INCIDENT ANALYSIS REPORT

Malware Execution & Workstation Compromise

Field	Details
Prepared By	Grace Smith
Date	9th April, 2026
Classification	CONFIDENTIAL
Incident Type	Malware Execution via Email Attachment
Severity	HIGH
Status	Under Investigation

1. Executive Summary

This report analyses a security alert that was triggered by an intrusion detection system(IDS) because a suspicious file was executed on an employee's workstation. The goal was to analyse the file by using threat intelligence tools and to determine whether its malicious or not.

By using VirusTotal for the threat intelligence analysis, I confirmed that the file is indeed malicious, with the detection scores showing that it is a known malware sample. The file was able to establish network communications with suspicious domains and URLs. This report provides a full account of the incident timeline, findings, attack methodology, recommendations, and conclusion based on available evidence.

2. Incident Overview

Attribute	Value
Incident Date	9th April, 2026
Detection Method	Intrusion Detection System (IDS)
Initial Vector	Malicious Email Attachment
Affected Asset	Employee Workstation
Notified Team	Security Operations Centre (SOC)
Analysis Platform	VirusTotal Threat Intelligence

2.1 Incident Timeline

Time	Event
1:11 p.m.	The employee received a phishing email that contained a malicious file attachment
1:13 p.m.	The employee downloaded the file and opened it
1:15 p.m.	Multiple unauthorized executable files are created on the employee's workstation.
1:20 p.m.	An intrusion detection system(IDS) detects the executable files and sends out an alert to the SOC.

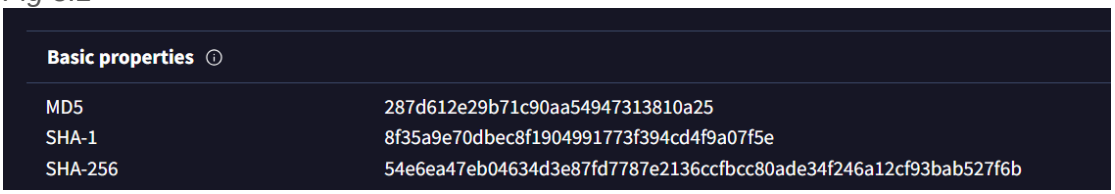
3. Findings

3.1 File-Based Indicators of Compromise (IOCs)

Hash Type	Hash Value
SHA-256	`54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`

MD5	287d612e29b71c90aa54947313810a25
SHA-1	8f35a9e70dbec8f1904991773f394cd4f9a07f5e

Fig 3.1



3.2 Network-Based Indicators of Compromise (IOCs)

After the execution, the malware was able to establish communication outside of the internal network and the following domains and URLs were contacted.

3.2.1 Contacted URLs

- https://www.virustotal.com/gui/url/0755c27d1c56812e9c7882139a4535dfa4156cc0efbb9523273fd9af50bcf337
- https://www.virustotal.com/gui/url/11c4f346050f46a47ae190d60a4c5b355ccd621fe758d6201009e3a64ecbea17

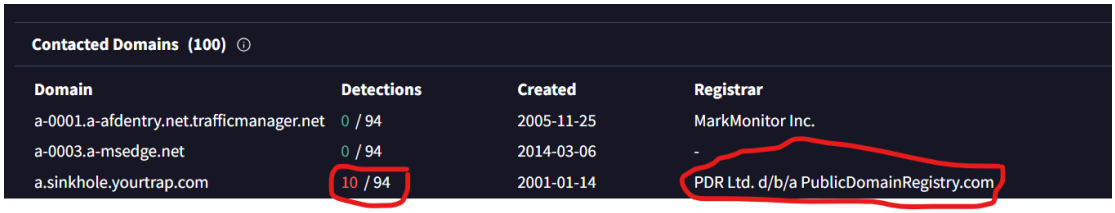
Fig 3.2

Both URLs were flagged as malicious or suspicious in VirusTotal analysis. As shown in Fig 3.2 above, both URLs have detection scores that pass as suspicious and strongly malicious.

3.2.2 Contacted Domains

- a-0001.a-afdentry.net.trafficmanager.net

Fig 3.3



Contacted Domains (100)

Domain	Detections	Created	Registrar
a-0001.a-afdentry.net.trafficmanager.net	0 / 94	2005-11-25	MarkMonitor Inc.
a-0003.a-msedge.net	0 / 94	2014-03-06	-
a.sinkhole.yourtrap.com	10 / 94	2001-01-14	PDR Ltd. d/b/a PublicDomainRegistry.com

This domain is hosted on Microsoft Azure Traffic Manager infrastructure (trafficmanager.net). It is a technique that is frequently used by threat actors to take advantage to trusted cloud platforms and avoid being compared with known indicators or identified. The domain a-afdentry.net is associated with malicious activity and was flagged accordingly on VirusTotal.

3.3 VirusTotal Detection Summary

Analysis via VirusTotal's multi-engine scanning platform yielded positive detections from numerous security vendors. Key findings include:

- The file was classified as malware by multiple AV engines.
- The SHA-256 hash matched known malware signatures in threat intelligence databases.
- Contacted network indicators (URLs and domains) are associated with malicious campaigns.
- Behavioral sandbox analysis showed executable file creation consistent with a dropper or loader payload.

4. Attack Analysis

4.1 Attack Vector & Initial Access

The attack was initiated via a phishing email containing a malicious attachment. This is consistent with the MITRE ATT&CK technique T1566.001 — Spearphishing Attachment. The employee got the email at 1:11 p.m. and opened the malicious attachment attachment two minutes late. This implies that the email was was formulated with enough social engineering tools that trigger prompt action or response. The rapid execution by the user suggests that the attacker might have used language that induced urgency, impersonated a trusted sender identity, or disguised the file as a legitimate document.

4.2 Execution Phase

Upon execution at 1:13 p.m., the file initiated a sequence of malicious actions. Within two minutes (1:15 p.m.), multiple unauthorized executable files were created on the workstation. This behavior is characteristic of a dropper or downloader malware variant — a type of malware designed to deliver and install additional payloads on the victim's system.

This maps to MITRE ATT&CK T1204.002 — User Execution: Malicious File, where the threat actor relies on end-user interaction to trigger the initial payload.

4.3 Persistence & Payload Delivery

The creation of multiple executable files on the compromised workstation indicates the malware was likely performing one or more of the following:

- Dropping secondary payloads (e.g., ransomware, RAT, spyware, or keylogger) onto the system.
- Establishing persistence mechanisms to survive system reboots.
- Modifying system configurations or registry entries to enable continued access.
- Communicating with external C2 infrastructure to receive further instructions.

The contacted domain a-0001.a-afdentry.net.trafficmanager.net strongly suggests C2 communication activity (MITRE ATT&CK T1071 — Application Layer Protocol). The use of Azure Traffic Manager provides the attacker with high availability, load balancing, and trusted infrastructure — complicating detection and takedown.

4.4 Defense Evasion

Several indicators suggest deliberate defense evasion techniques were employed by the threat actor:

- Use of a legitimate cloud provider (Azure Traffic Manager) for C2 to blend in with normal enterprise traffic.
- The file's execution resulted in the creation of child executables, potentially to obfuscate the true payload and complicate forensic analysis.
- A 5-minute gap between payload execution (1:15 p.m.) and IDS detection (1:20 p.m.) suggests the malware may have initially operated below the detection threshold.

4.5 MITRE ATT&CK Mapping

Tactic	Technique ID	Description
Initial Access	T1566.001	Spearphishing Attachment via Email
Execution	T1204.002	User Execution: Malicious File
Persistence	T1547	Boot/Logon Autostart Execution (suspected)
C2 Communication	T1071	Application Layer Protocol (HTTPS)
Defense Evasion	T1036	Masquerading / Trusted Infrastructure Abuse

5. Recommendations

Based on the findings and attack analysis, the following immediate and long-term recommendations are provided to contain the current incident and reduce future risk:

5.1 Immediate Containment Actions

- Isolate the affected workstation from the network immediately to prevent lateral movement and further C2 communication.
- Block the identified IOCs (SHA-256 hash, domains, and URLs) across all network security controls — firewalls, proxy filters, EDR platforms, and email gateways.

- Revoke active sessions and reset credentials for the affected employee account, as credentials may have been harvested.
- Initiate a full forensic image of the compromised workstation before any remediation to preserve evidence.
- Alert all SOC analysts to monitor for similar activity across the broader environment for signs of lateral spread.

5.2 Eradication & Recovery

- Wipe and reimage the affected workstation using a known-good baseline image.
- Scan all adjacent systems and shared network drives for the identified IOCs or similar file patterns.
- Restore any affected data from clean, verified backups.
- Verify that all dropped executables identified during analysis have been removed from the environment.

5.3 Email Security Improvements

- Implement or strengthen email attachment sandboxing to detonate suspicious files before delivery to end-users.
- Enforce strict DMARC, DKIM, and SPF policies to reduce spoofed sender delivery.
- Configure email filtering rules to block or quarantine executable file types (.exe, .bat, .vbs, .js, .ps1) delivered as attachments.
- Enable real-time threat intelligence feeds in the email security gateway to block known-malicious sender domains.

5.4 Endpoint & Network Security

- Ensure Endpoint Detection and Response (EDR) solutions are deployed on all workstations with up-to-date signatures and behavioral detection enabled.
- Configure the IDS/IPS to alert on unauthorized process creation, child executable spawning, and outbound traffic to known-malicious infrastructure.
- Implement application whitelisting to prevent execution of unauthorized binaries.
- Enable DNS filtering to block resolution of malicious or suspicious domains, including abuse of cloud infrastructure like Azure Traffic Manager.

5.5 User Awareness & Training

- Conduct mandatory phishing awareness training for all staff, with particular emphasis on the risks of opening email attachments from unknown or unexpected senders.
- Run regular simulated phishing campaigns to assess and improve employee resilience.
- Establish a clear, accessible mechanism for employees to report suspicious emails to the SOC without fear of repercussion.

5.6 Process & Policy Improvements

- Review and update the Incident Response Plan (IRP) to incorporate lessons learned from this incident.
- Define escalation paths and SLAs for phishing-related incidents to reduce response time from detection to containment.

- Ensure all critical IOCs identified during this investigation are shared with relevant threat intelligence sharing communities (e.g., ISAC, FS-ISAC).

6. Conclusion

This incident represents a successful phishing-based malware delivery campaign targeting an employee workstation within the organization. The attacker leveraged a malicious email attachment to gain initial access, executed a dropper payload capable of deploying additional malware, and established command-and-control communication via cloud infrastructure to evade detection.

The Intrusion Detection System performed effectively by identifying and alerting the SOC within five minutes of malicious executable creation, providing the security team with an opportunity to respond before further damage could occur. However, the fact that the attack succeeded in reaching the endpoint and executing its payload highlights critical gaps in pre-delivery controls, specifically around email attachment inspection and user awareness.

The indicators of compromise identified — including the SHA-256 file hash, contacted URLs, and the Azure-hosted domain — provide actionable intelligence that should be immediately operationalized across all defensive layers. The MITRE ATT&CK techniques observed in this incident are well-documented and have established detection and mitigation strategies that the organization should prioritize.

This incident underscores the persistent and evolving nature of phishing-based threats. A multi-layered defensive approach combining technical controls, threat intelligence integration, and continuous user education remains the most effective strategy to reduce the likelihood and impact of future incidents. Prompt containment, thorough forensic investigation, and disciplined remediation will be essential to ensuring full recovery from this event.

INCIDENT HANDLER'S JOURNAL

Date: 9th April	**Entry:** 01
Description	This report analyses a security alert that was triggered by an intrusion detection system(IDS) because a suspicious file was executed on an employee's workstation. The goal wass to analyse the file by using threat intelligence tools and to determine whether its malicious or not.
Tool(s) used	VirusTotal

The 5 W's	• **Who**? An employee (whose workstation was compromised) • **What** happened? The employee received a phishing email with a malicious file attachment, opened it, and it executed malware on their workstation • **When** did the incident occur? On **9th April, 2026**, between **1:11 p.m.** (email received) and **1:20 p.m.** (SOC alerted) — a 9-minute window from delivery to detection. • **Where** did the incident happen? On an **employee's workstation** within the organization's environment. • **Why** did the incident happen?A combination of factors: A. The employee opened an unsolicited email attachment without verifying its legitimacy B. Pre-delivery email security controls failed to flag or quarantine the malicious file C. The attacker exploited human error through social engineering (phishing), which remains one of the most effective and low-cost attack methods
Additional notes	The fact that the attack succeeded in reaching the endpoint and executing its payload highlights critical gaps in pre-delivery controls, specifically around email attachment inspection and user awareness.