Document 1: Incident Briefing (Initial Security Report) – 03:30 UTC, May 5, 2025

At 03:00 UTC, monitoring systems detected an abnormal data exfiltration from **SVR-ACME-01** (our primary web gateway server). The server became unresponsive shortly after. An incident was declared at 03:15 UTC. Initial triage findings:

- **Symptom:** SVR-ACME-01 exhibited high CPU usage, then a crash. A large spike in outbound traffic to an external IP (45.67.89.10) was observed 2 minutes before the crash.

- **Security Controls:** The host's antivirus did not trigger any alert. However, the network IDS flagged the outbound traffic as unusual (pattern not seen before).

- **Preliminary Hypothesis:** Could be a new form of malware or a zero-day exploit, as no known signatures caught it. The fact that the antivirus was silent suggests the attack might be using a novel method or is hiding well.

- **Actions Taken:** The server was isolated from the network at 03:20 UTC. A forensic image of memory and disk has been taken for analysis. Related systems are being scanned for any signs of compromise.

- **Next Steps:** Analyze the forensic data, check logs (if accessible), and look for any indicators of compromise (IoCs). The code name **"Blue Raven"** was found in a suspicious file on the server (see Document 4) – need to determine what that is.

Document 2: Encrypted Log Excerpt (Captured from SVR-ACME-01)

gAABAAEAAAD/////9QDKAAAAAAAAlwAAAAAAAAAkAAAAFABAAAEAAAABAABAAAAAAAAAAQAAAAAAAAAAAAAAA
C4Hq4A8AAACuAAAAGAAAAAEAAAABAAAAAQAAAAAAAAAeAAAASAAAABgAAABIAAAAAgAAAAEAAAACAAAA
/////wAAAAMAAAABAAAABQAAAAEAAAACAAAADAAAAAQAAAABAAAABwAAAAEAAAACAAAACAAAAAEAAAAB

Excerpt from `/var/log/traffic_dump.bin` *on SVR-ACME-01.* The above is a fragment of binary data that appears to be encrypted or compressed. The file is approximately 5 MB of similar high-entropy data. Attempts to open it as text show gibberish. It could be that the malware/attack dumped data and encrypted it before exfiltration (possibly the contents that were sent to the external IP).

Notably, a header string "gAABAAEAAAD" repeats, which might indicate use of a specific encryption or encoding format (possibly proprietary). Without the decryption key or knowledge of the malware, we cannot read this log. However, its presence is evidence of data collection by the attacker.

(Analyst Note: The encryption could be using a static key within the malware, to be cracked later if the malware binary is analyzed. See Document 3 for malware analysis.)

Document 3: Malware Analysis Summary – "Blue Raven" Exploit Analysis

File Analyzed: `svracme_blue_raven.exe` (extracted from memory dump of SVR-ACME-01).
Analyst: J. Doe, Malware Analyst Team.
Date: May 6, 2025.

Overview: The binary appears to be a custom malware dropper that was likely injected into SVR-ACME-01's process memory. It's not recognized by virus databases (zero-day). The malware's behavior was reconstructed as follows:

- It exploits a vulnerability in the **ACME Web Gateway 5.4** software running on SVR-ACME-01. Specifically, a buffer overflow in the handling of HTTP headers. This overflow allows remote code execution. Since ACME Web Gateway 5.4 is custom software (in-house developed), this is a **zero-day exploit** (previously unknown, no patch).

- **Exploit Trigger:** A specially crafted HTTP request was sent to the gateway, containing an extremely long `X-Custom-Auth` header. The overflow injected shellcode into the gateway process memory.

- **Payload Execution:** The shellcode fetched the `svracme_blue_raven.exe` payload (likely named after the code "Blue Raven") from the attacker's server and executed it in memory.

- **Malware Capabilities:**

    - Scans for interesting files (e.g., containing "password", "config") and dumps them.

    - Captures recent log files and keystrokes (if any interactive sessions).

    - Encrypts all collected data using AES-256 with a hardcoded key `BRAV0KEY` (the repeated `/////wAAA` pattern in the encrypted log suggests a constant header after encryption, likely an artifact of the encryption library).

    - Transmits the encrypted bundle to `45.67.89.10` over HTTP on port 8080 (observed in traffic).

    - Cleans up by deleting itself and any temporary files, and attempts to crash the system (perhaps to distract or hinder analysis).

- **Indicators:** The string "BlueRaven" appears as a variable name in the binary (likely the exploit codename). The binary also checks for the presence of file `raven.done` as a marker to not reinfect.

- **Conclusion:** The root cause is the exploitation of an unknown buffer overflow in our web gateway software (no CVE as it's in-house). The attacker used this to run their malware, which we've dubbed **Blue Raven**. This allowed them to steal data (the encrypted logs and files) and likely caused the outage by crashing the server after execution.

Document 4: Attacker Decoy Note (False Flag Ransom Note)

Found on SVR-ACME-01's desktop as `READ_ME.txt`:

> Your files have been encrypted by Black Cobra ransomware.
> Send 5 Bitcoin to address 1Mz4...xyz to get the decryption key.
> If you try to restore without paying, all data will be lost.
> We hacked your system because of weak passwords.

Analysis: This note claims a ransomware attack by "Black Cobra". However:

- The systems were not actually encrypted (no files were locked/encrypted except the malware's own log dump). The core data and OS were intact.

- This appears to be a **deceptive signal** planted by the attacker to mislead investigators into thinking it was a generic ransomware incident (which would divert attention from the true zero-day exploit).

- The mention of "weak passwords" is likely false; no evidence of password-based intrusion was found. All signs point to the exploit vector instead.

- The Bitcoin address given has not been seen in known ransomware cases; it's probably a wallet controlled by the attacker, but no ransom communication was actually made to the victim (us).

Conclusion: The note is a red herring. The real attack did not behave like typical ransomware. This was a targeted exfiltration attack using a zero-day, not primarily a financial ransomware operation.

Document 5: Post-Incident Root Cause Analysis (Excerpts)

Prepared by: Lead Investigator – Contoso Incident Response
Date: May 10, 2025 (after patching and recovery)

After thorough investigation, we conclude the following root cause of the cybersecurity incident:

- **Root Cause:** A **Zero-Day vulnerability** in the Contoso **ACME Web Gateway v5.4** was exploited. The vulnerability (a buffer overflow in header parsing) allowed remote code execution on SVR-ACME-01. The attacker did not need valid credentials or user interaction – the network-facing service was the entry point.

- **Exploit Codename:** Internally referred to as **"Blue Raven"**, based on strings found in the attack binary. No prior knowledge of this exploit existed; hence it bypassed our defenses.

- **Affected Infrastructure:** Primarily the server SVR-ACME-01 which ran the vulnerable service. Once compromised, the attacker's malware had access to that server's data and network credentials present in memory.

- **What the Attacker Did:** After gaining control, the attacker's payload collected sensitive configuration files (including an outdated database backup file containing customer data) and recent logs from the server. It then **encrypted these artifacts** and exfiltrated them to an external host. The attacker intentionally caused a system crash to cover tracks and dropped a fake ransom note (Document 4) to confuse the response team.

- **Discovery:** The incident was discovered by outbound traffic anomaly and subsequent crash alerts. The fake ransom note initially led the team to consider generic ransomware, but the forensic analysis (Document 3) of memory and the custom malware uncovered the zero-day usage.

- **Resolution:** Contoso developers created an emergency patch for the buffer overflow within 48 hours and applied it to all instances of ACME Web Gateway. We also improved monitoring on that server (adding an EDR solution that could catch such exploitation patterns in the future).

- **Lesson Learned:** Regular security auditing of in-house software might have caught this vulnerability before deployment. The incident underscores the importance of multi-layered security – while perimeter defenses were breached, network monitoring did help detect abnormal exfiltration. Also, be cautious of initial assumptions (the ransomware note was a clever deception).

Root cause confirmed: Unpatched code vulnerability (zero-day) leading to remote code execution on a critical server.