BUI

INNOVATION | DELIVERY | RESULTS

DarkWeb Intel Monitor

Executive Intelligence Report

Generated:	2026/03/29, 18:33:11
Generated by:	BUI Security Analyst
Classification:	Informational Content
Source:	BUI DarkWeb Intel Monitor

EXECUTIVE SUMMARY

Intelligence compiled: Sunday, 29 March 2026 at 18:33

DARK WEB POSTS
25
2 critical + 17 high

RANSOMWARE VICTIMS
100
21 active groups

INTEL ARTICLES
437
news + threat feeds

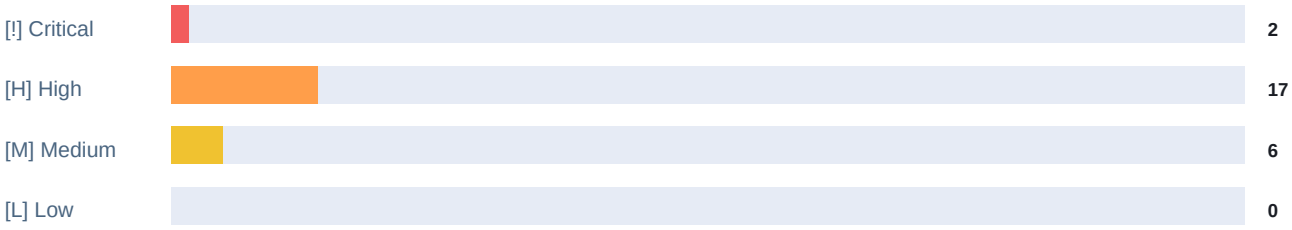
COUNTRIES AFFECTED
40
in dark web + ransomware

HIBP BREACHES
966
17504M+ accounts exposed

WATCHLIST ALERTS
0
0 unread

VULNERABILITIES
10
in feed

THREAT SEVERITY OVERVIEW -- DARK WEB + RANSOMWARE



TOP DARK WEB INCIDENTS

Country	Severity	Sectors	Summary
Israel	CRITICAL	Energy	Israel - Cardinal group claims breach of Israeli nuclear infrastr
Canada	CRITICAL		Canada - Telus Digital confirms massive data breach by ShinyHunte
South Korea	HIGH	Energy	ActionPower Suffers Suspected Crypto24 Ransomware Attack The Cryp
-	HIGH		Anubis Attack Hits Scalian and Schlam Stone & Dolan LLP The
France	HIGH	Telecom	Gentlemen Attack: Groupe Courtois, STS Travel & Durable Supe
-	HIGH		Arcterminal.xyz Data Breach Exposes User Emails and Wallets Arcte
Colombia	HIGH	Finance	Nubank Colombia Data Breach Exposes Customer Records Banco Nubank
Spain	HIGH		Centauro Data Breach Exposes 4.3 Million User Records Centauro.ne

RANSOMWARE ACTIVITY

Group	Victims	Top Sector
qilin	23	Not Found
nightspire	12	Not Found
handala	9	Not Found
incransom	8	Not Found
ALP-001	7	Technology
dragonforce	7	Consumer Services

THREAT INTELLIGENCE HIGHLIGHTS

Source	Date	Title
Palo Alto Unit 42	Thu, 26 Ma	Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran (Updated March
Palo Alto Unit 42	Thu, 26 Ma	Converging Interests: Analysis of Threat Clusters Targeting a Southeast Asian Go
Palo Alto Unit 42	Tue, 24 Ma	Threat Brief: Recruiting Scheme Impersonating Palo Alto Networks Talent Acquisit
Palo Alto Unit 42	Mon, 23 Ma	Google Authenticator: The Hidden Mechanisms of Passwordless Authentication
Palo Alto Unit 42	Fri, 20 Ma	Whos Really Shopping? Retail Fraud in the Age of Agentic AI
Palo Alto Unit 42	Thu, 19 Ma	Analyzing the Current State of AI Use in Malware

TOP CYBERSECURITY NEWS

Source	Date	Headline
Dark Reading	Fri, 27 Ma	China Upgrades the Backdoor It Uses to Spy on Telcos Globally
Dark Reading	Fri, 27 Ma	Wartime Usage of Compromised IP Cameras Highlight Their Danger
Dark Reading	Fri, 27 Ma	Infrastructure Attacks With Physical Consequences Down 25%
Dark Reading	Fri, 27 Ma	Google Sets 2029 Deadline for Quantum-Safe Cryptography
Dark Reading	Thu, 26 Ma	Coruna, DarkSword & Democratizing Nation-State Exploit Kits
Dark Reading	Thu, 26 Ma	Is the FCC's Router Ban the Wrong Fix?

DATA BREACHES / VULNERABILITIES / UNAUTH ACCESS

Category	Date	Title
Data Breach	Fri, 27 Ma	Arcterminal.xyz Data Breach Exposes User Emails and Wallets
Data Breach	Fri, 27 Ma	Nubank Colombia Data Breach Exposes Customer Records
Data Breach	Fri, 27 Ma	Centauro Data Breach Exposes 4.3 Million User Records
Vulnerability	Wed, 08 Oc	Critical Figma MCP Server Flaw Allows Remote Code Execution
Vulnerability	Mon, 06 Oc	Oracle Patches CVE202561882
Vulnerability	Wed, 17 Se	Shai-Hulud Worm Infects Over 500 NPM Packages in Sophisticated Supply Chain Atta
Unauth Access	Mon, 16 Ma	Peak Neuro Investigating Alleged Admin Panel Access Sale
Unauth Access	Wed, 11 Ma	GlobalNet Data Breach: Tunisian ISP Compromised

BREACH INTELLIGENCE -- TOP RECENT BREACHES

Breach	Domain	Date	Accounts
Synthient Credential Stuffin	-	2025-04-11	1957.5M
Collection #1	-	2019-01-07	772.9M
Verifications.io	verifications.io	2019-02-25	763.1M
Onliner Spambot	-	2017-08-28	711.5M
Data Enrichment Exposure Fro	-	2019-10-16	622.2M
Exploit.In	-	2016-10-13	593.4M