FORENSIC EVIDENCE PACKET

Scenario 2: "The Long Game" — Supporting Material

Distribute to IT/Cybersecurity Team at Exercise Start
FOR TRAINING USE ONLY

EXHIBIT A: DNS QUERY LOG EXTRACT

The following is a sample of anomalous DNS queries discovered by Systems Administrator Marcus Chen during a routine audit. These queries were extracted from the NCIA DNS resolver logs. The full log contains approximately 14,000 similar queries spanning the last 90 days.

Timestamp	Source IP	Query	Type
2026-06-02 03:14:22	10.1.10.5	aGVhZGVyOmN... .update-srv-04.cloud-sync.io	TXT
2026-06-02 03:14:25	10.1.10.5	cmVjb3JkOjEy... .update-srv-04.cloud-sync.io	TXT
2026-06-02 03:14:28	10.1.10.20	dXNlcmRhdGE6... .update-srv-04.cloud-sync.io	TXT
2026-06-02 03:14:31	10.1.20.50	ZW1wbG95ZWU6... .update-srv-04.cloud-sync.io	TXT
2026-06-02 03:14:34	10.1.10.5	cGFjc19jb25m... .update-srv-04.cloud-sync.io	TXT
... (14,000+ similar entries over 90 days)			

Analyst Notes

- The subdomain strings are **Base64-encoded** data chunks — a classic indicator of DNS tunneling. The attacker is breaking stolen data into small pieces, encoding each piece as a fake DNS query, and sending it to their external server. Because DNS traffic is almost never blocked or inspected, it slips right out.
- **Source IPs of interest:** 10.1.10.5 (Domain Controller), 10.1.10.20 (AODB Server), 10.1.20.50 (HR Workstation). These are the three compromised systems.
- The external domain **update-srv-04.cloud-sync.io** was flagged by the FBI's Cyber Division as a known C2 node associated with the **"Meridian Collective"** — an Eastern European organized cybercrime group specializing in infrastructure targets (utilities, transportation, logistics).
- DNS queries have been occurring between **2:00 AM and 5:00 AM local time** — when IT staffing is at zero.

EXHIBIT B: COMPROMISED SYSTEMS SUMMARY

Based on Marcus Chen's preliminary analysis, the following systems show evidence of unauthorized access.

System	IP Address	VLAN	Evidence of Compromise	Data at Risk
Domain Controller	10.1.10.5	10 (Server)	DNS tunneling queries originating from this host. Unauthorized service account created (svc_update_04) 87 days ago. Scheduled task running nightly data collection.	Active Directory: all usernames, password hashes, group memberships, email addresses. Domain admin credentials.

AODB Server	10.1.10.20	10 (Server)	DNS tunneling queries. Database export utility (bcp.exe) executed repeatedly via scheduled task. Large data volumes queried at off-hours.	90 days of flight data, gate assignments, passenger load counts, airline schedules. Possibly passenger manifest data (names, PNRs).
HR Workstation	10.1.20.50	20 (Admin)	DNS tunneling queries. This is the initial entry point — a spear-phishing email opened 90 days ago. Malware installed as a Windows service.	Employee PII: names, SSNs, addresses, phone numbers, emergency contacts, salary data. Approximately 340 employee records.

EXHIBIT C: THE INITIAL ENTRY — SPEAR PHISHING EMAIL

The following email was recovered from the HR workstation (10.1.20.50). It was opened 90 days ago by an HR coordinator. The attachment contained a macro-enabled document that installed the initial malware payload.

> **From:** benefits-admin@ncia-hr-portal.com [NOTE: This is NOT an NCIA domain]
> **To:** sandra.hayes@ncia.example
> **Date:** [90 days ago]
> **Subject:** ACTION REQUIRED: Updated Dental Benefits Enrollment — Sign by Friday
>
> Hi Sandra,
>
> HR leadership has approved updated dental benefit tiers for all full-time NCIA employees effective next quarter. Please review the attached enrollment form and return your signed copy by end of day Friday. If you do not respond, you will be auto-enrolled in the basic tier.
>
> See attached: **NCIA_Dental_Benefits_2026_Enrollment.docm**
>
> Thank you,
> Airport Benefits Administration

Key Details: The sending domain (ncia-hr-portal.com) is not owned by NCIA. It was registered one week before the email was sent. The .docm attachment (macro-enabled Word document) dropped a PowerShell-based backdoor that established persistence as a Windows service named "WinUpdateAssist." The malware uses living-off-the-land techniques — it runs using legitimate Windows tools (PowerShell, certutil, bcp.exe) to avoid triggering antivirus.

EXHIBIT D: NCIA NETWORK MAP — KNOWN COMPROMISE OVERLAY

Reference this alongside the evidence above. The three compromised systems span two VLANs. The attacker moved laterally from the Admin VLAN (initial foothold on the HR workstation) to the Server VLAN (Domain Controller and AODB). Other systems on both VLANs may also be compromised but have not yet been confirmed.

VLAN	Name	Subnet	Compromise Status	Key Concern
10	Server	10.1.10.0/24	**CONFIRMED — Domain Controller (10.1.10.5), AODB (10.1.10.20)**	If the Domain Controller is owned, the attacker has the keys to everything — every password hash, every system.
20	Admin / Corporate	10.1.20.0/24	**CONFIRMED — HR Workstation (10.1.20.50). Other workstations UNKNOWN.**	Initial entry point. Employee PII at risk. Other admin workstations may also be compromised.
30	Security Camera	10.1.30.0/24	UNKNOWN	If the NVR or PACS controller was accessed, the attacker knows camera coverage, door codes, and access patterns.

40	Retail / Vendor	10.1.40.0/24	UNKNOWN	Payment card data. PCI-DSS implications if this VLAN was touched.
50	Passenger Wi-Fi	10.1.50.0/24	Likely clean (isolated)	Should be fully segmented. Low concern unless segmentation failed.
60	Baggage / OT	10.1.60.0/24	UNKNOWN	Safety-critical OT systems. If compromised, could affect baggage handling or airside operations.

EXERCISE — FOR TRAINING USE ONLY