VOLEXITY

BLOG

Operation EmailThief: Active Exploitation of Zero-day XSS Vulnerability in Zimbra

FEBRUARY 3, 2022

by Steven Adair, Thomas Lancaster

[UPDATE] On February 4, 2022, Zimbra provided an update regarding this zero-day exploit vulnerability and reported that a hotfix for 8.8.15 P30 would be available on February 5, 2022. This vulnerability was later assigned CVE-2022-24682 and was fixed in version 8.8.15P30 Update 2 of Zimbra Collaboration Suite.

In December 2021, through its Network Security Monitoring service, Volexity identified a series of targeted spear-phishing campaigns against one of its customers from a threat actor it tracks as **TEMP_Heretic**. Analysis of the emails from these spear phishing campaigns led to a discovery: the attacker was attempting to exploit a

zero-day cross-site scripting (XSS) vulnerability in the Zimbra email platform. Zimbra is an open source email platform often used by organizations as an alternative to Microsoft Exchange.

The campaigns came in multiple waves across two attack phases. The initial phase was aimed at reconnaissance and involved emails designed to simply track if a target received and opened the messages. The second phase came in several waves that contained email messages luring targets to click a malicious attacker-crafted link. For the attack to be successful, the target would have to visit the attacker's link while logged into the Zimbra webmail client from a web browser. The link itself, however, could be launched from an application to include a thick client, such as Thunderbird or Outlook. Successful exploitation results in the attacker being able to run arbitrary JavaScript in the context of the user's Zimbra session. Volexity observed the attacker attempting to load JavaScript to steal user mail data and attachments. An overview of the full attack is given in Figure 1:

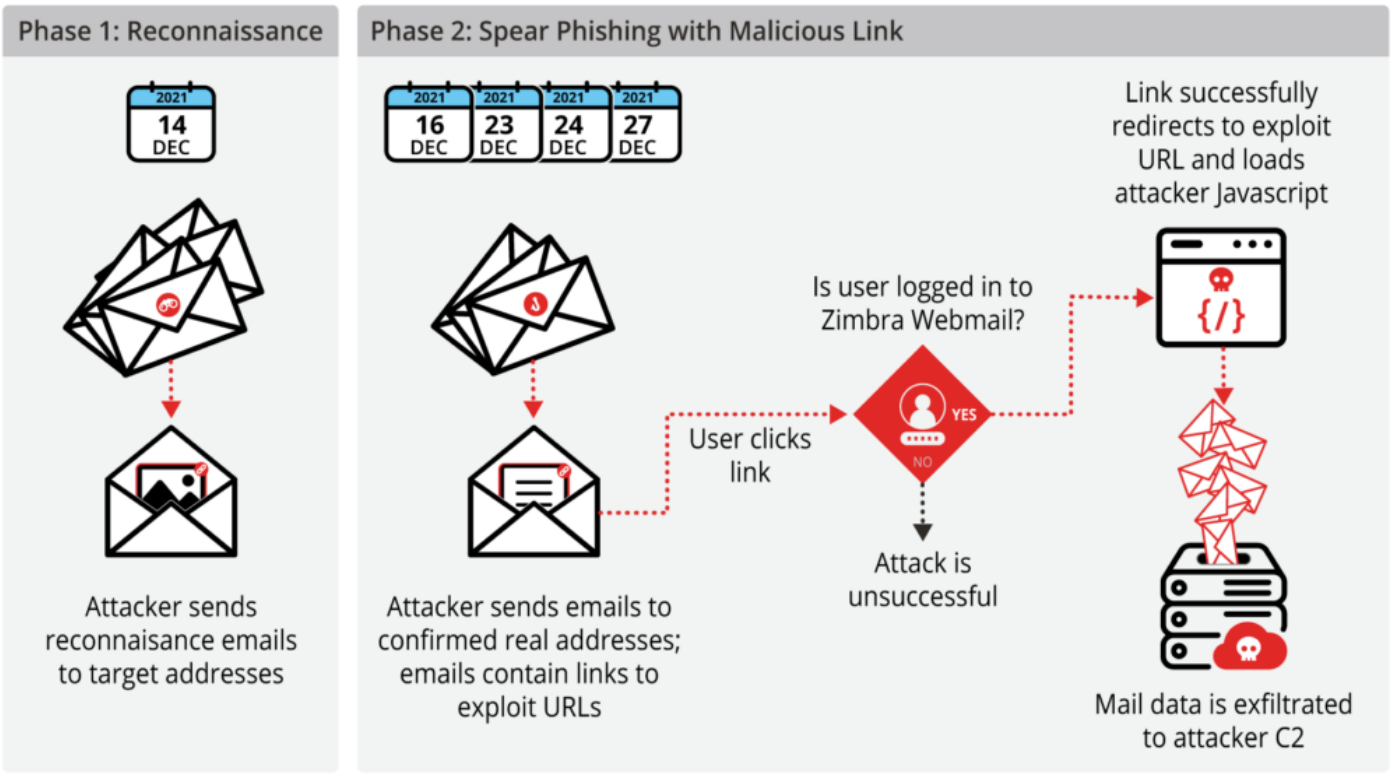

Figure 1. Overview of attack phases

While Volexity only observed TEMP_Heretic attempting email and attachment theft, the vulnerability could easily allow an attacker to perform other actions in the context of the user's Zimbra webmail session, such as the following:

- Exfiltrate cookies to allow persistent access to a mailbox.
- Send further phishing messages to a user's contacts.
- Present a prompt to download malware in the context of a trusted website.

At the time of writing, this exploit has no available patch, nor has it been assigned a CVE (i.e., this is a zero-day vulnerability). Volexity can confirm and has tested that the most recent versions of Zimbra—8.8.15 P29 & P30—remain vulnerable; testing of version 9.0.0 indicates it is likely unaffected. Based on BinaryEdge data, approximately 33,000 servers are running the Zimbra email server, although the true number is likely to be higher. According to Zimbra, there are 200,000 businesses, and over a thousand government and financial institutions, using the software.

Volexity has also been unable to attribute the observed activity to a previously known threat actor. However, based on a number of observed factors, Volexity believes the attacker is likely Chinese in origin. Volexity has observed TEMP_HERETIC targeting organizations in the following sectors:

- European Government
- Media

Spear-phishing Campaigns

Spear-phishing messages observed by Volexity were sent over a period of two weeks in December 2021 using 74 unique outlook.com email addresses created by the attacker. While there were variances, emails were frequently formatted as *<firstname>_<lastname><numbers>@outlook.com* or *<firstname><lastname><numbers>@outlook.com*. The attacker used names commonly used as feminine names for all the personas they created regardless of the email address, as observed from the email-friendly name field. The pattern of sending times suggests the attacker may have manually crafted content for each email before sending it, as they were often sent to consecutive recipients with gaps of a few minutes. Volexity was able to track all the messages TEMP_HERETIC sent and found the attacker conducted a single reconnaissance wave followed by multiple waves aimed at compromising email data.

Reconnaissance

The initial phase of the attack came in the form of spear-phishing campaign sent on December 14, 2021, UTC. It did not involve any type of social engineering lure outside of attempting to get the user to view or open the email. This first wave simply embedded remote images in the body of email messages. These emails contained no content other than the remote image and had generic subjects often associated with non-targeted spam. Below are a list of the subject line topics used for the initial reconnaissance emails.

- Invitations
- Refunds for airline tickets
- Warnings
- <no subject>

The image links in each email were unique per target. This was likely done to test the validity of email addresses, and to determine which accounts were more likely to open phishing email messages. However, Volexity ultimately did not note any correlation between reconnaissance emails and follow-on spear-phishing campaigns. Examples of URLs to remote images are shown below:

> hxxp://fireclaws.spiritfield[.]ga/[filename].jpeg?[integer]
> hxxp://feralrage.spiritfield[.]ga/[filename].jpeg?[integer]
> hxxp://oaksage.spiritfield[.]ga/[filename].jpeg?[integer]
> hxxp://claygolem.spiritfield[.]ga/[filename].jpeg?[integer]

The [integer] at the end of each URL was used to identify the specific victim. The subdomains were found to be unique per email, but it is unknown why they were chosen. Gaming enthusiasts may recognize that the subdomains correspond to the names of spells from the game Diablo II.

Malicious Emails

In the second attack phase, Volexity observed multiple spear-phishing campaigns run on December 16, 23, 24, and 27, 2021. In these campaigns, the attacker embedded links to attacker-controlled infrastructure. In some cases, it appears more of an effort was made to craft a lure that was more enticing to the targeted individual. Two different themes were used in the first wave of attacks. The first theme was interview requests purporting to be from various news organizations such as Agence France-Presse (AFP) and BBC. The second theme was invitations to a charity auction hosted by Sotheby's. In once instance, the attacker used the same "Jacqueline Martin" email address, where Jacqueline was used to represent both BBC and Sotheby's. Examples of these messages are shown below.

Figure 2. Example phishing email using human-rights themed targeting

Figure 3. Example phishing email using an auction theme

However, not all content was custom or otherwise made to stand out to the targets. The spear-phishing waves that followed were largely generic and mostly themed around the holiday season, notably purporting to be from various airlines or Amazon. The attacker sent numerous emails with Christmas and New Years greetings purporting to be from Air France, British Airways, Iberia Airways, Lufthansa, Southwest Airlines, and United Airlines. The attacker sent similar holiday greetings purporting to be from Amazon but also sent generic messages inviting the user to try Amazon Prime or get discounts on their purchases. Examples of these phishing messages are shown below.

Figure 4. Phishing email using Amazon Prime trial theme

Figure 5. Christmas themed phishing email

Subsequent waves from attack phase of the spear phishing campaigns used a similar URI pattern but with a consistent subdomain. The format is given below:

```
hxxps://update.secretstep[.]tk/[filename].jpeg?u=[integer]&t=[second_integer]
```

The second integer in this case was used to denote the target organization. Upon clicking the malicious link, the attacker infrastructure would attempt a redirect to a page on the targeted organization's Zimbra webmail host, with a specific URI format which—if the user is logged in—exploits a vulnerability allowing an attacker to load arbitrary JavaScript in the context of a logged-in Zimbra session. Since there is no available patch for this vulnerability, Volexity is not currently disclosing the required URI pattern required for successful exploitation. A beautified and marked-up copy of the code loaded by the attacker is given **here**.

The functionality of the attacker code is simple:

- Iterate through each email in the user's inbox and sent folders.
- For each email encountered, send the email body and any attachments to the configured callback address (mail.bruising-intellect[.]ml) via HTTP POST requests.

A screenshot of the main loop used for retrieving emails from a victim’s inbox is shown below:

Figure 6. Marked-up copy showing the inbox email theft code

The overall effect of this attack is that by getting a user to click a link in an email and leave their browser window open for any length of time, the attacker can steal the contents of their mailbox. The JavaScript code used to facilitate mail theft has to be customized per version of Zimbra, as the attacker needs to request a page containing a CSRF-Token in order to make subsequent requests to steal mail data.

An example of the POST data format in the event of a successful mail theft is given below.

Figure 7. Example POST data sent by the JavaScript containing full email body data.

Infrastructure Analysis and Attribution

Based on the infrastructure used in the attacks against its customer, Volexity was able to identify a number of additional domains and IP addresses used by the attacker based on simple passive DNS pivots. All identified infrastructure used Freenom domains hosted on AS399269, which belongs to BitLaunch (BLNWX). These appear to be virtual private servers that were likely purchased via bitlaunch.io, a service which allows for purchasing infrastructure using the Bitcoin currency.

All identified IP addresses were observed running Apache 2.4.6 on CentOS with PHP 5.4.16. When SSL is used, certificates were purchased via ZeroSSL. A full list of IOCs is given **here**. Notably, Scanbox-related activity Volexity previously described in its private reporting in August 2021 also used the same server settings (although without SSL).

In terms of attribution, none of the infrastructure identified by Volexity exactly matches infrastructure used by previously classified threat groups. However, based on the targeted organization and specific individuals of the targeted organization, and given the stolen data would have no financial value, it is likely the attacks were undertaken by a Chinese APT actor. Furthermore, there were three clues to suggest the attacker could be Chinese:

- The vast majority of emails were sent between 04:00 and 08:30 UTC, fitting hours of a working day of UTC + 8 hours.
- Emails were sent with headers indicating they were sent from a +0800 UTC time zone.
- The hard-coded headers used in the Zimbra requests generated by the attacker's JavaScript code contain a timezone set to "Asia/Hong_Kong".

Conclusion and Recommendations

While this Zimbra XSS vulnerabilty may not be as widereaching and damaging as the Microsoft Exchange vulnerability Volexity discovered and disclosed last year, it can still have catastrophic consequences for organizations that land in the crosshairs of an attacker with the exploit. At the time of this writing, there is no official patch or workaround for this vulnerability. Volexity has notified Zimbra of the exploit and hopes a patch will be available soon. A timeline of events related to this exploit is given below:

Exploits against mail servers have been numerous in the last few years. They continue to be a productive avenue for attackers wishing to steal data from organizations running on-premise mail services. Vulnerability data published by NIST reveals that Zimbra accumulated 23 severe and critical vulnerabilities since 2019. When software products are assigned many severe vulnerabilities, threat actors usually take note and invest in developing capabilities to exploit them. This is especially true if the product holds valuable information on relevant organizations, such as email.

Volexity recommends the following:

- All of the indicators **here** should be blocked at the mail gateway and network level.
- Users of Zimbra should analyze historical referrer data for suspicious access and referrers. The default location for these logs can be found at */opt/zimbra/log/access*.log*.
- Users of Zimbra should consider upgrading to version 9.0.0, as there is currently no secure version of 8.8.15.

If you believe your organization may been breached from this vulnerability or similar related activity, and you need assistance conducting an incident response investigation, please contact Volexity for further assistance.

This vulnerability and related threat activity were detailed to Volexity Threat Intelligence customers in TIB-20211224.

Appendix A: Related Infrastructure

value	entity_type	description
amazon-check[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
amazon-check[.]ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
amazon-check[.]gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
amazon-check[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
amazon-team[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
bruising-intellect[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
chargedboltsentry.spiritfield[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
findtruth[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
flameshock.spiritfield[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
iceywindflow[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
iceywindflow[.]gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
iceywindflow[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
mail.bruising-intellect[.]ml	hostname	Infrastructure used in conjunction with Zimbra 0-day; hosted malicious JS used to steal user mail and was C2 for that malicious JS
mx.newsonline[.]gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
news-online[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
news-voice[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
newsonline[.]gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
opticaleel.iceywindflow[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
playquicksand[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
playquicksand[.]gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day

value	entity_type	description
playquicksand[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
playquicksand[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
secretstep[.]tk	hostname	Infrastructure used in conjunction with Zimbra 0-day; initial domain used to redirect users to malicious Zimbra URL
shadowmaster.iceywindflow[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
shadownight.playquicksand[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
shadownight.spiritfield[.]ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
spiritfield[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
spiritfield[.]ga	hostname	Infrastructure used in conjunction with Zimbra 0-day; used in reconnaissance emails to validate if addresses were real before sending actual payload later
spiritfield[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
spiritfield[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
spiritx[.]ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
support.newsonline[.]gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
thunderchannel[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
thunderchannel[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
tigerstrike.iceywindflow[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
update.secretstep[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
winderosion.spiritfield[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
windsoft[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
windsource.thunderchannel[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
windsource.thunderchannel[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.amazon-check[.]ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.findtruth[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.iceywindflow[.]gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.news-online[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.news-voice[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day

value	entity_type	description
www.newsonline[.]gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.playquicksand[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.playquicksand[.]gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.spiritfield[.]ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.spiritx[.]ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.thunderchannel[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.thunderchannel[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.windsoft[.]cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
www.yahoo-corporation[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
yahoo-corporation[.]ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
yahoo-corporation[.]tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
yahoo-movie.spiritx[.]ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
108.160.133.32	ipaddress	Suspected related C2 server
172.86.75.158	ipaddress	Resolution for known domain associated with Zimbra exploitation
206.166.251.141	ipaddress	Resolution for known domain associated with Zimbra exploitation
206.166.251.166	ipaddress	Resolution for known domain associated with Zimbra exploitation

0day, APT, cve-2022-24682, espionage, exploits, spear phishing, xss, Zimbra