

Booba Project Strikes University of Illinois Chicago

October 2, 2026 2 min read Ransomware Attacks

Ransomware Alert

Booba Project Strikes University of Illinois Chicago

Web site : www.uic.edu

Date: 2026-10-02

Country: USA



@dexpose_io



DeXpose



dexpose.io

DEXPOSE

Target

University of Illinois
Chicago

Domain

uic.edu

Country

USA

Attacking Group

Booba Project

Date Reported

October 2, 2026

Summary

On **October 2, 2026**, the ransomware group **Booba Project** claimed responsibility for a cyberattack against **University of Illinois Chicago** (uic.edu), a leading institution in the USA. The attackers have reportedly obtained 344 GB of sensitive data, threatening to leak it unless negotiations are initiated.

Incident Report

Field	Details
Target	University of Illinois Chicago
Domain	uic.edu
Country	USA
Attacking Group	Booba Project
Date Reported	October 2, 2026
Threat Actor Statement	“Higher Education Stolen data: 344 GB.”

Recommended Security Actions

Ransomware attacks are increasingly targeting both enterprise and mid-sized organizations across all sectors. The following steps are critical to reduce impact and prevent future incidents:

- **Monitor continuously:** Use DeXpose’s dark web and infostealer monitoring platform to detect breached credentials, leaked databases, and threat actor chatter in near real-time—before damage spreads internally.

- **Conduct a compromise assessment:** Immediately initiate a full incident review to determine how attackers infiltrated your network, what data may have been exfiltrated, and whether any persistence mechanisms remain active.
- **Validate your backups:** Ensure that your backups are current, encrypted, and stored offline. Utilize immutable backup solutions to defend against ransomware encryption and deletion attempts.
- **Apply threat intelligence:** Integrate external threat feeds, including DeXpose-provided indicators of compromise (IOCs), into your SIEM or XDR platforms for real-time alerting and correlation.
- **Harden employee defenses:** Run phishing simulations and enforce multi-factor authentication (MFA) across all access points. Attackers often exploit weak or reused credentials sourced from the dark web.
- **Engage professional response teams:** Involve cybersecurity incident response experts, threat analysts, and legal counsel before initiating any dialogue with ransomware groups or ransom brokers.

How DeXpose Helps You Stay Ahead

At DeXpose, we specialize in early detection and proactive defense. Our hybrid threat intelligence solution combines automated deep/dark web crawling, Telegram and forum monitoring, and real analyst verification to deliver:

- Continuous scanning of ransomware group leak sites, stolen credential markets, and malware log dumps
- Timely alerts for breaches linked to your domains, email addresses, and key personnel
- Intelligence correlation that connects leaked credentials to infostealer malware infections, often weeks before a public ransom demand
- Real-time visibility into supply chain and third-party exposures through passive surveillance of dark web channels

Don't wait for public disclosure or ransom notices—gain visibility into your cyber exposure now.

- **Scan your domain for data breaches:**

[Free Dark Web Report](#)

- **Check employee or partner email exposure:**

[Email Data Breach Scan](#)

Disclaimer

DeXpose does **not engage** in the exfiltration, hosting, redistribution, or purchase of stolen data. All breach information reported here is collected from publicly accessible dark web sources and threat intelligence platforms. Our mission is to equip organizations with early-warning indicators, contextual threat insights, and actionable intelligence that help them secure their digital assets against evolving cyber threats.

Tags A*F*O USA Booba Project higher education University of Illinois Chicago www.uic.edu

On this page

Summary

Incident Report

Recommended Security Actions

How DeXpose Helps You Stay Ahead

Disclaimer

Is your organization exposed?

Run a free dark web report for your domain: breached credentials, infostealer logs and dark web mentions in seconds.

Domain or email address

Free report

More from the intel feed

All intel feeds

Ransomware Alert

VYPR Ransomware Strikes Construction Leader Gen3

Web site : www.gen3construction.com
Date: 2026-10-07
Country: USA



[@dexpose_io](#) [DeXpose](#) [dexpose.io](#) **DEXPOSE**

Oct 7, 2026 Ransomware Attacks

VYPR Ransomware Strikes Construction Leader Gen3

The VYPR ransomware group has targeted Gen3, a prominent U.S. construction subcontractor. The attack threatens to expose sensitive data unless negotiations are initiated.

[Read more](#)

Ransomware Alert

N0n Ransomware Assaults Company #1

Web site : Not Available
Date: 2026-10-06
Country : Non Disponibile

[@dexpose_io](#) [DeXpose](#) [dexpose.io](#) **DEXPOSE**

Oct 6, 2026 Ransomware Attacks

N0n Ransomware Assaults Company #1

The N0n ransomware group has claimed responsibility for a cyberattack on Company #1. Sensitive data may be published if demands are not met.

[Read more](#)

Ransomware Alert

Aurora Ransomware Targets Infomedia A/S in Denmark

Web site : <https://infomedia.dk>
Date: 2026-10-06
Country: Denmark



[@dexpose_io](#) [DeXpose](#) [dexpose.io](#) **DEXPOSE**

Oct 6, 2026 Ransomware Attacks

Aurora Ransomware Targets Infomedia A/S in Denmark

Infomedia A/S, Denmark's leading media monitoring company, has fallen victim to a ransomware attack by Aurora. Sensitive data, including financial records and employee details, were compromised.

[Read more](#)