DIGITAL FORENSICS & INCIDENT RESPONSE

INCIDENT INVESTIGATION REPORT

CONTOSO CORPORATION

Security Breach - 03 February 2026

Classification:	**CONFIDENTIAL**
Incident Date:	03 February 2026
Report Date:	16 February 2026
Lead Analyst:	DFIR Team

1. Executive Summary

A sophisticated, multi-stage cyber attack was identified across the CONTOSO domain on 03 February 2026, spanning approximately 3 hours and 29 minutes (08:00 – 11:29 UTC). Two primary threat actors — operating under compromised accounts CONTOSO\jennifer.hayes (WORKSTATION-25) and CONTOSO\sarah.mitchell (WORKSTATION-01) — conducted a coordinated campaign that progressed through credential theft, discovery, lateral movement, data staging, exfiltration, and ransomware deployment.

The attack resulted in the confirmed exfiltration of approximately 245 MB of highly sensitive intellectual property including M&A due diligence documents, board papers, R&D roadmaps, patent applications, and IT infrastructure documentation. Ransomware (svcupdate.exe) was subsequently deployed against D:\Shares\CompanyData on FILESERVER01, encrypting and deleting originals across multiple sensitive directories. CrowdStrike Falcon EDR was surgically disabled on WORKSTATION-01 through a Safe Mode boot bypass chain, leaving the endpoint fully unprotected prior to lateral movement.

Impact Assessment

Compromised Credentials	sarah.mitchell, jennifer.hayes (Domain Admin), backup.service
EDR Status	Completely removed via Safe Mode bypass
Data Exfiltration	245 MB (M&A documents, financial records, customer data, intellectual property)
Ransomware	1,247 files encrypted on FILESERVER01 (4.8 GB total)

Critical Findings

The attack succeeded despite operational EDR due to a sophisticated bypass technique:

- Windows Credential Guard: NOT ENABLED - allowed plaintext credential access
- LSASS Protected Process Light (PPL): NOT ENABLED - allowed memory dumping
- CrowdStrike Tamper Protection: ACTIVE - successfully blocked direct service termination
- Safe Mode Bypass: Attacker used bcdedit to boot into Safe Mode, where EDR drivers do not load
- EDR Kernel Driver: Cannot load in Safe Mode - complete security control bypass

This was not an EDR failure. This was a sophisticated adversary exploiting a legitimate Windows feature (Safe Mode) to bypass security controls.

2. Attack Overview

Phase	Time (UTC)	Actor / System	Key Activity
Initial Access	08:00 – 08:03	jennifer.hayes / WORKSTATION-25	Account active; multiple DC logons observed
Discovery	08:03 – 08:54	jennifer.hayes / DC01	AD object enumeration: user attributes, group membership

Phase	Time (UTC)	Actor / System	Key Activity
Credential Access	08:09 – 10:48	Multiple hosts	lsass.exe spawned from explorer.exe (WORKSTATION-05/11/16/18)
Lateral Movement	08:54 – 09:00	jennifer.hayes → FILESERVER01	PowerShell Remoting (WinRM) → SMB from WORKSTATION-02 to FILESERVER01 with elevated token
Initial Access (2nd actor)	10:47 – 10:48	sarah.mitchell / WORKSTATION-01	Outlook spawns encoded PowerShell; Mimikatz downloaded from 185.220.101.42
CrowdStrike EDR Disabled	10:49 – 10:52	sarah.mitchell / WORKSTATION-01	Stop blocked by tamper; Safe Mode bypass; kernel driver + service binary deleted; self-cleanup
Privilege Escalation	10:52	sarah.mitchell / WORKSTATION-01	EDR-free environment used for lateral move to 10.50.10.22 via harvested credentials
Collection (Round 1)	09:09 – 09:12	jennifer.hayes / FILESERVER01	Copy-Item staging: Board, M&A, R&D, IT directories → C:\Windows\Temp\backup
Exfiltration (Round 1)	09:18	jennifer.hayes / FILESERVER01	156 MB uploaded to 185.220.101.42 via HTTP POST; staging deleted
Ransomware Deploy	09:21 – 09:27	jennifer.hayes / FILESERVER01	svcupdate.exe encrypts files; README_DECRYPT.txt dropped
Persistence / Priv-Esc	11:08 – 11:12	jennifer.hayes / DC01	DCSync attack; BackupAdmin account created; added to Domain Admins
Collection (Round 2)	11:20 – 11:28	jennifer.hayes / FILESERVER01	Second staging and archive (data.zip 156 MB + exfil2.zip 89 MB)
Exfiltration (Round 2)	11:21 – 11:28	jennifer.hayes / FILESERVER01	Total 245 MB exfiltrated to 185.220.101.42
Ransomware Deploy (2)	11:27	jennifer.hayes / FILESERVER01	Second svcupdate.exe wave encrypts remaining share files
Cleanup	11:28 – 11:29	jennifer.hayes / FILESERVER01	Archives deleted; staging directories removed to cover tracks

3. Detailed Attack Timeline

3.1 Initial Access & Reconnaissance (08:00 – 08:54 UTC)

Jennifer Hayes' account was active from the start of the log window, authenticating to DC01 from multiple source IPs (10.50.10.15, 10.50.10.42, 10.50.10.72) in rapid succession — characteristic of credential reuse or pass-the-hash across sessions. At 08:24 and 08:30, the account accessed CN=david.palmer and CN=brian.turner objects on DC01 reading all user attributes (Event 4662) — consistent with LDAP-based user enumeration (T1087.002). 7-Zip (7zFM.exe) was launched at 08:48 from WORKSTATION-25, foreshadowing the collection phase.

3.2 Credential Access — LSASS Targeting (08:09 – 10:48 UTC)

Across multiple workstations, lsass.exe was spawned with explorer.exe as the parent process — a strong anomaly indicator, as lsass.exe is exclusively started by wininit.exe under normal Windows operation. This pattern indicates process injection or credential dumping tooling masquerading as legitimate processes.

Timestamp	System	Indicator
08:09:49	WORKSTATION-11	lsass.exe spawned from explorer.exe — anomalous parent
08:51:45	WORKSTATION-18	lsass.exe spawned from explorer.exe — anomalous parent
08:57:35	WORKSTATION-05	lsass.exe spawned from explorer.exe — Sysmon Event 1 confirmed
09:00:09	WORKSTATION-16	lsass.exe spawned from explorer.exe — anomalous parent
10:04:16	WORKSTATION-01	lsass.exe spawned from explorer.exe — anomalous parent
10:42:32	WORKSTATION-01	Sysmon Event 8 (CreateRemoteThread into lsass.exe) confirmed injection

At 10:47 on WORKSTATION-01, sarah.mitchell downloaded mimikatz.exe from 185.220.101.42 and masqueraded it as svchost.exe (T1036.004). Executed at 10:48:12 with sekurlsa::logonpasswords, LSASS memory was dumped confirming successful credential harvesting. CrowdStrike Falcon detected the tamper attempt and blocked service termination — triggering the EDR bypass chain documented in section 3.4.

3.3 Lateral Movement — jennifer.hayes to FILESERVER01 (09:00 UTC)

At 09:00:32, FILESERVER01 logged creation of wsmprovhost.exe with full token elevation, confirming an incoming WinRM/PowerShell Remoting session. A Logon Type 3 (Network) with Elevated Token: Yes from 10.50.10.22 at 09:00:35 was corroborated by Sysmon Event 3 on WORKSTATION-02 showing powershell.exe initiating the connection on port 52891 to FILESERVER01:445. Jennifer Hayes immediately enumerated SMB shares via Get-SmbShare and proceeded to access sensitive files.

3.4 CrowdStrike EDR Disable — Full Kill Chain (10:49 – 10:52 UTC)

This is the most forensically significant defensive evasion sequence in the incident. Sarah Mitchell executed a precise, multi-stage technique to completely remove CrowdStrike Falcon from WORKSTATION-01 — progressing through tamper protection bypass via Safe Mode boot manipulation to full kernel-level EDR destruction. The sequence is documented in full below.

Step 1 — Reconnaissance of Security Products (10:49:05 – 10:49:10)

Sarah Mitchell first profiled the endpoint's security stack using PowerShell:

```
Get-Service -Name "CSFalcon*"  → CrowdStrike Falcon Sensor | Status: Running | StartType: Automatic
Get-CimInstance Win32_SystemDriver -Name "CSAgent"  → State: Running | Driver loaded in kernel
Get-Process -Name "*crowd*,*carbon*,*defender*,*sentinel*"  → CSFalconService (PID:1844), CSFalconContainer (PID:2156)
```

Step 2 — Direct Stop Attempt Blocked by Tamper Protection (10:49:20)

Stop-Service -Name CSFalconService was attempted and returned Access Denied. CrowdStrike's tamper protection fired an Application Event ID 1000 alert (Technique: T1562.001 | Severity: CRITICAL | Action: Blocked). A second service stop attempt was blocked at 10:50:19 (Application Event 7036), confirming tamper protection was functioning correctly and the attacker could not terminate the EDR through conventional means.

Step 3 — edr_killer.exe Downloaded & Safe Mode Boot Configured (10:49:35 – 10:49:48)

Unable to stop the service directly, the attacker pivoted to a Safe Mode bypass technique:

- 10:49:35 — Invoke-WebRequest downloaded edr_killer.exe (856 KB) from 185.220.101.42, saved as C:\Windows\Temp\winupdate.exe (masquerading as a Windows update binary)

- 10:49:42 — bcdedit /set {current} safeboot network executed via Invoke-Expression with elevation, configuring the system to boot into Safe Mode with Networking. CrowdStrike issued a second EDR Alert (Event 1000): Boot Configuration Modification | T1562.009 | Action: Logged (cannot block bcdedit)
- 10:49:48 — New-ItemProperty created registry persistence key: HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\WinUpdate → C:\Windows\Temp\winupdate.exe — ensuring the EDR killer would auto-execute as SYSTEM at Safe Mode boot before any interactive logon
- 10:49:53 — Restart-Computer -Force -Timeout 5 forced an immediate reboot

Step 4 — Safe Mode Execution as SYSTEM: EDR Surgically Destroyed (10:51:06 – 10:51:51)

System Event ID 12 at 10:51:06 confirmed: "The operating system started in Safe Mode with Networking — EDR drivers NOT loaded (kernel drivers disabled in Safe Mode)." CrowdStrike's kernel driver CSAgent.sys cannot load in Safe Mode, rendering tamper protection inactive.

winupdate.exe then executed as SYSTEM (parent: wininit.exe, IntegrityLevel: System) and performed a complete surgical removal:

Time	Event ID / Source	Action
10:51:15	Sysmon Event 1	winupdate.exe spawned as SYSTEM from wininit.exe in Safe Mode
10:51:20	Security Event 4688	winupdate.exe created as SYSTEM — Safe Mode, EDR driver not loaded
10:51:22	Sysmon Event 23 (File Delete)	CSAgent.sys (kernel driver) deleted from C:\Windows\System32\drivers\
10:51:23	Sysmon Event 23 (File Delete)	CSFalconContainer.exe deleted from C:\Program Files\CrowdStrike\
10:51:26	PowerShell Module Log	Remove-Item C:\Program Files\CrowdStrike -Recurse -Force — entire EDR directory wiped
10:51:22	System Event 7045	CSFalconService registered as DELETED — service removed from system
10:51:29	Sysmon Event 1	bcdedit /deletevalue {current} safeboot — Safe Mode flag removed for clean reboot
10:51:36	Sysmon Event 23 (File Delete)	winupdate.exe self-deleted to remove evidence of EDR killer
10:51:39	Sysmon Event 12 (Registry Delete)	HKLM\...\SafeBoot\Network\WinUpdate registry key deleted — removing Safe Mode persistence entry
10:51:41	Security Event 1074	Forced reboot back to Normal Mode via winlogon.exe
10:51:51	Sysmon Event 23 (File Delete)	CSFalconService.exe service binary deleted

Step 5 — EDR Removal Confirmed; Normal Boot Resumed (10:52:02)

System Event ID 12 at 10:52:02 recorded: "Boot Mode: Normal | EDR Status: NOT PRESENT — CrowdStrike removed | System vulnerable to attack." Sarah Mitchell's logon at 10:52:02 was recorded with a note: "Safe Mode: False | Normal boot — EDR disabled."

Verification at 10:52:40: Get-Service -Name "CSFalcon*" returned ERROR: Cannot find service — EDR successfully removed. System Event 7000 confirmed at 10:52:56: CSFalconService failed to start — The system cannot find the file specified.

From this point forward, WORKSTATION-01 operated with no endpoint detection capability for the remainder of the incident.

3.5 Discovery & File Share Enumeration (09:03 – 09:06 UTC)

Within minutes of gaining access to FILESERVER01, jennifer.hayes conducted systematic reconnaissance via PowerShell Remoting: Get-SmbShare to enumerate all shares, followed by Get-ChildItem -Recurse across Board, MergersAcquisitions (filtering *.docx,*.xlsx,*.pdf), ResearchDevelopment, and IT_Architecture directories. High-value documents were accessed via Event 4663 (READ_DATA) including M&A due diligence reports, board strategy papers, patent applications, product roadmaps, AD design documents, and firewall ACL exports.

3.6 Data Staging & Exfiltration (09:09 – 09:18 UTC)

Jennifer Hayes created C:\Windows\Temp\backup and used Copy-Item to stage Board papers, M&A files (Acquisition_Target_Analysis_TechCorp.xlsx 2.4 MB; Due_Diligence_Report_CONFIDENTIAL.pdf 5.8 MB), R&D files (Product_Roadmap_2026-2027_SECRET.xlsx 1.2 MB), and IT Architecture documentation (Network_Topology_Diagram_2026.vsdx 4.2 MB). At 09:18:06, PowerShell Script Block logging confirmed: Upload complete: 156 MB transferred | HTTP 200 OK. The staging directory was immediately destroyed with Remove-Item -Recurse -Force.

3.7 Ransomware Deployment (09:21 – 09:27 UTC and 11:27 UTC)

svcupdate.exe (1.2 MB) was dropped to C:\Windows\Temp\ and executed with --path D:\Shares\CompanyData --encrypt. The ransomware encrypted files (Sysmon Event 11: .encrypted extension created), timestomped encrypted files (Sysmon Event 2), deleted originals (Sysmon Event 23), and dropped README_DECRYPT.txt. The binary self-deleted at 09:27:20. A second ransomware wave was launched at 11:27 targeting remaining plaintext files across all share directories.

3.8 DCSync & Domain Persistence (11:08 – 11:12 UTC)

DC01 logged a Replication Synchronization request (Event Category: DCSync_Attack) originating from 10.50.10.22 at 11:08:45, followed by Event 4662 reads against the krbtgt account, Domain Admins membership, and multiple high-value user objects. This confirms a DCSync attack (T1003.006) providing the attacker with password hashes for all accounts including krbtgt — enabling Golden Ticket creation. Jennifer Hayes subsequently created BackupAdmin, adding it to both the local Administrators group and Domain Admins at 11:12.

4. MITRE ATT&CK Technique Mapping

Tactic	Technique	ID	Evidence
Initial Access	Spearphishing Attachment	T1566.001	OUTLOOK.EXE spawning hidden PowerShell with encoded command
Execution	PowerShell	T1059.001	Encoded & obfuscated PS1 execution; Invoke-Expression char array obfuscation
Execution	Windows Management Instrumentation	T1047	Invoke-Command / WMI to lateral host 10.50.10.22

Tactic	Technique	ID	Evidence
Persistence	Create Account	T1136.001	BackupAdmin account created by jennifer.hayes on DC01
Persistence	Account Manipulation	T1098	BackupAdmin added to Domain Admins
Privilege Escalation	Valid Accounts: Domain Accounts	T1078.002	jennifer.hayes / sarah.mitchell compromised credentials
Defense Evasion	Masquerading	T1036.004	mimikatz.exe renamed svchost.exe; edr_killer.exe renamed winupdate.exe
Defense Evasion	Safe Mode Boot	T1562.009	bcdedit safeboot + SafeBoot\Network registry persistence to bypass EDR kernel driver
Defense Evasion	Disable/Modify Tools	T1562.001	CSFalconService terminated; CSAgent.sys kernel driver deleted; CrowdStrike directory wiped
Defense Evasion	Timestomp	T1070.006	svcupdate.exe changed encrypted file creation times (Sysmon Event 2)
Defense Evasion	File Deletion	T1070.004	Staging dirs, archives, tooling (winupdate.exe, svcupdate.exe) deleted post-operation
Defense Evasion	Indicator Removal on Host	T1070.001	SafeBoot registry key deleted; bcdedit /deletevalue to restore normal boot and hide evidence
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001	svchost.exe (Mimikatz) sekurlsa::logonpasswords; CreateRemoteThread to lsass (Sysmon Event 8)
Credential Access	OS Credential Dumping: DCSync	T1003.006	Replication Synchronization against DC01 from 10.50.10.22 — krbtgt hash obtained
Discovery	Account Discovery: Domain Account	T1087.002	LDAP reads against multiple CN user objects in DC01 (Event 4662)
Discovery	File and Directory Discovery	T1083	Get-ChildItem -Recurse across Board, M&A, R&D, IT shares
Discovery	Network Share Discovery	T1135	Get-SmbShare on FILESERVER01; Event 5140 share access
Discovery	Security Software Discovery	T1518.001	Get-Service CSFalcon*; Get-Process *crowd*,*carbon*,*defender*,*sentinel*; Get-CimInstance CSAgent
Lateral Movement	Remote Services: Windows Remote Management	T1021.006	wsmprovhost.exe elevated session; PowerShell Remoting to FILESERVER01
Lateral Movement	Remote Services: SMB/Windows Admin Shares	T1021.002	admin$ share access; payload copy to \\10.50.10.22\C$
Collection	Data from Network Shared Drive	T1039	Copy-Item across Board, M&A, R&D, IT share directories
Collection	Archive Collected Data	T1560.001	Compress-Archive to data.zip (156 MB) and exfil2.zip (89 MB)

Tactic	Technique	ID	Evidence
Exfiltration	Exfiltration Over C2 Channel	T1041	HTTP POST to 185.220.101.42:80 — 245 MB total across two sessions
Impact	Data Encrypted for Impact	T1486	svcupdate.exe encrypts D:\Shares\CompanyData — ransomware (two waves)
Impact	Inhibit System Recovery	T1490	Safe Mode bypass kills EDR; CSAgent.sys deleted disables recovery

5. Indicators of Compromise

5.1 Network IOCs

Indicator	Type	Context
185.220.101.42	IP Address	C2 & exfiltration server (Tor exit node); HTTP:80, nginx/1.18.0
http://185.220.101.42/tools/mimikatz.exe	URL	Mimikatz download location
http://185.220.101.42/tools/edr_killer.exe	URL	EDR removal tool download
http://185.220.101.42/upload	URL	Exfiltration endpoint (HTTP POST)
http://10.50.10.15.200/payload.ps1	Internal URL	Stage-2 payload delivery from potentially compromised internal host
10.50.10.22	Internal IP	Lateral movement target; DCSync source; WindowsUpdateService implant installed

5.2 File & Process IOCs

Indicator	Path	Context
svcupdate.exe	C:\Windows\Temp\svcupdate.exe	Ransomware binary (1.2 MB, SHA256: a1b2c3d4e5f6789...)
svchost.exe (Mimikatz)	C:\Users\sarah.mitchell\AppData\Local\Temp\svchost.exe	Mimikatz masquerading as svchost.exe
winupdate.exe	C:\Windows\Temp\winupdate.exe	edr_killer.exe renamed (856 KB, SHA256: d4e5f6a7b8c9...) — executed as SYSTEM in Safe Mode
payload.exe	C:\Users\sarah.mitchell\AppData\Local\Temp\payload.exe	Second stage implant deployed post-EDR removal
update.exe	\\10.50.10.22\C$\Windows\Temp\update.exe	Lateral payload installed as WindowsUpdateService

Indicator	Path	Context
README_DECRYPT.txt	D:\Shares\CompanyData\README_DECRYPT.txt	Ransom note dropped by svcupdate.exe
*.encrypted	D:\Shares\CompanyData**	Encrypted files — originals deleted post-encryption

5.3 Registry IOCs

Key	Value	Context
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\WinUpdate	C:\Windows\Temp\winupdate.exe	Safe Mode autorun persistence for EDR killer — key deleted post-execution

5.4 Account IOCs

Account	Activity	Status
CONTOSO\jennifer.hayes	Primary exfiltration, lateral movement, ransomware, DCSync, account creation	COMPROMISED — DISABLE IMMEDIATELY
CONTOSO\sarah.mitchell	Second actor; Outlook initial access, Mimikatz, EDR bypass, lateral movement	COMPROMISED — DISABLE IMMEDIATELY
BackupAdmin	Backdoor account created 11:12; added to Domain Admins and local Administrators	MALICIOUS — DELETE IMMEDIATELY
krbtgt	Hash extracted via DCSync — Golden Ticket risk for entire domain	RESET REQUIRED (x2, 48hr apart)

6. Immediate Containment Actions Required

- **CRITICAL:** Disable CONTOSO\jennifer.hayes and CONTOSO\sarah.mitchell domain accounts immediately
- **CRITICAL:** Delete BackupAdmin account and remove from all groups
- **CRITICAL:** Reset krbtgt password TWICE with 48-hour interval — invalidates all Kerberos tickets and Golden Tickets
- **CRITICAL:** Block 185.220.101.42 at perimeter firewall and proxy (all protocols)
- **HIGH:** Isolate FILESERVER01, WORKSTATION-01, WORKSTATION-02, WORKSTATION-25 from network
- **HIGH:** Isolate and forensically image 10.50.10.22 — WindowsUpdateService implant installed; DCSync sourced from this host
- **HIGH:** Rebuild WORKSTATION-01 — CrowdStrike fully removed at kernel level; payload.exe executed; trust cannot be restored
- **HIGH:** Rotate credentials for all accounts with logons to FILESERVER01 and DC01 during incident window

- **HIGH:** Conduct enterprise-wide LSASS dump hunt — all workstations where lsass.exe had anomalous parent processes
- **MEDIUM:** Audit all accounts recently added to Domain Admins, local Administrators, and backup operator groups
- **MEDIUM:** Preserve all affected system memory and disk images before remediation for legal evidence
- **MEDIUM:** Notify legal, compliance, and executive leadership — regulatory breach notification obligations apply

7. Exfiltrated Data Summary

Category	Files Confirmed Exfiltrated	Sensitivity
Board Papers	Board_Meeting_Agenda_Feb_2026.docx, Strategic_Plan_2026-2028_CONFIDENTIAL.pptx	BOARD CONFIDENTIAL
M&A — Project Phoenix	Acquisition_Target_Analysis_TechCorp.xlsx (2.4 MB), Due_Diligence_Report_CONFIDENTIAL.pdf (5.8 MB)	HIGHLY SENSITIVE
R&D / IP	Product_Roadmap_2026-2027_SECRET.xlsx (1.2 MB), Patent_Application_AI_Algorithm_2026.pdf (3.1 MB)	SECRET / IP
IT Architecture	Network_Topology_Diagram_2026.vsdx (4.2 MB), Active_Directory_Design_Document.docx (890 KB), Firewall_Rules_and_ACLs.xlsx (650 KB)	IT RESTRICTED
Total Exfiltrated	~245 MB across two HTTP POST sessions to 185.220.101.42	CRITICAL EXPOSURE

Report prepared by DFIR Team | 03 February 2026 | CONFIDENTIAL — Handle Accordingly