Embargo Ransomware Campaign Expands to Cloud: Storm-0501 Ramps Up Hybrid Attack Tactics

Credit: Embargo ransomware escalates attacks to cloud environments (bleepingcomputer.com)

---

1. Relevance to the Community:
The Embargo ransomware campaign specifically targets critical sectors, including *hospitals, government, manufacturing, transportation*, and *law enforcement* agencies. Organizations in these sectors rely heavily on cloud-based operations, making this escalation a significant threat.

Impact on the Community:
Victims could face widespread disruption, including theft of sensitive data, compromise of cloud environments, and system-wide file encryption. This could severely impact operational continuity and result in financial loss due to ransomware payments and system recovery.

---

2. Threat Identification and Context:

- **Threat Actor:** *Storm-0501*, originally a ransomware affiliate for Sabbath, is behind the Embargo campaign. They have expanded their operations by deploying ransomware payloads from gangs like Hive, BlackCat, and LockBit.
- **Motivation:** Financial gain through ransomware-as-a-service (RaaS) models.
- **Target Sectors:**
  - Hospitals
  - Government
  - Manufacturing
  - Transportation
  - Law enforcement agencies

TTPs:

- **Initial Access:** Through stolen credentials, exploiting known vulnerabilities (e.g., *CVE-2022-47966, CVE-2023-4966, CVE-2023-29300*).
- **Lateral Movement:** Tools like *Impacket* and *Cobalt Strike* are used for lateral movement.
- **Data Exfiltration:** Use of *Rclone* for data exfiltration.
- **Persistence:** Hijacking cloud synchronization accounts, leveraging *Microsoft Entra ID* (formerly Azure AD).
- **Execution:** Use of PowerShell cmdlets and Group Policy Objects (GPOs) to deploy the Embargo ransomware.

MITRE ATT&CK Mappings:

- *T1078*: Valid Accounts
- *T1566*: Phishing
- *T1210*: Exploitation of Remote Services
- *T1071*: Application Layer Protocol
- *T1047*: Windows Management Instrumentation

---

3. Indicators of Compromise (IOCs):

Indicator	Description	First Observed
CVE-2022-47966	Vulnerability (Zoho ManageEngine)	Ongoing Exploits

Indicator	Description	First Observed
CVE-2023-4966	Vulnerability (Citrix NetScaler)	Ongoing Exploits
CVE-2023-29300	Vulnerability (ColdFusion 2016)	Ongoing Exploits
hxxp://maliciousurl[.]com/rclone.exe	Malicious domain for Rclone tool	August 2024
hxxp://maliciousdomain[.]com/embargo_ransomware	Embargo ransomware payload	August 2024

These IOCs validate the actors' pivot to targeting hybrid cloud infrastructures, and stolen credentials and known vulnerabilities are their primary entry points.

---

4. Vulnerability and Exploit Information:

- **Critical Vulnerabilities:**
  - *CVE-2022-47966* (Zoho ManageEngine)
  - *CVE-2023-4966* (Citrix NetScaler)
  - *CVE-2023-29300* (ColdFusion 2016)

Organizations should patch these vulnerabilities immediately to prevent adversaries from exploiting them.

---

5. Attack Patterns and TTPs:

The ransomware group's attack sequence begins with exploiting cloud credentials, moving laterally through compromised environments, and deploying ransomware or maintaining persistent access via:

- **PowerShell cmdlets**: For disabling security tools.
- **Impacket and Cobalt Strike**: For lateral movement and persistence.

Detection Techniques:

- Monitor abnormal *Microsoft Entra ID* logins and changes.
- Detect PowerShell and scheduled task usage targeting domain admin accounts.

---

6. Incident Reporting and Case Studies:

- **Case Study:**
  - In August 2024, *American Radio Relay League (ARRL)* was hit by Embargo ransomware, and attackers received a $1 million ransom payment in exchange for a decryptor(Embargo ransomware esca…).
  - Earlier in May, *Firstmac Limited*, a major Australian mortgage lender, was breached with 500GB of sensitive data leaked when ransom negotiations failed .

---

7. Mitigation and Defense Recommendations:

- **Immediate Actions:**
  - Patch known vulnerabilities: *CVE-2022-47966*, *CVE-2023-4966*, *CVE-2023-29300*.
  - Enforce multi-factor authentication (MFA) for all privileged accounts, especially for *Microsoft Entra ID*.

    - Strengthen monitoring of cloud synchronization accounts.
- **Best Practices:**
    - Regularly audit cloud credentials and access logs.
    - Deploy *endpoint detection and response (EDR)* solutions capable of detecting lateral movement tools like Cobalt Strike.

---

8. Threat Actor Attribution and Profiling:

- **Attribution:** *Storm-0501*, initially affiliated with *Sabbath ransomware*, now deploys *Embargo* in collaboration with other RaaS groups like *LockBit* and *BlackCat*.
- **Tactics:** Focus on leveraging both on-premises and cloud environments, escalating attacks to hybrid infrastructures for maximum disruption.

---

9. Real-Time Updates and Alerts:

This campaign is currently active, with ongoing attacks targeting cloud and hybrid environments. The need for immediate action is critical, particularly for sectors with high cloud reliance.

---

10. Collaborative Tools and Resources:

- No specific open-source tools are mentioned, but *Impacket*, *Cobalt Strike*, and *Rclone* are used maliciously by the actors. Organizations should configure detection rules to track these tools.

---

11. Vulnerability and Threat Intelligence Correlation:

- Vulnerabilities like *CVE-2022-47966* and *CVE-2023-4966* have been exploited by the group in previous incidents(Embargo ransomware esca…), indicating a direct correlation between these vulnerabilities and the current wave of attacks.

---

12. Legal and Regulatory Considerations:

- **GDPR Compliance:** Organizations hit by Embargo may face regulatory consequences if customer or operational data is breached. Data recovery and reporting to authorities must comply with regulations like *GDPR*.

---

13. Continuous Monitoring and Feedback Loop:

- Organizations should continuously monitor their cloud environments for suspicious activities, especially involving *Microsoft Entra ID*. Threat intelligence feeds focused on hybrid cloud attacks should be prioritized.

---

14. Anonymity and Data Sensitivity:

- No specific data sensitivity concerns were mentioned, but any collected data during the attacks should be anonymized before sharing with third parties or regulatory bodies.

---

15. Strategic Threat Trends and Predictions:

The pivot to cloud and hybrid environments signifies a growing trend in ransomware campaigns, mainly targeting cloud synchronization accounts and privileged access in cloud infrastructures. This trend is expected to continue into 2025 with more sophisticated tactics.