IHAU REPORT.

Author: Giovanni
Role: Incident Handling Assessment Unit.
Date: 17/11/24.

1. INCIDENT INFORMATION

Incident type: ransomware attack with double extortion (system lockdown and data publication threat).
Attachment name: LockBit 2.0.
Date and time of detection: 17/11/24; 6:15 pm.
Alleged origin: third-party (weak link) supply chain attack via phishing mail. Assets involved: IT systems (servers, endpoints), sensitive data (employee personal data, intellectual property and financial data), credentials and access.

2. CLASSIFICATION OF THE INCIDENT

Gravity: CRITICAL

2.1 INTERNAL IMPACT

Disruption of business continuity resulting in loss of productivity.

Economic damages purchasing the compromised systems and hiring incident response and forensics experts.

Psychological harm from employees to secure personal data such as payroll and health data.

2.2 EXTERNAL IMPACT

REPUTATIONAL: loss of customer trust and reliability of the company as well as damage to corporate image.

LEGAL: Penalties for violations of GDPR, NIS that can bring penalties of up to 4% of global turnover.

COMMERCIAL: loss of customers and relational compromise with suppliers.

DAMAGES FROM PUBLISHED DATA: Identity theft and fraud through the use of exposed personal and financial data.
Intellectual property or strategic information may end up in the hands of competitors.

3. DETECTION AND COLLECTION OF REPORTS

INITIAL IDENTIFICATION OF THE INCIDENT:

Internal reports: employees who disclosed locked systems and inaccessible files.

Automatic alerts: monitoring systems that have detected abnormal activity, such as encryption attempts and unauthorized access.

Ransom note: Ransom payment via Bitcoin (12 BitCoins~ 1M€)

System and network logs: examine suspicious activity, unauthorized connection attempts, exfiltrations, and data encryption.

Confirmation of ransomware type: LockBit.

4. COMMUNICATIONS AND INVOLVEMENT

4.1 COMMUNICATION INTERNAL SUBJECTS

CISO Chief Information Security Officer

On 11/17/24 at 6:30 p.m., via urgent email and follow-up with Meeting Teams, information was shared about the type of incident (ransomware attack and data exfiltration), the impacted systems (file servers, ERP, and backups accessed), and the actions performed (compromised systems isolated and evidence collection).
Strategic oversight by the CISO required for critical decisions (notification to the CSIRT and management of the redemption note).

DPO Data Protection Officer

On 11/17/24 at 7:00 pm, through operational briefing, information of potential exfiltration of personal data related to customers and employees was shared; personal data breach under GDPR.
It is required by the DPO, impact analysis to determine the need for notification to the Data Protection Authority.

IRT (Incident Response Team) and MARIT (Managing and Responding Incident Team).

On 11/17/24 at 7:15 pm via urgent IRT and MARIT emails, the summary report was shared where the alleged origins of the attack and the authorities potentially involved such as GDPR and NIS are listed.

The IRT team is required to:

1. Mapping of compromised systems.
2. Blocking communications with the ransomware infrastructure.
3. Checking the status of backups and preparing for restoration.

While it is required of the MARIT team to:

1. Preparation of a draft notification for the competent authority.
2. Updating the corporate incident log.

4.2 COMMUNICATION EXTERNAL PARTIES

POSTAL POLICE

On 17/11/24 at 8:00 p.m., via pec mail, the ransomware attack was reported at the cybercrime section of the postal police, indicating the name of the attackers' group, the ransom note and the evidence highlighted in the logs of the affected systems, as well as the actions taken by the company.
Investigative assistance is required to identify the perpetrators and prevent publication of exfiltrated data and recommendations on any further legal or security measures to be taken.

5. SUMMARY ATTACK

In this particular case, cyber criminals do not just lock systems encryption, but exfiltrate sensitive data (double extortion).
Although the backup allows for restoration of operations without paying the ransom, the threat to publish the data becomes a pressure weapon to push the company to pay.

Incident Response Report - Supply Chain Attack: LockBit 2.0

Author: Manuel C.

Role: Incident Response Team (IRT)

Date: 17/11/2024

1. Executive Summary

- **Attack Type:** Ransomware Supply Chain Attack (LockBit 2.0)

- **Impact:** Encryption of critical data, threat of exfiltration of sensitive data, potential regulatory violation (e.g., GDPR).

- **Date of detection:** November 17, 2024

- **Current status:** Compromised systems isolated, communications blocked, backups verified for integrity

2. Timeline of the incident

Phase	**Date/Time**	**Details**
Input initial	14/11/2024, 08:00	Supplier compromise in the supply chain.
Survey	17/11/2024, 18:15	Encrypted files detected on endpoints.
Insulation and reply	17/11/2024, 20:00	Network segmented, blockage of the malicious traffic
Verification of backup	18/11/2024, 12:00	Integrity confirmed for backup of the 13/11/2024.

3. Indicators of Compromise (IoC)

Suspicious files detected:

- Encrypted files with the extension " .lockbit "
- Executables detected:
  encryptor.exe, lockbit_loader.ps1

Suspicious connections:

- **IP:** 45.77.89.12, 91.213.233.177 .
- **Domains:** lockbitc2.xyz , data-leak.org .
- **Port used:** 443 (HTTPS).

Instruments detected:

- **Encryption:** Tools such as AES-256 with dynamic keys.

- **Exfiltration:** Using PowerShell and Python scripts to transfer data.

4. Mapping Compromised Systems

Endpoint:

- Laptops and desktops (Windows 10)
- File server (Windows Server 2019)

Encrypted data volume: ~15 TB.

Compromised priority systems:

- Server authentication (Active directory).
- Enterprise database (SQL Server).
- Corporate shares containing legal and financial documents.

5. Immediately Implemented Countermeasures

Network insulation:

- Segmentation via VLAN for compromised systems.
- Restricted access to the devices involved.

Blocking malicious communications:

- Firewall rules for blocking IPs and C2 domains:

```
iptables -A OUTPUT -d
45.77.89.12 -j DROP
iptables -A OUTPUT -d
91.213.233.177 -j DROP
```

- IDS/IPS update with specific rules:

```
alert tcp →any any
(msg: "LockBit C2 Traffic";content: "lockbit";sid:1000002;)
```

Removal of malicious files:

- Tools used: Autoruns,

  Sysinternals Suite.

6. Status of Backups and Restore

Verification:

- Last valid backup: 13/11/2024.
- Hash SHA-256 confirmed on critical files.

Preparation for restoration:

- Test carried out in an isolated environment (sandbox).
- Backups transferred to secure offline storage.

7. Evaluation of Data Exfiltration

Estimated exfiltrated volume: ~2.5 GB.

Data Involved:

- Customer list and contract information.
- HR documents with personal information (name, CF, IBAN.)

Investigations confirmed by:

- Network logs: transfers to external IPs.
- Script files: powershell_upload.ps1 , ftp_transfer.py.

Mitigations implemented:

- Notification to affected users in accordance with GDPR.
- Involvement of legal authorities.

8. Corrective Actions and Future Improvements

Technical improvements:

- Implementation of a Data Loss Prevention (DLP) system.
- Strengthening remote access criteria with MFA.
- Updating backup policies (frequency, immutability).

Training:

- Awareness sessions for staff on the risks of phishing and ransomware.

Future response plan:

- Regular testing of ransomware attack simulations.
- Continuous monitoring with advanced SIEMs.

9. Tools and Technologies Used

EDR: CrowdStrike Falcon.

Firewall: Cisco ASA with custom rules.

IDS/IPS: Snort.

Forensic analysis: FTK Imager, Wireshark.

Backup: Veeam Backup & Replication.

The incident was addressed in a timely and structured manner, using a combination forensic techniques, advanced tools, and containment strategies.

Current status:

- The compromised systems have been completely isolated and there is no further communication with the ransomware's command and control (C2) infrastructure.

  In addition, some research from:

  Nino and Team Torstino

  (Microsoft Incident Response (formerly DART/CRSP)) They suggest the possibility of decrypting files using a Homemade decryptor,make themselves available to help our case.

- Backups have been verified and ready for restoration, ensuring a secure basis for resuming business operations.

- It has been confirmed that approximately 2.5 GB of sensitive data has been exfiltrated, with notifications being made to data subjects and reports to authorities

Impact:

- Critical business data has been preserved through backups, and operations can resume without paying the ransom.
- However, data exfiltration poses a significant risk to corporate reputation and regulatory compliance (e.g., GDPR).

Evaluation:

- The incident revealed gaps in supply chain management and early threat detection mechanisms.
- It also provided an opportunity to improve incident response processes, strengthening the resilience of the enterprise infrastructure.

Future Recommendations:

- As mentioned above, The implementation of a DLP (Data Loss Prevention) system to prevent future exfiltration.
- Increased collaboration with suppliers to ensure they meet safety standards.
- Regularly running ransomware attack simulations and IRT playbook updates.
- Expansion of real-time monitoring through SIEM tools and the addition of an SOC (Security Operations Center).

This coordinated response not only mitigated the immediate risks, but also laid the foundation for a proactive and resilient security.

MARIT Report - Incident Registry and Competent Authority Notification.

Author: Daniline
Role: Managing and Responding Incident Team (MARIT)
Date: 18/11/2024

1. Recording the incident

Incident: #2024-017-LB
Date and time of detection: 17/11/2024, 6:15 p.m.
Incident type: Ransomware (LockBit 2.0) with double extortion Severity:
Critical

Summary description of the incident:
A ransomware attack compromised corporate systems by encrypting critical data and threatening to publish exfiltrated sensitive data (~2.5 GB). Compromised systems include file servers, corporate databases, and network shares. The attacking group demanded a ransom of 12 Bitcoin (~€1M). The origin of the attack was traced to a supply chain compromise via phishing.

Actions taken:
1. Isolation and segmentation of compromised systems.
2. Blocking communications to identified C2 servers.
3. Verification and preparation of backups for systems recovery.
4. Collection of forensic evidence.

2. Notification to Competent Authorities

2.1 Data Protection Authority (GDPR Compliance)

Date sent notification: 18/11/2024,
09:00 Mode: PEC
Notification details:

- *Incident Description*: Ransomware attack with exfiltration of personal data, including sensitive data of employees (name, social security number, IBAN) and business customers.
- *Data volume exfiltrated*: ~2.5 GB.
- *Associated risks*: Identity theft, financial fraud, privacy violation.
- *Actions Taken*: Segregation of compromised systems, blocking communication with malicious servers, initiating recovery via backup, notifying affected parties.

Request: Evaluation by the Authority for further guidance or regulatory requirements, particularly with regard to notices to interested parties and anticipated penalties.

2.2 Computer Security Incident Response Team (CSIRT)

Date sent notification: 18/11/2024,
10:30 a.m. Mode: NIS incident portal.
Notification details:

- Incident Description: Ransomware attack with compromise of business continuity and risk to national data security (e.g., intellectual property).
- Indicators of Compromise (IoC):
  - Suspect IPs: 45.77.89.12, 91.213.233.177.
  - Domains: lockbitc2.xyz, data-leak.org.
  - Malicious files: encryptor.exe, lockbit_loader.ps1.

- Estimated impact: Encryption of critical IT systems (15 TB) and reputational threat corporate data publication.
- Measures taken: C2 traffic blocking, backup integrity check, ongoing forensic investigation.

Request: Technical assistance to mitigate the impact of the attack and investigative collaboration to track the operations of the LockBit 2.0 group.

3. Updating Corporate Accident Registry

Registry ID: #MARIT-2024-017
Opening date: 17/11/2024
Incident category: Ransomware with data exfiltration Next
actions:
1. Timely communication to the relevant authorities.
2. Continuous monitoring to detect further malicious activity.
3. Recommendation to the IT department to update supply chain vulnerability management plan.

4. Notification to stakeholders

Date of sending notifications: 18/11/2024, 2:00 p.m.
Mode: Certified email with tracking of receipts.

Content of the notification:

- Subject: Personal data breach notification
- Body of the message:
  - Dear [Username],
  - We inform you that a cybersecurity incident has resulted in unauthorized access to your personal data, including [specify type of data].
  - We are taking all necessary steps to mitigate the risk and prevent future incidents. To protect yourself, we recommend that you carefully monitor your financial transactions and change any compromised credentials.
  - We deeply apologize for the inconvenience and are available for any clarification at [insert contact].

Number of notified users: 3,000 (including employees and customers).

5. Conclusions and Next Steps

The incident revealed vulnerabilities in vendor management and data protection. The incident log has been updated, and notifications relevant authorities and stakeholders have been completed.

Next actions:

1. Collaborate with CSIRT and Postal Police for additional investigations.
2. Initiate a review of the incident management plan.
3. Implement additional supply chain controls (e.g., periodic security assessments).

Current status of the incident: CLOSED (being monitored).