PRACTICAL - 10

DATE: 11-04-2025

Case Study: FinBank LockBit 3.0 Threat Case Study

Organization Profile:

Name: FinBank (pseudonym)

Industry: Financial Services

Employees: 20,000+

Customer Base: 10 million+ globally

Cybersecurity Maturity Level: Advanced (Tier 3 SOC)

Threat Scenario:

- In early 2024, FinBank's CTI team observed increased chatter on the dark web indicating potential targeting of financial institutions by the LockBit 3.0 ransomware group. The group was actively exploiting a zero-day vulnerability in an enterprise VPN product (CVE-2024-XXXXX).

Threat Intelligence Collection:

Sources:

1. **Open-source intelligence (OSINT):** Dark web forums, Twitter/X, GitHub
2. **Closed-source feeds:** Commercial threat intelligence platforms (e.g., Recorded Future, Mandiant)
3. **Internal telemetry:** SIEM alerts, endpoint detection logs
4. **Human intelligence (HUMINT):** Info-sharing through FS-ISAC (Financial Services Information Sharing and Analysis Center)

Indicators Collected:

1. IPs and URLs of known command-and-control servers

2. Hashes of LockBit 3.0 payloads

3. Tactics, Techniques, and Procedures (TTPs) associated with LockBit.

Response and Mitigation:

1. IOC Ingestion:
CTI team pushed indicators into the SIEM and EDR platforms for real-time detection.

2. Proactive Threat Hunting:
Analysts ran retrospective analysis on logs for the past 90 days. One employee's VPN access logs showed anomalies.

3. Patch Management:
VPN software was identified as vulnerable. A patch was deployed within 24 hours across all endpoints.

4. User Awareness:
Targeted phishing simulation was run for finance team employees. Multiple clickers received retraining.

5. SOC Escalation Rules Updated:
SIEM was updated to raise critical alerts if any LockBit TTPs were observed.

Outcomes:

1. The attack was detected early during the reconnaissance phase.

2. No systems were encrypted or data stolen.

3. The organization avoided potential losses of over $5 million, including ransom payments, downtime, and reputational damage.

Key Takeaways:

1. Proactive CTI reduces risk: Timely ingestion of intelligence helped prevent lateral movement.

2. Threat sharing matters: Collaboration with FS-ISAC offered valuable early warnings.

3. Patch fast, hunt faster: Rapid patching and internal threat hunting were crucial.

4. Human layer is critical: Phishing awareness can’t be underestimated.

Tools & Technologies Used:

1. SIEM: Splunk Enterprise

2. EDR: CrowdStrike Falcon

3. Threat Intel Feeds: Recorded Future, Mandiant

4. Threat Sharing: FS-ISAC, MITRE ATT&CK framework

5. VPN: Fortinet (patched)

Conclusion:

- The incident reinforced the importance of continuous vigilance, collaborative intelligence sharing, and layered defense strategies, including technical controls and user awareness training. Ultimately, FinBank avoided significant financial and reputational loss, proving that when cybersecurity maturity meets swift execution, even sophisticated threats like LockBit 3.0 can be successfully mitigated.