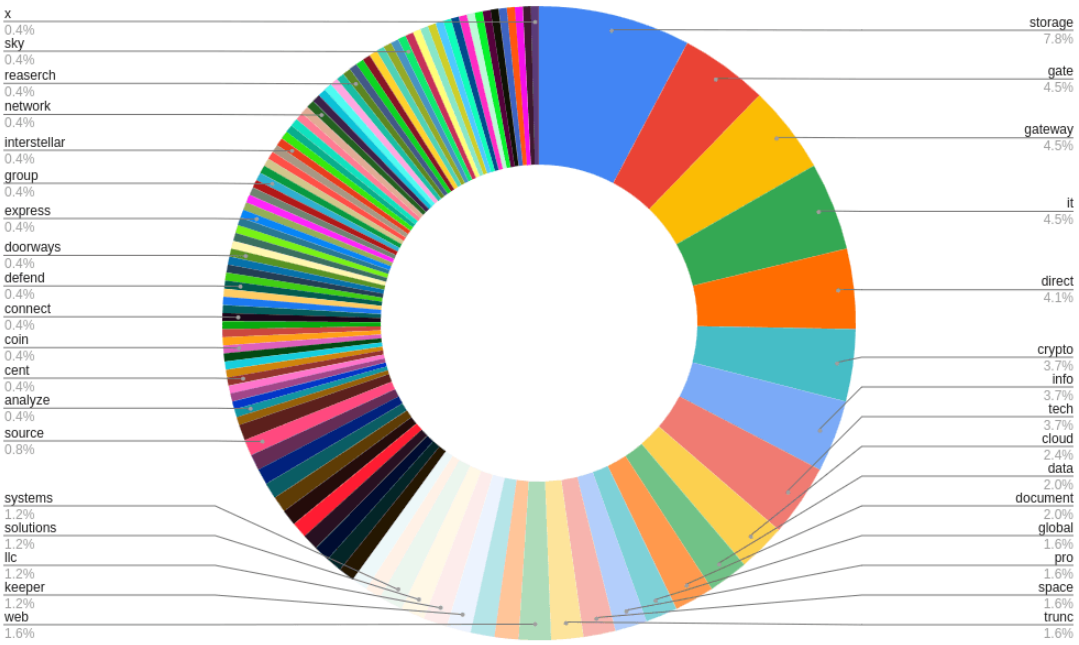
BlueCharlie, Previously Tracked as TAG-53, Continues to Deploy New Infrastructure in 2023

Research (Insikt)

Posted: 2nd August 2023

By: Insikt Group

Insikt Group has been tracking the threat activity group BlueCharlie, associated with the Russia-nexus group Callisto/Calisto, COLDRIVER, and Star Blizzard/SEABORGIUM. BlueCharlie, a Russia-linked threat group active since 2017, focuses on information gathering for espionage and hack-and-leak operations. BlueCharlie has evolved its tactics, techniques, and procedures (TTPs) and built new infrastructure, indicating sophistication in adapting to public disclosures and improving operations security. While specific victims are unknown, past targets include government, defense, education, political sectors, NGOs, journalists, and think tanks.



Breakdown of terms used in BlueCharlie activity since November 2022

Recently, Insikt Group observed BlueCharlie build new infrastructure for likely use in phishing campaigns and/or credential harvesting, which consists of 94 new domains. Several of the TTPs seen in the recent operation depart from past activity, suggesting that BlueCharlie is evolving its operations, potentially in response to public disclosures of its operations in industry reporting. Since Insikt Group's initial tracking of the group in September 2022, we have observed BlueCharlie engage in several TTP shifts. These shifts demonstrate that these threat actors are aware of industry reporting and show a certain level of sophistication in their efforts to obfuscate or modify their activity, aiming to stymie security researchers.

To counter BlueCharlie's threat, network defenders should enhance phishing defenses, implement FIDO2-compliant multi-factor authentication, use threat intelligence, and educate third-party vendors. BlueCharlie's continued use of phishing and its historical adaptation to public reporting suggest it will remain active and evolve further in its operations.

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