BUI

INNOVATION | DELIVERY | RESULTS

DarkWeb Intel Monitor

Executive Intelligence Report

Generated:	2026/07/12, 16:34:42
Generated by:	BUI Security Analyst
Classification:	Informational Content
Source:	BUI DarkWeb Intel Monitor - tools.bui.systems/darkweb

BUI | www.bui.co

For cybersecurity services, threat intelligence consulting, and incident response, contact BUI at www.bui.co

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

EXECUTIVE SUMMARY

Intelligence compiled: Sunday, 12 July 2026 at 16:34

DARK WEB POSTS
177
14 critical + 85 high

RANSOMWARE VICTIMS
100
10 active groups

INTEL ARTICLES
690
news + threat feeds

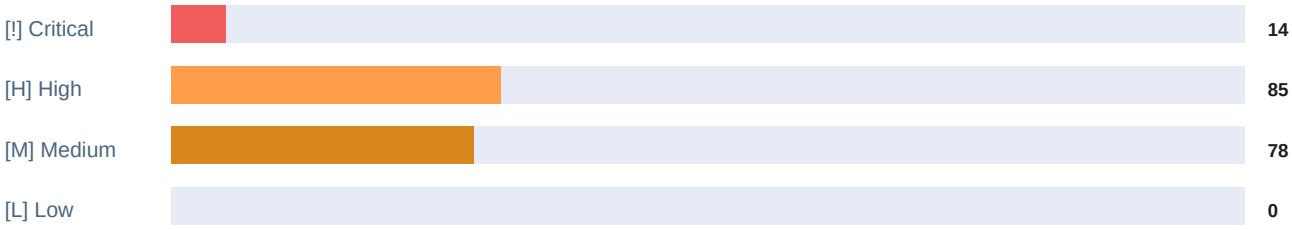
COUNTRIES AFFECTED
77
in dark web + ransomware

HIBP BREACHES
1016
17678M+ 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
China	CRITICAL	Defence	USB drives carrying China-linked malware infected Japanese milita
-	CRITICAL		Smashing Security podcast #472: AI gets hacked, and BitLocker get
-	CRITICAL		GigaWiper Merges Three Malware Families Into One Destructive Back
-	CRITICAL		Microsoft Warns of GigaWiper Backdoor Built to Destroy Windows PC
-	CRITICAL	Government	DHS to unveil replacement council for critical infrastructure cyb
-	CRITICAL		The Anatomy of a Shadow AI Supply-Chain Breach: Lessons from the
-	CRITICAL		FortiBleed Credential Theft Connected to INC and Lynx Ransomware
-	CRITICAL		Sysdig Details JADEPUFFER, the First Documented Agentic Ransomwar

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

RANSOMWARE ACTIVITY

Group	Victims	Top Sector
Deadlock	54	Not Found
thegentlemen	19	Business Services
lockbit5	9	Business Services
qilin	8	Financial Services
m3rx	3	Business Services
titan	2	Business Services

THREAT INTELLIGENCE HIGHLIGHTS

Source	Date	Title
Palo Alto Unit 42	Fri, 10 Ju	No Manners Here: The Ruthless Rise of The Gentlemen Ransomware
Palo Alto Unit 42	Tue, 07 Ju	Vidar Stealer Unmasked: Code Signing Abuse, Go Loaders and File Inflation
Palo Alto Unit 42	Thu, 02 Ju	How We Added WebAuthn to a Browser-Based RDP Client
Palo Alto Unit 42	Wed, 01 Ju	Phantom Squatting: AI-Hallucinated Domains as a Software Supply Chain Vector
Palo Alto Unit 42	Fri, 26 Ju	Threat Brief: Mitigating Large-Scale Credential Attacks
Palo Alto Unit 42	Thu, 25 Ju	CL-STA-1062 Targets Southeast Asian Governments and Critical Infrastructure

TOP CYBERSECURITY NEWS

Source	Date	Headline
Dark Reading	Fri, 10 Ju	Jen Ellis: Connecting Cyber Community With Political Machinery
Dark Reading	Fri, 10 Ju	Cybercriminals Flock to Healthcare Businesses as Attacks Surge
Dark Reading	Fri, 10 Ju	Fresh ATM Crypto Software Bugs: Jackpot or Bust?
Dark Reading	Fri, 10 Ju	More Countries Jump on the Social Media 'Ban Wagon'
Dark Reading	Fri, 10 Ju	AI Coding: Do Security Risks Outweigh Productivity Gains?
Dark Reading	Thu, 09 Ju	Iran's Cyber Crosshairs Focus Beyond Critical Infrastructure

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	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
Data Breach	Tue, 02 Ju	Breaking Confinement: How a Corrections Vendor Exposed Inmate Communications | U
Vulnerability	Sun, 12 Ju	CVE-2026-15502 - AojiaoZero Antaris PayPal IPN Payment ipn.php _rewardPurchase s
Vulnerability	Sun, 12 Ju	CVE-2026-15501 - AstrBotDevs AstrBot MCP Test Endpoint tools.py ToolsRoute.test_
Vulnerability	Sun, 12 Ju	CVE-2026-61876 - LuCI DHCPv6 Lease Hostname Stored Cross-Site Scripting
Unauth Access	Wed, 08 Ju	Adult Supervision: How OnlyFans takedowns quietly police compromised domains | U
Unauth Access	Mon, 06 Ju	Own Goal: Inside the Cyber Risks of the 2026 World Cup | UpGuard

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.