SOC145 - Ransomware Detected

📋 Security Incident Investigation Report

> Incident ID: IR-2021-0523
>
> **Report Date:** 20 July 2025
>
> **Lead Analyst:** Febrian Ramadhan
>
> **Incident Status:** Closed

---

1. Executive Summary

> On May 23, 2021, a high-priority alert (SOC145) indicated a ransomware attack on the host MarkPRD. The investigation confirmed the execution of a malicious payload, ab.exe, identified as a variant of the Avaddon Ransomware. The attacker's primary tactic was the immediate destruction of system recovery mechanisms, including the deletion of Volume Shadow Copies, to prevent data restoration. The host was successfully contained to halt further damage.

---

2. Attack Narrative & Timeline

Attack Chronology

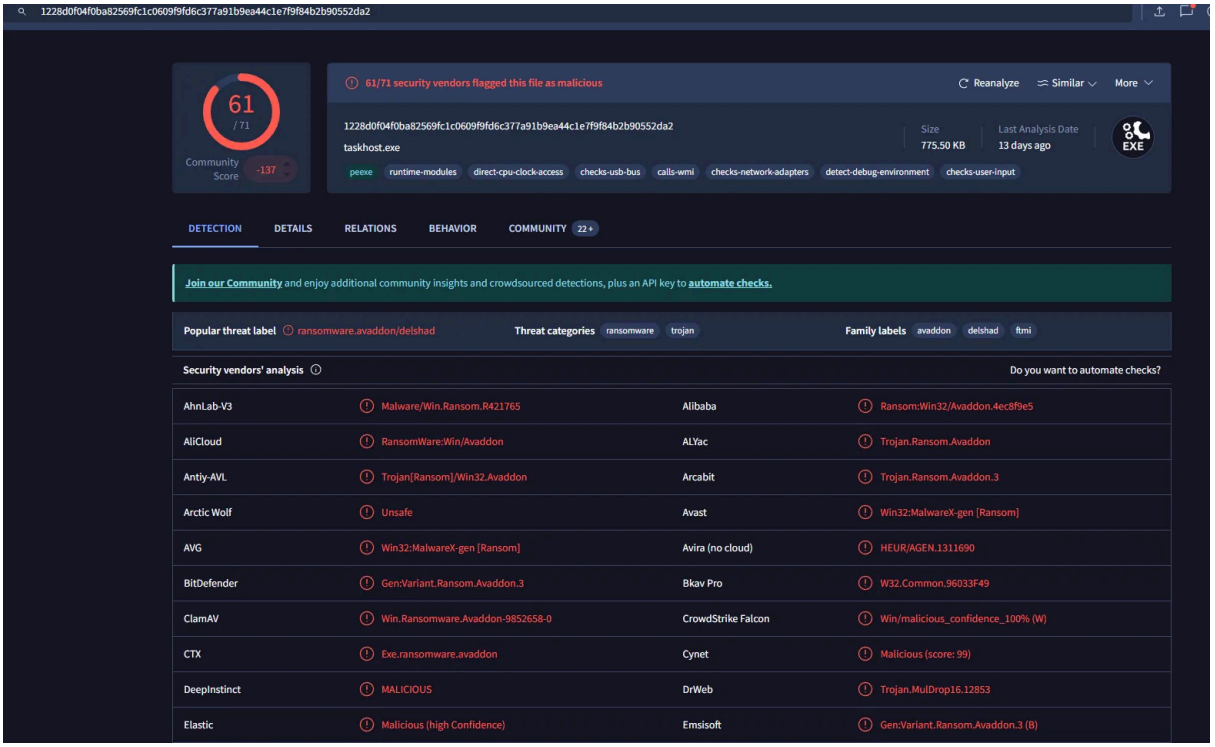
Timestamp (UTC)	Tactic (MITRE ATT&CK)	Activity Description	Data Source
May 23, 2021, 07:32 PM	**T1204.002 - User Execution**	The primary ransomware payload, ab.exe, was executed on the host MarkPRD.	EDR Logs
May 23, 2021, 07:32 PM	**T1490 - Inhibit System**	System utilities vssadmin.exe, wmic.exe,	EDR Logs

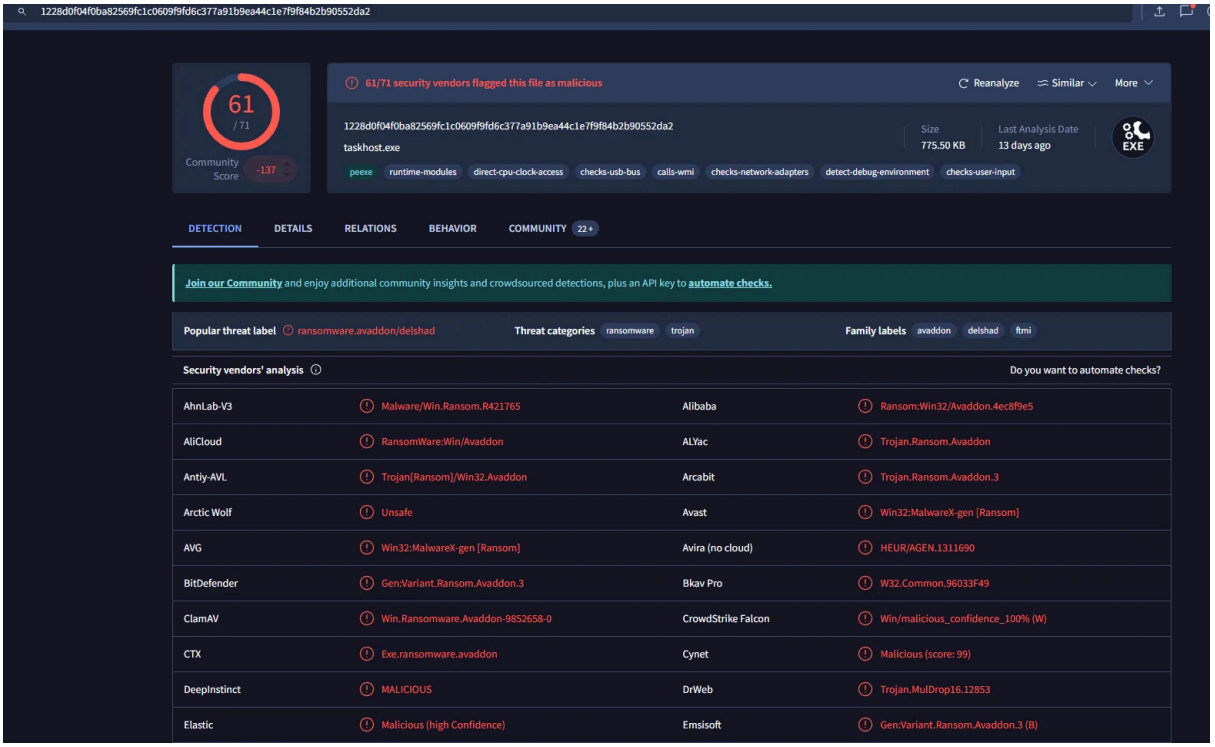
	Recovery	and wbadmin.exe were executed to delete Volume Shadow Copies and system backups.	
May 23, 2021, 07:32 PM	**T1561.002 - Modify System Recovery**	The bcdedit.exe process was executed, indicating an attempt to tamper with the system's boot configuration.	EDR Logs
May 23, 2021, 07:32 PM	**T1486 - Data Encrypted for Impact**	The file encryption routine began, triggering the SOC145 - Ransomware Detected alert.	EDR Alert

3. Technical Analysis

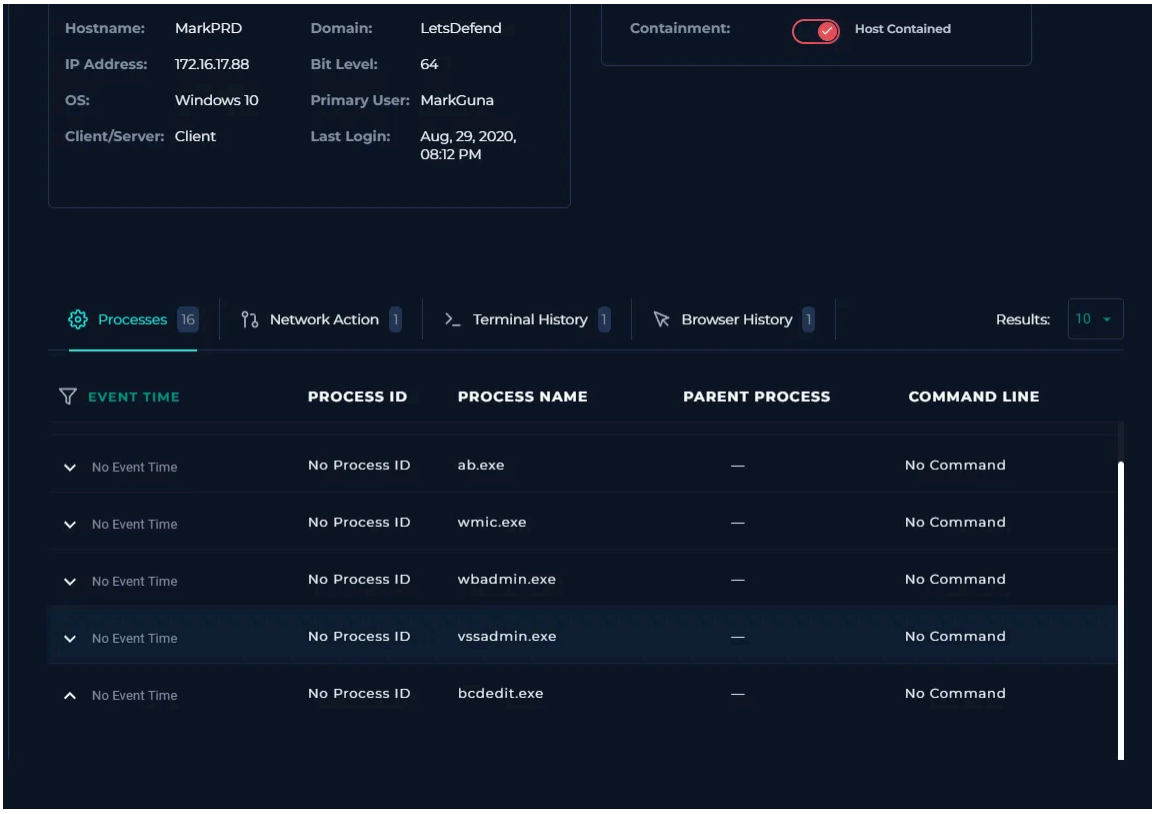
Endpoint Analysis

- **Host Identified:** MarkPRD (IP: 172.16.17.88)
- **Suspicious Processes:**
  - **Process Names:** ab.exe, vssadmin.exe, wmic.exe, wbadmin.exe, bcdedit.exe
  - **Parent Process:** Not captured by EDR, likely due to rapid, successive execution to evade detection.
  - **Command Line:** Not captured by EDR.
- **Malicious File:**
  - **File Name:** ab.exe
  - **Path:** Not specifically identified.
  - **Hash (MD5):** 0b486fe0503524cfe4726a4022fa6a6b
- **VirusTotal Analysis:** Detected by **61 out of 71 vendors** as Ransomware, with the primary variant identified as ransomware.avaddon/delshad.





- **Behavioral Analysis:**
  - The sequential execution of vssadmin, wmic, and bcdedit is a clear TTP (Tactic, Technique, and Procedure) of modern ransomware. This behavior aims to cripple system recovery capabilities before commencing the primary encryption routine.



Network Analysis

- **Suspicious Connections:** No outbound network connections were detected from the ab.exe process during the observation period.
- **Analysis:** This strongly indicates that this ransomware variant is an "offline" or "smash-and-grab" type. It does not require communication with a Command & Control (C2) server to initiate encryption, as the cryptographic keys are likely embedded within the payload itself.

Log & Email Analysis

- Not applicable for this incident, as the initial access vector did not originate from email or specific server logs. The investigation centered on endpoint behavior.

---

4. Scope of Impact

- **Impacted Assets:**
  - MarkPRD - Status: Contained & Isolated. Re-imaging is recommended.
- **Impacted Accounts:**

    - MarkGuna (Primary User) - Password reset is recommended as a precaution.
- **Impacted Data:**
    - **Data Type:** Unknown, assumed all local files on the host were at risk of encryption.
    - **Data Exfiltration:** No Evidence Found

---

5. Indicators of Compromise (IOCs)

IOC List

IOC Type	Value	Context
File Hash (MD5)	0b486fe0503524cfe4726a4022fa6a6b	Ransomware Payload
File Name	ab.exe	Ransomware Payload

---

6. Recommendations

Immediate Actions (Completed)

- Host MarkPRD has been isolated from the network via the EDR platform.

Short-Term Hardening (1-2 Weeks)

- **Eradication:** The compromised host MarkPRD must be fully re-imaged from a trusted, clean source.
- **Threat Hunting:** Conduct an environment-wide hunt for the file hash 0b486fe... to ensure no other systems are compromised.
- **IOC Blocking:** Ensure the malicious file hash is globally blocked by all endpoint security solutions.

Long-Term Strategic (1-3 Months)

- **Endpoint Hardening:** Implement policies (e.g., via AppLocker or EDR) to restrict or strictly monitor the execution of sensitive system utilities like vssadmin.exe and bcdedit.exe by non-administrative accounts.
- **Backup Resiliency:** Review the backup strategy to ensure critical data copies are stored in an immutable or air-gapped location, protecting them from deletion by ransomware.

- **Behavioral Detection:** Create a high-severity correlation rule in the SIEM/EDR to alert when the specific sequence of vssadmin, wmic, bcdedit is executed within a short timeframe on a single host.

---

7. Lessons Learned

- **What Went Well?**
  - The EDR's behavioral detection engine successfully identified the ransomware activity despite its rapid execution.
  - The ability to quickly isolate the host via the platform was critical in preventing potential lateral movement.
- **Areas for Improvement?**
  - Visibility into command-line arguments needs enhancement. A more aggressive EDR logging policy or the deployment of Sysmon could capture these crucial forensic details in the future.
  - Detection could be shifted earlier in the kill chain. An alert should be triggered upon the execution of backup deletion utilities, rather than waiting for the encryption phase to begin. This points to an opportunity for more proactive behavioral rule creation.