BUI

INNOVATION | DELIVERY | RESULTS

DarkWeb Intel Monitor

Executive Intelligence Report

Generated:	2026/07/26, 18:19:29
Generated by:	BUI Security Analyst
Classification:	Informational Content
Source:	BUI DarkWeb Intel Monitor - tools.bui.systems/darkweb

EXECUTIVE SUMMARY

Intelligence compiled: Sunday, 26 July 2026 at 18:19

DARK WEB POSTS
274
20 critical + 134 high

RANSOMWARE VICTIMS
100
29 active groups

INTEL ARTICLES
758
news + threat feeds

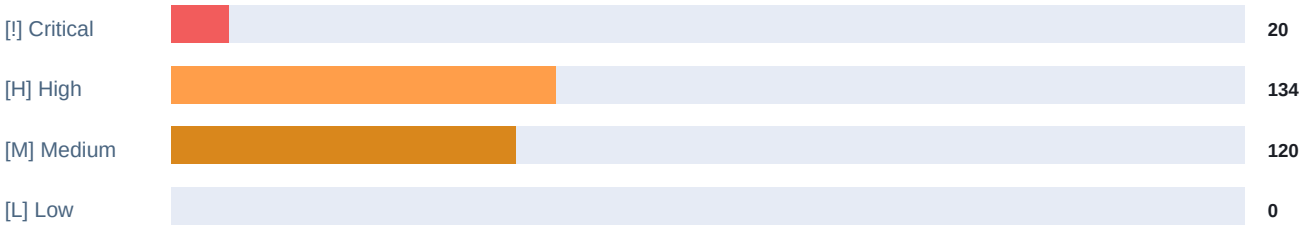
COUNTRIES AFFECTED
87
in dark web + ransomware

HIBP BREACHES
1020
17764M+ accounts exposed

WATCHLIST ALERTS
0
0 unread

VULNERABILITIES
55
in feed

THREAT SEVERITY OVERVIEW -- DARK WEB + RANSOMWARE



TOP DARK WEB INCIDENTS

Country	Severity	Sectors	Summary
Australia	CRITICAL		Russian espionage group using novel Zimbra exploit to steal sensi
China	CRITICAL	Defence	USB drives carrying China-linked malware infected Japanese milita
-	CRITICAL		Smashing Security podcast #472: AI gets hacked, and BitLocker get
-	CRITICAL		Russian Hackers Used a Zimbra Zero-Day to Steal Emails Without Li
-	CRITICAL		OpenAI Models Breached Hugging Face During Internal Cyber Test Op
-	CRITICAL		SonicWall customers under threat as attackers exploit 2 zero-days
-	CRITICAL		Microsofts July 2026 Patch Tuesday fixes 622 flaws and 2 exploite
Unpatched Curs	CRITICAL		Unpatched Cursor Zero-Day Lets Malicious Git Repositories Trigger

RANSOMWARE ACTIVITY

Group	Victims	Top Sector
thegentlemen	23	Other
qilin	15	Professional Services
ExfilSquad	14	Government & Defense
Deadlock	10	Manufacturing
m3rx	4	Professional Services
incransom	3	Healthcare

THREAT INTELLIGENCE HIGHLIGHTS

Source	Date	Title
Palo Alto Unit 42	Thu, 23 Ju	Russian Global Webmail Espionage
Palo Alto Unit 42	Fri, 17 Ju	Three Steps to the Terminal: A Siemens ROX II Zero-Day Trilogy
Palo Alto Unit 42	Thu, 16 Ju	AI, Automation and Attacks: Unpacking the Unit 42 2026 Global Incident Response
Palo Alto Unit 42	Wed, 15 Ju	The npm Threat Landscape: Attack Surface and Mitigations (Updated July 15)
Palo Alto Unit 42	Wed, 15 Ju	TuxBot v3: Inside an IoT Botnet Framework With LLM-Assisted Development
Palo Alto Unit 42	Fri, 10 Ju	No Manners Here: The Ruthless Rise of The Gentlemen Ransomware

TOP CYBERSECURITY NEWS

Source	Date	Headline
Dark Reading	Fri, 24 Ju	CISOs vs. Boards: Myth or Misunderstanding?
Dark Reading	Fri, 24 Ju	Escape Artists: 'Incorrigible' AI Models Resist Rehabilitation
Dark Reading	Fri, 24 Ju	Vatican's Official Prayer App Leaks 700K+ Global Users' PII
Dark Reading	Fri, 24 Ju	Default Azure Automation Setting Enables Cross-Tenant Identity Takeover
Dark Reading	Fri, 24 Ju	Europe's Multilingual Reality Exposes AI Security Gaps
Dark Reading	Thu, 23 Ju	Russian Hackers Exploit Zimbra Zero-Day Against US, Ukraine Targets

DATA BREACHES / VULNERABILITIES / UNAUTH ACCESS

Category	Date	Title
Data Breach	Tue, 21 Ju	Open House: How an Unauthenticated MCP Server Exposed India's Largest Real E
Data Breach	Wed, 08 Ju	Adult Supervision: How OnlyFans takedowns quietly police compromised domains | U
Data Breach	Mon, 06 Ju	Own Goal: Inside the Cyber Risks of the 2026 World Cup | UpGuard
Vulnerability	Sun, 26 Ju	CVE-2026-17497 - NoteGen arbitrary OS command execution via Tauri shell:allow-ex
Vulnerability	Sun, 26 Ju	CVE-2026-17496 - NoteGen chat preview XSS via unsanitized AI/skill HTML renderin
Vulnerability	Sun, 26 Ju	CVE-2026-17459 - perwendel spark SparkJava ExternalResourceHandler.jav staticFil
Unauth Access	Tue, 21 Ju	Open House: How an Unauthenticated MCP Server Exposed India's Largest Real E
Unauth Access	Wed, 08 Ju	Adult Supervision: How OnlyFans takedowns quietly police compromised domains | U

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