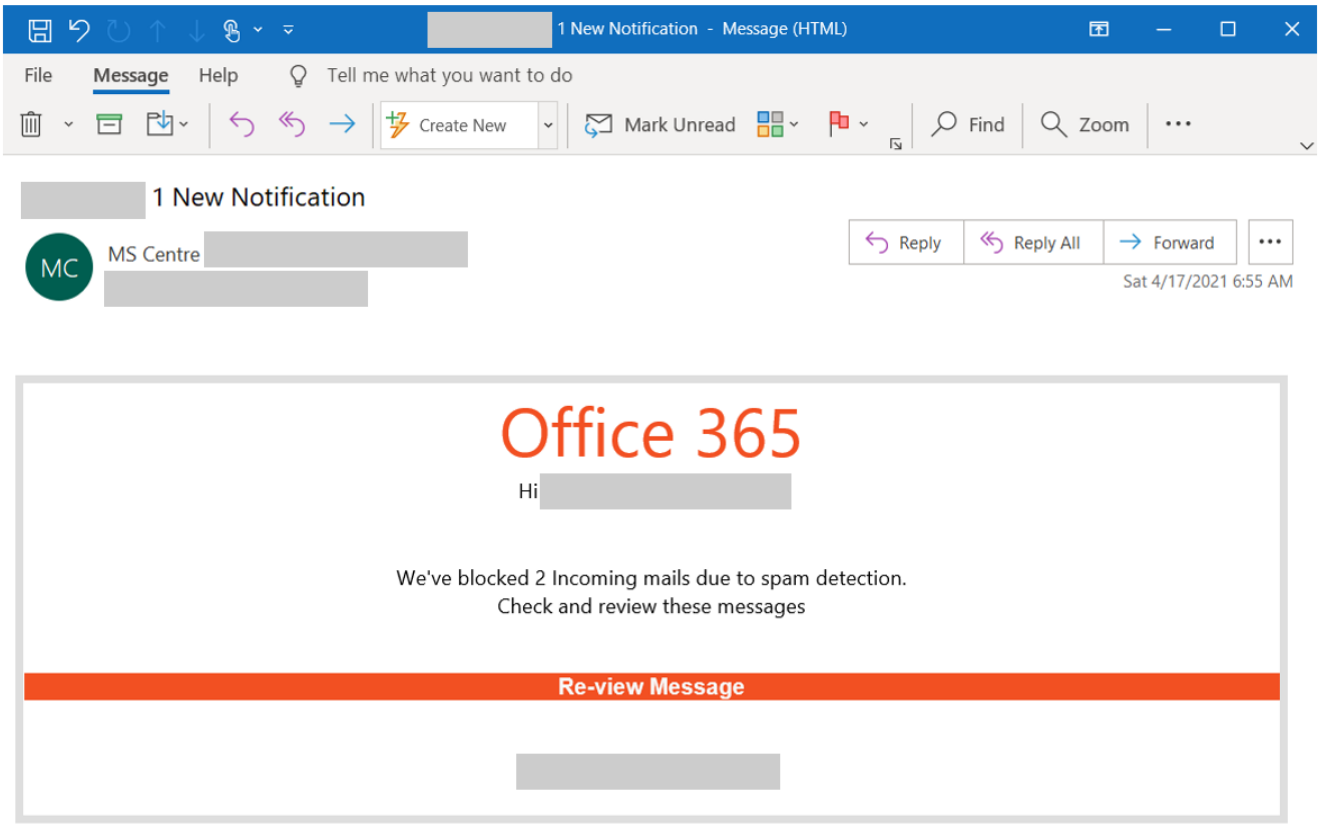


Figure 2. Sample phishing email masquerading as an Office 365 notification

Once recipients hover their cursor over the link or button in the email, they are shown the full URL. However, since the actors set up open redirect links using a legitimate service, users see a legitimate domain name that is likely associated with a company they know and trust. We believe that attackers abuse this open and reputable platform to attempt evading detection while redirecting potential victims to phishing sites.

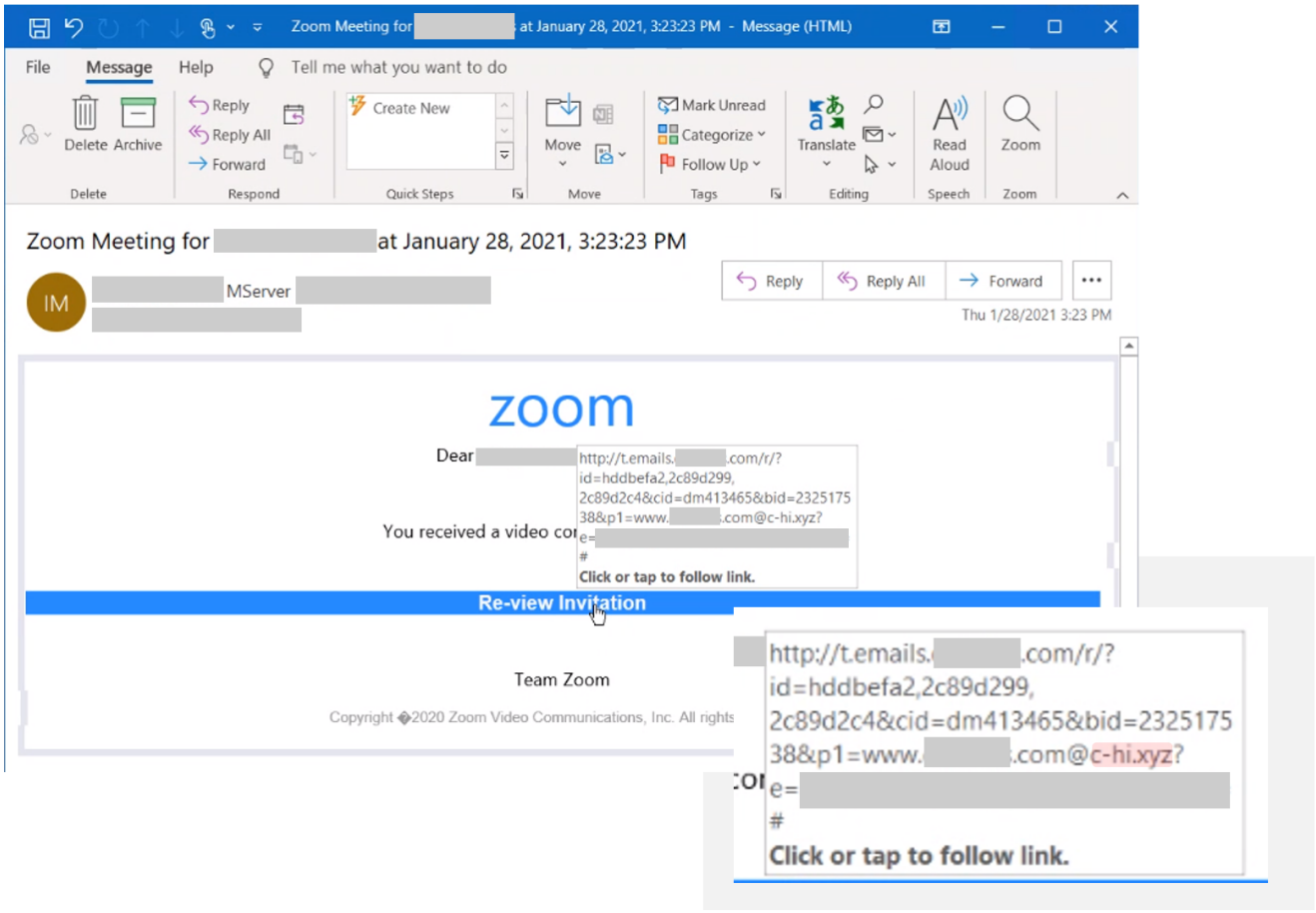


Figure 3. Hover tip showing an open redirect link with a legitimate domain and phishing link in the URL parameters

The final domains used in the campaigns observed during this period mostly follow a specific domain-generation algorithm (DGA) pattern and use .xyz, .club, .shop, and .online TLDs. The “Re-view invitation” button in Figure 3 points to a URL with a trusted domain followed by parameters, with the actor-controlled domain (c-hi[.]xyz) hidden in plain sight.

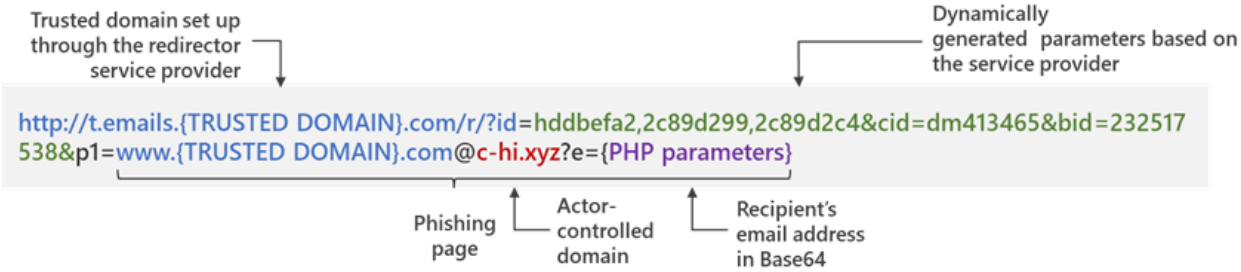


Figure 4. The actor-controlled domain uses a DGA pattern and a .XYZ top-level domain

In August, we detected a fresh spam run from this campaign that used a slightly updated Microsoft-spoofing lure and redirect URL but leveraged the same infrastructure and redirection chain.

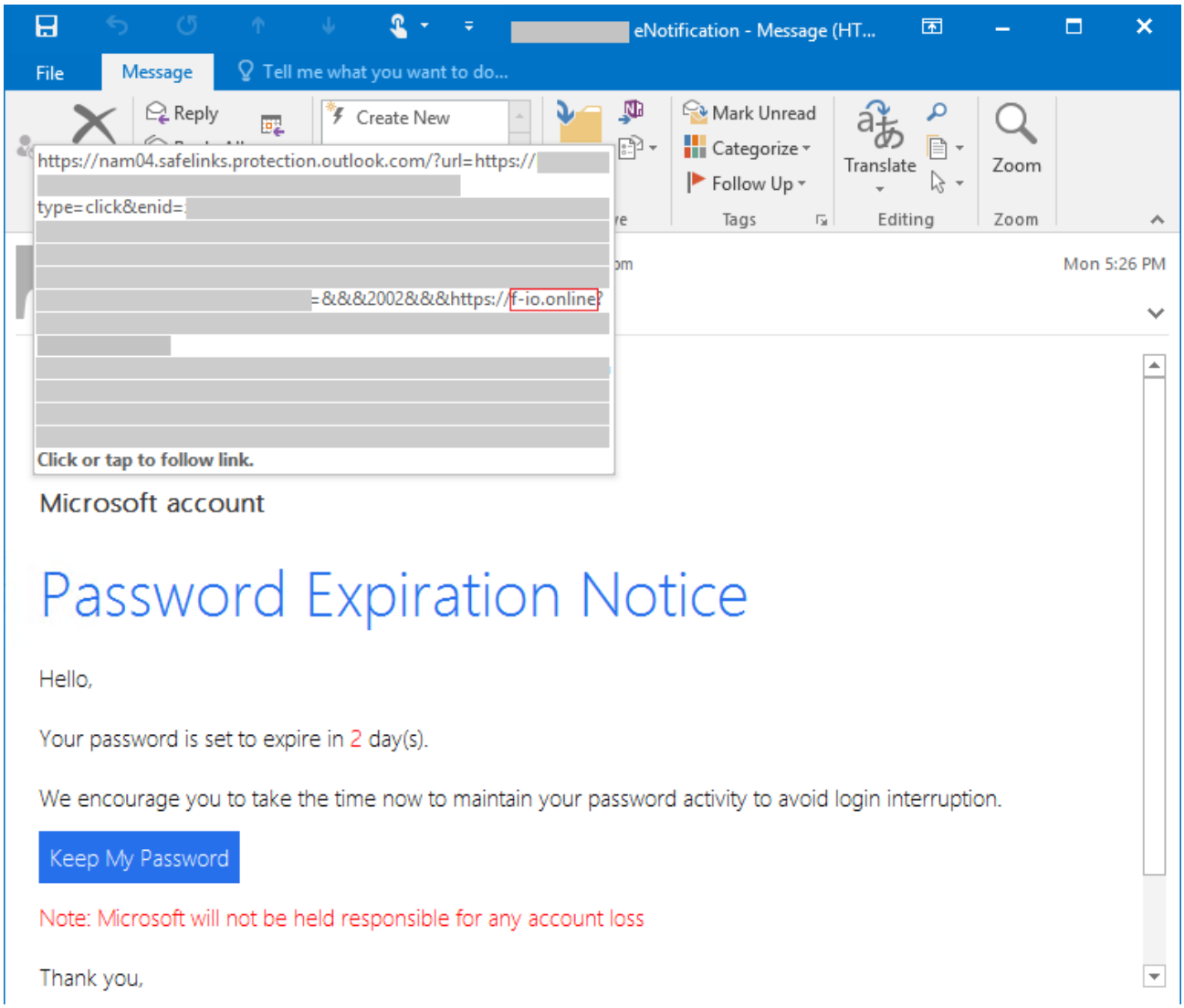


Figure 5. Sample phishing email from a recent spam run from this phishing campaign

These crafted URLs are made possible by open redirection services currently in use by legitimate organizations. Such redirection services typically allow organizations to send out campaign emails with links that redirect to secondary domains from their own domains. For example, a hotel might use open redirects to take email recipients to a third-party booking website, while still using their primary domain in links embedded in their campaign emails.

Attackers abuse this functionality by redirecting to their own malicious infrastructure, while still maintaining the legitimate domain in the full URL. The organizations whose open redirects are being abused are possibly unaware that this is even occurring.

Redirecting to phishing pages

Users who clicked one of the crafted redirect links are sent to a page in attacker-owned infrastructure. These pages used Google reCAPTCHA services to possibly evade attempts at dynamically scanning and checking the contents of the page, preventing some analysis systems from advancing to the actual phishing page.

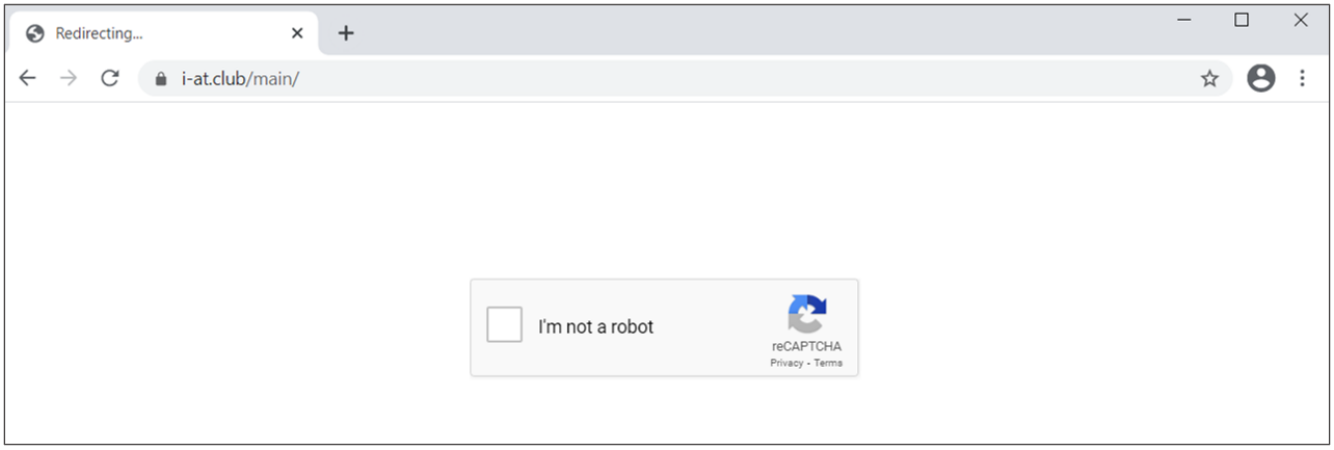


Figure 6. reCAPTCHA service used by phishing page

Upon completion of the CAPTCHA verification, the user is shown a site that impersonates a legitimate service, such as Microsoft Office 365, which asks the user for their password. The site is prepopulated with the recipient's email address to add legitimacy to the request. This technique leverages familiar single sign-on (SSO) behavior to trick users into keying in corporate credentials or other credentials associated with the email address.

To do this, attackers send unique URLs to each recipient with PHP parameters that cause tailored information to render in the phishing page. In some instances, phishing pages are specially crafted to include company logos and other branding tied to the recipient's domain.

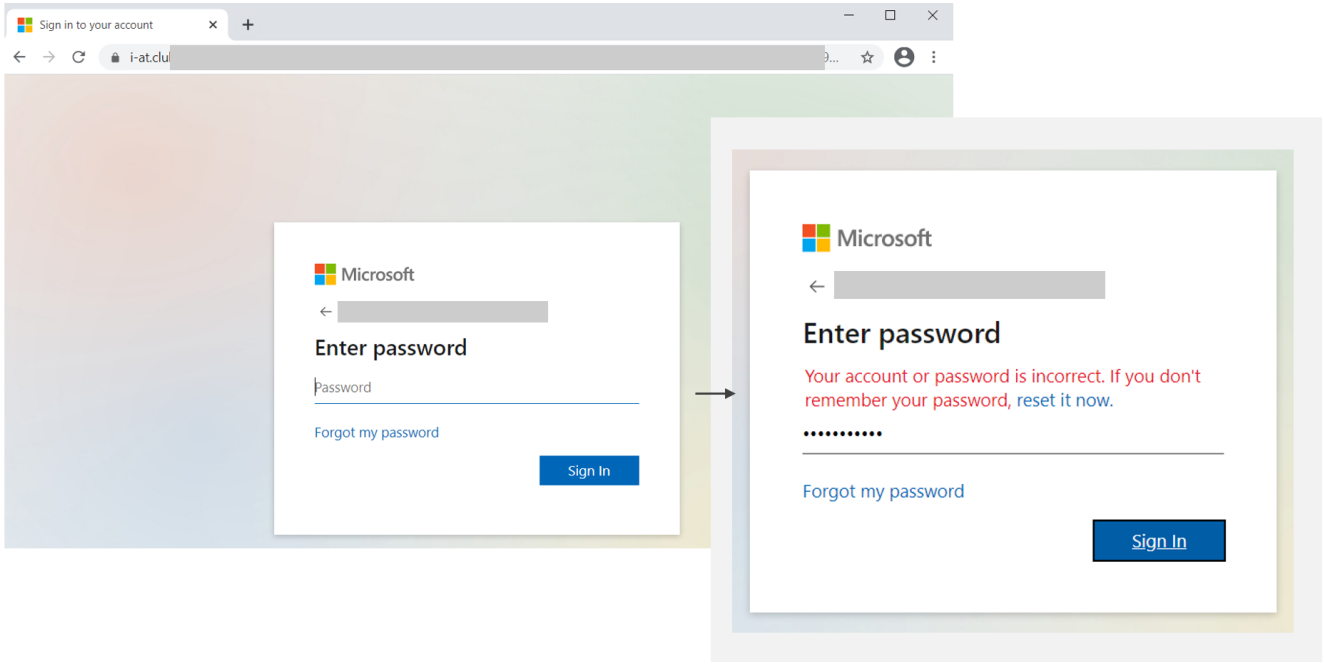


Figure 7. Fake sign-in page prefilled with the recipient email address alongside a fake error message prompting users to re-enter their passwords

If the user enters their password, the page refreshes and displays an error message stating that the page timed out or the password was incorrect and that they must enter their password again. This is likely done to get the user to enter their password twice, allowing attackers to ensure they obtain the correct password.

Once the user enters their password a second time, the page directs to a legitimate Sophos website that claims the email message has been released. This adds another layer of false legitimacy to the phishing campaign.

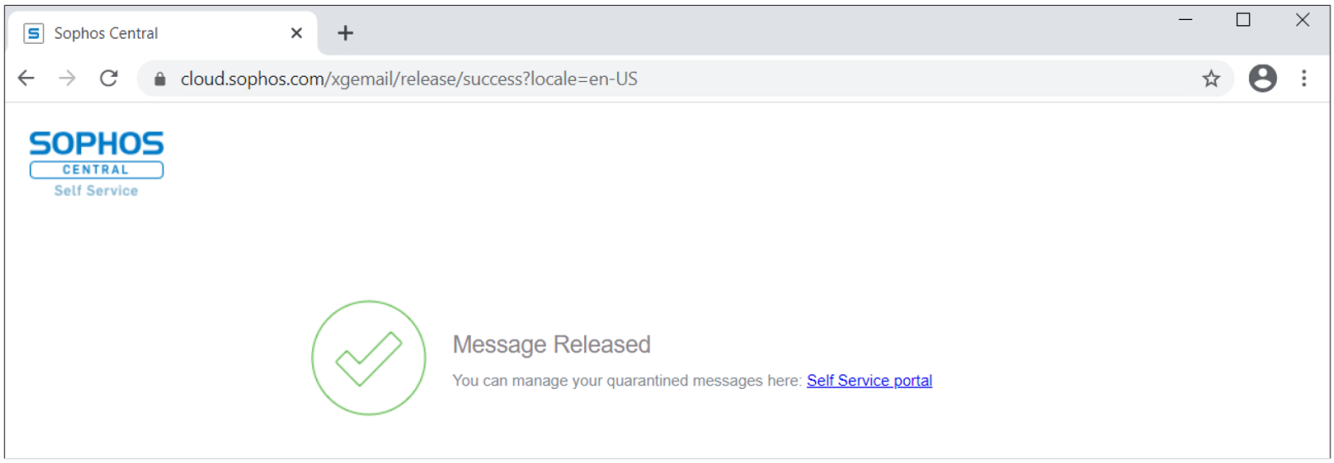


Figure 8. Legitimate Sophos page displayed after users re-enter their passwords

Tracking attacker-controlled domains

Some of the domains used in this campaign include the following:

- c-tl[.]xyz
- a-cl[.]xyz
- j-on[.]xyz
- p-at[.]club
- i-at[.]club
- f-io[.]online

For the observed campaigns, the sender infrastructure was fairly unique and notable as the actors used a wide variety of sender domains, with most of the domains having at least one of the following characteristics:

- Free email domains
- Compromised legitimate domains
- Domains ending in *.co.jp*
- Attacker-owned DGA domains

Many of the final domains hosting the phishing pages follow a specific DGA pattern:

- *[letter]-[letter][letter].xyz*
- *[letter]-[letter][letter].club*

The free email domains span a wide variety of ccTLDs, such as:

- de
- com.mx
- com.au
- ca

The attacker-owned DGA domains follow a few distinct patterns, including:

- *[word or string of characters]-[word][number], incrementing by one, for example: masihtidur-shoes08[.]com*
- *[number][word or string of characters]-[number], incrementing by one, for example: 23moesian-17[.]com*

- *[word][word][number], incrementing by one, for example: notoficationdeliveryamazon10[.]com*
- *[word or letters][number]-[number], incrementing by one, for example: dak12shub-3[.]com*

While these are the most prevalent patterns observed by Microsoft security researchers, over 350 unique domains have been observed during these campaigns.

How Microsoft Defender for Office 365 protects against modern email threats

The abuse of open redirectors represents an ongoing threat that Microsoft experts constantly monitor, along with other threat trends and attacker techniques used in attacks today. Microsoft's breadth of visibility into threats combined with our deep understanding of how attackers operate will continue to inform the advanced protection delivered by Microsoft Defender for Office 365 against email-based attacks.

For mitigations against the abuse of open redirector links via known third-party platforms or services, users are advised to follow the recommended best practices of their service providers, such as updating to the latest software version, if applicable, to prevent their domains from being abused in future phishing attempts.

Microsoft Defender for Office 365 protects customers from this threat by leverages its deep visibility into email threats and advanced detection technologies powered by AI and machine learning. We strongly recommend that organizations configure recommended settings in Microsoft Defender for Office 365, such as applying anti-phishing, Safe Links, and Safe Attachments policies. We also recommend installing the Report Message add-in for Outlook to enable users to report suspicious messages to their security teams and optionally to Microsoft.

Attack simulation lets organizations run realistic, yet safe, simulated phishing and password attack campaigns in your organization. These simulated attacks can help identify and find vulnerable users before a real attack makes a real impact.

Investigation capabilities in Microsoft Defender 365 allows organizations to respond phishing and other email-based attacks. Microsoft 365 Defender correlates signals from emails and other domains to deliver coordinated defense. Microsoft Defender for Endpoint blocks malicious files and other malware as well as malicious behavior that result from initial access via email. Microsoft Defender SmartScreen integrates with Microsoft Edge to block malicious websites, including phishing sites, scam sites, and other malicious sites, while Network protection blocks connections to malicious domains and IP addresses.

Learn how you can stop credential phishing and other email threats through comprehensive, industry-leading protection with Microsoft Defender for Office 365.

Microsoft 365 Defender Threat Intelligence Team

Advanced hunting queries

To locate possible credential phishing activity, run the following advanced hunting queries in Microsoft 365 Defender.

Open redirect URLs in t-dot format

Find URLs in emails with a leading "t", indicating possible open redirect URLs. Note: the use of a redirector URL does not necessitate malicious behavior. You must verify whether the emails surfaced via this AHQ are legitimate or malicious.

```
EmailUrlInfo
| where Url matches regex @"s?\:\/\/(?:www\.)?t\.(?:[\w\-\.]+\/+)+(?:r|redirect)\/?\?"
```

Open redirect URLs pointing to attacker infrastructure

Find URLs in emails possibly crafted to redirect to attacker-controlled URLs.

```
EmailUrlInfo
//This regex narrows in on emails that contain the known malicious domain pattern in the
URL from the most recent campaigns
| where Url matches regex @"^[a-zA-Z]\-[a-zA-Z]{2}\.(xyz|club|shop|online)"
```

Indicators of compromise

Following is a list of domains that match the DGA pattern used in sender addresses in this and other malicious campaigns. Note that these have not all been observed in mail flow related to this campaign.

masihtidur-shoes08[.]com	masihtidur-shoes07[.]com	masihtidur-shoes04[.]com
masihtidur-shoes02[.]com	masihtidur-shoes01[.]com	wixclwardwual-updates9[.]com
wixclwardwual-updates8[.]com	wixclwardwual-updates7[.]com	wixclwardwual-updates6[.]com
wixclwardwual-updates5[.]com	wixclwardwual-updates10[.]com	wixclwardwual-updates1[.]com
zxcsaxb-good8[.]com	zxcsaxb-good6[.]com	zxcsaxb-good5[.]com
zxcsaxb-good4[.]com	zxcsaxb-good3[.]com	zxcsaxb-good10[.]com
trashxn-euyr9[.]com	trashxn-euyr7[.]com	trashxn-euyr6[.]com
trashxn-euyr5[.]com	trashxn-euyr3[.]com	trashxn-euyr20[.]com
trashxn-euyr2[.]com	trashxn-euyr19[.]com	trashxn-euyr18[.]com
trashxn-euyr17[.]com	trashxn-euyr16[.]com	trashxn-euyr15[.]com
trashxn-euyr14[.]com	trashxn-euyr12[.]com	trashxn-euyr11[.]com
trashxn-euyr10[.]com	trashxn-euyr1[.]com	berangberang-9[.]com
berangberang-7[.]com	berangberang-12[.]com	berangberang-6[.]com
notoficationdeliveryamazon8[.]com	berangberang-8[.]com	berangberang-3[.]com
berangberang-4[.]com	berangberang-10[.]com	berangberang-11[.]com
berangberang-13[.]com	berangberang-5[.]com	77support-update23-4[.]com
posher876ffffff-30[.]com	posher876ffffff-5[.]com	posher876ffffff-25[.]com
fenranutc0x24ai-11[.]com	organix-xtc21[.]com	fenranutc0x24ai-13[.]com
fenranutc0x24ai-4[.]com	fenranutc0x24ai-17[.]com	fenranutc0x24ai-18[.]com
adminsecurity102[.]com	adminsecurity101[.]com	23moesian-17[.]com
23moesian-10[.]com	23moesian-11[.]com	23moesian-26[.]com
23moesian-19[.]com	23moesian-2[.]com	cokils2ptys-3[.]com
cokils2ptys-1[.]com	23moesian-20[.]com	23moesian-15[.]com
23moesian-18[.]com	23moesian-16[.]com	sux71a37-net19[.]com
sux71a37-net1[.]com	sux71a37-net25[.]com	sux71a37-net14[.]com

sux71a37-net18[.]com	sux71a37-net15[.]com	sux71a37-net12[.]com
sux71a37-net13[.]com	sux71a37-net20[.]com	sux71a37-net11[.]com
sux71a37-net27[.]com	sux71a37-net2[.]com	sux71a37-net21[.]com
bimspelitskalix-xuer9[.]com	account-info005[.]com	irformainsition0971a8-net16[.]com
bas9oiw88remnisn-12[.]com	bas9oiw88remnisn-27[.]com	bas9oiw88remnisn-26[.]com
bas9oiw88remnisn-11[.]com	bas9oiw88remnisn-10[.]com	bas9oiw88remnisn-5[.]com
bas9oiw88remnisn-13[.]com	bas9oiw88remnisn-1[.]com	bas9oiw88remnisn-7[.]com
bas9oiw88remnisn-3[.]com	bas9oiw88remnisn-20[.]com	bas9oiw88remnisn-8[.]com
bas9oiw88remnisn-23[.]com	bas9oiw88remnisn-24[.]com	bas9oiw88remnisn-4[.]com
bas9oiw88remnisn-25[.]com	romanseyilefreaserty0824r-2[.]com	romanseyilefreaserty0824r-1[.]com
sux71a37-net26[.]com	sux71a37-net10[.]com	sux71a37-net17[.]com
maills-activitymove02[.]com	maills-activitymove04[.]com	solution23-servviue-26[.]com
maills-activitymove01[.]com	copris7-yearts-6[.]com	copris7-yearts-9[.]com
copris7-yearts-5[.]com	copris7-yearts-8[.]com	copris7-yearts-37[.]com
securityaccount102[.]com	copris7-yearts-4[.]com	copris7-yearts-40[.]com
copris7-yearts-7[.]com	copris7-yearts-38[.]com	copris7-yearts-39[.]com
romanseyilefreaserty0824r-6[.]com	rick845ko-3[.]com	rick845ko-2[.]com
rick845ko-10[.]com	fasttuamz587-4[.]com	winb2as-wwersd76-19[.]com
winb2as-wwersd76-4[.]com	winb2as-wwersd76-6[.]com	org77supp-minty662-8[.]com
winb2as-wwersd76-18[.]com	winb2as-wwersd76-1[.]com	winb2as-wwersd76-10[.]com
org77supp-minty662-9[.]com	winb2as-wwersd76-12[.]com	winb2as-wwersd76-20[.]com
account-info003[.]com	account-info012[.]com	account-info002[.]com
laser9078-ter17[.]com	account-info011[.]com	account-info007[.]com
notoficationdeliveryamazon1[.]com	notoficationdeliveryamazon20[.]com	notoficationdeliveryamazon7[.]com
notoficationdeliveryamazon17[.]com	notoficationdeliveryamazon12[.]com	contackamazon1[.]com
notoficationdeliveryamazon6[.]com	notoficationdeliveryamazon5[.]com	notoficationdeliveryamazon4[.]com
notoficationdeliveryamazon18[.]com	notoficationdeliveryamazon13[.]com	notoficationdeliveryamazon3[.]com
notoficationdeliveryamazon14[.]com	gaplerr-xt5[.]com	posher876ffffff-29[.]com
kenatipurecehkali-xt3[.]com	kenatipurecehkali-xt13[.]com	kenatipurecehkali-xt4[.]com
kenatipurecehkali-xt12[.]com	kenatipurecehkali-xt5[.]com	wtbwts-junet1[.]com
kenatipurecehkali-xt6[.]com	hayalanphezor-2sit[.]com	hayalanphezor-1sit[.]com
noticesumartyas-sc24[.]com	noticesumartyas-sc13[.]com	noticesumartyas-sc2[.]com

noticesumartyas-sc17[.]com	noticesumartyas-sc22[.]com	noticesumartyas-sc5[.]com
noticesumartyas-sc4[.]com	noticesumartyas-sc21[.]com	noticesumartyas-sc25[.]com
appgetbox3[.]com	notoficationdeliveryamazon19[.]com	notoficationdeliveryamazon10[.]com
appgetbox9[.]com	appgetbox8[.]com	appgetbox6[.]com
notoficationdeliveryamazon2[.]com	appgetbox7[.]com	appgetbox5[.]com
notoficationdeliveryamazon23[.]com	appgetbox10[.]com	notoficationdeliveryamazon16[.]com
hvgjgj-shoes08[.]com	hvgjgj-shoes13[.]com	jgkxjhx-shoes09[.]com
hvgjgj-shoes15[.]com	hvgjgj-shoes16[.]com	hvgjgj-shoes18[.]com
hvgjgj-shoes20[.]com	hvgjgj-shoes12[.]com	jgkxjhx-shoes02[.]com
hvgjgj-shoes10[.]com	jgkxjhx-shoes03[.]com	hvgjgj-shoes11[.]com
hvgjgj-shoes14[.]com	jgkxjhx-shoes05[.]com	jgkxjhx-shoes04[.]com
hvgjgj-shoes19[.]com	jgkxjhx-shoes08[.]com	hpk02h21yyts-6[.]com
romanseyilefreaserty0824r-7[.]com	gets25-amz[.]net	gets30-amz[.]net
gets27-amz[.]net	gets28-amz[.]net	gets29-amz[.]net
gets32-amz[.]net	gets3-amz[.]net	gets31-amz[.]net
noticesumartyas-sc19[.]com	noticesumartyas-sc23[.]com	noticesumartyas-sc18[.]com
noticesumartyas-sc15[.]com	noticesumartyas-sc20[.]com	noticesumartyas-sc16[.]com
noticesumartyas-sc29[.]com	rick845ko-1[.]com	bas9oiw88remnisn-9[.]com
rick845ko-5[.]com	bas9oiw88remnisn-21[.]com	bas9oiw88remnisn-2[.]com
bas9oiw88remnisn-19[.]com	rick845ko-6[.]com	bas9oiw88remnisn-22[.]com
bas9oiw88remnisn-17[.]com	bas9oiw88remnisn-16[.]com	adminmabuk103[.]com
account-info008[.]com	suppamz2-piryshj01-3[.]com	dak12shub-1[.]com
securemanageprodio-02[.]com	securemanageprodio-05[.]com	securemanageprodio-01[.]com
dak12shub-3[.]com	dak12shub-9[.]com	dak12shub-8[.]com
dak12shub-6[.]com	dak12shub-10[.]com	dak12shub-4[.]com
securemanageprodio-03[.]com	org77supp-minty662-7[.]com	winb2as-wwersd76-7[.]com
org77supp-minty662-10[.]com	bimspelitskalix-xuer2[.]com	gets34-amz[.]net
gets35-amz[.]net	service-account-7254[.]com	service-account-76357[.]com
service-account-7247[.]com	account-info004[.]com	service-account-5315[.]com
bas9oiw88remnisn-14[.]com	solution23-servviue-23[.]com	organix-xtc18[.]com
romanseyilefreaserty0824r-4[.]com	hayalanphezor-7sit[.]com	bimspelitskalix-xuer7[.]com
securemanageprodio-04[.]com	solution23-servviue-15[.]com	solution23-servviue-1[.]com

suppamz2-piryshj01-9[.]com	suppamz2-piryshj01-6[.]com	solution23-servviue-25[.]com
solution23-servviue-7[.]com	solution23-servviue-16[.]com	solution23-servviue-11[.]com
solution23-servviue-27[.]com	romanseyilefreaserty0824r-5[.]com	cokils2ptys-6[.]com
solution23-servviue-9[.]com	solution23-servviue-19[.]com	solution23-servviue-8[.]com
solution23-servviue-17[.]com	solution23-servviue-18[.]com	suppamz2-piryshj01-1[.]com
solution23-servviue-30[.]com	solution23-servviue-13[.]com	solution23-servviue-12[.]com
solution23-servviue-10[.]com	solution23-servviue-4[.]com	solution23-servviue-20[.]com
solution23-servviue-24[.]com	solution23-servviue-5[.]com	solution23-servviue-14[.]com
service-account-7243[.]com	service-account-735424[.]com	service-account-8457845[.]com
service-account-374567[.]com	service-account-764246[.]com	service-account-762441[.]com
gxnhfghnjzh809[.]com	xcfhjxfyxnhnjzh10[.]com	accountservicealert002[.]com
accountservicealert003[.]com	care887-yyrtconsumer23-24[.]com	bas9oiw88remnisn-15[.]com
care887-yyrtconsumer23-23[.]com	care887-yyrtconsumer23-27[.]com	care887-yyrtconsumer23-25[.]com
care887-yyrtconsumer23-26[.]com	laser9078-ter11[.]com	bimspelitskalix-xuer6[.]com
laser9078-ter10[.]com	hayalanphezor-6sit[.]com	hayalanphezor-4sit[.]com
hayalanphezor-3sit[.]com	romanseyilefreaserty0824r-3[.]com	solution23-servviue-6[.]com
ressstauww-6279-3[.]com	ressstauww-6279-10[.]com	sytesss-tas7[.]com
ressstauww-6279-7[.]com	ressstauww-6279-1[.]com	hvgjgj-shoes01[.]com
ketiak-muser14[.]com	ketiak-muser13[.]com	ketiak-muser15[.]com
spammer-comingson01[.]com	spammer-comingson02[.]com	spammer-comingson04[.]com
spammer-comingson05[.]com	spammer-comingson07[.]com	posidma-posidjar01[.]com
posidma-posidjar03[.]com	posidma-posidjar05[.]com	posidma-posidjar06[.]com
tembuslah-bandar01[.]com	tembuslah-bandar02[.]com	tembuslah-bandar03[.]com
tembuslah-bandar04[.]com	tembuslah-bandar05[.]com	tembuslah-bandar06[.]com
tembuslah-bandar07[.]com	tembuslah-bandar08[.]com	tembuslah-bandar09[.]com
tembuslah-bandar10[.]com		