Russian Hackers Breached 80+ Organizations Using Roundcube XSS Flaw

By Eswar

Published: 2024-02-20 · Archived: 2026-04-05 15:11:07 UTC

The Russia-based threat group TAG-70 has been discovered to be exploiting Roundcube webmail servers with a recently disclosed Cross-Site Scripting vulnerability CVE-2023-5631.

Their targets include government, military, and national infrastructure-related entities. This threat actor overlaps with Winter Vivern, TA473, and UAC-0114 threat group.

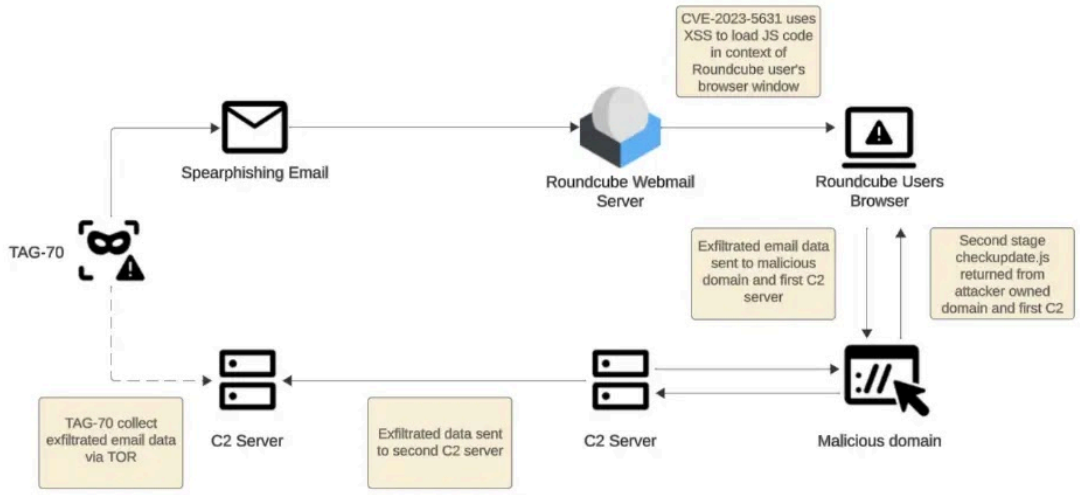
However, this Roundcube targeting campaign has been conducted since October 2023, attacking over 80 organizations, primarily in Georgia, Poland, and Ukraine.

Live Account Takeover Attack Simulation

How do Hackers Bypass 2FA?

Live attack simulation Webinar demonstrates various ways in which account takeover can happen and practices to protect your websites and APIs against ATO attacks .

Moreover, this is the only recent campaign from the Russia-aligned threat groups targeting email servers.



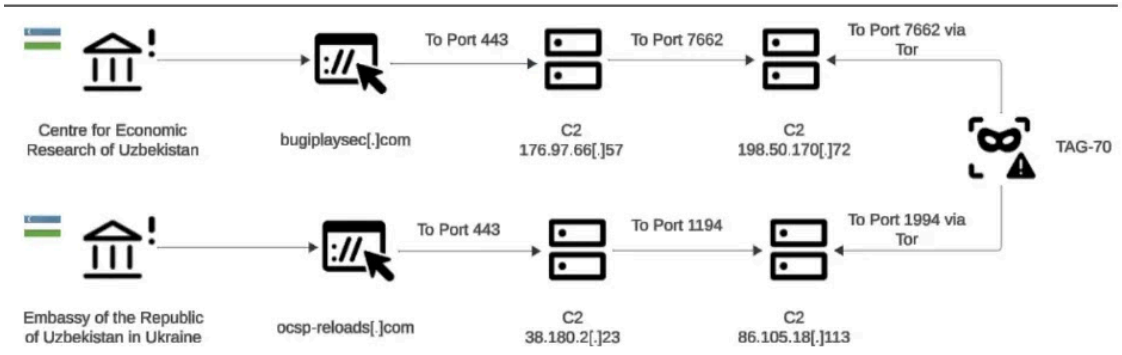
Roundcube Exploitation Attack Flow (Source: Recorded Future)

As part of the ongoing war between Ukraine and Russia, several Russia-based cyber-espionage groups were attacking governmental entities in Europe as a means of gathering intelligence about the war effort and planning, relationships and negotiations, military and economic assistance, and other information that could help in fighting the war.

According to the reports shared with Cyber Security News, TAG-70 has previously created a spoofed website of the MInistry of Foreign Affairs of Ukraine for luring users to download a malicious software under the impersonation of “scanning infected PCs for viruses”.

In March 2023, TAG-70 was attributed to the exploitation of the Zimbra webmail portal via CVE-2022-27926 to gain access to the emails of military, government, and diplomatic European organizations that are involved in the Russia-Ukraine war.

Considering the sophistication and attack vectors of this threat actor indicates a well-funded and skilled threat actor behind these operations.



TAG-70 Operation in March 2023 (Source: Recorded Future)

However, their recent XSS zero-day exploitation of Roundcube webmail servers was investigated, revealing that the threat actors were using this vulnerability to list and exfiltrate victims' mailbox contents without any interaction from the victim except by opening the malicious email.

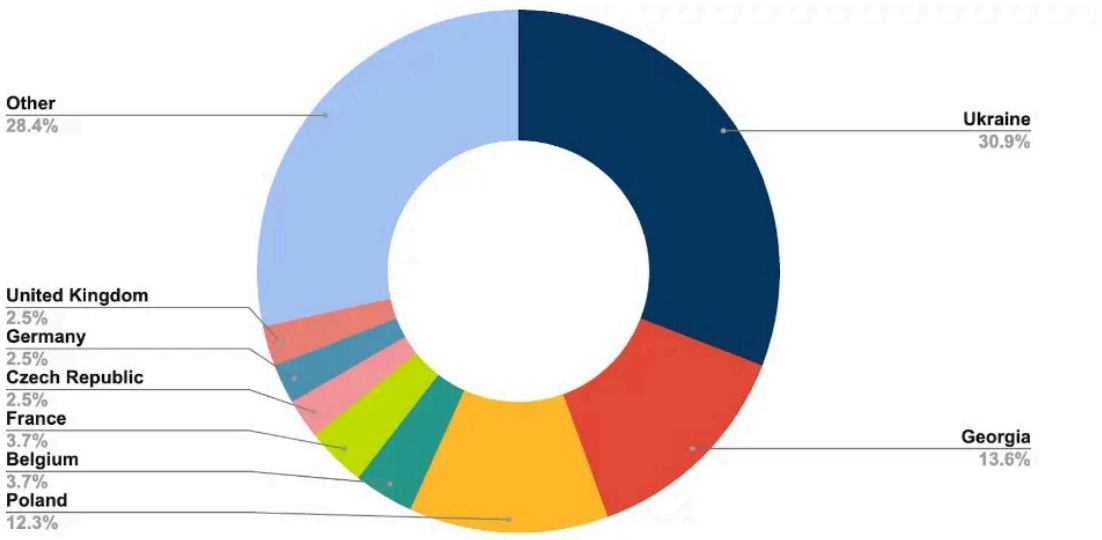
Threat Analysis

In February 2023, suspicious activity was discovered, which involved a C2 IP address 198.50.170[.]72 over TCP port 7662.

However, this IP was later attributed to the domain bugiplaysec[.]com, owned by TAG-70. This domain was found to communicate with a victim IP address over port 443.

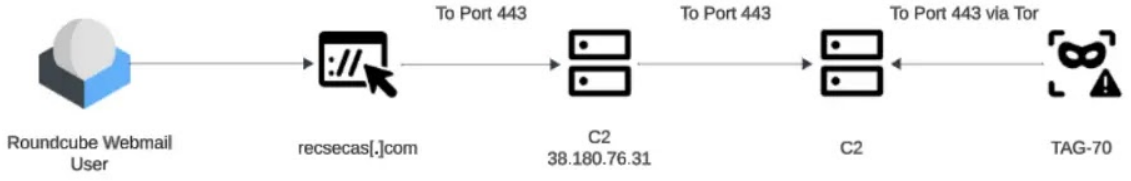
Additionally, a similar activity was found between an IP address associated with the Embassy of the Republic of Uzbekistan in Ukraine.

This IP address was communicating with another C2 domain ocsp-reloads[.]com resolving to 38.180.2[.]23. In both of the scenarios, TAG-70 administered the C2 domains via Tor.



Geographic spread of victims of TAG-70s Roundcube exploit (Source: Recorded Future)

As of this recent Roundcube webmail server exploitation campaign, TAG-70 used an infrastructure configuration with a domain recsecas[.]com and C2 38.180.76.[.]31 tunneling to another C2 administered via Tor.



TAG-70 Operational Infrastructure in October 2023 (Source: Recorded Future)

Indicators Of Compromise

Domains:

- bugiplaysec[.]com
- hitsbitsx[.]com
- ocsp-reloads[.]com
- recsecas[.]com

IP Addresses:

- 38.180.2[.]23
- 38.180.3[.]57
- 38.180.76[.]31
- 86.105.18[.]113
- 176.97.66[.]57
- 176.97.76[.]118
- 176.97.76[.]129
- 198.50.170[.]72

Malware Samples (SHA256):

- 6800357ec3092c56aab17720897c29bb389f70cb49223b289ea5365314199a26
- ea22b3e9ecdfd06fae74483deb9ef0245aefdc72f99120ae6525c0eaf37de32e

Stay updated on Cybersecurity news, Whitepapers, and Infographics. Follow us on LinkedIn & Twitter.

Source: https://cybersecuritynews.com/russian-hackers-xss-flaw/