Operation EmailThief, TEMP_Heretic - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:10:06 UTC

APT group: Operation EmailThief, TEMP_Heretic

Names	Operation EmailThief *(Volexity)* TEMP_Heretic *(Volexity)*
Country	China
Motivation	Information theft and espionage
First seen	2021
Description	(Volexity) 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.
Observed	Sectors: Government, Media. Countries: Europe.
Tools used	
Information	<https://www.volexity.com/blog/2022/02/03/operation-emailthief-active-exploitation-of-zero-day-xss-vulnerability-in-zimbra/>

Last change to this card: 04 February 2022

Download this actor card in PDF or JSON format
