BUI INNOVATION™ DELIVERY RESULTS

# DarkWeb Intel Monitor

## Executive Intelligence Report

| | |
|---|---|
| **Generated:** | 2026/11/15, 13:44:45 |
| **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, 15 November 2026 at 13:44

**DARK WEB POSTS**
744
27 critical + 291 high

**RANSOMWARE VICTIMS**
100
25 active groups

**INTEL ARTICLES**
1240
news + threat feeds

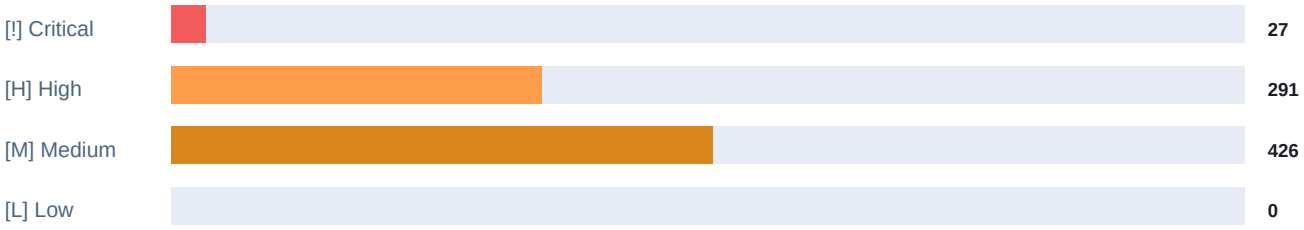
**COUNTRIES AFFECTED**
113
in dark web + ransomware

**HIBP BREACHES**
1052
17858M+ accounts exposed

**WATCHLIST ALERTS**
0
0 unread

**VULNERABILITIES**
245
in feed

## THREAT SEVERITY OVERVIEW -- DARK WEB + RANSOMWARE




## TOP DARK WEB INCIDENTS

| Country | Severity | Sectors | Summary |
|---|---|---|---|
| - | CRITICAL | Telecom | Unpatched Check Point Gateways Are Being Wiped exploiting PHP2She |
| - | CRITICAL | Defence | New SignDrop Exploit Can Abuse Windows Defender to Bypass Securit |
| China | CRITICAL | | Researchers uncover Volt Typhoons covert, ephemeral network The C |
| Philippines | CRITICAL | Defence | Philippines-based American pleads guilty to running expansive fra |
| - | CRITICAL | | German Municipality Targeted in Suspected AI-Driven Zero-Day Atta |
| - | CRITICAL | Education | Untitled <p>If anybody reads this OpenAI post and thinks AI |
| - | CRITICAL | | Untitled <p><a href="hxxps://www[.]csoonline[.]com/artic |
| China | CRITICAL | | Prolific Chinese espionage group exploits BeyondTrust zero-day Re |

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

## RANSOMWARE ACTIVITY

| Group | Victims | Top Sector |
|---|---|---|
| incransom | 27 | Other |
| PixelLeaks | 20 | Technology |
| N0n | 15 | Retail & E-Commerce |
| settra | 5 | Retail & E-Commerce |
| Curious Worm | 3 | Technology |
| akira | 3 | Manufacturing |

## THREAT INTELLIGENCE HIGHLIGHTS

| Source | Date | Title |
|---|---|---|
| Palo Alto Unit 42 | Thu, 12 No | Attackers Use Autonomous AI to Target Semiconductor, Defense and Civil Society S |
| Palo Alto Unit 42 | Wed, 11 No | ARTEX and AI-Powered Red Teaming Tools: What Defenders Need to Know |
| Palo Alto Unit 42 | Wed, 11 No | The XG Files: Falcon C2 Flying Under The (Browser) Radar |
| Palo Alto Unit 42 | Fri, 06 No | Turning Up the Heat: Inside the Attacks on Europes Refrigeration Systems |
| Palo Alto Unit 42 | Mon, 02 No | Unit 42 Threat Intelligence Highlights - Nov. 2, 2026 |
| Palo Alto Unit 42 | Thu, 29 Oc | Threat Brief: Critical Vulnerabilities in PHP: CVE-2026-109618, CVE-2026-109619 |

## TOP CYBERSECURITY NEWS

| Source | Date | Headline |
|---|---|---|
| Dark Reading | Fri, 13 No | ArcticRAT Cybercrime Gang Profiles Victim Finances With AI |
| Dark Reading | Fri, 13 No | Attackers in Binance Breach Targeted Known Weakness, Missing Controls |
| Dark Reading | Thu, 12 No | Getting Past the Post-Quantum Cryptography Discovery Phase |
| Dark Reading | Thu, 12 No | Cyber Experts Weigh In: How to Fight Artex & AntiFox |
| Dark Reading | Thu, 12 No | Extortion Group Luna Moth Flits Into Law Firms a Second Time |
| Dark Reading | Thu, 12 No | Inside an AI Attack Against a US Retailer |

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 | 2026-11-15 | US Flights Halted as FAA Communications Systems Fail |
| Data Breach | 2026-11-15 | IBM Purchases AuthMind to Detect Agents Operating Off-Scope |
| Data Breach | 2026-11-15 | Chinese Actor Automates Attacks on US Defense, Chip Firms |
| Vulnerability | Sun, 15 No | CVE-2026-129449 - DrayTek Vigor2960 mainfunction[.]cgi sub_14914 command injecti |
| Vulnerability | Sun, 15 No | CVE-2026-82663 - Give - Peer-to-Peer <= 2.9.5 - Authorization Bypass to Team |
| Vulnerability | Sun, 15 No | CVE-2026-82568 - Give - Peer-to-Peer <= 2.9.3 - Unauthenticated SQL Injection |
| Unauth Access | 2026-11-15 | US Flights Halted as FAA Communications Systems Fail |
| Unauth Access | 2026-11-15 | IBM Purchases AuthMind to Detect Agents Operating Off-Scope |

## 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.