

INCIDENT EVIDENCE PACK

Business Email Compromise & Ransomware Containment — Finance

Finance department — Microsoft 365 account compromise with a blocked ransomware deployment

Prepared for **Contoso Manufacturing** · by Dana Okafor

REFERENCE INC-386D924B	STATUS ● Resolved	SEVERITY High severity
DETECTED 12 May 2026, 02:14 UTC	CLOSED 14 May 2026, 16:00 UTC	NIS2 Reportable
PREPARED BY Dana Okafor	ORGANIZATION Contoso Manufacturing	GENERATED 14 May 2026

1 AFFECTED USERS	7 EVIDENCE ITEMS	10 TIMELINE EVENTS	4 AUDIT RECORDS
---------------------	---------------------	-----------------------	--------------------

IN THIS PACK

01 Executive summary

03 Response timeline

05 Evidence index

07 Root cause & lessons learned

09 Sign-off

02 Incident details

04 Response actions

06 NIS2 milestone status

08 Audit activity

01 Executive summary

CLIENT-READY

A finance user's Microsoft 365 account was compromised via a business email compromise (BEC) phishing lure. The threat actor created a hidden inbox-forwarding rule and attempted to deploy ransomware on a production file server. Detection, containment, eradication, and recovery were completed the same day with no data loss.

IMPACT

Estimated 1 affected user(s). 7 evidence artifact(s) collected with full chain-of-custody.

02 Incident details

TITLE	Business Email Compromise & Ransomware Containment — Finance	REFERENCE	INC-386D924B
STATUS	Resolved	SEVERITY	High
DETECTED	12 May 2026, 02:14 UTC	CLOSED	14 May 2026, 16:00 UTC
REPORTED BY	Dana Okafor	ORGANIZATION	Contoso Manufacturing

03 Response timeline

10 EVENTS

12 May · 02:14	Anomalous sign-in from foreign geography Impossible-travel sign-in for finance user jordan.mercer from 45.148.10.77 (Sofia, BG) using legacy auth, bypassing MFA. Risk level: High. Microsoft Entra ID Protection	Event
12 May · 05:41	Endpoint ransomware attempt blocked on FS-PROD-01 Detection EDR-2026-4471: svc-bkp.exe attempted mass file encryption (T1486). Process killed and quarantined automatically. SentinelOne EDR	Event
12 May · 06:10	Incident declared — SOC engaged Northwind SOC declared a High-severity incident and opened a bridge with Contoso IT. Client stakeholders notified. Dana Okafor (SOC Lead)	Note
12 May · 06:32	Compromised account disabled & sessions revoked Disabled jordan.mercer, revoked all refresh tokens, reset credentials, and enforced MFA re-registration. Priya Nair (Analyst)	Containment
12 May · 06:48	Malicious inbox forwarding rule removed Hidden rule "...\" forwarding invoices to an external address was deleted; mailbox audit re-enabled. Priya Nair (Analyst)	Containment
12 May · 07:05	C2 and phishing infrastructure blocked at perimeter Firewall and secure web gateway rules added for 193.42.33.104 and secure-invoice-review[.]com. Contoso Network Team	Containment
12 May · 09:20	Legacy authentication disabled tenant-wide Conditional Access policy blocking legacy auth protocols rolled out to all users; loader binary hash added to EDR blocklist. Dana Okafor (SOC Lead)	Eradication
12 May · 13:40	FS-PROD-01 validated and returned to service No files were encrypted (EDR blocked pre-execution). Host reimaged as precaution and integrity-verified against backup manifest. Contoso IT Ops	Recovery

13 May · 10:00	Finance user restored with hardened access Recovery jordan.mercer re-enabled after credential reset, phishing-resistant MFA enrollment, and mailbox review. Priya Nair (Analyst)
14 May · 16:00	Client debrief delivered & incident closed Note Executive summary and evidence pack delivered to Contoso leadership. Incident formally closed with agreed follow-up actions. Dana Okafor (SOC Lead)

04 Response actions

CONTAINMENT 12 May · 06:32 — Compromised account disabled & sessions revoked 12 May · 06:48 — Malicious inbox forwarding rule removed 12 May · 07:05 — C2 and phishing infrastructure blocked at perimeter	ERADICATION 12 May · 09:20 — Legacy authentication disabled tenant-wide	RECOVERY 12 May · 13:40 — FS-PROD-01 validated and returned to service 13 May · 10:00 — Finance user restored with hardened access
---	--	---

05 Evidence index7 ARTIFACTS

#	FILE	TYPE	SIZE	UPLOADED	BY
1	chain-of-custody.pdf	PDF	193 B	14 May 2026	Dana Okafor
2	containment-firewall-block.png	IMG	70 B	14 May 2026	Dana Okafor
3	phishing-email-headers.txt	TXT	139 B	14 May 2026	Dana Okafor
4	indicators-of-compromise.csv	CSV	152 B	14 May 2026	Dana Okafor
5	edr-detection-fs-prod-01.json	JSON	108 B	14 May 2026	Dana Okafor
6	inbox-rule-hidden-forward.png	IMG	70 B	14 May 2026	Dana Okafor
7	m365-signin-log-finance.csv	CSV	193 B	14 May 2026	Dana Okafor

06 NIS2 milestone status

✓ Early warning Early warning submitted to the competent authority within 24 hours. No cross-border impact identified. Deadline 24 hours Met on time
✓ Incident notification Full notification submitted within 72 hours with confirmed impact assessment and remediation status. Deadline 72 hours Met on time
✓ Final report Final report delivered with root-cause analysis, remediation evidence, and preventative recommendations. Deadline 1 month Met on time

07 Root cause & lessons learned

ROOT CAUSE

A finance user was targeted by a business email compromise phishing campaign impersonating a supplier’s accounts-payable team. The attacker replayed captured credentials over a legacy authentication protocol not covered by the tenant’s MFA policy, then created a hidden inbox-forwarding rule and attempted lateral movement to a production file server where an endpoint ransomware payload was blocked pre-execution.

LESSONS LEARNED

MFA coverage gaps on legacy authentication were the decisive weakness; blocking legacy auth tenant-wide closes this path. Automated EDR containment prevented data loss. Faster supplier-change verification and phishing-resistant MFA for finance roles would have prevented initial access.

08 Audit activity

4 RECORDS

TIMESTAMP (UTC)	ACTION	ACTOR
14 May 2026, 20:40 UTC	INCIDENT_UPDATED	Dana Okafor
14 May 2026, 20:40 UTC	NIS2_ENABLED	Dana Okafor
14 May 2026, 20:40 UTC	INCIDENT_UPDATED	Dana Okafor
14 May 2026, 20:40 UTC	INCIDENT_CREATED	Dana Okafor

09 Sign-off

INCIDENT LEAD

Dana Okafor

Signature & date

REVIEWED / APPROVED

Signature & date