BlueDelta Exploits Ukrainian Government Roundcube Mail Servers to Support Espionage Activities

Research (Insikt)

Posted: 20th June 2023

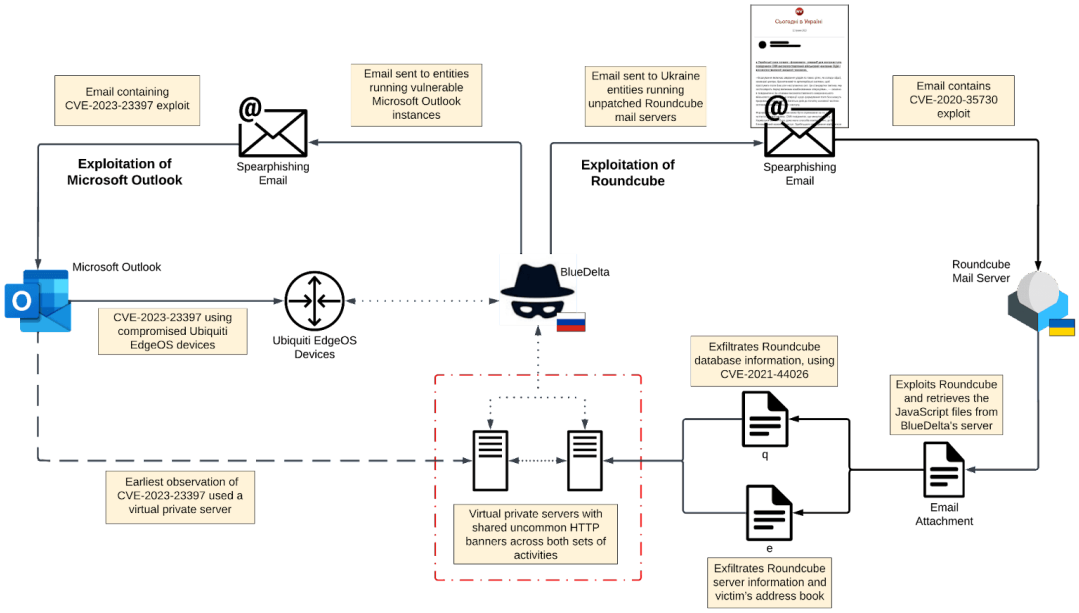
By: Insikt Group®

Recorded Future's Insikt Group, in partnership with Ukraine's Computer Emergency Response Team (CERT-UA), has uncovered a campaign targeting high-profile entities in Ukraine that was cross-correlated with a spearphishing campaign uncovered by Recorded Future's Network Traffic Intelligence. The campaign leveraged news about Russia's war against Ukraine to encourage recipients to open emails, which immediately compromised vulnerable Roundcube servers (an open-source webmail software), using CVE-2020-35730, without engaging with the attachment. We found that the campaign overlaps with historic BlueDelta activity exploiting the Microsoft Outlook zero-day vulnerability CVE-2023-23397 in 2022.

The BlueDelta activity, identified by Insikt Group, appears to have been operational since November 2021. The campaign overlaps with activity attributed by CERT-UA to APT28 (also known as Forest Blizzard and Fancy Bear), which multiple Western governments attribute to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). In this operation, BlueDelta primarily targeted Ukrainian organizations, including government institutions and military entities involved in aircraft infrastructure.

The BlueDelta campaign used spearphishing techniques, sending emails with attachments exploiting vulnerabilities (CVE-2020-35730, CVE-2020-12641, and CVE-2021-44026) in Roundcube to run reconnaissance and exfiltration scripts, redirecting incoming emails and gathering session cookies, user information, and address books. The attachment contained JavaScript code that executed additional JavaScript payloads from BlueDelta-controlled infrastructure. The campaign displayed a high level of preparedness, quickly weaponizing news

content into lures to exploit recipients. The spearphishing emails contained news themes related to Ukraine, with subject lines and content mirroring legitimate media sources.



BlueDelta Outlook and Roundcube spearphishing infection chain overlap

BlueDelta has demonstrated a long-standing interest in gathering intelligence on entities in Ukraine and across Europe, primarily among government and military/defense organizations. The most recent activity very likely represents a continued focus on these entities and specifically those within Ukraine. We assess that BlueDelta activity is likely intended to enable military intelligence-gathering to support Russia's invasion of Ukraine and believe that BlueDelta will almost certainly continue to prioritize targeting Ukrainian government and private sector organizations to support wider Russian military efforts.

Recorded Future's collaboration with CERT-UA further emphasizes the importance of partnerships between industry and governments to enable collective defense against strategic threats — in this case, Russia's war against Ukraine.

To read the entire analysis with endnotes, click here to download the report as a PDF.