Emotet Malware Outbreak via Malicious Macro

Case #CASE-2026-009

LEAD INVESTIGATOR
Benjamin Taylor

TOTAL ITEMS
8 Evidence Items

STATUS
OPEN

PROJECT / TYPE
Malware Infection

INCIDENT DURATION
5 days

CURRENT PHASE
Preparation & First Actions

Investigation Team

- **John Scott** (Investigator)
- **Aria Hernandez** (Investigator)
- **Leo King** (Investigator)
- Avery Walker (Viewer)
- Avery Wright (Viewer)

Case Attributes

Malware Family	Emotet	**Detection Source**	EDR
Affected Department	Finance	**Automated Action Taken**	Quarantined

Case Description

Emotet banking trojan infection spreading through internal network via malicious Word document.

Table of Contents

1. Disclaimer and Reading Guide

This report has been written based on the facts found during an investigation into a cyber security incident. The investigation conclusions and findings are based on the materials delivered for inspection and discovered during the investigation. All findings in this report are subject to change if new evidence is discovered or presented to the investigation team.

1.1. Timestamps

Unless otherwise stated, all timestamps are presented in Coordinated Universal Time (UTC) following the ISO 8601 format: YYYY-MM-DDTHH:MM:SSZ.

1.2. Statements of Probability

Chance	Statement
1-10%	Very Unlikely, Almost certainly not
11-40%	Unlikely, Improbable
41-60%	Even Chance
61-90%	Probably, Likely
90-99%	Very Likely, Almost Certainly

1.3. Statements of Confidence

- **High Confidence**: Evidence strongly supports the statement with no contrary evidence
- **Medium Confidence**: Evidence supports the statement but other evidence could surface
- **Low Confidence**: Missing evidence, major questions unanswered

2. Distribution List

Name	Role	Method of delivery
James Wilson	Chief Information Security Officer	Secure email
Sarah Chen	VP of Information Technology	Secure email
Michael Torres	General Counsel	Encrypted USB
Emily Johnson	Chief Risk Officer	Secure email

3. Intended Audience

This document is prepared for multiple audiences:

Executive Summary: Board members, C-suite executives, and non-technical stakeholders **Technical Sections**: Security operations team, IT infrastructure team, and incident responders
Recommendations: IT management, security architects, and compliance officers

Technical jargon is minimized in the main body; detailed technical findings are in the appendices.

4. Executive Summary

On 2026-01-26, multiple workstations were infected with Emotet malware after an employee opened a malicious Word document attached to a phishing email. The malware established persistence and attempted to spread laterally using stolen credentials.

Twelve workstations were confirmed infected before containment. The EDR solution successfully blocked credential theft on 8 of the 12 systems. All infected machines have been reimaged, and network-wide credential rotation has been completed.

No evidence of secondary payload delivery (such as ransomware) was observed.

5. Business Impact Analysis

5.1. Immediate Impact

- **Service Disruption**: Customer-facing portal unavailable for 4 hours during containment
- **Productivity Loss**: 150 employees unable to access email for 6 hours
- **Incident Response Costs**: Emergency engagement of external IR firm

5.2. Short-Term Consequences

- **Financial**: Estimated direct costs of €75,000 (IR services, overtime, emergency hardware)
- **Operational**: Delayed product launch by 2 weeks due to resource reallocation
- **Compliance**: Mandatory breach notification to Data Protection Authority within 72 hours

5.3. Long-Term Ramifications

- **Reputational**: Potential customer trust erosion; proactive communication recommended
- **Regulatory**: Possible GDPR investigation; maximum penalty exposure of €10M
- **Insurance**: Cyber insurance claim filed; deductible of €50,000 applies

6. Investigation Limitations

The following limitations affected the scope and depth of this investigation:

- **Log Retention**: Firewall logs were only available for the past 30 days due to storage constraints. Events prior to this window could not be analyzed.
- **Endpoint Coverage**: EDR solution was deployed on 85% of endpoints. The remaining 15% (primarily legacy systems) had limited visibility.
- **Memory Forensics**: Live memory acquisition was not possible on 3 systems that had already been rebooted before the IR team arrived.
- **Third-Party Dependencies**: Logs from the cloud email provider were requested but not received within the investigation timeline.

Recommendation: Implement centralized log management with minimum 90-day retention for all security-relevant data sources.

7. Investigation Goals and Research Questions

7.1. Investigation Research Questions

1. What vulnerability or weakness was exploited to gain initial access?
2. What is the complete timeline of attacker activity?
    - First observed activity
    - Lateral movement events
    - Data access or exfiltration attempts
3. Which user credentials were compromised?
    - How were they obtained?
    - Were they used for further access?
4. Was any personally identifiable information (PII) accessed?
    - Customer data?
    - Employee data?
    - Financial information?
5. What remediation steps are required to prevent recurrence?

8. Investigation Details

8.1. Infection Vector

The initial infection occurred when user `klee` opened an email attachment named `Invoice_Q4_2024.docm`. The email appeared to come from a legitimate supplier, suggesting possible supply chain compromise or email thread hijacking.

8.1.1. Malware Behavior

Upon macro execution:

1. PowerShell script downloaded Emotet loader from `hxxp://45.XX.XX.XX/wp-content/update.exe`
2. Loader established persistence via scheduled task: `WindowsUpdateCheck`
3. Emotet harvested credentials from browsers and email clients
4. Attempted lateral movement via SMB using harvested credentials

8.1.2. Indicators of Compromise

Network IOCs:

- C2 servers: `45.XX.XX.XX:443`, `91.XX.XX.XX:8080`, `185.XX.XX.XX:443`
- User-Agent: `Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0)`

Host IOCs:

- File hash (SHA256): `a1b2c3d4e5f6...` (Emotet loader)
- Registry: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WindowsUpdate`
- Scheduled Task: `WindowsUpdateCheck`

8.1.3. Infected Systems

Hostname	User	Infection Time	Lateral Movement Attempted
WS-FIN-001	klee	09:15 UTC	Yes
WS-FIN-002	jpark	09:32 UTC	No
WS-HR-003	msmith	09:45 UTC	Yes
...	...	...	...

Image 7

Image 4

Evidence macro: **Dell OptiPlex 7090 #322** (Workstation #240dcd54)

9. Conclusions and Recommendations

9.1. Conclusions

The investigation findings support the following conclusions based on the evidence analyzed.

9.2. Recommendations

Recommendations
Disable macros in Office documents from internet sources
Implement application whitelisting on workstations
Deploy network segmentation for finance department
Block PowerShell for standard users
Enable Microsoft ASR rules for Office applications

10. Timeline

26/01/2026, 19.05.08	**Case (Emotet Malware Outbreak via Malicious Macro) created** Case opened: Emotet Malware Outbreak via Malicious Macro Emotet banking trojan infection spreading through internal network via malicious Word document.
27/01/2026, 11.05.08	**Stakeholder update** Status update provided to management
27/01/2026, 15.05.08	**Investigation milestone** Key finding documented during analysis
28/01/2026, 5.05.08	**Stakeholder update** Status update provided to management
28/01/2026, 22.05.08	**Stakeholder update** Status update provided to management
29/01/2026, 19.05.11	**Stakeholder update** Status update provided to management
30/01/2026, 0.05.08	**Investigation milestone** Key finding documented during analysis
31/01/2026, 19.05.09	**Phase: Containment** Incident phase changed from Preparation & First Actions to Containment
31/01/2026, 19.11.39	**Case open** Case reopened. Status changed from CLOSED to OPEN.
31/01/2026, 19.12.19	**File added to case: beautiful-sunset-sea-coast-scenery-digital-art-4k-wallpaper-uhdpaper.com-781@0@i.jpg** Filename: beautiful-sunset-sea-coast-scenery-digital-art-4k-wallpaper-uhdpaper.com-781@0@i.jpg, Size: 1712377 bytes
31/01/2026, 19.12.20	**File added to case: car-road-forest-sunset-mountain-scenery-4k-wallpaper-uhdpaper.com-878@1@m.jpg** Filename: car-road-forest-sunset-mountain-scenery-4k-wallpaper-uhdpaper.com-878@1@m.jpg, Size: 2023040 bytes

31/01/2026, 19.12.22

File added to case: colorful-abstract-background-digital-art-4k-wallpaper-uhdpaper.com-724@1@l.jpg

Filename: colorful-abstract-background-digital-art-4k-wallpaper-uhdpaper.com-724@1@l.jpg, Size: 1820749 bytes

31/01/2026, 19.12.23

File added to case: colorful-abstract-circle-26-4k.jpg

Filename: colorful-abstract-circle-26-4k.jpg, Size: 1074242 bytes

31/01/2026, 19.12.25

File added to case: colorful-abstract-wave-27-4k.jpg

Filename: colorful-abstract-wave-27-4k.jpg, Size: 1143860 bytes

31/01/2026, 19.12.56

File added to case: Antigravity.exe

Filename: Antigravity.exe, Size: 159603760 bytes

11. Evidence Inventory

ID	ITEM DESCRIPTION	LOCATION
1	**Mobile Phone: Samsung Galaxy S24 #149**	Remote - Cloud
2	**Mobile Phone: Samsung Galaxy S24 #617**	Evidence Locker B
3	**Tablet: Evidence item #489**	IT Storage Room A
4	↳ Paper Documents: Evidence item #310	Remote - Cloud
5	**Workstation: Dell OptiPlex 7090 #082**	Remote - Cloud
6	**Workstation: Dell OptiPlex 7090 #322**	Evidence Locker B
7	↳ Network Capture (PCAP): Full packet capture #115	Forensic Lab
8	**Workstation: Lenovo ThinkStation P340 #082**	On-site Server Room

12. Detailed Item Reports

1 Mobile Phone: Samsung Galaxy S24 #149

UUID: 21648DEA-8A3C-4EAD-A7D8-AD19BB920089

ITEM DETAILS

Type	Mobile Phone	**Location**	Remote - Cloud
Legal Owner	[TEST] SOC Team Alpha	**Primary User**	[TEST] David Davis
Imei	745902714646195	**Make**	HP
Model	Model-986	**Faraday Bag**	true
Sim Present	true		

2 Mobile Phone: Samsung Galaxy S24 #617

UUID: 8F486577-BDF7-4A48-9FE4-E9451D42D3A0

ITEM DETAILS

Type	Mobile Phone	**Location**	Evidence Locker B
Legal Owner	[TEST] European Data Protection Board	**Primary User**	[TEST] Chloe Campbell
Imei	360807924808316	**Make**	Samsung
Model	Model-745	**Faraday Bag**	false
Sim Present	true		

TRIAGE FLAGS: Illegal content | Malware | Return

INVESTIGATOR NOTES

Ella Moore — 31/01/2026, 19.05.11

Initial analysis shows signs of unauthorized access. Further review needed.

Charlotte Williams — 31/01/2026, 19.05.11

Initial analysis shows signs of unauthorized access. Further review needed.

Charlotte Hernandez — 31/01/2026, 19.05.11

Initial analysis shows signs of unauthorized access. Further review needed.

3 Tablet: Evidence item #489

UUID: 14A12CF4-2835-4B04-A27C-FA436588DBE4

ITEM DETAILS

Type	Tablet	**Location**	IT Storage Room A
Legal Owner	[TEST] Chloe Campbell	**Primary User**	[TEST] Riley Brown
Imei	609353241231606	**Make**	Samsung
Model	Model-181	**Faraday Bag**	false
Sim Present	true		

TRIAGE FLAGS: No evidence

Contains Components:

↳ Paper Documents: Evidence item #310

4 Paper Documents: Evidence item #310

UUID: 59AEBDC4-AF83-410E-9712-790D97430DD1

ITEM DETAILS

Type	Paper Documents	**Location**	Remote - Cloud
Legal Owner	[TEST] TechVentures Ltd	**Primary User**	[TEST] Incident Response Unit
Page Count	598		

TRIAGE FLAGS: Return

↗ **Parent Device:** Tablet: Evidence item #489

INVESTIGATOR NOTES

Benjamin Taylor 31/01/2026, 19.05.09

Memory analysis completed. No evidence of code injection found.

5 Workstation: Dell OptiPlex 7090 #082

UUID: C96CABDE-5005-4A28-9273-7EC635C6F1CF

ITEM DETAILS

Type	Workstation	**Location**	Remote - Cloud
Legal Owner	[TEST] Anthony Campbell	**Primary User**	[TEST] Aurora King
Make	Samsung	**Model**	Model-800
Hostname	WS-DEV-74	**Mac Address**	c6:9e:b6:21:2e:87
Is Encrypted	true	**Serial Number**	002850340533584

INVESTIGATOR NOTES

Isabella Adams — 31/01/2026, 19.05.09

Malware samples extracted and submitted to sandbox for analysis.

Charlotte Williams — 31/01/2026, 19.05.09

Network connections logged during live acquisition.

6 Workstation: Dell OptiPlex 7090 #322

UUID: 240DCD54-CA3A-4D04-84B6-807BAA2436C4

ITEM DETAILS

Type	Workstation	**Location**	Evidence Locker B
Legal Owner	[TEST] Global Finance Group	**Primary User**	[TEST] TechVentures Ltd
Make	Apple	**Model**	Model-257
Hostname	WS-FIN-33	**Mac Address**	6c:f0:aa:55:a3:22
Is Encrypted	false	**Serial Number**	146714740436032

Contains Components:

↳ Network Capture (PCAP): Full packet capture #115

INVESTIGATOR NOTES

Avery Walker — 31/01/2026, 19.05.10

Memory analysis completed. No evidence of code injection found.

Isabella Adams — 31/01/2026, 19.05.10

Memory analysis completed. No evidence of code injection found.

7 Network Capture (PCAP): Full packet capture #115

UUID: 80D0CE37-F99A-419C-8F80-E9B0C6B30BCE

ITEM DETAILS

Type	Network Capture (PCAP)	**Location**	Forensic Lab
Legal Owner	Unknown	**Primary User**	[TEST] Anthony Campbell
Source	Value for source	**Endpoints Count**	512
Contains Encrypted	true		

↗ **Parent Device:** Workstation: Dell OptiPlex 7090 #322

8 Workstation: Lenovo ThinkStation P340 #082

UUID: 2C7192C0-5522-4663-BF7B-F9FA81648CA8

ITEM DETAILS

Type	Workstation	**Location**	On-site Server Room
Legal Owner	[TEST] Aurora Adams	**Primary User**	[TEST] RetailMax Inc
Make	HP	**Model**	Model-700
Hostname	WS-DEV-44	**Mac Address**	40:b6:01:e9:4a:fe
Is Encrypted	true	**Serial Number**	664981156086334

INVESTIGATOR NOTES

Isabella Adams — **31/01/2026, 19.05.09**

Memory analysis completed. No evidence of code injection found.

13. Glossary of Terms

Term	Explanation
Credential Stuffing	Automated attack using leaked username/password combinations against login pages
DMARC	Domain-based Message Authentication, Reporting & Conformance - email authentication protocol
Forensic Image	Bit-for-bit copy of a storage device for analysis
Hash	Fixed-size output from a cryptographic function used to verify data integrity
MFA	Multi-Factor Authentication - requiring multiple verification methods
Phishing	Social engineering attack using fraudulent communications to obtain sensitive information
Ransomware	Malware that encrypts files and demands payment for decryption
SIEM	Security Information and Event Management - centralized logging and alerting platform
SQL Injection	Attack inserting malicious SQL code into application queries
WAF	Web Application Firewall - security solution protecting web applications