DarkWeb Intel Monitor

Executive Intelligence Report

Generated:	2026/08/02, 19:47:27
Generated by:	BUI Security Analyst
Classification:	Informational Content
Source:	BUI DarkWeb Intel Monitor - tools.bui.systems/darkweb

EXECUTIVE SUMMARY

Intelligence compiled: Sunday, 2 August 2026 at 19:47

DARK WEB POSTS
382
23 critical + 177 high

RANSOMWARE VICTIMS
100
21 active groups

INTEL ARTICLES
807
news + threat feeds

COUNTRIES AFFECTED
95
in dark web + ransomware

HIBP BREACHES
1022
17766M+ accounts exposed

WATCHLIST ALERTS
0
0 unread

VULNERABILITIES
55
in feed

THREAT SEVERITY OVERVIEW -- DARK WEB + RANSOMWARE

[!] Critical	23
[H] High	177
[M] Medium	182
[L] Low	0

TOP DARK WEB INCIDENTS

Country	Severity	Sectors	Summary
United States	CRITICAL		Smashing Security podcast #478: This job interview could destroy
China	CRITICAL	Defence	USB drives carrying China-linked malware infected Japanese milita
South Korea	CRITICAL	Finance	South Korea Warns of State-Backed Watering Hole Attacks South Kor
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

RANSOMWARE ACTIVITY

Group	Victims	Top Sector
thegentlemen	33	Manufacturing
qilin	15	Manufacturing
CRPxO	11	Financial Services
krybit	5	Professional Services
coinbasecartel	4	Other
cmdorganization	4	Professional Services

THREAT INTELLIGENCE HIGHLIGHTS

Source	Date	Title
Palo Alto Unit 42	Fri, 31 Ju	The Xcode Assassin Returns: A Deep Dive Into the Latest XCSSET Version
Palo Alto Unit 42	Thu, 30 Ju	Chinese-Speaking Threat Actor Harnesses AI Models for Autonomous Cyberattacks
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)

TOP CYBERSECURITY NEWS

Source	Date	Headline
Dark Reading	Fri, 31 Ju	CISA Issues Fresh SBOM Guidance. Did They Get It Right?
Dark Reading	Fri, 31 Ju	The Morning After We Pull a Root of Trust, Nobody Owns It
Dark Reading	Fri, 31 Ju	Interpol Leverages Global System to Curtail Fraud Payments
Dark Reading	Fri, 31 Ju	DROP Platform Lets Californians Reduce Digital Footprint
Dark Reading	Fri, 31 Ju	USA Fencing Lunges Into the Hidden Identity Challenge in Amateur Sports
Dark Reading	Thu, 30 Ju	Minnesota Water Utility Attacks Expose Sector's Cyber-Risks

DATA BREACHES / VULNERABILITIES / UNAUTH ACCESS

Category	Date	Title
Data Breach	2026-08-02	US CISA Urged to Order OT Security Improvements
Data Breach	2026-08-02	Anthropic, OpenAI AI Sandbox Failures Expose Testing Risks
Data Breach	2026-08-02	Okta Buys Permiso to Extend ITDR Beyond Native Identity Logs
Vulnerability	Sun, 02 Au	CVE-2026-65321 - PyAthena 3.35.4 SQL Injection via DefaultParameterFormatter DEL
Vulnerability	Sun, 02 Au	CVE-2026-10774 - PSA key-slot leak in Bluetooth Mesh subnet deletion leading to
Vulnerability	Sun, 02 Au	CVE-2026-9856 - Path Traversal in huggingface/transformers
Unauth Access	2026-08-02	US CISA Urged to Order OT Security Improvements
Unauth Access	2026-08-02	Anthropic, OpenAI AI Sandbox Failures Expose Testing Risks

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