

THREAT ACTOR FROM RUSSIAN FEDERATION



# RomCom

38 mentions in the last 2 weeks



224 articles in the last 12 months



Using open-source data collected by Feedly AI.

## Overview

ROMCOM is an evolving and sophisticated threat actor group that has been using the malware tool ROMCOM for espionage and financially motivated attacks. They have targeted organizations in Ukraine and NATO countries, including military personnel, government agencies, and political leaders. The ROMCOM backdoor is capable of stealing sensitive information and deploying other malware, showcasing the g... [See More](#)

## Aliases

- Storm-0978
- UAT-5647


## Article count



## Targets

No targeted countries have been identified by [MISP](#)

Top targeted industries and organizations

INDUSTRIES	ORGANIZATIONS	ARTICLES	ATTACK REPORTED
<div></div> <div>No attack has been detected in the time frame selected</div>			

Top malware families associated with this threat actor

 Loading...

Tactics, Techniques, and Procedures

Last mentioned 

 Loading...

Exploited vulnerabilities

 Loading...

Detection Rules

RULE	ARTICLES	COUNT	ACTION
Sigma rules	<u>1</u>	3	<div>Download</div>
YARA rules	<u>5</u>	6	<div>Download</div>

Threat intelligence reports



RomCom exploits Firefox and Windows zero days in the wild



↗ [CVE-2024-9680](#) • by tnavda / 11d  
submitted by /u/tnavda [link] [comments]

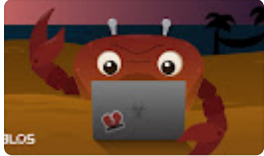
Also in Chocolatey Blog, Cybersecurity | Secu..., +24 feeds



## RomCom Backdoor Attacks Use Zero-Day Exploits in Mozilla and Windows (CVE-2024-9680 & CVE-2024-49039)

🔗 2 CVEs • SOCRadar® Cyber Intelligence Inc. by Ameer Owda / 12d •  
🔗 IoC > 18 hashes, 9 domains, and 10 IPs • 🔗 15 TTPs

Recent research has revealed how the RomCom cyber threat group exploited two zero-day vulnerabilities in Mozilla and Microsoft products to deploy their namesake backdoor.



## UAT-5647 targets Ukrainian and Polish entities with RomCom malware variants

by digicat / 52d  
submitted by /u/digicat [link] [comments]

## News



## RomCom Hacker Group Exploits Firefox and Windows Zero-Day Vulnerabilities

↗ [RomCom exploits Firefox Windows zero-days](#) •  
Cybersecurity on Medium by Kr1pt7c / 4d

The Russian-aligned RomCom group has been exploiting two critical Zero-Day vulnerabilities:

Also in Security Affairs, Cyberattacks News, +70 feeds

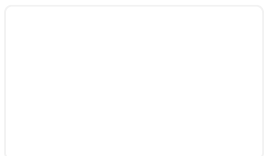


## Russian Hackers Use Firefox and Windows Vulnerabilities in Global Cyberattack

🔗 2 CVEs • CySecurity News - Latest Information Sec... by Ridhika Singh / 6d  
• 🔗 4 TTPs

A sophisticated cyberattack carried out by the Russian cyber threat group RomCom APT has raised alarms within the global cybersecurity community.... How the Attack Unfolded RomCom APT used two critical vulnerabilities to carry...

Also in NetmanageIT CTO Corn..., #zeroday, +7 feeds



## PoC Exploit Released for Windows Task Scheduler Zero-day Flaw, Exploited in Wild

🔗 [CVE-2024-49039 \(CVSS 8.8 ex\)](#) • Cyber Security News by Guru Baran / 6d  
• 🔗 7 TTPs

Security researchers have linked the exploitation of CVE-2024-49039 to the Russia-aligned threat actor known as RomCom.... Finally, the RomCom backdoor is installed, granting attackers full control over the compromised system.

Also in Microsoft Security A..., Google Alert, +18 feeds



## Zero-Day Exploit Code Released for Windows Task Scheduler Flaw (CVE-2024-49039), Actively Exploited by RomCom Group

🔗 2 CVEs • Cybersecurity News by do son / 6d • 🔗 6 TTPs

A proof-of-concept (PoC) exploit code for CVE-2024-49039, a zero-day vulnerability in Windows Task Scheduler, has been publicly released, raising concerns about increased attacks. Analysis suggests that this vulnerability allow...

Also in Microsoft Security A..., Google Alert, +18 feeds

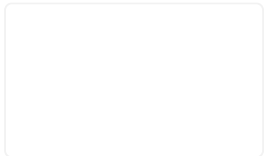


## RomCom Exploits Zero Days In Recent Backdoor Campaigns

🔗 2 CVEs • Latest Hacking News by Abeerah Hashim / 7d • Original source: WeLiveSecurity / 12d • 🔗 9 TTPs

The threat actor group RomCom have exploited two zero days in its recent backdoor campaigns.... on Latest Hacking News

Also in Hacker News, Google Alert, +1 feeds



## 2nd December – Threat Intelligence Report

🔗 6 CVEs • Check Point Research by tomeresp@checkpoint.com / 7d • 🔗 10 TTPs

Researchers found that Russia-linked group RomCom has exploited two zero-day vulnerabilities in Firefox and Windows to target victims in Europe and North America.

[See 44 more articles and social media posts](#)

Made with  feedly