BUI

INNOVATION | DELIVERY | RESULTS

# DarkWeb Intel Monitor

## Executive Intelligence Report

| | |
|---|---|
| **Generated:** | 2026/05/24, 17:31:40 |
| **Generated by:** | BUI Security Analyst |
| **Classification:** | Informational Content |
| **Source:** | BUI DarkWeb Intel Monitor - tools.bui.systems/darkweb |

## EXECUTIVE SUMMARY

Intelligence compiled: Sunday, 24 May 2026 at 17:31

**DARK WEB POSTS**
348
25 critical + 173 high

**RANSOMWARE VICTIMS**
100
25 active groups

**INTEL ARTICLES**
922
news + threat feeds

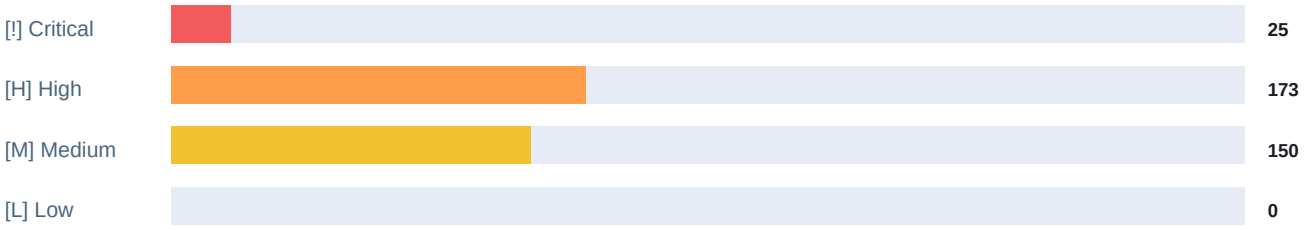
**COUNTRIES AFFECTED**
97
in dark web + ransomware

**HIBP BREACHES**
994
17591M+ accounts exposed

**WATCHLIST ALERTS**
0
0 unread

**VULNERABILITIES**
121
in feed

## THREAT SEVERITY OVERVIEW -- DARK WEB + RANSOMWARE




## TOP DARK WEB INCIDENTS

| Country | Severity | Sectors | Summary |
|---|---|---|---|
| Cisco zero | CRITICAL | | Cisco zero-day under ongoing attack by persistent threat group Th |
| - | CRITICAL | | Major tech manufacturer Foxconn confirms cyberattack hit North Am |
| - | CRITICAL | | Pwn2Own Berlin 2026, Day Three: DEVCORE Crowned Master of Pwn, $1 |
| - | CRITICAL | | Pwn2Own Berlin 2026, Day Two: $385,750 more, Microsoft Exchange f |
| - | CRITICAL | | CVE-2026-42897: Microsoft confirms active exploitation of Exchang |
| - | CRITICAL | Education | mutreasury Allegedly Breached: Admin Credentials and API Keys Exp |
| - | CRITICAL | Telecom | Ivanti customers confront yet another actively exploited zero-day |
| - | CRITICAL | Government | A DOD contractors API flaw exposed military course data and servi |

## RANSOMWARE ACTIVITY

| Group | Victims | Top Sector |
|---|---|---|
| **thegentlemen** | 13 | Transportation/Logistics |
| **qilin** | 11 | Construction |
| **nova** | 10 | Education |
| **dragonforce** | 7 | Not Found |
| **akira** | 7 | Not Found |
| **payload** | 7 | Manufacturing |

## THREAT INTELLIGENCE HIGHLIGHTS

| Source | Date | Title |
|---|---|---|
| Palo Alto Unit 42 | Fri, 22 Ma | Tracking Iranian APT Screening Serpens 2026 Espionage Campaigns |
| Palo Alto Unit 42 | Fri, 22 Ma | Paved With Intent: ROADtools and Nation-State Tactics in the Cloud |
| Palo Alto Unit 42 | Thu, 21 Ma | The npm Threat Landscape: Attack Surface and Mitigations (Updated May 21) |
| Palo Alto Unit 42 | Wed, 20 Ma | Tracking TamperedChef Clusters via Certificate and Code Reuse |
| Palo Alto Unit 42 | Fri, 15 Ma | Gremlin Stealer's Evolved Tactics: Hiding in Plain Sight With Resource File |
| Palo Alto Unit 42 | Mon, 11 Ma | Inside AD CS Escalation: Unpacking Advanced Misuse Techniques and Tools |

## TOP CYBERSECURITY NEWS

| Source | Date | Headline |
|---|---|---|
| Dark Reading | Fri, 22 Ma | Akamai Joins Growing Chorus of Vendors Betting Big on Secure Enterprise Browsers |
| Dark Reading | Fri, 22 Ma | Verizon DBIR: Healthcare Fends Off Increased Social Engineering Attacks |
| Dark Reading | Fri, 22 Ma | China's Webworm Uses Discord, Microsoft Graphs to Hack EU Governments |
| Dark Reading | Thu, 21 Ma | Google API Keys Remain Active After Deletion |
| Dark Reading | Thu, 21 Ma | AI Agents Are Shifting Identity Security Budget Dynamics |
| Dark Reading | Thu, 21 Ma | Chinese APTs Share Linux Backdoor in Central Asia Telco Attacks |

## DATA BREACHES / VULNERABILITIES / UNAUTH ACCESS

| Category | Date | Title |
|---|---|---|
| Data Breach | Sun, 24 Ma | France Sees More Violent Attacks on Crypto Holders Than Any Other Country |
| Data Breach | Sat, 23 Ma | UK: £355,880.10 confiscation order secured following proceeds of crime hearing |
| Data Breach | Sat, 23 Ma | Rhode Island’s workers’ compensation notifies those affected by Janu |
| Vulnerability | Sun, 24 Ma | CVE-2026-9382 - Edimax BR-6675nD POST Request formPPTPSetup buffer overflow |
| Vulnerability | Sun, 24 Ma | CVE-2026-9381 - Edimax BR-6675nD POST Request formPPPoESetup buffer overflow |
| Vulnerability | Sun, 24 Ma | CVE-2026-9380 - Edimax BR-6675nD POST Request formL2TPSetup buffer overflow |
| Unauth Access | Sun, 24 Ma | France Sees More Violent Attacks on Crypto Holders Than Any Other Country |
| Unauth Access | Sat, 23 Ma | UK: £355,880.10 confiscation order secured following proceeds of crime hearing |

## 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 |