ESET Research: Mass campaign aimed at stealing Zimbra email users' credentials under way, European countries top targets

DUBAI, UNITED ARAB EMIRATES, August 30, 2023 /EINPresswire.com/ -- ESET researchers have uncovered a mass-spreading phishing campaign aimed at collecting Zimbra account users' credentials. The campaign has been active since at least April 2023 and is still ongoing. Zimbra Collaboration is an open-core collaborative software platform, a popular alternative to enterprise email solutions. The campaign's targets are a variety of small and medium businesses and governmental entities. According to ESET telemetry, the largest number of targets are located in Poland; however, victims in other European countries such as Ukraine, Italy, France and the Netherlands are also targeted. Latin American nations were hit too; Ecuador tops the list of detections in that region.

Despite this campaign not being particularly technically sophisticated, it is still able to spread and successfully compromise organizations that use Zimbra Collaboration. "Adversaries leverage the fact that HTML attachments contain legitimate code, with the only telltale element being a link pointing to the malicious host. In this manner, it is much easier to circumvent reputation-based antispam policies, especially compared to more prevalent phishing techniques, where a malicious link is directly placed in the email body," explains ESET researcher Viktor Šperka, who discovered the campaign.

"Target organizations vary; adversaries do not focus on any specific vertical – the only thing connecting victims is that they are using Zimbra," adds Šperka. The popularity of Zimbra Collaboration among organizations expected to have lower IT budgets ensures that it stays an attractive target for adversaries.

Initially, the target receives an email with a phishing page in the attached HTML file. 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. After opening the attachment, the user is presented with a fake Zimbra login page customized according to the targeted organization. In the background, the submitted credentials are collected from the HTML form and sent to a server controlled by the adversary. Then, the attacker is potentially able to infiltrate the affected email account. 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. The campaign observed by ESET relies only on social engineering and user interaction; however, this may not always be the case.

For more technical information about campaign against Zimbra, check out the blogpost "Mass-spreading campaign targeting Zimbra users" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant
Vistar Communications
+971559724623 ext.
email us here