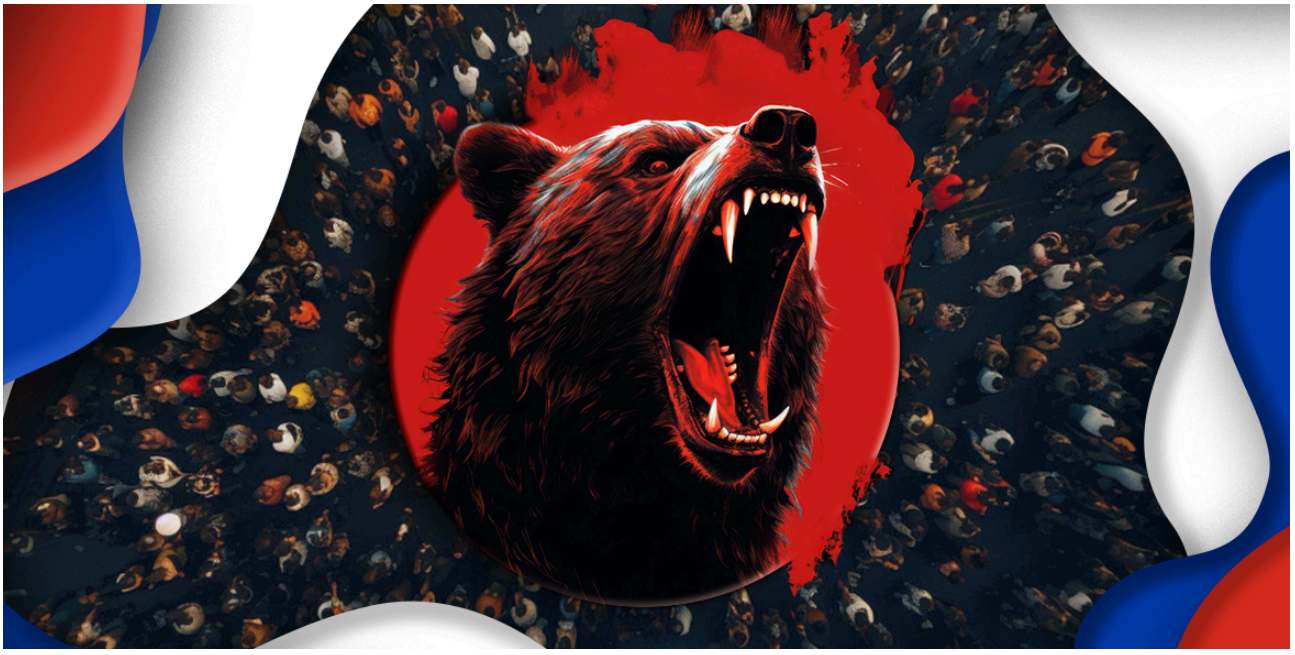
The Cluster25 Blog - Duskrise

Published: 2024-03-27 · Archived: 2026-04-06 00:47:57 UTC



The Bear and The Shell: New Campaign Against Russian Opposition

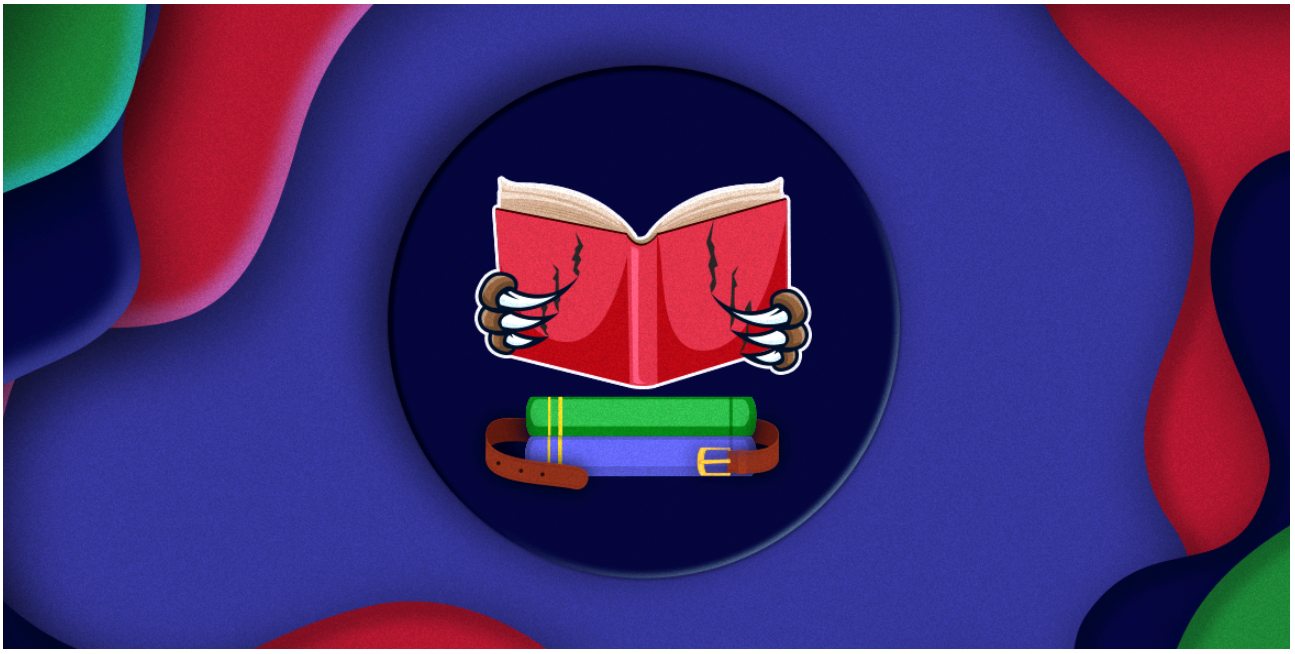
30 January 2024

The Bear and The Shell: New Campaign Against Russian Opposition By Cluster25 Threat Intel Team January 30, 2024 Cluster25 uncovered a newly initiated campaign likely associated with a Russian APT (Advanced Persistent Threat) group. The

The Duck is Hiring in Italy: DUCKTAIL Spread via Compromised LinkedIn Profiles

25 October 2023

The Duck is Hiring in Italy: DUCKTAIL Spread via Compromised LinkedIn Profiles By Cluster25 Threat Intel Team October 25, 2023 Cluster25 observed a malicious campaign that employs LinkedIn messages as a vector for executing identity



CVE-2023-38831 Exploited by Pro-Russia Hacking Groups in RU-UA Conflict Zone for Credential Harvesting Operations

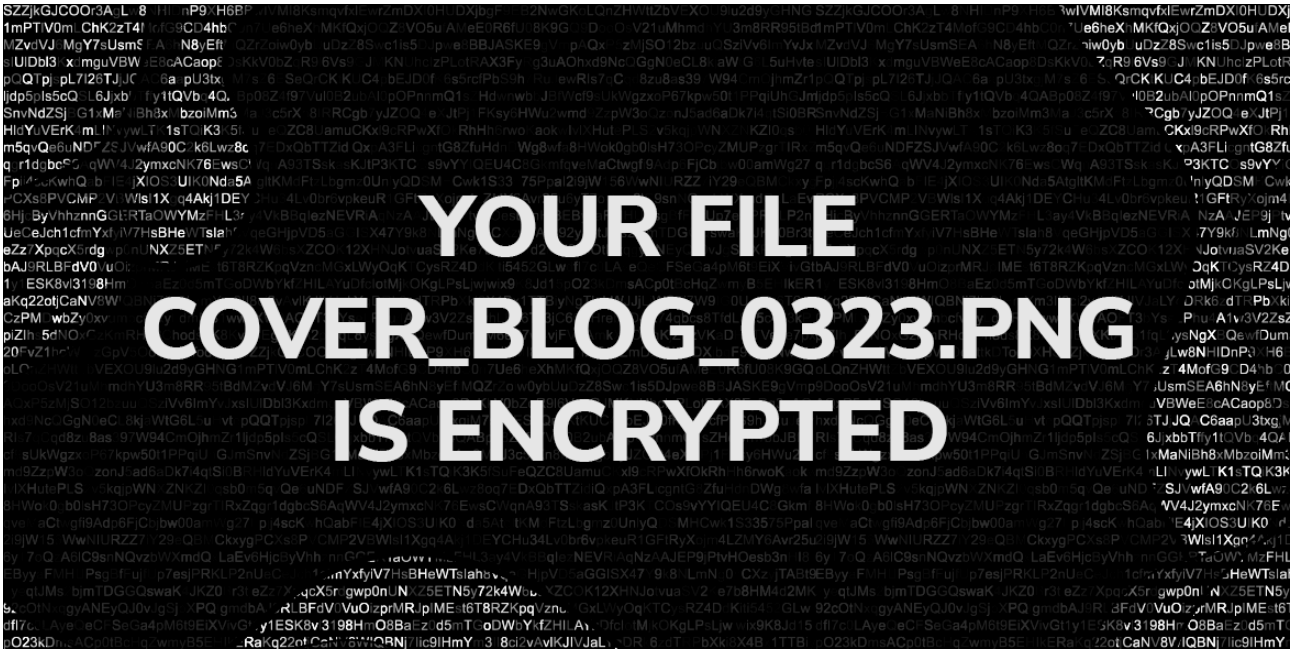
12 October 2023

CVE-2023-38831 Exploited by Pro-Russia Hacking Groups in RU-UA Conflict Zone for Credential Harvesting Operations By Cluster25 Threat Intel TeamOctober 12, 2023 Cluster25 observed and analyzed several phishing-based attacks to be linked to a Russia-nexus nation-State

The Fraud Gala: Exploring a Recent BEC Campaign

25 August 2023

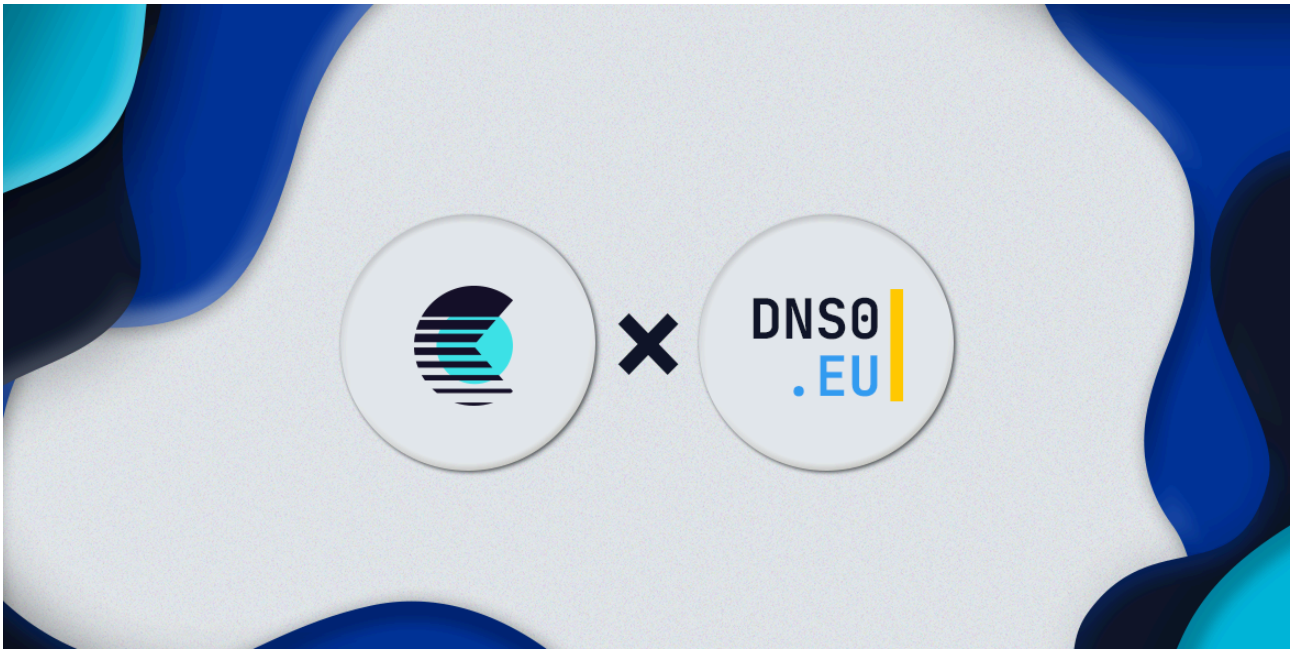
The Fraud Gala: Exploring a Recent BEC Campaign By Cluster25 Threat Intel Team August 25, 2023 In the modern digital era, businesses operate on a global scale, exchanging information, collaborating, and conducting financial transactions



Back in Black: BlackByte Ransomware returns with its New Technology (NT) version

22 May 2023

Back in Black: BlackByte Ransomware returns with its New Technology (NT) version By Cluster25 Threat Intel Team May 22, 2023 BlackByte is a Ransomware-as-a-Service (RaaS) group that is known for the use of the



Cluster25 has become partner of DNS0 Project

2 May 2023

Cluster25 has become partner of DNS0 Project By Cluster25 Threat Intel Team May 2, 2023
