

# Resurgence of Voicemail-themed Phishing Attacks Targeting Key Industry Verticals in US

[zscaler.com/blogs/security-research/resurgence-voicemail-themed-phishing-attacks-targeting-key-industry](https://zscaler.com/blogs/security-research/resurgence-voicemail-themed-phishing-attacks-targeting-key-industry)



## Summary

Since May 2022, ThreatLabz has been closely monitoring the activities of a threat actor which targets users in various US-based organizations with malicious voicemail-notification-themed emails in an attempt to steal their Office365 and Outlook credentials. The tactics, techniques, and procedures (TTPs) of this threat actor have a high overlap with a previous voicemail campaign that [ThreatLabz analyzed in July 2020](#).

In this new instance of the campaign, the threat actor has targeted users in US-based organizations in specific verticals including software security, US military, security solution providers, healthcare / pharmaceutical, and the manufacturing supply chain.

As Zscaler was one of the targeted organizations, it gave us a good insight into the full attack chain and motives of this threat actor.

## Key points

- Voicemail-themed phishing campaigns continue to be a successful social engineering theme used by this threat actor to lure victims in opening a malicious attachment.
- Multiple key industry verticals in the US such as military, software security vendors, healthcare, pharmaceuticals, and the manufacturing supply chain were targeted by this threat actor.

- The goal of the threat actor is to steal credentials of Office365 and Outlook accounts, both of which are widely used in large enterprises.
- A CAPTCHA is used by the threat actor to guard the final credential phishing page from automated URL analysis algorithms.
- Each URL is specifically crafted for the targeted individual and the targeted organization.
- The campaign is active at the time of publishing this report.

## **Attack chain**

---

The attack flow involves a voicemail-themed notification email sent to the victim. The email contains an HTML attachment which, when opened, will redirect the user to a credential phishing site. The goal of the threat actor is to harvest Office 365 credentials of the victim.

We will describe each component of the attack-chain in more detail in this report.

## **Attack chain [Technical analysis]**

---

### **Email analysis**

---

The email theme is focused on a voicemail notification that tells the victim they have a missed voicemail, prompting the user to open the HTML attachment. This social engineering technique has worked successfully for the threat actor in previous campaigns.

Figure 1 shows an example of the email sent to the victim. The "From" field of the email was crafted specifically to align with the targeted organization's name.

From Zscaler.com| Optima Cell Telephone <info@marklines.com> ☆  
Subject [🚨] V\_audio missed on 6/14/2022 08:17 AM  
To [REDACTED]@zscaler.com ☆



You have a new voicemail from (WIRELESS CALLER)

## YOU HAVE A NEW VOICEMAIL!

You have a new voice mail from **(WIRELESS CALLER)**.

Listen by opening the enclosed attachment.

Sent by NetSapiens

1 attachment: 📎 VM\_Tuesday, June 14, 2022-5560.htm 754 bytes

📎 VM\_Tuesday, June 14, 2022-5560.htm 754 bytes

*Figure 1: Voicemail-themed email sent to a user at Zscaler*

Analysis of the email headers shows that the threat actor leveraged email servers located in Japan. Figure 2 shows the headers for one of the emails.

```

1  [A] A VN was left on you device.eml x
2  Delivered-To: @zscaler.com
3  Received: by 2002:a05:600c:500b:0:0:0:0 with SMTP id n11csp1624413wmr;
4  Fri, 10 Jun 2022 07:41:08 -0700 (PDT)
5  X-Google-Smtp-Source: ABdhPjXMedf1Uuq0ajj/1/q1sUgUfln0J...9afzwdUQTGMCleNdTXwvHeehi
6  X-Received: by 2002:a17:902:bb90:b0:163:ad4c:624b with SMTP id m16-20020a170902b99000...44840363pls.87.1654872068440;
7  Fri, 10 Jun 2022 07:41:08 -0700 (PDT)
8  ARC-Seal: i=1; a=rsa-sha256; t=1654872068; cv=none;
9  d=google.com; s=arc-20160816;
10 b=xQAYN8J1LIAsZX2LoiP09PscVq0/7050ZvlpskCnhMibc90FtoX0Myv1UwJndAaMn7
11 IudAYHwM3ai52IncSWeTp038DdeQ1o9w/rMvW155jSqHzePcM+Cs+0R+rCaPs18LT0Zz
12 tRELZgdf8uZPByeMj51XseXb/uMyw+Y4bu66zh5DPkxmFrdN0qJFb2oFwrdEUR6182L
13 m9JjEuMVY3RRPjIG92g8DHUUN+es0HBh43smKVhV9mw2GyYQK0DeYJTMVw91E-Szr4i
14 pvPv...
15 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
16 h=mime-version:date:message-id:subject:to:from:content-disposition
17 :content-transfer-encoding;
18 bh=2HqgtJCHLe4C1Sq5Bz8fd7645TZEEN7zRR+55WRxY+;
19 b=BqnY+EXGhqAbehAgNzcb4qn6Bn105oK10ovN0Lo5eWMh3txbblTKXsU+wDSDJGqNP
20
21 MRDRzfc6PzB7gCRREtvm1shUawG5qIsdTbFwFk59vipmz55o0H6+tpsF0q80ZNLyS
22 a4G=/refpe1IPV1Fhe5xxEhdawXA08aTxdh10iqNLL280TgV/S8rZL3TK8HNK9ZFHLX
23 BKrEQ5Wyn93antqby75cD5+k41lz8Mj/SxvAzd3501ryKtSFoaZa6Lau5fCWGXhpCTS3
24 xMl0...
25 ARC-Authentication-Results: i=1; mx.google.com;
26 spf=pass (google.com: domain of ad-8jsuo@eat-inc.jp designates 157.7.188.21 as permitted sender) smtp.mailfrom=ad-8jsuo@eat-inc.jp
27 Return-Path: <ad-8jsuo@eat-inc.jp>
28 Received: from mail505.heteml.jp (mail505.heteml.jp. [157.7.188.21])
29 by mx.google.com with ESMTPS id q3-20020a656a8300000b003fb1476fa3bsi38831928pgu.363.2022.06.10.07.41.08
30 for @zscaler.com>
31 (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
32 Fri, 10 Jun 2022 07:41:08 -0700 (PDT)
33 Received-SPF: pass (google.com: domain of ad-8jsuo@eat-inc.jp designates 157.7.188.21 as permitted sender) client-ip=157.7.188.21;
34 Authentication-Results: mx.google.com;
35 spf=pass (google.com: domain of ad-8jsuo@eat-inc.jp designates 157.7.188.21 as permitted sender) smtp.mailfrom=ad-8jsuo@eat-inc.jp
36 Received: from localhost.localdomain (localhost.localdomain [127.0.0.1])
37 by mail505.heteml.jp (Postfix) with QMPP id 3BB867C10F7
38 for @zscaler.com> Fri, 10 Jun 2022 23:41:07 +0900 (JST)
39 Received: from unknown (HELO mail505.heteml.jp) (mail@wkjn.jp[127.0.0.1])
40 by mail505.heteml.jp with SMTP; 10 Jun 2022 23:41:07 +0900
41 Received: from 20.222.90.215 (20.222.90.215)
42 by mail505.heteml.jp (HETEML-Fsecure);
43 Fri, 10 Jun 2022 23:39:43 +0900 (JST)
44 X-Virus-Status: clean(HETEML-Fsecure);
45 Content-Type: text/html; name="=UTF-8?Q?=E2=99=AC_VM=5F443147=2Ehtm?="
46 Content-Transfer-Encoding: base64
47 Content-Disposition: attachment;
48 filename="=utf-8'%E2%99%AC%20VM_443147.htm
49 X-Ms-Exchange-Organization-MessagingDirectionality: Originating
50 X-Ms-Exchange-Organization-AuthAs: Internal
51 X-Ms-Exchange-Organization-AuthMechanism: 02
52 X-Ms-Exchange-Organization-AuthSource:
53 NwMPP22MB00914.namprd22.prod.outlook.com
54 X-Ms-Exchange-Organization-Network-Message-ID:
55 ffe8bf42-c85a-42c8-a084-08d75b722819

```

Figure 2: Email header

```

toor@ubuntu:~$ dig @1.1.1.1 eat-inc.jp txt +short
"v=spf1 include:spf.heteml.jp ~all"

```

Figure 3: Mail server details

## HTML attachment analysis

For the purpose of analysis, we will consider the HTML attachment with the MD5 hash: dd0ddbc951de5cad9c8ace516c514693

Figure 4 shows the HTML attachment sent in the email which contains encoded JavaScript.

```

VM_443147.html [3]
1  <script language="javascript">document.write( unescape(
' %3C!DOCTYPE%20html%20PUBLIC%20%22-%2F%2Fw3c%2F%2FDTD%20XHTML%201.0%20Transitional%2F%2FEN%22%20%22http%3A%2F%2Fw
ww.w3.org%2FTR%2F%2Fhtml%2F%2FDTD%2F%2Fhtml1-transitional.dtd%22%3E%0D%0A%3Chtml%20xmlns%3D%22http%3A%2F%2Fwww.w3.org%2
F1999%2F%2Fhtml%22%3E%0D%0A%3Chead%3E%0D%0A%3Cmeta%20http-equiv%3D%22Content-Type%22%20content%3D%22text%2Fhtml%3B%
20charset%3Dutf-8%22%20%2F%3E%0D%0A%3Ctitle%3EPlease%20wait...%3C%2Ftitle%3E%0D%0A%3Cscript%3E%20%0D%0Awindow. loc
ation.replace(%22http%3A%2F%5C%2F%5C%5C%5C%2F%5C%5C%2F%2F%2Fzscaler.zscaler.briccorp.com%2F
IuY29t%22)%3B%0D%0A%3C%2Fscript%3E%0D%0A%3C%2Fhead%3E%0D%0A%3Cbody%3E%0D%0A%3C%2Fbody%3E%0D%0A%3C%2Fhtml%3E' )
);</script>

```

Figure 4: HTML attachment

Figure 5 shows the resulting code after deobfuscation.

```
<!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>Please wait...</title>
<script>
window.location.replace("http://\\\\"\\\\"\\\\"zscaler.zscaler.briccorp.com/");
</script>
</head>
<body>
</body>
</html>
```

Figure 5: Decoded JavaScript from the HTML attachment

This code redirects the user to an attacker-controlled URL using window.location.replace()

## URL analysis

### [Stage-1 URL] - Redirector

The URL inside the HTML attachment is a redirector URL which redirects the user to the final credential phishing page.

In each instance of the attack, the URL followed a consistent format which included the name of the targeted organization as well as the email address of the targeted individual. Figure 6 below highlights the format.

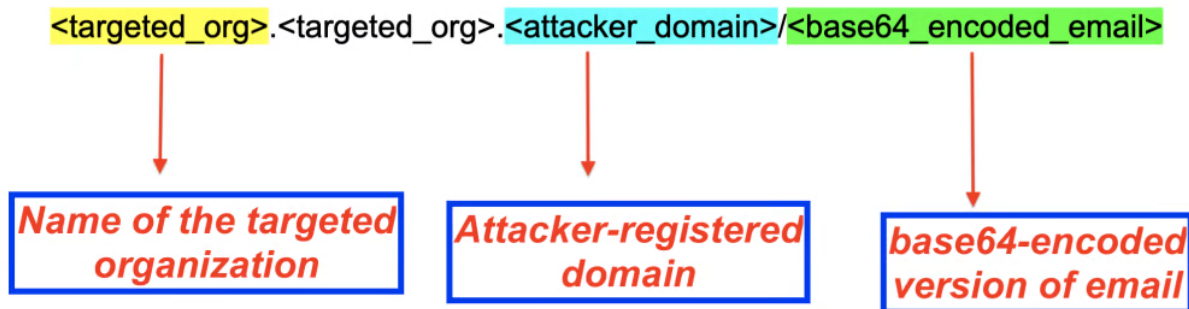


Figure 6: Stage-1 URL format

For instance, when an individual in Zscaler was targeted, the URL used the following format:

zscaler.zscaler.briccorp[.]com/<base64\_encoded\_email>

Since the format of the URL gives away critical information about the target, we used that information from our collected telemetry to enumerate the list of targeted organizations and individuals.

Based on analysis of this telemetry, we can conclude with a high confidence level that the targets chosen by the threat actor are organizations in the US military, security software developers, security service providers, healthcare / pharmaceutical and supply-chain organizations in manufacturing and shipping.

It is important to note that if the URL does not contain the base64-encoded email at the end; it instead redirects the user to the Wikipedia page of MS Office or to office.com.

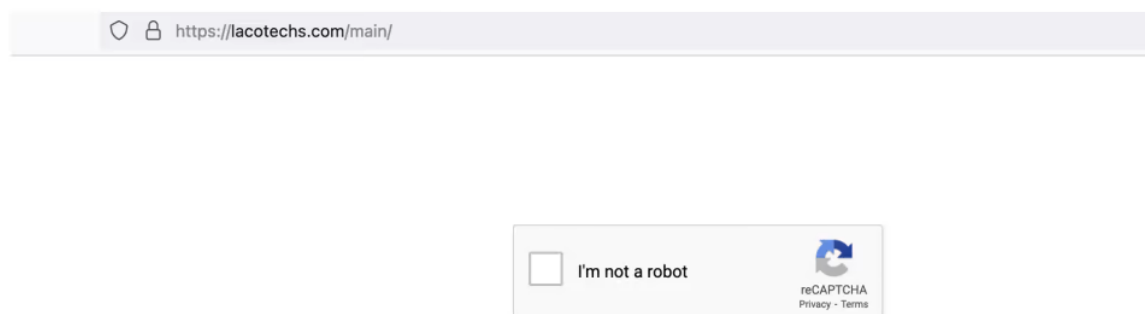
## [Stage 2 URL] CAPTCHA check

---

The Stage 1 URL in the HTML attachment will redirect the user to the Stage 2 URL which requires the user to solve a Captcha before presenting the actual Office credential phishing page.

For Captcha, it uses the Google reCAPTCHA technique. This helps the threat actor evade automated URL analysis tools. A similar technique was used in the [July 2020 instance of a voicemail-themed campaign](#).

Figure 7 and 8 show 2 examples of captcha displayed by the Stage 2 URLs.



*Figure 7: Captcha displayed by the phishing page*

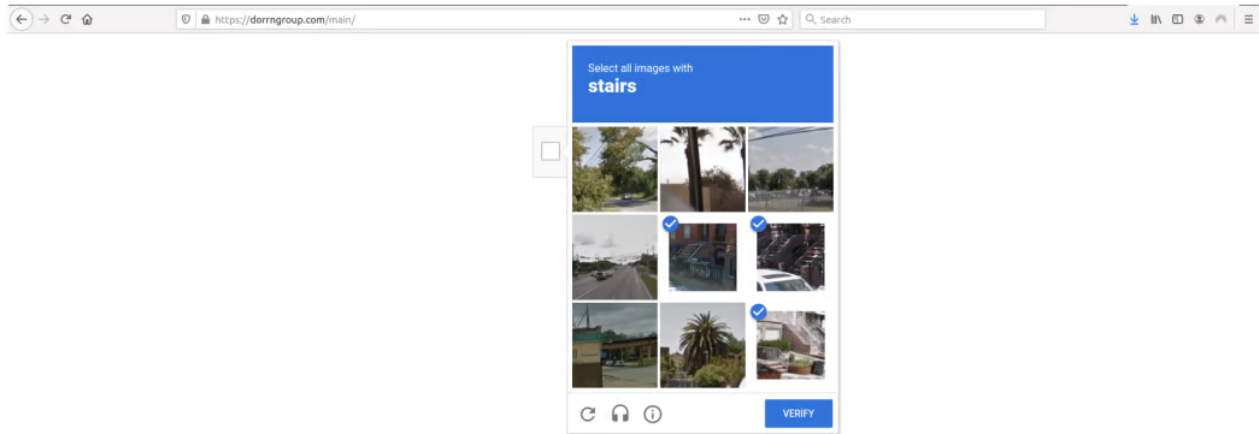


Figure 8: Captcha displayed by the phishing page

### [Stage 3 URL] - Credential phishing page

Once the user solves the Captcha successfully, they will be redirected to the final credential phishing page which attempts to steal the Office 365 credentials of the user as shown in Figure 9.

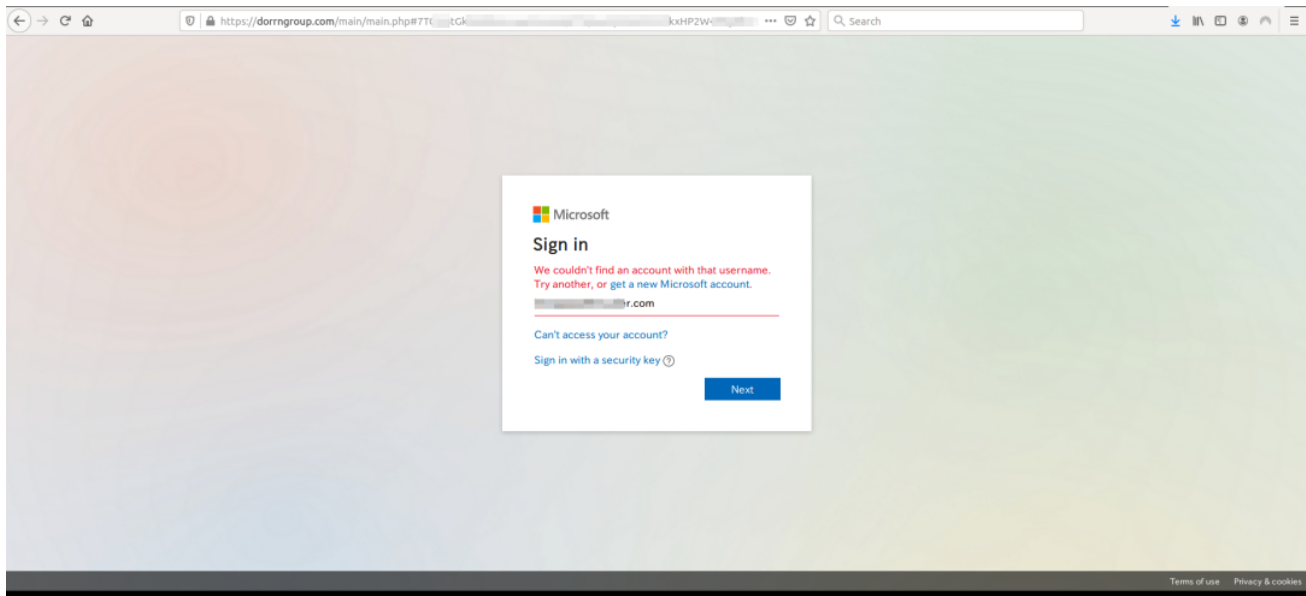


Figure 9: Actual credential phishing page of Office 365

### Zscaler's detection status

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

[HTML.Phish.Microsoft](#)  
[HTML.Phish.Office365](#)  
[HTML.Phish.Zscaler](#)

Figure 10 shows the detection status of Zscaler's credential phishing detection system.

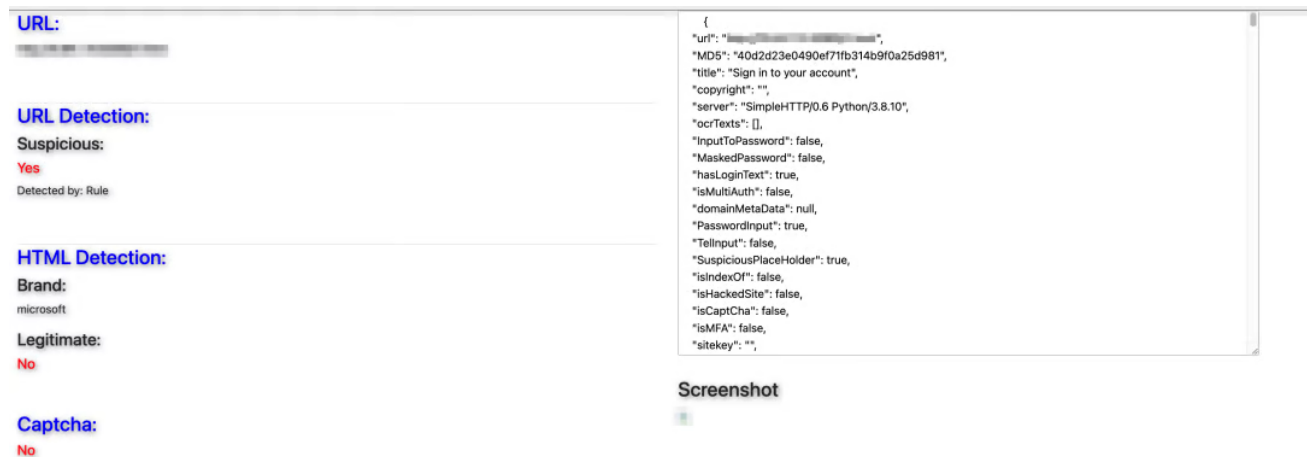


Figure 10: URL detection by Zscaler's credential phishing detection system

## Conclusion

Voicemail-themed phishing campaigns continue to be a successful social engineering technique for attackers since they are able to lure the victims to open the email attachments. This combined with the usage of evasion tactics to bypass automated URL analysis solutions helps the threat actor achieve better success in stealing the users' 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)

# attacker-registered domains

briccorp[.]com  
bajafullrntent[.]com  
bpirninerals[.]com



lovitafood-tw[.]com  
dorrngroup[.]com  
lacotechs[.]com  
brenthavenhg[.]com  
spasfotech[.]com  
mordematx[.]com  
antarnex[.]com