Ransomware Post-Mortem

Where the Kill Chain Could Have Been Broken

sales@briskinfosec.com

Initial Access :

How They Got In

Attackers gained entry through one of three common vectors - a phishing email with a malicious attachment, an exposed RDP port with weak credentials, or a vulnerable public-facing application.

MITRE ATTACK : T1566 (Phishing) · T1190 (Exploit Public-Facing Application) · T1078 (Valid Accounts)

Where It Could Have Been Broken:

- Email security gateway filtering malicious attachments
- MFA enforced on all remote access points
- Patch management closing known CVEs within defined SLA
- Regular VAPT identifying exposed services before attackers do

sales@briskinfosec.com

Execution and Persistence :

They Are In. Now They Stay.

Once inside, the attacker executed a malicious payload and established persistence mechanisms to survive reboots, credential resets, and basic incident response attempts.

MITRE ATTACK : T1059 (Command and Scripting Interpreter) · T1547 (Boot or Logon Autostart) · T1053 (Scheduled Task)

Where It Could Have Been Broken:

- Endpoint Detection and Response (EDR) flagging unusual script execution
- Application whitelisting preventing unauthorized executable launches
- Host-level security hardening removing unnecessary interpreters
- Scheduled task monitoring detecting persistence mechanisms early

sales@briskinfosec.com

Privilege Escalation :

User to Admin in Hours

Using local exploits, credential dumping tools like Mimikatz, or misconfigured service accounts, the attacker elevated privileges from a standard user to domain administrator level.

MITRE ATTACK : T1068 (Exploitation for Privilege Escalation) · T1003 (OS Credential Dumping) · T1078 (Valid Accounts)

Stage 3

Where It Could Have Been Broken:

- Privileged Access Management (PAM) limiting admin account exposure
- Credential dumping detection via EDR behavioral rules
- Regular access control reviews identifying over-permissioned accounts
- Least privilege enforcement across all service accounts

sales@briskinfosec.com

Lateral Movement :

Spreading Across Network

With elevated privileges, the attacker moved laterally across the network using legitimate tools - PsExec, WMI, RDP - to reach high-value systems, backup servers, and domain controllers.

MITRE ATTACK : T1021 (Remote Services) · T1570 (Lateral Tool Transfer) · T1018 (Remote System Discovery)

Where It Could Have Been Broken:

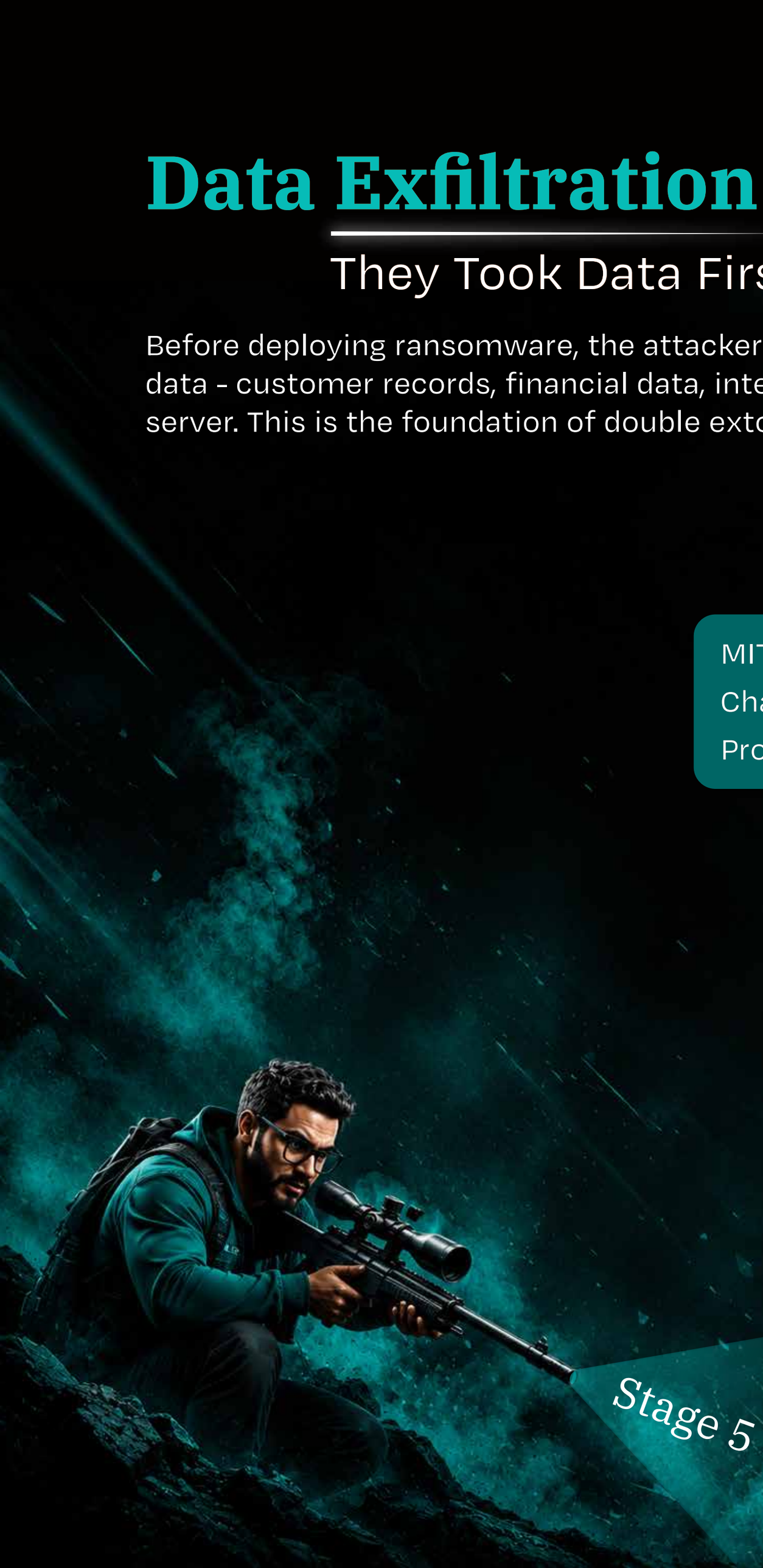
- Network segmentation containing the blast radius
- Zero Trust architecture requiring re-authentication between segments
- Lateral movement detection identifying unusual east-west traffic
- SOC monitoring flagging anomalous RDP and WMI activity

sales@briskinfosec.com

Data Exfiltration :

They Took Data First

Before deploying ransomware, the attacker staged and exfiltrated sensitive data - customer records, financial data, intellectual property - to an external server. This is the foundation of double extortion.



MITRE ATTACK : T1041 (Exfiltration Over C2 Channel) · T1048 (Exfiltration Over Alternative Protocol) · T1567 (Exfiltration to Cloud Storage)

Where It Could Have Been Broken:

- DNS filtering detecting communication with known malicious infrastructure
- DLP controls monitoring and blocking large outbound data transfers
- DSPM identifying where sensitive data lives before it can be staged
- Egress traffic monitoring alerting on anomalous outbound volumes

sales@briskinfosec.com

Ransomware Deployment :

The Moment Everything Stopped

After weeks of quiet preparation, the attacker deployed ransomware simultaneously across all reachable systems encrypting files, deleting shadow copies, disabling backup agents, and leaving a ransom note.

MITRE ATTACK : T1486 (Data Encrypted for Impact) · T1490 (Inhibit System Recovery) · T1489 (Service Stop)

Where It Could Have Been Broken:

- Immutable offline backups surviving encryption attempts
- Ransomware Readiness Assessment finding recovery gaps early
- EDR behavioral detection stopping encryption processes in real time
- Incident Response plan enabling immediate containment decisions

sales@briskinfosec.com

Every Stage Had a Moment Where It Could Have Been Stopped

Kill Chain Summary :

Stage	Attacker Action	Defensive Gap	What Would Have Stopped It
1	Initial Access	Unpatched exposure	VAPT, MFA, Email Security
2	Execution	No EDR	EDR, Application Whitelisting
3	Privilege Escalation	Over-permissioned accounts	PAM, Least Privilege
4	Lateral Movement	Flat network	Segmentation, ZT, SOC Monitoring
5	Exfiltration	No DLP	DLP, DSPM, DNS Filtering
6	Deployment	No immutable backup	Ransomware Readiness Assessment

sales@briskinfosec.com

Is Your Organization Ready for a

Ransomware Attack ?

Ransomware Readiness Assessment reveals gaps across the kill chain before attackers exploit them during an incident.

Book a Meeting

BriskInfosec™
VULNERABILITY TO VICTORY

sales@briskinfosec.com