# Malware Analysis Report

**Analyst:** Samuel Jemal
**Date of Investigation:** 29 October 2025
**Incident Type:** Trojan (Data Exfiltration Simulation)
**Severity Level:** High
**Status:** Closed

## 1. Executive Summary

On October 28, 2025, an endpoint alert flagged suspicious process execution on a Windows host. The observed behavior included unusual outbound network connections and a process writing to user Documents folder. The sample was analyzed using online sandboxing and static analysis tools. The investigation concluded the executable was a Trojan designed to collect keystrokes and exfiltrate files. Containment was performed and IOC blocking reduced further activity.

## 2. Tools Used

- VirusTotal – Hash and URL reputation
- Any.Run – Dynamic sandbox analysis
- Hybrid Analysis – Behavioral report
- Wireshark – Network capture analysis
- Strings / PEiD – Static inspection
- MITRE ATT&CK; Framework – TTP mapping

## 3. Analysis Process

- Alert Triage: Security agent reported an unknown process 'update_helper.exe' creating network connections to suspicious domains.
- Sample Retrieval: Hash 'e3b0c442...' identified; sample referenced in VirusTotal with behavioral flags.
- Static Analysis: Extracted strings showed C2 domain patterns and base64-encoded configuration.
- Dynamic Analysis: Any.Run sandbox executed sample: observed file enumeration, keystroke collection routines, and periodic POST to C2 endpoint.
- Network Analysis: Wireshark capture revealed POST requests to IP 203.0.113.45 on port 443 with anomalous user-agent strings.
- Containment: Host isolated, process terminated, indicators added to firewall and EDR blocklists.

## 4. Findings

| Indicator Type | Value | Description |
|---|---|---|
| File Name | update_helper.exe | Suspicious executable |
| SHA256 | e3b0c44298fc1c149afbf4c8996fb924 | Unique sample hash |
| C2 Domain | cfg-server[.]example | Command and control |
| IP Address | 203.0.113.45 | C2 host |
| Observed Behavior | Keystroke logging, file collection | Data exfiltration routines |

## 5. MITRE ATT&CK; Mapping

| Phase | Technique ID | Technique Name |
|---|---|---|
| Initial Access | T1190 | Exploit Public-Facing Application (simulated delivery) |
| Execution | T1059 | Command and Scripting Interpreter |
| Persistence | T1547.001 | Registry Run Keys / Startup Folder |

| | | |
|---|---|---|
| Credential Access | T1056.001 | Keylogging |
| Exfiltration | T1041 | Exfiltration Over C2 Channel |

## 6. Containment & Remediation

- Isolated affected host from network immediately.
- Removed executable from disk and terminated persistent services.
- Blocked C2 domain and IP at perimeter firewall and EDR.
- Reset credentials for impacted accounts and enforced MFA.
- Performed full endpoint scan and restored affected files from backups.

## 7. Recommendations

- Harden endpoint protection and ensure EDR telemetry is centralized in SIEM.
- Implement network segmentation to limit lateral movement.
- Enforce MFA and rotate credentials after suspected compromise.
- Regular user awareness training to avoid social engineering paths.
- Maintain offline backups and test restore procedures.

## 8. Lessons Learned

- Early detection by endpoint sensors was crucial to prevent data exfiltration.
- Proactive blocking of known malicious infrastructure reduces risk.
- Invest in better visibility for lateral movement detection.

## 9. Analyst Signature

Name: Samuel Jemal
Role: SOC Analyst (Intern)
Date: 29 October 2025