Cyberops oblig3

Julia Vister

April 2025

Chapter 1

Task A

You are a university (education sector) in one of the Nordic countries, and there is a request (to the student) to identify the threat landscape regarding ransomware operations, including trends, threat groups, TTPs, and information on the financial impact of successful attacks for the period of June 2024 to January 2025. The stakeholder requires an operational deliverable – report - (no need for indicators of compromise and detection engineering in the operational deliverable – but for sure, give an emphasis on TTPs).

The following intelligence requirements have been defined.

- What ransomware threat groups were active against the Nordic education sector during the time period of June 2024 and January 2025?
- What TTPs - tactics, techniques, and procedures - were used by these groups during attacks during this time frame?
- What are the observable trends in ransomware attacks that targeted the education sector?
- What were the financial impacts of these ransomware attacks on Nordic educational institutions?

Collection Management Plan

1. Collection Objectives

   The objectives are tied directly to each intelligence requirement. This means identifying threat groups, TTPs, trends and financial impact.

2. Source types & Validation

   - MIRE ATT&CK - used for TTP mapping and is a well established CTI framework.
   - Threat Intelligence Blogs - used for group names, attack timelines and trends. Is often peer-reviewed and an industry-standards reporting.

3. Collection methods

   - Manual search using Google and other vendor websites, used for gathering blogs and research.
   - Framework lookup using ATT&CK, used for TTP classification.
   - Feed monitoring through Twitter used for real-time updates.

4. Sources mapped to the IRs

   - Active ransomware groups - Twitter, blogs, CTI reports
   - What TTPs were used? - MITRE ATT&CK, CTI reports
   - What are the trends? - Blogs and reports
   - Financial impacts? - Public disclosures and news articles

3. Identify frameworks that you will use for the overall process, including intelligence analysis frameworks (e.g., diamond model, ATT&CK framework, and other taxonomies) and tools (e.g., different software, including TIP if you need one)

The MITRE ATT&CK framework can be used to classify and analyze TTPs. The Diamond model helps in visualizing the relationship between adversary, capability, infrastructure and victim - and how attackers operate. To organize the data spreadsheets will be used.

4. The intelligence deliverables are reports (separate documents of the main report you will submit). Prepare style guides / templating approaches based on your audience (e.g., strategic, operational/tactical), explain them, and consider the inclusion of infographics, timelines, etc. One figure equals one thousand words at times.

This style guide is meant to be readable by both strategic decision-makers and technical analysts and therefore has a layered communication style. Firstly the language should be:

- for strategic: outcome-focused and plain.
- for operational: technical and precise

All acronyms should be defined. The formatting should be clear and have numbered sections with subheadings. Bold lettering for key points and actor names. The formatting should follow a clean and professional design with consistent spacing. Visual elements should be used to improve understanding.

Chapter 2

Task B - Collection

IR	Data collected	Source Type	Source title and Link	Notes
IR1	LockBit	CISCO Threat Intelligence Report	Talos Year In Review 2024	The educational sector was the most targeted sector by ransomware actors. LockBit is linked to the targeting of education sector.
IR1	8base, Akira, LockBit 3.0	Threat Intelligence Report	SOCRadar Nordic region threat landscape report 2024	8Base, Akira and LockBit 3.0 are the top ransomware groups in nordic regions. Akira and LockBit 3.0 have education as targets. Sweden was heavily targeted.
IR2	LockBit 3.0 TTPs is: T1486 (Data encrypted for impact), T1021.001 (Remote Desktop Protocol)	MITRE ATT&CK	attack.mitre.org	LockBit's known attack tactics.
IR3	Ransomware trend: peaks during academic breaks in spring/summer	CISCO Threat Intelligence Report	Talos Year In Review 2024	Ransomware actors appear more active during the spring and summer, which overlap when schools are closed for break and employees on vacation.
IR4	Financial threats such as ransom payments, data loss and reputational harm	Risk summary	Talos Year In Review and SOCRadar	

Table 1.1: Collection table

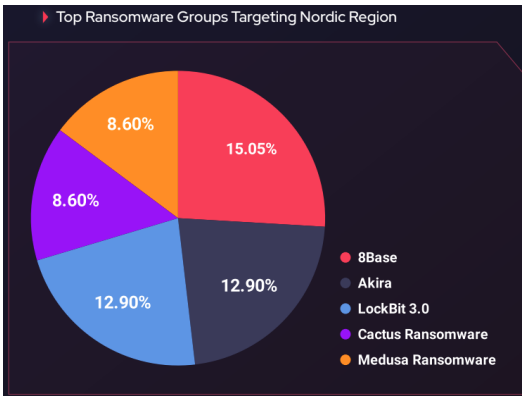

Figure 1.1: Top threat groups in Nordic

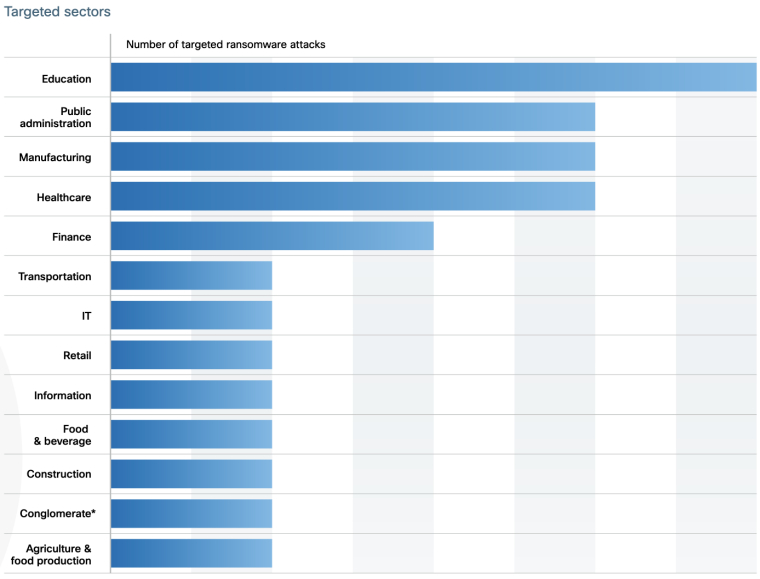

Figure 1.2: Targeted Sectors of ransomware attacks

Chapter 2

Task C - Processing

All collected data has been processed and organized into spreadsheets, as well as visual representation with diamond models.

2.0.1 Spreadsheets

In this part, screenshots of 4 (four) spreadsheets are included to show the organization of threat actors, TTPs, financial impact and trends of attacks in the northern region. Similar information has been grouped logically together so that cross-references between actors, attack impact and techniques are simplified.

Threat Actor	Origin	% of Total Attacks	Target Sectors	Attack Style	Notes
8Base	Unknown	15.05%	Manufacturing, Professional Services	Double Extortion, Ransomware-as-a-Service (RaaS)	Very active, SMB-focused
Akira	Unknown	12.9%	Education, Finance, Manufacturing	Ransomware, Data Exfiltration, Data leakage	Focused on municipalities
LockBit 3.0	Russia	12.9%	Manufacturing, IT, Education	RDP exploitation, Encryption, Phishing, Ransomware	Mature RaaS operation

Figure 2.1: Spreadsheet of threat actors

TTP ID	Name	Tactic Category	Threat Actor	Description
T1566.001	Phishing: Spearphishing Attachment	Initial Access	***8Base***	Email attachments with malware
T1078	Valid Accounts	Initial Access	***Akira***	Using stolen credentials
T1486	Data Encrypted for Impact	Impact	***LockBit 3.0***	Encrypts system data for ransom
T1190	Exploit Public-Facing Application	Initial Access	***Akira, LockBit 3.0***	Attack on vulnerable external apps
T1041	Exfiltration over C2 Channel	Exfiltration	***8Base***	Steals data before encryption
T1133	External remote services	Initial Access	**Akira**	Exploits remote services such as VPNs, Citrix, or Remote Desktop Protocol (RDP)

Figure 2.2: Spreadsheet of TTPs

Trend Observed	Description	Report/Source	Impact
Seasonal Attack Peaks	Attacks peak in spring/summer	Cisco 2024 Report	Staff absence exploited
Legacy Devices Targeted	Attackers exploit EOL hardware	Cisco 2024 Report	Universities running old NAS/firewalls at risk

Figure 2.3: Spreadsheet of attack trends

Incident Example	Ransom Value	Data Breached	Downtime	Notes
Akira attack on Bjuvs Kommun	Unknown	200GB sensitive files	Unknown	Data leak + reputational damage
General Average	~$423,000	Varies	~4 days	Based on global averages Cisco collected

Figure 2.4: Spreadsheet of financial impact

2.0.2 Visual Models

Diamond Model - Akira Ransomware

- Adversary: Akira Ransomware Group
- Infrastructure: Public-facing apps, RDP services, external remote services.
- Capability: Credential abuse, Encryption, Leakage
- Victim: Universities

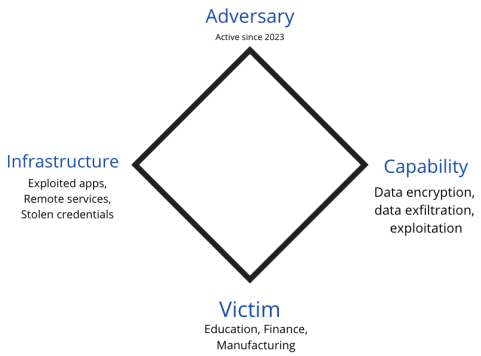

Figure 2.5: Diamond Model of Akira Ransomware Group

Kill Chain Stage	LockBit 3.0 Activity
1. Reconnaissance	Scans for vulnerable targets (especially education, healthcare, IT sectors). Uses tools to find exposed RDP/VPN services and outdated systems.
2. Weaponization	Prepares ransomware payloads and droppers, potentially delivered via phishing or exploits. Often customizes payloads for each victim.
3. Delivery	Gains access through spearphishing emails, malicious attachments, or exploiting public-facing applications (T1190).
4. Exploitation	Exploits weaknesses like unpatched VPNs or RDP misconfigurations (T1021.001). Uses valid accounts (T1078) if available.
5. Installation	Installs ransomware binary and tools (e.g., Mimikatz, Cobalt Strike). Establishes persistence.
6. Command & Control (C2)	Communicates via encrypted channels, sometimes hands-off after deployment (as LockBit is RaaS).
7. Actions on Objectives	Encrypts systems (T1486), deletes backups, and exfiltrates sensitive data. Then launches ransom note and leak threat (double extortion).

Figure 2.6: Cyber Kill Chain for Lockbit 3.0 with 7 stages.

Chapter 3

Task D - Analysis & Production

3.0.1 IR1: Active ransomware threat groups

Through data collection and analysis, it was revealed that the most active ransomware groups that targeted the Nordic education sector in the time frame June 2024 to January 2025 were 8Base, Akira and LockBit 3.0. They were responsible of multiple ransomware attacks against institutions operating in education. Multiple Swedish companies and government institutions, especially a county, were targeted.

3.0.2 IR2: TTPs used by threat groups

Analysis revealed that the most common TTPs in ransomware groups were T1190 (exploiting public applications), T1078 (credential abuse), T1566.001 (spearphishing) and T1486 (encryption of data). 8Base utilized spearphishing and data exfiltration, Akira exploited public vulnerabilities and abused remote services, and LockBit 3.0 exploited mostly exploited Remote Desktop Protocol (RDP).

3.0.3 IR3: Observable trends

Increase in ransomware attacks during periods of reduced IT staff, which particularly happened during academic breaks. In this time frame, that means summer break. Educational institutions have limited cybersecurity budgets and slow patch cycles, and therefore was targeted.

3.0.4 IR4: Financial impacts of ransomware attacks

Specific financial data for Nordic education institutions was limited, though trends collected from Cisco 2024 report, indicated an average ransom demand, and operational downtime on four days. Universities faced consequences due to loss of trust.

3.1 Report

Cyber Threat Intelligence Report: Ransomware Landscape Targeting Education Sector in Nordic Countries

Between June 2024 and January 2025, ransomware attacks against educational institutions in the Nordic increased. **8Base, Akira and LockBit 3.0,** who are all ransomware groups, were the most active during this period. Attacks peaked during academic breaks and unpatched systems were targeted. The financial impact included ransomware demands alongside downtime and reputational damage. This report provides actionable intelligence based on analyzed threat trends, actors, TTP (Tactic, Technique, Procedures) mappings, and financial impacts, along with recommendations.

Intelligence requirements

IR1: Identify active ransomware groups targeting the Nordic education sector.
IR2: Analyze TTPs used by these groups.
IR3: Identify trends in ransomware activity.
IR4: Assess the financial impact of ransomware attacks on education institutions.

Threat Actor Overview

- **8Base:** 15.05% , targeted education with double extortion.
- **Akira:** 12.9% , targeted education with public data leaks.
- **LockBit 3.0:** 12.9% , targeted education with RDP and public-facing services.

The education sector was attractive due to lower cybersecurity budgets, reliance on systems, and predictable staff absences during academic breaks.

Tactics, Techniques, and Procedures (TTPs)

- T1190: used by Akira and Lockbit 3.0, exploitation.
- T1078: used by Akira, stolene credentials.
- T1566.001: used by 8Base, spearphishing.
- T1486: used by LockBit 3.0, data encryption.

Exploitation of external services and credential theft were the most common attacks across all major ransomware groups.

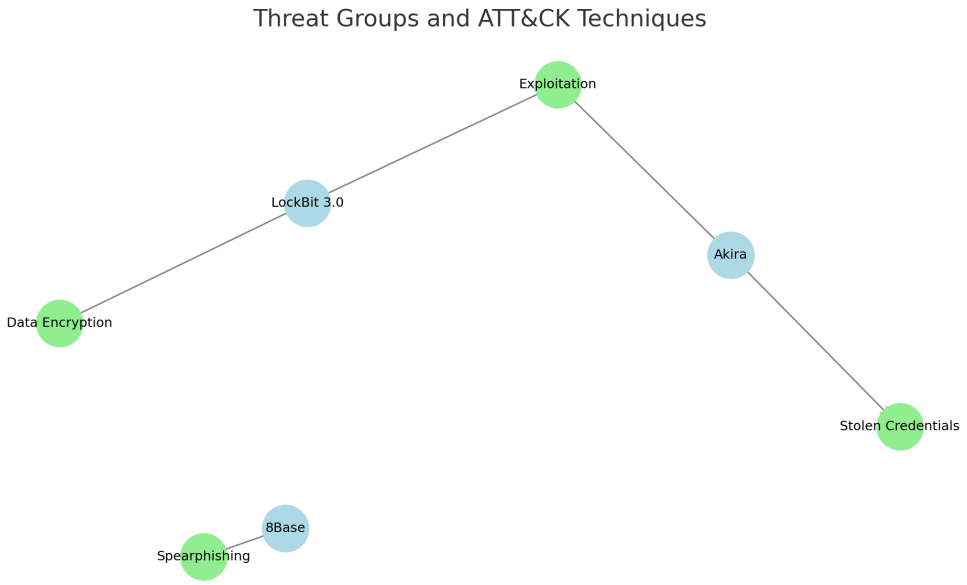

Figure 3.1: Network graph representing the relationships between threat groups and the MITRE ATT&CK techniques used.

Ransomware Attack Trends

- Seasonal attack peaks: Increased activity during academic breaks.
- Legacy system vulnerability: Exploited to gain initial access.
- Shift to double extortion: Exfiltration and leakage of data.

Financial and operational effects

- Average ransome demand: around $400 000 USD.
- Average downtime: around 4 days.
- Example: Akira leaked municipal data from Bjuvs Kommun.

Gaps and limitations in collection

Limitations existed regarding specific ransom payment disclosures and detailed breach reports for Nordic universities. Some findings were generalized from broader education sector data, but were validated across sources.

Recommendations

Strategic recommendations:

- Prioritize patching of public-faces application and legacy systems.
- Increase cybersecurity staff and monitoring during holidays.
- Strengthen backup strategies.

Operational recommendations:

- Implement network traffic analysis to detect exfiltration patterns.
- Harden and monitor RDP access points.

References

- Cisco Talos 2024 Year in Review Report [3]
- SOCRadar Nordic Region Threat Landscape Report 2024 [2]
- MITRE ATT&CK Framework [1]

Bibliography

[1] Zurich Global Information Security Matt Brenton. Lockbit 3.0, 2025.

[2] SOCRadar. Nordic region threat landscape report 2024, 2024.

[3] Cisco Talos. 2024 year in review report, 2024.