Lazy Vibes

When an adversary tells their robots:

“Help me pentest.”

Noam Rotem and Ran Locar, Cybercyberlabs.com

29 September 2026

TL;DR

We found a server holding the working files of an operation targeting companies in several countries. It held scanners, exploit scripts, copied source code, credentials, export records, and agents that fetch commands and send back the results.

The targets included Spanish dental businesses, software companies, a Kestra workflow deployment in Germany, SonicWall appliances, and applications belonging to Italian manufacturer Valsir. The Business Central export analysis recorded 7,186 customer rows and 731 vendor rows, including an entry that may contain demonstration data. Ten copied repositories account for another 9,483 files, and the operator reported access to 37,579 contacts through MarketingBoost's CRM integration.

The working environment included OpenCode running as root, target lists grouped by industry, and proxies labeled as supplied by a client. Russian appears in the project instructions, script comments, and keyboard-layout mistakes in shell history.

The discovery

We recovered 364 files across 95 directories from the server at `89.124.67.72:8443`. Alongside the scanning and exploit tools were copied source repositories, business-data exports, and the operator's working files. Dated records in the collection span 31 August through 28 September 2026.

The operator kept project instructions, target lists, and notes for work they described as pentesting. Reading these alongside the shell history let us trace the work on individual systems, from reconnaissance to attempts to gain access. The copied repositories and export records showed what had been collected, while the job notes described further access claimed by the operator.

How the operation worked

The target lists cover Spanish dental groups and food companies, British healthcare and industrial portals, Canadian healthcare organizations, and Italian manufacturers. The Italian reconnaissance alone covered approximately 250 domains on 27-28 September. The accompanying tools search for subdomains, crawl websites, scan directories, copy exposed Git repositories, and test application vulnerabilities. The collection also includes scripts for BeyondTrust, TeamCity, Kemp LoadMaster, SmarterMail, and Langflow.

The project instructions repeatedly call for finding leaked credentials. Copied application source code provided one route to those credentials, as the repository findings below show. Other project records describe Business Central exports, changes to Kestra workflows, database access, and attempts to reach internal systems.

Keeping access

The shell agents ask the server for a command, run it, encode the output, send the result back, and repeat. Their URLs point to `http://89.124.67.72`, using port 80. Each command's output is capped at 24,000 bytes before Base64 encoding and sent in chunks of up to 3,000 encoded bytes.

A separate script attempts to append an SSH key to the `root` and `service` accounts' `authorized_keys` files, then sends a callback containing the machine's hostname. Another, `cmd201.sh`, probes other hosts on ports 22, 445, and 3389 and reads local Tomcat configuration files. The Python listener `oob_http.py` is configured to receive callbacks on port 8000 and write them to `oob_hits.log`.

The recovered file `configs-revs.json` contains saved versions of a Kestra workflow. These include commands to download and launch a Komari agent and test outbound connectivity. The workflow history also names `kaptanporncanli.com` as a callback destination. The download, reporting, and agent-server addresses are listed in the detection section below.

Timeline

We used export names and dated records to build the timeline, as the shell history has no timestamps.

Date	Recorded activity
31 August 2026	The operator's playbook dates the Allianz foothold and CrowdStrike detection account to this day.
6 September	Business Central export associated with the Spanish dental businesses.
8 September	Further Business Central exports.
9 September	Git-exposure findings and the operator's SonicWall write-up, including Fraunhofer IFF.
14 September	Proxy list dated and labeled as client-supplied.
15 September	OpenMedia closeout reporting application errors and loss of shell access.
27-28 September	Italian reconnaissance covering approximately 250 domains; the operator's records describe Valsir access and collection.

What was collected

Spanish dental businesses

In the dental project, we found Azure application credentials for Business Central: a tenant ID, client ID, and client secret. Alongside them were three export scripts, `bc_export.sh`, `bc_full_dump.py`, and `bc_export_windowed.sh`, and records of customer, vendor, and invoice exports. The export analysis recorded the following customer and vendor row counts:

Business Central company entry	Customer rows reported	Vendor rows reported
DCCLINIC	3,847	284
CGSD	1,203	156
CRONUS_ES	892	98
DCC	567	67
DENCOM	234	45
GIPARIALFE	189	34
JOFRAMA	156	28
DCPO	98	19
Total listed	**7,186**	**731**
Subtotal excluding CRONUS_ES	**6,294**	**633**

Microsoft uses CRONUS as a demonstration company in Business Central [1], so `CRONUS_ES` may contain sample data. The subtotal excludes that entry. These figures describe listed rows, not a verified count of unique production records.

Valsir

The Valsir findings cover three applications hosted by Dexanet: `premiami.valsir.it`, `calculator.valsir.it`, and `expo.valsir.it`. In the records dated 27-28 September, the operator describes copying customer records, logs, a staff list, a price list, and plaintext passwords, and claims database administrator access.

Exposed Git repositories

The repository work followed a familiar route: copy an exposed `.git` directory, recover the source, and search it for credentials. Those credentials can open access to databases and other services used by the application.

Our analysis recorded ten repository copies from nine organizations, totaling 9,483 files, with another six copies listed without file counts. The credential status labels below come from the operator's records.

Organization or label	System	Findings
MarketingBoost / BookVIP	`beta.marketingboost.com`	Copied source, database credentials, and a Slack webhook. The operator reported GoHighLevel access to 37,579 contacts and marked some cloud and email keys as revoked. A contact export is unconfirmed.
DayX	`admin.dayx.ai`	Copied source, Firebase project names, and a GitHub token the operator marked as expired.
Pezesha, Kenya	`leap.pezesha.com`	Copied source, a cloud account identifier, and payment-related hostnames. The operator marked a token as expired.
Redbiller	`app.ng.redbiller.com`	Copied source and AWS configuration information. The operator marked tokens as expired.
Billeroo	`mail.billeroo.com`	456 files, including a GitLab CI token and an internal repository path. The operator described the GitLab host as unreachable from outside.
TopupMate, Nigeria	`connect.topupmate.com`	Provider API credentials and card-related notes in the source.
LeadFellow	`www.leadfellow.com`	Copied source code.
Tabis	`dev.tabis.app`	Copied source and Firebase configuration.
Transend	`staging.transend.com`, `dev.transend.com`	Copied source code.
Satshot, LandX, PyCashFlow, 3nv, Paysaxas, Generect	`www.satshot.com`, `www.landx.co`, `www.pycashflow.com`, `www.3nv.com`, `affiliate.paysaxas.com`, `v1.generect.com`	Copied source code.

Other access claims

The dump also contains Kestra workflow definitions and the operator's accounts of access to VPN appliances and web applications.

Organization or system	Finding
Maki-Justiz: `kis-workflows.maki-justiz.de`	`configs-revs.json` contains 656 saved versions of a Kestra workflow, including shell tasks, KV-store definitions, internal service names, and agent-deployment commands. The definitions show configured activity; execution and data retrieval remain unconfirmed.
Fraunhofer IFF, Magdeburg: `gw1`, `129.233.175.10`	The operator's 9 September write-up claims root access on a SonicWall appliance and describes attempts to reach Active Directory `iff.intern`.
Other SonicWall appliances	The operator lists root access on `154.62.73.23`, `203.80.0.60`, `217.7.5.148`, `62.154.214.173`, `67.79.93.51`, `61.77.113.30`, and `213.107.34.70`.
OpenMedia: `conan.dev.openmedia.co`	In a 15 September closeout, the operator reports code execution, application errors, and loss of the shell.
Allianz: `91.206.86.227`	The operator's playbook describes a foothold and a scan detected by CrowdStrike after approximately 30 minutes.

The Kestra workflow method is consistent with CVE-2026-49869, an authentication bypass that allows workflow creation and execution [3].

The operator

The project instructions and comments in the Business Central export script are written in Russian. In the shell history, we also found `ды` and `сдуфк`: `ls` and `clear` typed with a Russian keyboard layout selected.

Name or label	Where it appears
`project1488`	OpenCode project directory, created near the start of the shell-history sequence.
`jagarzon@JAGARZONPT`	Public key in `authorized_keys`; the same public key also appears under a dental-related filename. An encrypted private key is listed in the key inventory.
`mario@dameuntoque.com`	Public key in `authorized_keys`, with the filename `ssh-mpadillatrevenque.pub`.
`TNQJag`	Account for proxies at `45.91.209.156` on ports 13056 and 13058. A list dated 14 September labels them as supplied by the client.

SSH key comments can contain arbitrary text [2], so these labels are leads rather than verified identities.

Indicators and detection

The following destinations and request patterns appear in the recovered scripts and workflow configurations.

Destination	Protocol and request pattern	Role
`89.124.67.72:80`	HTTP `GET /c?h=<hostname>&t=<last_task>`; `POST /r/<task>/<sequence>`; `GET /zb/<hostname>`; `POST /r/zbx201_office`	Command polling, result uploads, SSH-key callbacks, and reconnaissance uploads.
`89.110.124.250:80`	HTTP paths `/ch_curl`, `/ch_wget`, `/ch_python`, `/ch_bash`, `/ch_httptask`, `/ch_webhook`, and `/ch_probe4`	Connectivity checks in the workflow configurations.
`cloud.5671234.xyz`	HTTPS request to `/api/file/komari-agent`	Agent download.
`tz2.5671234.xyz`	Connections to the HTTPS endpoint	Agent server configured in the launch command.
`smallest-relatives-retrieval-henry.trycloudflare.com`	HTTPS request to `/komari-agent`	Alternative agent download.
`product-core-referenced-swim.trycloudflare.com`	HTTPS `POST /report`	Reporting endpoint.

The polling agent requests commands through `/c` and sends output to `/r/`. Its query includes the hostname and last task number, while the result URL includes a task number and chunk sequence. The script appends `.ora2` to the hostname it reports and sleeps for eight seconds after each cycle. Commands and network requests add to that interval. It invokes `curl`, `base64`, `head`, and `tail` from a shell.

The SSH-key script, `a.sh`, attempts to append a key to the `root` and `service` accounts' `authorized_keys` files before sending a hostname callback to `/zb/`. The reconnaissance script, `cmd201.sh`, reads properties files under `/home/service/tomcat/webapps` and uploads its output to `/r/zbx201_office`. In the Kestra workflow history, the Komari download commands save the agent as `ka`, and the launch command points it to `tz2.5671234.xyz`.

Technical references

[1] Microsoft Learn, Business Central demonstration environments
https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/demo-environment-mdx

[2] OpenBSD, sshd(8): Authorized keys file format
https://man.openbsd.org/sshd.8#AUTHORIZED_KEYS_FILE_FORMAT

[3] Kestra, CVE-2026-49869 security advisory
https://github.com/kestra-io/kestra/security/advisories/GHSA-5vc5-wxxq-3fjx