BUI

INNOVATION | DELIVERY | RESULTS

DarkWeb Intel Monitor

Executive Intelligence Report

Generated:	2026/07/19, 15:24:46
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, 19 July 2026 at 15:24

DARK WEB POSTS
222
17 critical + 108 high

RANSOMWARE VICTIMS
100
21 active groups

INTEL ARTICLES
729
news + threat feeds

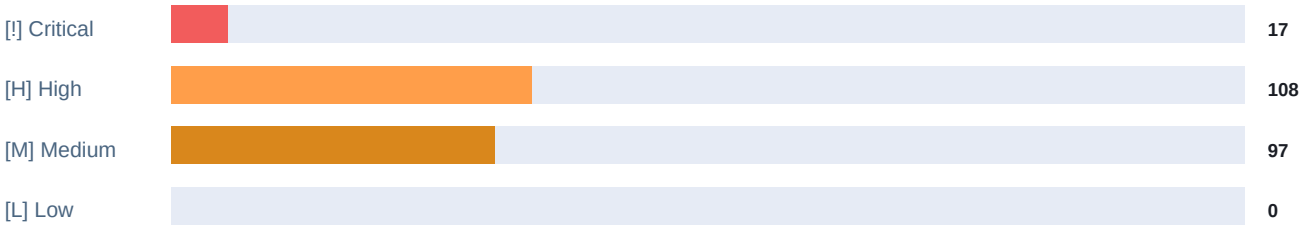
COUNTRIES AFFECTED
77
in dark web + ransomware

HIBP BREACHES
1018
17685M+ 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
-	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
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

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

RANSOMWARE ACTIVITY

Group	Victims	Top Sector
thegentlemen	23	Manufacturing
qilin	15	Agriculture and Food Productio
dragonforce	12	Business Services
incransom	10	Agriculture and Food Productio
krybit	5	Business Services
play	5	Telecommunication

THREAT INTELLIGENCE HIGHLIGHTS

Source	Date	Title
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
Palo Alto Unit 42	Tue, 07 Ju	Vidar Stealer Unmasked: Code Signing Abuse, Go Loaders and File Inflation

TOP CYBERSECURITY NEWS

Source	Date	Headline
Dark Reading	Fri, 17 Ju	Inc Ransomware Exploits SonicWall SMA Zero-Days
Dark Reading	Fri, 17 Ju	The Real AI Threat Is Blind Trust
Dark Reading	Fri, 17 Ju	Gold Eagle Clearinghouse Targets Security Gap, but How Is Unclear
Dark Reading	Fri, 17 Ju	Google Bets 'Agentic Defense' Strategy Can Outpace Attackers
Dark Reading	Thu, 16 Ju	Agentic AI: Taming the Unpredictable
Dark Reading	Thu, 16 Ju	1M+ Emails Use Hidden Text to Dupe AI Security Filters

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	Mon, 13 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, 19 Ju	CVE-2026-53380 - media: rzv2h-ivc: Fix concurrent buffer list access
Vulnerability	Sun, 19 Ju	CVE-2026-53379 - media: i2c: ov8856: free control handler on error in ov8856_ini
Vulnerability	Sun, 19 Ju	CVE-2026-53378 - drm/colorop: Fix blob property reference tracking in state life
Unauth Access	Mon, 13 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

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