ESET Research: Russian RomCom group exploits new vulnerability, targets companies in Europe and Canada

DUBAI , DUBAI, UNITED ARAB EMIRATES, August 22, 2025 /EINPresswire.com/ -- ESET researchers have discovered a previously unknown vulnerability in WinRAR, exploited in the wild by Russia-aligned group RomCom. According to ESET telemetry, malicious archives were used in spearphishing campaigns between July 18 to July 21, 2025, targeting financial, manufacturing, defense, and logistics companies in Europe and Canada. The aim of the attacks was cyberespionage. This is at least the third time that RomCom has been caught exploiting a significant zero-day vulnerability in the wild

“On July 18, we observed a malicious DLL named msedge.dll in a RAR archive containing unusual paths that caught our attention. Upon further analysis, we found that the attackers were exploiting a previously unknown vulnerability affecting WinRAR, including the then-current version 7.12. On July 24, we contacted the developer of WinRAR; the same day the vulnerability was fixed in beta version with a full version released few days later. We advise WinRAR users to install the latest version as soon as possible to mitigate the risk,” says ESET researcher Peter Strýček who made the discovery along with another ESET researcher Anton Cherepanov. The vulnerability, CVE-2025-8088, is a path traversal vulnerability, which is made possible via the use of alternate data streams.

Disguised as an application document, the weaponized archives exploited a path traversal flow to compromise its targets. In the spearphishing email, the attackers sent a CV hoping that a curious target would open it. According to ESET telemetry, none of the targets were compromised. The attackers, however, had conducted reconnaissance beforehand and the emails were highly targeted. Successful exploitation attempts delivered various backdoors used by RomCom group – specifically, a SnipBot variant, RustyClaw, and the Mythic agent.

ESET Research attributes the observed activities to RomCom with high confidence based on the targeted region, tactics, techniques, and procedures (TTPs), and the malware used. RomCom (also known as Storm-0978, Tropical Scorpius, or UNC2596) is a Russia-aligned group that conducts both opportunistic campaigns against selected business verticals and targeted espionage operations. The group's focus has shifted to include espionage operations collecting intelligence, in parallel with its more conventional cybercrime operations. The backdoor used by the group is capable of executing commands and downloading additional modules to the victim's machine. It is not the first time that RomCom has used exploits to compromise its victims. In 2023-06, the group performed a spearphishing campaign targeting defense and governmental entities in Europe, with lures related to the Ukrainian World Congress.

"By exploiting a previously unknown zero-day vulnerability in WinRAR, the RomCom group has shown that it is willing to invest serious effort and resources into its cyberoperations. The discovered campaign targeted sectors that align with the typical interests of Russian-aligned APT groups, suggesting a geopolitical motivation behind the operation," concludes Strýček.

For a more detailed analysis and technical breakdown of RomCom's latest campaign, check out the latest ESET Research blogpost "RomCom exploits a new vulnerability in the wild, this time in WinRAR" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts, and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here