BUI INNOVATION™ DELIVERY RESULTS

DarkWeb Intel Monitor

Executive Intelligence Report

Generated:	2026/11/22, 20:50:43
Generated by:	BUI Security Analyst
Classification:	Informational Content
Source:	BUI DarkWeb Intel Monitor - tools.bui.systems/darkweb

DISCLAIMER: For informational use only. BUI accepts no liability. Redistribution prohibited. (c) 2026 BUI. All rights reserved.

EXECUTIVE SUMMARY

Intelligence compiled: Sunday, 22 November 2026 at 20:50

DARK WEB POSTS
801
30 critical + 306 high

RANSOMWARE VICTIMS
100
31 active groups

INTEL ARTICLES
1427
news + threat feeds

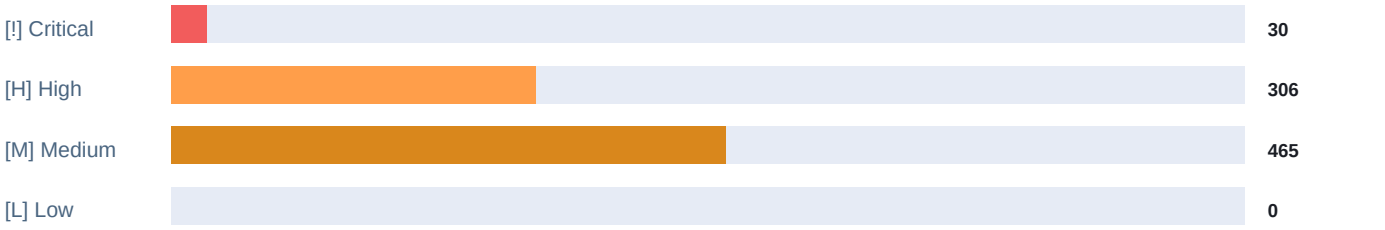
COUNTRIES AFFECTED
114
in dark web + ransomware

HIBP BREACHES
1054
17863M+ accounts exposed

WATCHLIST ALERTS
0
0 unread

VULNERABILITIES
253
in feed

THREAT SEVERITY OVERVIEW -- DARK WEB + RANSOMWARE



TOP DARK WEB INCIDENTS

Country	Severity	Sectors	Summary
-	CRITICAL		Sean Cairncross out as national cyber director During his tenure,
-	CRITICAL	Government	Security Affairs newsletter Round 605 by Pierluigi Paganini INTER
-	CRITICAL	Energy	Cairn AI Framework Used in Autonomous Zero-Day Exploitation Amazo
-	CRITICAL	Telecom	Unpatched Check Point Gateways Are Being Wiped exploiting PHP2She
-	CRITICAL	Defence	New SignDrop Exploit Can Abuse Windows Defender to Bypass Securit
China	CRITICAL		Researchers uncover Volt Typhoons covert, ephemeral network The C
-	CRITICAL	Education	Untitled <p>If anybody reads this OpenAI post and thinks AI
-	CRITICAL		Untitled <p><a href="hxxps://www[.]csoonline[.]com/artic

DISCLAIMER: For informational use only. BUI accepts no liability. Redistribution prohibited. (c) 2026 BUI. All rights reserved.

RANSOMWARE ACTIVITY

Group	Victims	Top Sector
everest	10	Technology
safepay	9	Other
SoulGroup	8	Healthcare
pear	6	Professional Services
settra	6	Retail & E-Commerce
incransom	5	Government & Defense

THREAT INTELLIGENCE HIGHLIGHTS

Source	Date	Title
Palo Alto Unit 42	Fri, 20 No	Dialing for Data: Inside the Coms High-Profile Heists
Palo Alto Unit 42	Tue, 17 No	Borrowed Code, Real Consequences: What OPTIMJACK Teaches Us
Palo Alto Unit 42	Mon, 16 No	QUIC and Covert: Novel HTTP/3-Powered RATs Target Southeast Asian Governments
Palo Alto Unit 42	Thu, 12 No	Attackers Use Autonomous AI to Target Semiconductor, Defense and Civil Society S
Palo Alto Unit 42	Wed, 11 No	ARTEX and AI-Powered Red Teaming Tools: What Defenders Need to Know
Palo Alto Unit 42	Wed, 11 No	The XG Files: Falcon C2 Flying Under The (Browser) Radar

TOP CYBERSECURITY NEWS

Source	Date	Headline
Dark Reading	Fri, 20 No	China's 'Armory Castle' Lays Siege to VMware vCenter Zero-Day
Dark Reading	Fri, 20 No	In Security, Words Matter as Much as Tools, Maybe More
Dark Reading	Fri, 20 No	What We Missed: Nvidia CEO Scandal Rocks AI Industry
Dark Reading	Thu, 19 No	Qwen Incidents Show Self-Hosted AI Models Need Stronger Steering
Dark Reading	Thu, 19 No	Second Norwegian Energy Company Breached in 2 Days
Dark Reading	Thu, 19 No	Critical PHP Flaws Allow Code Execution, but Don't Panic 'PHP2Shell'-Style

DISCLAIMER: For informational use only. BUI accepts no liability. Redistribution prohibited. (c) 2026 BUI. All rights reserved.

DATA BREACHES / VULNERABILITIES / UNAUTH ACCESS

Category	Date	Title
Data Breach	2026-11-22	Kirsten Davies's White House Promotion Leaves CMMC in Limbo
Data Breach	2026-11-22	House Lawmakers Push US AI Models to Counter China
Data Breach	2026-11-22	Cogent to Buy Specular to Sharpen Vulnerability Priorities
Vulnerability	Sun, 22 No	CVE-2026-132147 - Debbugs Arbitrary File Read Vulnerability
Vulnerability	Sun, 22 No	CVE-2026-131794 - WordPress YellowPencil Visual CSS Style Editor plugin <= 7.
Vulnerability	Sun, 22 No	CVE-2026-131793 - WordPress Contact Form to Any API plugin <= 3.0.7 - Cross S
Unauth Access	2026-11-22	Kirsten Davies's White House Promotion Leaves CMMC in Limbo
Unauth Access	2026-11-22	House Lawmakers Push US AI Models to Counter China

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

DISCLAIMER: For informational use only. BUI accepts no liability. Redistribution prohibited. (c) 2026 BUI. All rights reserved.