

# DarkWeb Intel Monitor

## Executive Intelligence Report

---

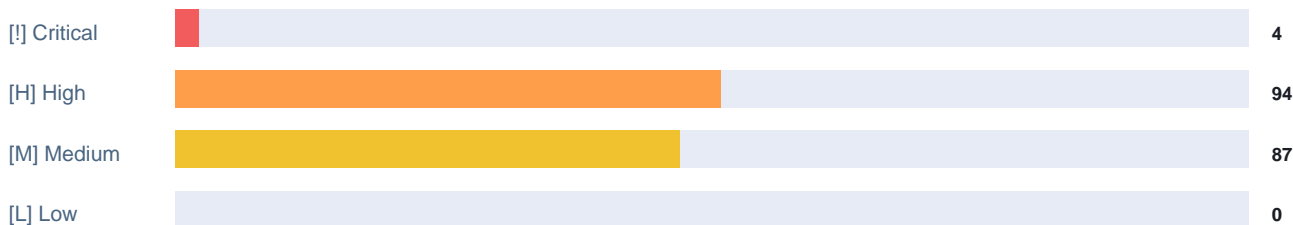
<b>Generated:</b>	2026/04/05, 20:21:43
<b>Generated by:</b>	BUI Security Analyst
<b>Classification:</b>	Informational Content
<b>Source:</b>	BUI DarkWeb Intel Monitor - tools.bui.systems/darkweb

## EXECUTIVE SUMMARY

Intelligence compiled: Sunday, 5 April 2026 at 20:21



## THREAT SEVERITY OVERVIEW -- DARK WEB + RANSOMWARE



## TOP DARK WEB INCIDENTS

Country	Severity	Sectors	Summary
Iran	CRITICAL		Smashing Security podcast #460: Never knock on the door of a nucl
Canada	CRITICAL		Canada - Telus Digital confirms massive data breach by ShinyHunte
Israel	CRITICAL	Energy	Israel - Cardinal group claims breach of Israeli nuclear infrastr
Russia	CRITICAL	Defence	Smashing Security podcast #457: How a cybersecurity boss framed h
-	HIGH	Government	SECURITY AFFAIRS MALWARE NEWSLETTER ROUND 91 Security Affairs Mal
-	HIGH		Security Affairs newsletter Round 571 by Pierluigi Paganini INTER
Germany	HIGH		Qilin ransomware group claims the hack of German political party
-	HIGH		UNC1069 Targets Node.js Maintainers via Fake LinkedIn, Slack Prof

## RANSOMWARE ACTIVITY

Group	Victims	Top Sector
dragonforce	19	Not Found
thegentlemen	17	Not Found
nightspire	10	Not Found
incransom	7	Not Found
netrunner	6	Healthcare
lapsus\$	5	Healthcare

## THREAT INTELLIGENCE HIGHLIGHTS

Source	Date	Title
Security Affairs	Sun, 05 Ap	SECURITY AFFAIRS MALWARE NEWSLETTER ROUND 91
Security Affairs	2026-04-05	SECURITY AFFAIRS MALWARE NEWSLETTER ROUND 91
Security Affairs	Sun, 05 Ap	Image or Malware? Read until the end and answer in comments :)
Security Affairs	Sun, 05 Ap	Security Affairs newsletter Round 571 by Pierluigi Paganini INTERNATIONAL EDITIO
Security Affairs	2026-04-05	Image or Malware? Read until the end and answer in comments :)
Security Affairs	2026-04-05	Security Affairs newsletter Round 571 by Pierluigi Paganini INTERNATIONAL EDITIO

## TOP CYBERSECURITY NEWS

Source	Date	Headline
Dark Reading	2026-04-05	Black Hat USA
BleepingComputer	Sun, 05 Ap	Hackers exploit React2Shell in automated credential theft campaign
The Register	2026-04-05	Researchers didnt want to glamorize cybercrims. So they roasted them
BleepingComputer	2026-04-05	Hackers exploit React2Shell in automated credential theft campaign
The Register	2026-04-05	Researchers didnt want to glamorize cybercrims. So they roasted them
Help Net Security	Sun, 05 Ap	Week in review: Axios npm supply chain compromise, critical FortiClient EMS bugs

**DATA BREACHES / VULNERABILITIES / UNAUTH ACCESS**

Category	Date	Title
Data Breach	Sun, 05 Ap	How often do threat actors default on promises to delete data?
Data Breach	Sat, 04 Ap	The breach lasted 25 minutes. How long will the litigation last?
Data Breach	Sat, 04 Ap	Hong Kong Hospital Authority apologises for data breach involving 56,000 patient
Vulnerability	Sun, 05 Ap	CVE-2026-5579 - CodeAstro Online Classroom Parameter updatedetailsfromfaculty.ph
Vulnerability	Sun, 05 Ap	CVE-2026-5578 - CodeAstro Online Classroom Parameter addassessment.php sql injec
Vulnerability	Sun, 05 Ap	CVE-2026-5577 - Song-Li cross_browser details Endpoint uniquemachine_app.py sql
Unauth Access	Sun, 05 Ap	How often do threat actors default on promises to delete data?
Unauth Access	Sat, 04 Ap	The breach lasted 25 minutes. How long will the litigation last?

**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