The 2026 Cyber-Attack Case Study on heain-core

How Far Can One Leaked Credential Reach?
A Master and Two Workers, Five Scenes from Real Attacks of Oct–Nov 2026:
Separated Approver Keys, Encrypted Backup and Core Rounds C17–C20

Jakkrit Boonma (จักรกฤษ บุญมา)

Independent Researcher · ORCID: 0009-0000-7165-3787 · jaggid.boonma@yahoo.co.th

Date: 13 November 2026

Implementation: heain-core (commit 9808fa7, test packages v1.3.0-t7), HP Z840 Workstation

Repository: github.com/JakkritB/heain-core (casestudies/cyber/)

Abstract

In October–November 2026 several major attacks began not with a new vulnerability but with a valid credential in the wrong place: a token on an engineer's laptop at Binance [2][3], a stale app credential at ConnectWise [5][6], leaked firewall admin passwords [7][8], an updater that did not enforce signature checks at Notepad++ [9], and internet-exposed refrigeration management pages in Europe [13][14]. Ransomware at IDCF Cloud stopped about 495 organizations relying on one centre at once [10][11].

On an HP Z840 the author built a 3-machine lab after the project's real Windows lab (one Master, two Workers) and simulated only attack effects in five scenes: L1 an insider machine taken; L2 an admin account taken; L3 a false update; L4 the LAN cut, the Master down and the Master's disk lost for good; L5 cold rooms commanded from a stolen login, an outside vendor and a one-night campaign. The attacker holds only "leaked" certificate or key files, and every scene prints the real outcome (asis) beside heain's.

The final run (core 9808fa7) passed all 93 checks with no open finding. A taken Worker reached nothing above itself and was cut off at the Master 1.2 seconds after revocation through P5. A taken admin account could only propose when the approver and CA keys were off the Master, but L2a shows that with every key on one machine, as by default, four-eyes means nothing. All five false releases were refused; the shop worked on with the cable cut or the Master down; and a restored Master led the lab again in 9.2 seconds. Findings F1–F6 led to four core rounds (C17–C20), changes to heain-setup, and one finding on real Windows awaiting the author's decision (F4).

Keywords: *HEAIN Framework, heain-core, Cybersecurity, Insider Compromise, Privileged Access, Four-Eyes Approval, Software Supply Chain, Signed Releases, Ransomware Resilience, Encrypted Backup, OT Security, Cold Chain*

1. Introduction

1.1 Background

Earlier case studies of the HEAIN Framework tested heain-core on disasters, the southern border, the Senate selection and the 2026 MP election [23]. Each assumed honest users and asked whether the system withstands mistakes and failures. This case asks the reverse: if one valid credential falls into an attacker's hands, how far does the damage spread, and how fast can it be cut off?

The question came from incidents worldwide while the author was setting up the project's real Windows lab (an ASUS as Master and two HP Z8 G4 as Workers). The author had the case designed from those incidents and run first on an HP Z840, separate from the real lab [1]. The author chose L1–L4 from the study's findings, had L5 added to the first round as the most recent news, and placed L6 (valid rights misused in volume) in round two.

1.2 Real Incidents Used as Sources

Table 1 summarizes the incidents used, by pattern. Each is written as the organization disclosed or the press reported, with the status of the information. The common thread is that most major incidents came not from a new vulnerability but from valid rights in the wrong place.

Pattern	Incident and status	What happened, as reported	Scene	Source
A Insider machine taken, then spread to high privilege	Binance, 29 Oct 2026, about US$6.3 billion (Binance confirmed; FBI attribution 31 Oct)	Engineer's machine infected → access to the wallet team engineer → deploy token found on a laptop → signing service called; sources still differ on the origin	L1	[2][3][4]
B Stale app rights used	ConnectWise Cloud Backup, 15–16 Oct 2026 (company confirmed; Microsoft assesses Storm-0940)	A stale Microsoft 365 app credential used; the app made itself Global Administrator in at least 2 tenants	L2	[5][6]
C Admin account taken, then a lingering admin created	FortiGate: FBI and USSS advisory, 6 Oct 2026 (ongoing)	Leaked passwords used, owners locked out, extra admin accounts created	L2	[7][8]
D False update	Notepad++, Jun–Dec 2025, disclosed Feb 2026 (project confirmed)	Hosting taken; some update requests diverted to a fake installer; older updaters did not enforce signature checks	L3	[9]

Pattern	Incident and status	What happened, as reported	Scene	Source
E Whole centre down	IDCF Cloud, Japan, 7 Oct 2026 (company confirmed)	Admin rights to the virtualization platform taken, VMs encrypted; about 495 organizations stopped; by 27 Oct, 206 recovered	L4	[10][11]
	Thailand among the 10 countries most hit by ransomware (Check Point, Q1 2026)	Main entry points are VPNs and remote systems exposed to the internet	L4	[12]
F Control devices commanded remotely	Supermarket refrigeration, 10–11 Oct and 2 Nov 2026 (French authorities' attribution 9 Nov)	First wave forced defrost mode, second raised temperatures, via internet-exposed controller management pages; about 700 stores; at least 15 fires	L5	[13][14][15]
	EFS France, early Nov 2026 (EFS confirmed an attack via a vendor)	Cold rooms and plasma freezers set through an outside vendor's system; the 110 °C figure is a press report	L5	[16][17]

Table 1 — Real incidents behind the scenes (sources checked 12–13 Nov 2026)

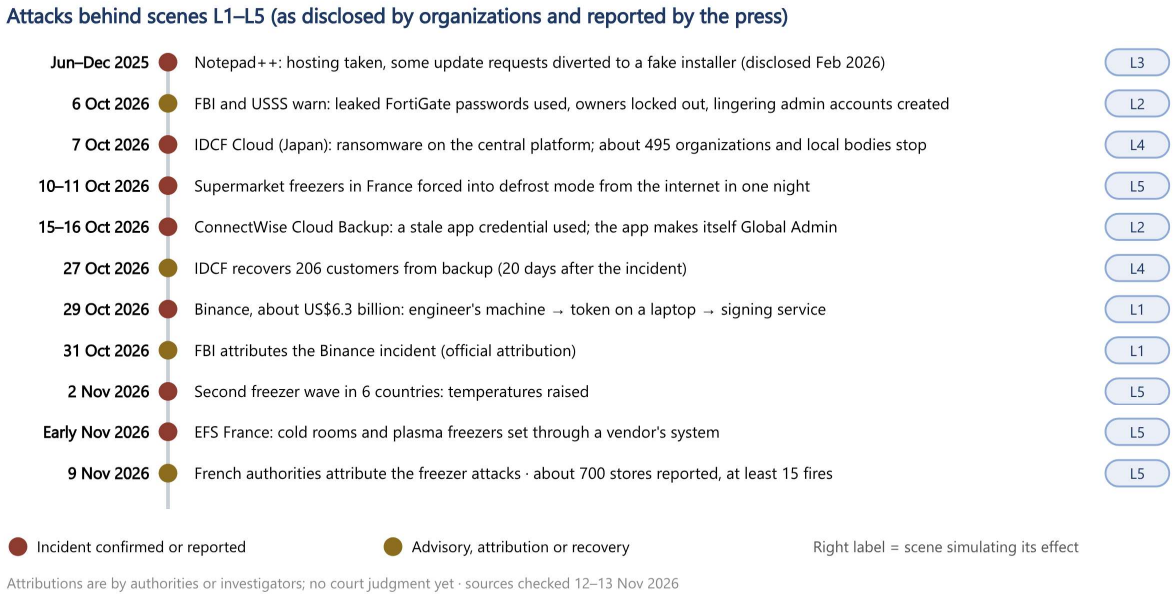


Figure 1 — Attacks behind scenes L1–L5 in time order [2]–[17]

1.3 Status of the Incident Information

> This section relates incidents as the attacked organizations disclosed them, as authorities warned, or as the press reported. They are not facts decided by a court. Attributions are assessments by authorities or investigators. This paper judges no one's liability and tests or simulates no company's product. Faults in the lab are entirely synthetic and tied to no real company or vendor.

In several incidents the origin still differs between sources; for Binance, some reports say it began with a fake Homebrew and others with a fake pyenv [2][3]. The lab scenes therefore do not simulate how a machine was entered, but start where all sources agree: the attacker already holds one valid credential.

1.4 Research Questions

1. **RQ1** If an insider machine is taken with its certificate and key, how far can the attacker go, and how fast can that machine be cut off?
2. **RQ2** Can a taken admin account create lingering rights, and how must keys be placed for two-person approval (four-eyes) to mean anything?
3. **RQ3** Can a fake or altered release get into a node, and does a broken release spread through the whole system?
4. **RQ4** When the cable is cut, the centre goes down, or the centre's disk is lost for good, does work on site stop, and can it be recovered?
5. **RQ5** Can control devices be commanded from a stolen login, from an outside vendor, or in bulk in one night?
6. **RQ6** Does core need changing, and what can be fixed by configuration or the installer alone?

1.5 Scope

- **Effects only:** the attacker has only "leaked" files (certificates, keys, a disk); no malware, no intrusion tools, and no product vulnerability is tested.
- **Synthetic data:** the shop, cold rooms, vendor and releases are fictional; the binaries in releases are the project's own.
- **Round one is L1–L5:** L6 and other large topics (power, water, internet, banking) come in later rounds.
- **A simulated lab on one machine:** the real Windows lab runs separately per the project manual; related findings from it (F4, F5) are included in section 4.
- **This deployment is the author's hypothetical design,** not any organization's system, and not reviewed by any agency.

2. Simulation Principles and Scene Mapping

Every scene has the same frame: real incident behind it → what is simulated (effects only) → asis → heain → pass criteria → what is measured. Pass criteria are written as automatic checks in the scene's script (PASS/FAIL). Things that are not yet the desired behavior but are not script errors are recorded separately as FINDINGs for the author to decide whether to fix. Table 2 shows the question each scene answers.

Scene	What the attacker holds	asis (as in the real incident)	Mechanisms tested
L1 Worker taken	z8-1's certificate and key	A token on an engineer's machine deploys and calls the signing service at once	Tier roles, P5, node revocation
L2a Admin taken (keys together)	The Master's whole disk	Extra admins created with no one else agreeing	Four-eyes with keys on one machine
L2b Admin taken (keys apart)	The Master's disk (without approver and CA keys)	An app makes itself Global Administrator	Four-eyes, key separation, audit
L3 False update	5 kinds of false release, admin key	The updater installs an installer from the attacker's server	Releases signed 2 of 3, P5, canary, rollback
L4 Cable cut, Master down, disk lost	Ransomware's effect: Master stopped or disk gone	The centre goes down and every branch stops	STANDALONE, journal, role ceiling, encrypted backup
L5 Cold rooms	Shop login, vendor system, one-night campaign	Freezers in hundreds of stores set in one night	p5.thresholds, p5.quota, untrusted_source, max_uses

Table 2 — Scenes L1–L5, what the attacker holds, and the mechanisms tested

3. Method

3.1 The Simulated Lab

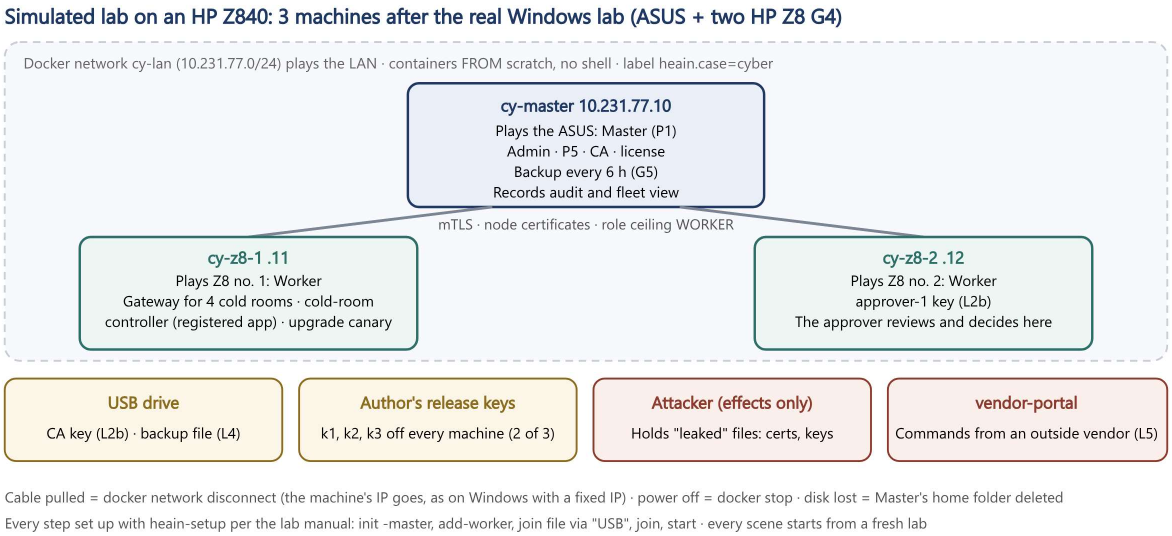


Figure 2 — The simulated 3-machine lab on an HP Z840 and what lies outside it

The lab has 3 containers built from an empty image (FROM scratch) holding only the heain-core package and the case's tools, with no shell (Figure 2). cy-master plays the ASUS; cy-z8-1 and cy-z8-2 play the two HP Z8s. All sit on a docker network playing the LAN. Setup uses heain-setup at every step per the lab manual, join files travel through a folder playing the USB drive, and every scene starts from a fresh lab.

Pulling the LAN cable is done by disconnecting a container from the network, which removes the machine's IP as on Windows with a fixed IP. Powering off stops the container, and a permanently failed disk deletes the Master's home folder. This detail matters, because F1 arose from the IP vanishing with the cable, which earlier tests that cut routes with a proxy had never met.

3.2 Lab Gaps Fixed in heain-setup

Before writing the scenes, the author checked what the lab built by heain-setup lacked and found five gaps. All were fixed in the installer without touching core (Table 3).

#	Gap	What was added
G1	The ASUS holds the admin, approver-1 and CA keys; if taken, the attacker can issue an approver-1 certificate itself, so moving only the approver is not enough	approver export/import/pending/approve/reject and ca export/import; the CA key is kept off the machine and used only when adding a Worker
G2	With the cable pulled the IP goes, so a node listening only on that IP cannot serve apps on the same machine	-bind all: the node listens on every interface; local apps use 127.0.0.1
G3	Apps on a Worker cannot get certificates, because the Master has a provisioning CA only in web mode	A lab Master always has a provisioning CA
G4	Revoking a Worker requires calling the API directly	revoke-worker -name: admin proposes, the approver approves
G5	No way to recover the Master when its disk is lost for good	backup setup / backup / restore: password-encrypted backups; core backs up every 6 hours, keeps 8

Table 3 — Lab gaps and what was added to heain-setup

3.3 Core Mechanisms Used

Mechanism	What it does	Scenes
Tier roles	A Worker certificate cannot use the Master's admin API or impersonate another machine	L1
P5 and four-eyes	Every change of rights is a proposal; the proposer cannot approve their own	L1, L2, L3, L5
security.revoked_nodes	A node revoked through P5 fails TLS or gets 403 on every channel	L1
upgrade.release_keys	A release must carry N of M Ed25519 signatures [19] and the binary hash must match	L3
Rollout and rollback	Canary first; a release that fails to start rolls back on its own and halts the rollout	L3
STANDALONE and journal	Cut from its parent, a node works on within policy, journals, and sends up once, in order	L4
Role ceiling	A Worker does not take over for a Master holding the CA, license and approvals	L4
Node backup	Backs up node state including the Raft snapshot [22]	L4
p5.thresholds, p5.quota	A pre-approved range, and a daily quota beyond which commands wait for a person	L5
untrusted_source, max_uses	Commands from outside sources always wait for a person; a grant is usable only the set number of times (C18)	L5

Table 4 — Core mechanisms the scenes test

3.4 Systems Compared

Here asis is not a model of any one system but what happened in the real incident as reported. Every scene prints an asis line beside the heain result, to show how differently far the same credential takes an attacker (Table 5).

Aspect	asis	heain
Insider machine taken	A token on the machine reaches the signing service	A Worker certificate serves only the Worker's role
Admin taken	Creates a lingering admin alone	Can only propose; needs an approver on another machine
Updates	Older updaters do not enforce signatures	Without release keys, nothing is accepted
Centre down	Every branch stops	Branches work on under existing policy and journal
Centre's disk lost	206 of about 495 recovered in 20 days	Recovered from an encrypted backup; existing Workers return by themselves
Control devices	Management page on the internet; commands take effect at once	Out of range or from outside waits for a person; a grant is single-use

Table 5 — What one credential did in the real incidents (asis) compared with heain

3.5 Rounds and Environment

Round	Date	Content	Cyber case result
cy1	12 Nov 2026	Lab, G1–G4, scenes L1–L5 first run (core 2fa7628)	All passed; F1 (L4) and F2 (L5) found
c17	12–13 Nov	C17, C18, role ceiling (F3), G5, full regression	L4 failed 1 check after Master restore
c17b	13 Nov	Cold-room controller retries on 503; v1.3.0-t6 released (98426aa)	All passed
c19, c19b	13 Nov	C19 (F5) and rerun	L4 failed the same way; real cause found (F6)
c20	13 Nov	C19 + C20, full regression, v1.3.0-t7 released (9808fa7)	L1 14, L2 15, L3 17, L4 34, L5 13, all passed

Table 6 — Rounds of the cyber case on the HP Z840

All rounds ran on the HP Z840 with scripts committed and pushed only when they passed in full, verified with git ls-remote. The pass counts in this paper come from round c20. The reported times come from confirmation runs on the same code in the development machine (a Linux container) on the same day, because the Z840 results record only a summary per scene.

4. Core and Tooling Work Arising from This Case

The case produced six findings. Four were fixed in core by the project's usual procedure: write a proposal, have the author decide, then run the full regression of every case study. The other two were fixed, or await fixing, outside core (Table 7).

#	Found in	What happened	Fix	Status
F1	L4 (cy1)	With the cable pulled the IP vanished; the Worker tried to promote, could not bind its port, then stopped watching its parent, so a second cable pull went undetected	C17: check the address is still on the machine before promoting; a failed promote goes back to watching the parent and reopens the old tier	Closed (t6)
F2	L5 (cy1)	An approved grant could be reused within its lifetime; a taken app could reuse an earlier approval to command a device again	C18: p5.bindings[type].max_uses, durably counted; once used up, 403 and audited	Closed (t6)
F3	L4 (c17)	With the Master off, a Worker took over and did not hand back	heain-setup: lab Workers get role ceiling WORKER; init -master -takeover allows takeover	Closed (t6)
F4	Real Windows lab	Defender deleted garbled files, naming them Trojan:Win32/Gracing.I	Temporary: an exclusion for the install folder	Awaiting the author
F5	Real Windows lab	An nvidia-smi console window popped up every minute	C19: start child programs with a hidden window	Closed (t7)
F6	L4 (c17, c19b)	A freshly started Master said app certificates were "invalid" while its registry was still loading; Workers remembered that and refused apps with 403	C20: answer 503 during start-up, take a Raft snapshot before backup, never copy open Raft files	Closed (t7)

Table 7 — Findings F1–F6 and their fixes

C17 fixes the path when a Worker is cut off in a way that removes the machine's own IP. Before leaving its tier to promote, the node checks that the address it needs is still on the machine. If not, the machine itself is the one cut off, so it does not promote, audits P6.promotion_skipped and keeps watching its parent. A promotion that fails for another reason also returns to watching (P6.promotion_failed). The STANDALONE decision, the witness and the journal are unchanged.

C18 adds max_uses per action type in p5.bindings. Unset means unlimited, as before, so incident-bound video searches in the southern-border case can still be reused within 48 hours, while commands to devices are set to single use. The count sits in the same transaction as the check and survives restarts.

C20 came from an intermittent failure in L4 that round c17b had treated only at the symptom, by having the controller retry. Round c19b failed the same way again with 403, so the real cause was traced. Every time the Master starts, whether from a restart, an upgrade or a restore, there is a window of about one second in which the app-certificate registry has not finished loading. In that window the Master answered that a certificate was "invalid" instead of "cannot check yet", and Workers remembered that answer. C20 fixes three parts. S1 answers 503 with Retry-After during start-up, so Workers use their last remembered answer instead. S2 makes the backup wait for the registry to load in full, then store the Raft state as a fresh snapshot before writing the backup file; this was found during the fix, because without the wait L4 failed every time. S3 no longer copies the open Raft files into the backup.

G5 backups are encrypted with AES-256-GCM [20], with a key derived from the password by PBKDF2-SHA256 at 600,000 iterations [21]. A lost password means no recovery, as the author chose. The file holds core's node backup and heain-setup's configuration, and restore checks that the new machine has the Master's IP.

5. Results

5.1 L1 A Worker Machine Taken

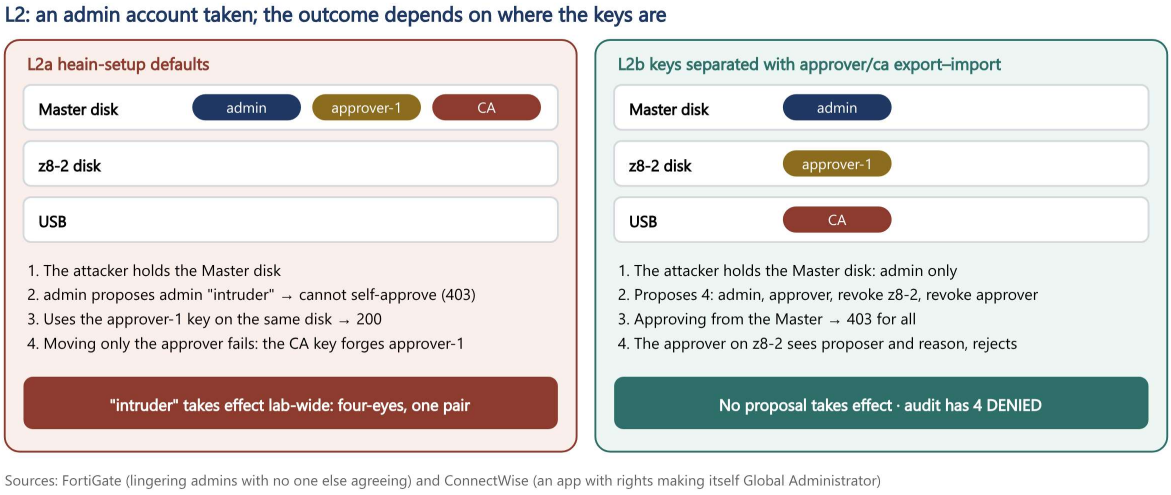
The attacker holds z8-1's disk, that is, the machine's certificate and key, comparable to the engineer's laptop in the Binance incident (Table 8).

Step	Result
Using z8-1's certificate	Master's admin API (fleet view, configuration) 403; proposing itself as admin through P5 403; approving pending items 403
Deploy and impersonation	Requesting a new app registration token 403; posing as z8-2 in the Master's farm 403; sending jobs to z8-2 403
Revocation	Admin alone cannot revoke (403); revoke-worker: admin proposes, the approver approves
Effect of revocation	The Master refuses z8-1 after 1.2 seconds, z8-2 after 11.2 seconds; certificate renewal fails (TLS handshake fails)
The rest	z8-2 normal; the fleet view no longer counts z8-1; audit has security.revoked_nodes and the refusals

Table 8 — L1 results (14/14 passed)

A Worker's certificate takes the attacker only as far as the Worker's role, with no path to higher rights. This differs from the real incident, where a token on one machine reached the signing service directly. The taken machine itself is still compromised: apps running on z8-1 are in the attacker's hands until revocation. heain limits spread upward; it does not protect that machine.

5.2 L2 An Admin Account Taken



Sources: FortiGate (lingering admins with no one else agreeing) and ConnectWise (an app with rights making itself Global Administrator)

Figure 3 — L2a and L2b: what a taken admin account achieves depends on where the keys are

L2a uses heain-setup's defaults, which keep the admin, approver-1 and CA keys on the Master's disk (Figure 3). The admin key alone cannot approve its own proposal (403), but the attacker uses the approver-1 key on the same disk and approves (200). "intruder" thus gains the admin role lab-wide, taking effect on z8-2 too. Moving the approver to z8-2 alone is not enough, because the CA key still on the Master can issue a new approver-1 certificate. L2a therefore shows a weakness by design, not a failure: four-eyes on one machine is one pair of eyes.

L2b moves the approver-1 key to z8-2 and keeps the CA key on a USB drive. The attacker holding the Master disk proposes four items: add an admin, add an approver, revoke z8-2, and revoke the approver-1 certificate. Approving from the Master gets 403 for each. The approver on z8-2 sees all four, the proposer and the reason, and rejects them; none takes effect anywhere. Adding a Worker requires bringing the CA key back first, so the attacker cannot create machines or approvers. Real changes still work as usual: proposed at the Master, approved at z8-2, taking effect on z8-1 (15/15 passed).

5.3 L3 False Updates

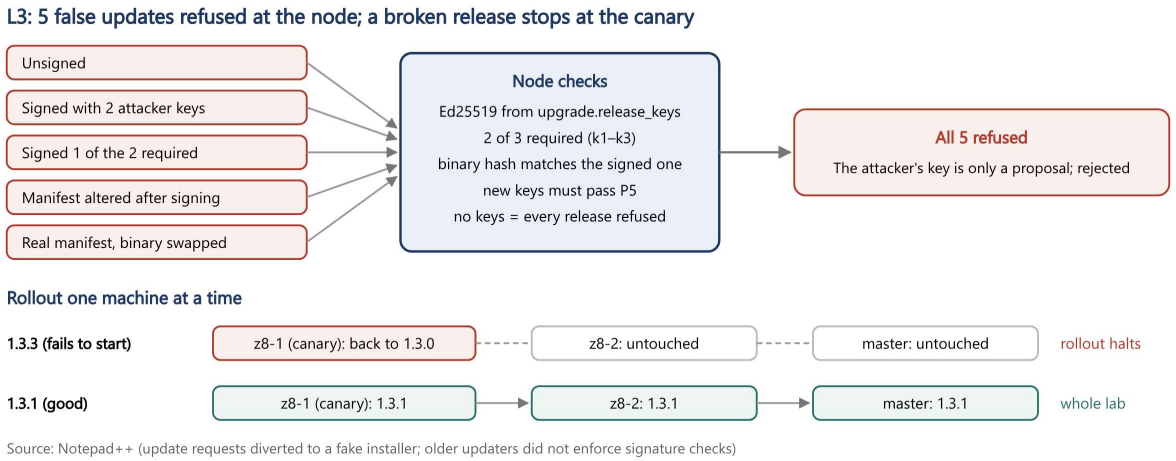


Figure 4 — L3: five false releases and a rollout one machine at a time

The author's release keys k1, k2 and k3 are kept off every machine, with two of three required (Figure 4). Before the keys are set through P5, the node refuses even a correctly signed release (400). Once set, a release that is unsigned, signed with two attacker keys, signed with only one of two, has a manifest altered after signing, or has a real manifest with a swapped binary as in the Notepad++ incident, is refused in every case. An attacker holding the admin key can propose adding their own release key, but it is only a proposal, and the approver rejects it.

Release 1.3.3, correctly signed but unable to start, goes to z8-1, the canary, first. z8-1 rolls itself back to 1.3.0, the rollout halts, and z8-2 and the Master are untouched. The good release 1.3.1 goes out in order to z8-1, z8-2 and the Master, and the lab is whole again (17/17 passed).

5.4 L4 Cable Cut, Master Down, and the Master's Disk Lost

L4 has three parts on two kinds of lab. The cable part uses a lab where a Worker may take over for the Master (-takeover), so a cut-off Worker must pass through the promotion path fixed by C17. The Master-down part uses the default lab, where Workers have role ceiling WORKER. The shop has 4 cold rooms at -20 °C on z8-1 and a pre-approved range of -25 to -18 °C (Table 9).

Part	Result
z8-1 cable pulled	STANDALONE after 10.3 s; the Master sees z8-1 as stale; z8-1 alone approves -23 °C (in range) and holds -16 °C (out of range) for a person; all rooms stable; journaled; z8-2 unaffected
Cable back	Normal after 33.0 s (waiting for the Master to answer steadily for 30 s, by design); the Master receives journal 1..96; the pending -16 °C command reaches the approver and is rejected; no duplicates
C17	While cut off, z8-1 does not promote, since its own address went with the cable, and keeps watching the Master; a second cable pull is STANDALONE again in 8.3 s; the journal continues without duplicates
Master off	backup setup: core backs up every 6 hours; a 24 KB backup to USB with no readable key or certificate; both Workers work on; in-range commands approved; no Worker takes over; the Master powered back, lab complete in 59.3 s
Master disk lost	A wrong password cannot open the file; the backup holds a Raft snapshot, not the open Raft files (C20); after restore the Master leads the lab in 9.2 s and both Workers rejoin its fleet by themselves; policy fully back; audit has backup.restored; app certificates issued before the backup still work; the shop works on

Table 9 — L4 results (34/34 passed)

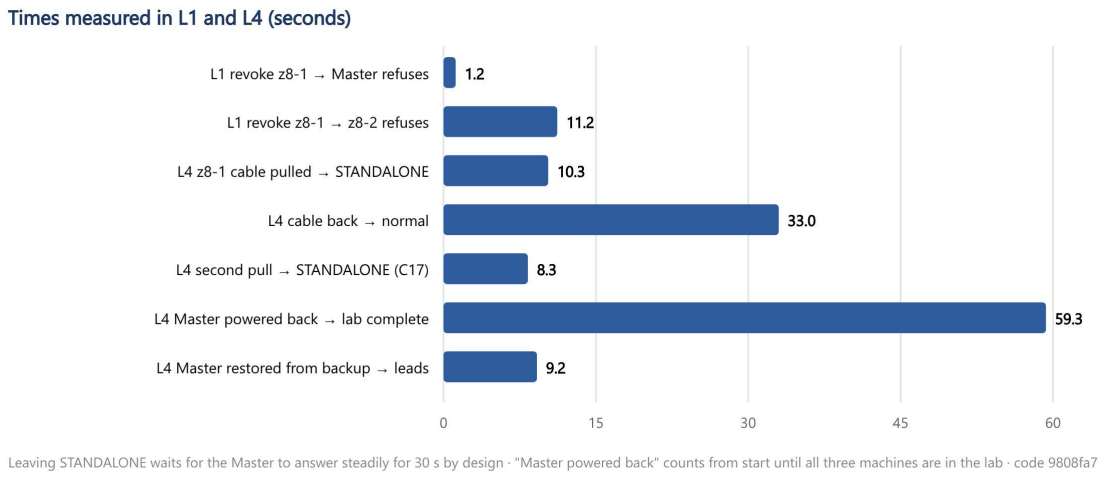
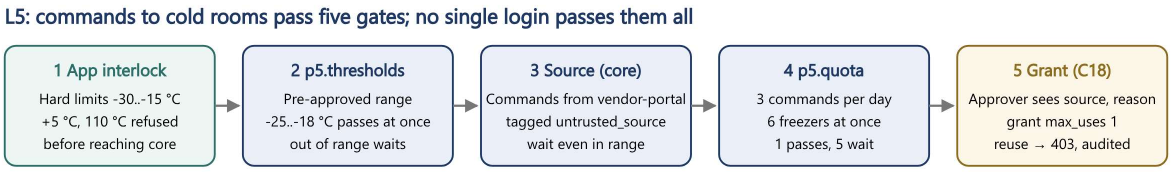


Figure 5 — Times measured in L1 and L4 (confirmation run on code 9808fa7)

In the IDCF incident, the downed centre stopped every organization relying on it, and 20 days later about 206 of 495 had recovered [10][11]. In the lab, the shop worked on under existing policy both with the cable cut and with the Master down, and its records caught up once, in order, on return (Figure 5). The comparison does not say that a large platform could recover in seconds; it says that when policy also lives on site, the centre going down is not the site stopping.

5.5 L5 Cold Rooms



Outcome for each kind of attacker

Actor	asis (real incident)	heain (L5)
Stolen shop login	Sets values at once	-16 °C waits, then rejected; room stays at -20 °C
Vendor's system	Sets values via the vendor (EFS)	Only a proposal; single use once approved
One-night campaign	Hundreds of stores in one night	Past the quota every command waits, with reason
Compressor stops	—	Above -12 °C: controller alerts, audited, readable at Master

Gate 1 lives in the app and is lost if the app on the machine is taken · gates 2–5 live in core and apply to every command through core

Figure 6 — L5: the gates a command must pass to reach a cold room, and the outcome for each kind of attacker

The synthetic cold-room controller is an app registered on z8-1. Policy is set at the Master through P5: a range of -25 to -18 °C, a quota of 3 commands per day, and single-use grants (Figure 6).

- **Shop staff:** set cr1 to -22 °C, in range, effective at once.
- **Stolen shop login:** set cr2 to -16 °C, out of range; it waits for the approver while cr2 stays at -20 °C; the approver rejects it.
- **Dangerous values:** +5 °C and 110 °C are refused by the controller's interlock before being proposed (hard limits -30 to -15 °C).
- **Outside vendor:** a -19 °C command is in range, but core tags it untrusted_source, so it waits for a person; the approver sees the source vendor-portal and approves after checking; the grant cannot be reused (C18: 403, audited).
- **One-night campaign:** six rooms commanded at once; 1 passes because 2 of the day's quota were already used; the other 5 wait, each stating quota_reached.
- **Compressor stops:** cr4 warms above -12 °C; the controller alerts, readable from z8-1's audit at the Master.

No single login, single vendor system or one-night campaign gets through every gate (13/13 passed). One caution: the interlock belongs to the app. If the app on the machine is taken, the first gate is gone, but gates two to five live in core and apply to every command that passes through core.

5.6 System Correctness

Set	Result
gofmt, vet (linux, windows), unit, cross-compile gate	Pass
12 live sets	apps 22, app_registry 20, subtree 16, standalone 42, reclaim 20, sibling_failover 14, cert_last_known 20, cross_node_jobs 16, app_jobs 21, setup_lab 27, setup_quickstart 19, setup_web 18
Earlier case studies	Southern border rounds 0 (21) and 1 (36); CineNexus rounds 1 (25), 2 (26), 3 (36), 6 (39), 7 (35)
Cyber case	L1 14, L2 15, L3 17, L4 34, L5 13; failures 0, findings 0
Test packages 1.3.0-t7	Windows installers amd64/arm64, deb amd64/arm64 and .dmg; tested on the packages: lab 27, quickstart 19, web 18, license 23
Release	Pre-release v1.3.0-t7 on JakkritB/heain-core and heainframework/heain-testers (16 files per repo); verified with ls-remote

Table 10 — Checks in round c20 on the HP Z840 (core 9808fa7, 13 Nov 2026)

Round c17, the first core change of this case, ran the full regression of every case study, including disaster, trials E1–E4, the Senate selection and the MP election, and all passed except the MP national-scale round, which was not run. Round c20 touched only Master start-up, backup and starting child programs on Windows, so it ran the sets covering those parts.

6. Discussion

6.1 Answers to the Research Questions

- **RQ1:** A taken Worker certificate reaches only the Worker's role and was cut off 1.2 seconds at the Master and 11.2 seconds at the other Worker after the approver approved the revocation. The taken machine itself is still compromised.
- **RQ2:** An admin account can only propose if the approver and CA keys are off the admin's machine. If they are on the same machine, four-eyes means nothing (L2a). Key separation is therefore a condition, not an option.
- **RQ3:** All five false releases were refused, new keys must pass P5, and a broken release stops at the canary. Installers people download themselves lie outside this control (6.3).
- **RQ4:** Sites work on under existing policy both with the cable cut and with the Master down, and a Master whose disk is lost can be recovered from an encrypted backup, after fixes C17 and C20.

- **RQ5:** No. Commands out of range, from outside sources, or over quota wait for a person every time, and after C18 an approval can be used only once.
- **RQ6:** Core needed four rounds (C17–C20); the rest was fixed with heain-setup and configuration (G1–G5, role ceiling). F4 still awaits the author's decision.

6.2 What Can Be Done Now against What Needs a Decision

Item	Doable now	Needs a decision or investment
Separate approver and CA keys from the Master	Yes (approver and ca export/import)	Whether it should be a mandatory install step
Release keys off machines, 2 of 3	Yes	Who holds each key
Encrypted backup every 6 hours	Yes (backup setup)	Where the password is kept; lost means unrecoverable
max_uses for commands to devices	Yes (set through P5)	—
Worker role ceiling	Lab default	Reclaim on Workers (separate proposal)
Signing the Windows installer (F4)	—	Drop garble on Windows, Authenticode, or submission to Microsoft
Per-app call ceiling (L6)	—	Code review in round two; may need a core proposal

Table 11 — Separating what the existing tools can do now from what needs a decision or investment

6.3 Limitations

- **Effects simulated on one machine:** the lab is Linux containers on an HP Z840, not real Windows. Windows-specific findings (F4, F5) come from the real lab, which has not yet run every scene.
- **The attacker holds only files:** core's own code was not tested for vulnerabilities; there is no pentest or fuzzing in this case.
- **Defaults are still weak:** heain-setup still keeps every key on the Master at install time; users must move them per the manual, or the outcome is that of L2a.
- **Installers outside control:** core checks the releases it receives but not the installers people download. The Windows installer is not yet Authenticode-signed and the .dmg is ad-hoc signed; only SHA256SUMS in the release protects them.
- **Interlock in the app:** if the app on the machine is taken, the first gate of L5 is gone; the remaining gates are in core.

- **The taken machine itself:** heain limits upward spread but does not protect data and apps on that machine before revocation.
- **Measured times:** from confirmation runs in the development machine on the same code, not measurements on a real network.
- **Incident information:** several incidents are still under investigation; origins and figures may change.

7. Conclusion and Recommendations

The first cyber round tested heain-core on a question earlier cases did not ask: when one valid credential leaks, how far can the damage spread? The most important result is not refusals working as designed but two things the simulation made visible. First, two-person approval means something only when the keys are in different places, which the installer's defaults do not yet ensure. Second, real cable pulls and Master restarts exposed problems earlier tests had never met, so core needed four rounds (C17–C20). After them every scene and every earlier case study gives the same results.

1. Have heain-setup move the approver and CA keys off the Master as a step of installation, not an optional extra.
2. Decide the long-term fix for F4 before handing test packages to outside testers, and consider signing installers to close the false-update gap where core has no control.
3. Set max_uses to 1 for every command type that reaches a device in the next cases (power, water).
4. Run scenes L1–L5 on the real Windows lab per the manual and compare times with the simulation.
5. Round two: L6, valid rights misused in volume, and the large topics from the backlog.

References

[1] Boonma, J. casestudies/cyber/ in the heain-core repository, 2026; project documents claude/study-2026-11-12-cyber-lab-cases, claude/plan-2026-11-12-cyber-round1 and the core proposals claude/proposal-2026-11-12-core-c17-c18, claude/proposal-2026-11-13-core-c19 and claude/proposal-2026-11-13-core-c20.

[2] Start With Identity. Binance says a fake job interview and an internal AI tool led attackers to its wallet signing service. 3 November 2026. startwithidentity.com/blog/2026-11-03-binance-says-fake-job-interview-and-internal-ai-tool-led-to-wallet-signing-service/

[3] 9to5Mac. The record $6.3B Binance heist started with a fake Homebrew install on Mac. 4 November 2026. 9to5mac.com/2026/11/04/security-bite-the-record-6-3b-binance-heist-started-with-a-fake-homebrew-install-on-mac/

[4] SOCRadar. October 2026: Binance Heist, ConnectWise Breach, and More. 2026. socradar.io/blog/major-cyber-attacks-october-2026/

[5] BleepingComputer. Hackers breach Microsoft 365 tenants via ConnectWise supply chain attack. October 2026. bleepingcomputer.com/news/security/hackers-breach-microsoft-365-tenants-via-connectwise-supply-chain-attack/

[6] Dark Reading. Microsoft Links Storm-0940 to ConnectWise Supply Chain Attack. 2026. darkreading.com/cyberattacks-data-breaches/microsoft-storm-0940-connectwise-supply-chain-attack

[7] FBI and U.S. Secret Service. Cybersecurity Advisory (FortiGate credential abuse). 6 October 2026. ic3.gov/CSA/2026/261006.pdf

[8] BleepingComputer. FBI: Ongoing FortiBleed attacks lock out FortiGate VPN admins. October 2026. bleepingcomputer.com/news/security/fbi-ongoing-fortibleed-attacks-lock-out-fortigate-vpn-admins

[9] eSecurity Planet. Notepad++ Update Servers Hijacked in Targeted Supply Chain Attack. 2026. esecurityplanet.com/threats/notepad-update-servers-hijacked-in-targeted-supply-chain-attack/

[10] BleepingComputer. Ransomware attack disrupts Japan's IDCF Cloud used by govt clients. October 2026. bleepingcomputer.com/news/security/ransomware-attack-disrupts-japans-idcf-cloud-used-by-govt-clients/

[11] @IT (ITmedia). 495社の仮想サーバを止めた IDCF ランサムウェア攻撃の全容 [The full picture of the IDCF ransomware attack that stopped 495 companies' virtual servers]. 29 October 2026. atmarkit.itmedia.co.jp/ait/spv/2610/29/news044.html (in Japanese).

[12] SecurityBrief Asia. Ransomware shifts to fewer groups as Thailand targeted. 2026. securitybrief.asia/story/ransomware-shifts-to-fewer-groups-as-thailand-targeted

[13] Censys. European Refrigeration Controller Exposure: A Second Attack Wave. November 2026. censys.com/blog/european-refrigeration-controller-exposure-sitrep

[14] BleepingComputer. France blames Iranian hackers for supermarket attacks that sparked fires. 9 November 2026. bleepingcomputer.com/news/security/france-blames-iranian-hackers-for-supermarket-attacks-that-sparked-fires

[15] The Record. France blames Iran for fridge cyberattacks. November 2026. therecord.media/france-blames-iran-for-fridge-cyberattacks

[16] Euronews. Cyberattaque des chambres froides de l'Établissement français du sang. 4 November 2026. fr.euronews.com/2026/11/04/cyberattaque-des-chambres-froides-de-letablissement-francais-du-sang-piratees (in French).

[17] Le Quotidien du Médecin. Des chambres froides de l'EFS victimes d'une cyberattaque d'un prestataire. November 2026. lequotidiendumedecin.fr/sante-societe/des-chambres-froides-de-letablissement-francais-du-sang-victimes-dune-cyberattaque-dun-prestataire (in French).

[18] CSIS. Significant Cyber Incidents. csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[19] Josefsson, S. and Liusvaara, I. "Edwards-Curve Digital Signature Algorithm (EdDSA)." RFC 8032, IRTF, 2017.

[20] Dworkin, M. "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC." NIST SP 800-38D, 2007.

[21] OWASP. Password Storage Cheat Sheet (PBKDF2-HMAC-SHA256: 600,000 iterations). cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html; Moriarty, K. et al. "PKCS #5: Password-Based Cryptography Specification Version 2.1." RFC 8018, IETF, 2017.

[22] Ongaro, D. and Ousterhout, J. "In Search of an Understandable Consensus Algorithm." USENIX ATC, 2014.

[23] Boonma, J. "The 2026 House of Representatives Election Case Study on heain-core." 11 November 2026 (companion paper).

Author and copyright holder: Mr. Jakkrit Boonma (Independent Researcher) | ORCID: 0009-0000-7165-3787 |

Email: jaggid.boonma@yahoo.co.th

© 2026 Jakkrit Boonma. All rights reserved. Ownership and copyright in this document belong to Mr. Jakkrit Boonma from the date of publication, under applicable copyright law.