
# Lockbit5

Technical Analysis — Cti

**REVERSE-ENGINEERED REPORT**

**RansomLook** · ransomlook.io
File last modified: 2026-07-04

Sample SHA-256: `6d0166d181db1f6c381c3ff5fff4fe4106fbc17bc29316e3cf3f65136ee4803c`

# LockBit 5.0 (x64 hardened — "Corteva/Solstice" lure)

**Sample:** `6d0166d181db1f6c381c3ff5fff4fe4106fbc17bc29316e3cf3f65136ee4803c` **Classification:** Ransomware — LockBit 5.0 generation (x64 hardened build) **Report date:** 2026-06-21 **Basis:** binary-only reverse engineering

## 1. Key Judgements

- **Sample 3 is a LockBit 5.0-generation x64 hardened build** — full 5.0 obfuscator/packer (MBA + global-PRNG opaque predicates + per-string runtime crypto + import-by-hash), distinct from the older 3.0-base lineage. (High confidence.)
- **It ships a masquerade identity:** the file impersonates **"Corteva / Solstice Google Photos"** (a fake updater for a real agriculture brand) and **requests administrator elevation** via its manifest. This is a deliberate social-engineering / distribution disguise and the single most useful host IOC obtainable without execution. (High confidence.)
- **The decrypted payload was recovered and analysed offline.** Its crypto stack is **identified** (by constants/structure, not test-vector-validated) as **X25519 (key wrap) + ChaCha20-20 (file cipher) + Keccak-f1600/SHAKE256 (KDF/integrity)** — the modern LockBit 5.0 stack, and **distinct from Sample 1's** SSSE3-ChaCha(22)+RSA-1024, independently confirming the lineage split. (High confidence on primitive identity; end-to-end key-wiring inferred, not byte-traced.)
- **The payload's behaviour is now evidenced (no detonation needed):** multi-threaded **chunked/partial file encryption**, **RunPE process-hollowing (** `runpe_hollow_process` **; plaintext target string** `\defrag.\svchost` **)**, **ETW bypass**, **network self-propagation** (ARP + subnet + async port-scan), **event-log clearing**, **service/process termination**, and a **Geo/UI-language fence**. (High confidence — from the payload's own verbose dev strings + owner functions.)
- **Operator-origin signal — the payload avoids Russian-locale hosts:** it aborts when `GetUserDefaultUILanguage()==0x419` (the Russian/ru-RU LCID — a confirmed CIS-exclusion check) or when `GetUserGeoID()==0xC9` (raw value 201; its country is not asserted — Russia's GEOID is 203, so 201 is a distinct unconfirmed region). Combined with a configurable **operation-mode flag** ( `g_operation_mode` , static default `0x0A` ; modes local / network / all) and `;` -delimited target-path CLI arguments, this is a Russian-locale-aware ransomware build, consistent with the LockBit RaaS affiliate model (the dropped note recruits affiliates). (High confidence on the UILang check; GeoID country unverified. Recovered by Ghidra decompilation of the entry monolith.)
- **The embedded configuration was decrypted** (config-string crypto cracked = XOR incrementing `0x57++` keystream): recovered the **target drive scope** (A–Z + `ADMIN$` SMB), **exclusion lists** (folders/files/extensions), **explicit VM-disk targeting** ( `vhdx` / `avhdx` ), the **full CLI argument set** ( `-fast` / `-full` / `-nomutex` / `-d` / `-b` / `-m` /…), **operation-mode keywords** ( `all` / `local` / `net` ), and the note filename `ReadMeForDecrypt.txt` . (High confidence — offline, *`scripts/35_decode_config.py`* .)
- **Ransom note + three onions are MBA-encoded and assembled at runtime** (not under the static XOR config); recovered from an authorized detonation ( `ReadMeForDecrypt.txt` ). DLS `lockbitapt67g6rw…onion` , chat `lockbitsuppyx2jeg…onion` , affiliate `lockbitfbinpwhby…onion` ; version tag `ChuongDong v1.06 | x64` . The note brands as "LockBit 5.0 … since 2019" and recruits affiliates. (High confidence — primary evidence from victim disk.)
- **There is no monolithic packed payload at the loader level**; protection is per-string on-demand decryption. (High confidence.)

- **Confirmed by live detonation (isolated VM, x64dbg):** the ransom note (3 onions + version) was read **from the malware's own process memory**; `defrag.exe` **was executed** (RunPE target); and **network drives** `N:` **and** `M:` **were mounted and encrypted**. The active SMB port-scan host-discovery did **not** execute (no reachable peer on the isolated host-only lab), so the scan port was not observed. (Direct observation.)

---

## 2. Actor / Tooling Assessment

The operator is fielding the **modern LockBit 5.0 toolchain** and customising each build: - **Per-build masquerade:** Sample 3 carries a "Corteva/Solstice Google Photos" disguise baked into resources — indicating the actor tailors lure metadata per campaign/target while reusing the protected 5.0 core. - **Anti-triage priority:** MBA + global-PRNG opaque predicates + import-by-hash + per-string runtime crypto mean automated unpackers and "detonate-and-scrape" sandboxes recover almost nothing from the file at rest. - **Admin-by-design:** the `requireAdministrator` manifest shows the operator expects the victim (or an exploited delivery chain) to launch with elevation — consistent with a lure that a user double-clicks expecting a software "update".

Detection content built for LockBit 3.0 (config-blob YARA, residual templates, old onion sets) **will not fire** on this 5.0-generation build.

---

## 3. Capability Summary (evidenced)

| Capability | Status |
|---|---|
| Masquerade / fake product identity | **Confirmed** — Corteva / Solstice Google Photos (resources) |
| Admin elevation request | **Confirmed** — manifest `requireAdministrator` |
| MBA obfuscation | **Confirmed** |
| Global-PRNG opaque predicates | **Confirmed** |
| Per-string runtime decryption + cache | **Confirmed** — `sub_1400027A0`, 28 IDs / 78 sites |
| Import-by-hash (empty IAT) | **Confirmed** |
| Encrypted on-file string/config pool | **Confirmed** — `.rdata` ≈ 541 KB, ent ≈ 8.00 |
| Monolithic packer (loader) | **Absent** — `.rdata` 0 % in-place decrypt |
| **File-encryption cipher (payload)** | **Confirmed — ChaCha20 (standard, 20-round, 256-bit)** |
| **Key wrap (payload)** | **Confirmed — X25519 (Curve25519 ECDH)** |
| **KDF / integrity (payload)** | **Confirmed — SHAKE256 / Keccak-f1600** |
| **Chunked / partial encryption** | **Confirmed** — `EncryptPartly`, chunk map + FILEMETA footer |
| **RunPE process-hollowing → defrag.exe / svchost** | **Confirmed** — `runpe_hollow_process`; plaintext target string `\defrag.\svchost`; `defrag.exe` **execution observed live during detonation** |
| **ETW bypass** | **Confirmed** — `"Etw not patched!"` at payload startup |
| **Network self-propagation (code present)** | **Confirmed in code** — spreader `FUN_1400CC110` reachable from `payload_main`; ARP (`GetIpNetTable`) + subnet enum + async ConnectEx/IOCP port-scan + `mpr.dll` (dev strings). **Active scan not observed executing** (isolated lab, no reachable peer). Mapped network-drive (`N:` / `M:`) encryption **observed live** |
| **Event-log clearing** | **Confirmed** — EvtOpenSession channel enumeration |
| **Service / process kill** | **Confirmed** — SCM enum + process-kill failed-cache |
| **Geo / UI-language fence** | **Confirmed** — abort on UILang `0x419` (Russian LCID, CIS-exclusion) / GeoID `0xC9` (raw 201, country unverified) |
| **Operation-mode flag** | **Confirmed** — `g_operation_mode` default `0x0A`; modes: 0xA/0xB local, 0xC net (network — confirmed live), 0xE undetermined; keywords all/local/net |
| **CLI / target arguments** | **Confirmed** — `;`-delimited wide path list (`/`, `\` normalized) |
| **Recovery inhibition (VSS shadow delete)** | **Confirmed** — dynamic `vssapi.dll` + `ole32.dll`, COM `IVssBackupComponents` (no shell) |

| Capability | Status |
|---|---|
| Persistence / mutex / self-delete | **Not found** (no strings even encrypted-adjacent; not asserted) |
| Embedded config (exclusions/CLI/modes/drives) | **Recovered** — XOR `0x57++` keystream cracked ( `scripts/35_decode_config.py` ) |
| VM-disk targeting | **Confirmed** — `vhdx` / `avhdx` in target list |
| Onions / note body | **Recovered from detonation** (runtime-MBA-assembled, not static) — 3 onions below |
| Public key (X25519) | runtime material (not embedded) |

## 4. Behavioural Profile (evidenced from the decrypted payload)

Unlike the prior loader-only assessment, the **decrypted payload exposes behaviour statically** (it is a verbose/debug build with left-in dev strings). Confirmed, no detonation required:

- **Impact:** multi-threaded **chunked / intermittent file encryption** (ChaCha20 body cipher, per-file X25519-wrapped key, per-chunk SHAKE256-derived keystream + Keccak integrity hash, FILEMETA footer). Ransom note `ReadMeForDecrypt.txt` . → **T1486**.
- **Defense evasion: RunPE process-hollowing** ( `runpe_hollow_process` ; plaintext target string `\defrag.\svchost` ) ( `T1055.012` ); **ETW patching** at startup ( `T1562.006` ); **Windows event-log clearing** ( `T1070.001` ).
- **Inhibit recovery: VSS shadow-copy deletion** via dynamically-loaded `vssapi.dll` + `ole32.dll` (COM `IVssBackupComponents` , no `vssadmin` / `wmic` shell — stealthier, harder to catch on command-line telemetry) ( `T1490` ); plus **service stop + process termination** with a failed-kill cache ( `T1489` ).
- **Propagation (SMB lateral movement — code-evidenced):** the payload contains a network spreader ( `FUN_1400CC110` , reachable from `payload_main` ): host discovery via `GetIpNetTable` (ARP) + subnet enumeration → `ws2_32` async **ConnectEx/IOCP port scan** → file encryption on `ADMIN$` /SMB shares (dev string "Starting search on share %ls") feeding the encryption pipeline ( `T1021.002` / `T1135` ). **Live-observed:** mapped network drives `N:` / `M:` mounted + encrypted. **Not observed:** the active socket port-scan (no reachable peer in the isolated lab). No PsExec self-copy evidenced. **Geo + UI-language fence** before running ( `T1614.001` ).

What is still **not** asserted (genuinely runtime-only): the onion DLS endpoints, the full ransom-note text, the victim/campaign X25519 public key, and the exact target-extension / exclusion lists. Persistence mechanism and shadow-copy/backup-deletion commands were not located in the recovered strings and are not claimed.

## 5. Detection & Hunting Guidance

**On-disk / static:** - Hash-block SHA-256 / MD5. - **Masquerade hunt:** files presenting as `Solstice Google Photos.exe` / CompanyName `Corteva` / ProductName "Solstice Google Photos" that are **not** signed by the legitimate vendor; flag the combination of that version-info with a `requireAdministrator` manifest and an empty import table. - **Structural hunt** (family-level): PE32+ with empty IAT, a single very-high-entropy `.rdata` (~0.5 MB, ent ≈ 8.0), and a `.data` virtual size in the multi-MB range over a ~1 KB raw size.

**Behavioural / runtime (EDR):** the payload behaviour is now known — hunt these chains directly: - A process (esp. one masquerading as "Solstice Google Photos") that performs **RunPE process-hollowing** (CreateProcess suspended → WriteProcessMemory section writes → SetThreadContext/

ResumeThread) into `defrag.exe` (execution observed live) / svchost; plaintext target string `\defrag.\svchost`. High-severity. - **ETW provider tampering** at process start, followed by **Windows event-log channel clearing** (EvtOpenSession / EvtClearLog). - **Shadow-copy deletion via COM** (process loads `vssapi.dll` + `ole32.dll` and calls `IVssBackupComponents` directly) — **will not appear as a `vssadmin` / `wmic` / `bcdedit` command line**; hunt on the `vssapi.dll` load by a non-backup process instead. - **Mass file modification with a trailing FILEMETA footer** + ransom note `ReadMeForDecrypt.txt` dropped per directory. - **Internal port-scanning / ARP-table enumeration / SMB share access** from the same process (lateral spread). - **Service-control enumeration + bulk process termination** preceding encryption. - IOCs that remain runtime-only (onions, note text, public key) → still capture **process memory** of a contained sample.

**Network:** no static C2/onion to block from this file; pivot on the **internal port-scan / ARP spread** behaviour instead.

---

## 6. Operational Comparison with the 3.0-base lineage

| Defender concern | S1 (3.0-base) | S3 (5.0, this report) |
|---|---|---|
| Harvest config from file | Yes | **Yes — operational config (exclusions/CLI/modes/drives) decrypted; onion/note/key not embedded** |
| 3.0 detection content effective | Yes | **No** |
| Static unpack yields payload | Yes (APLib blob) | **No loader unpack (per-string); payload recovered by emulation** |
| Distinctive host IOC at rest | onions/note | **masquerade identity + structural** |
| Time-to-IOC | Low | **Moderate (lure metadata + decrypted config help)** |

S3's lure metadata + the now-decrypted operational config give defenders concrete on-disk hunts that do not require live detonation.

---

## 7. Analytical Confidence & Gaps

- **High confidence:** LockBit 5.0-generation x64 identity; obfuscation architecture; loader decryptor + 28-ID inventory; absence of a monolithic packer; masquerade identity; **payload crypto stack (X25519 + ChaCha20-20 + Keccak/SHAKE256) + key-derivation chain; payload file-encryption pipeline; payload behaviour map; decrypted operational config** (all from the decrypted payload, offline).
- **Gap (acknowledged, not hedged):** the **runtime configuration** — onion endpoints, ransom-note body, victim/campaign **public key**, target-extension / exclusion lists — **plus the command-line interface and behaviour-flag map**, which are inlined into the payload's 83 KB MBA entry monolith ( `payload_main 0x140113F60` , Hex-Rays-undecompilable) and materialise at runtime. All share the same MBA + per-record + runtime-decode armor. Re-confirmed unreachable statically four independent ways (loader + payload emulation captures, MBA accessor analysis, encrypted-but-visible `.rdata` string sweep). Closing it needs an API-faithful emulator extension or contained-detonation memory capture. **The file-cipher identity gap is now CLOSED** (was the prior report's main open item).

---

## 8. Recommendations

1. **Block** the file hashes; deploy both the masquerade hunt (Corteva/Solstice version-info + `requireAdministrator` + empty IAT) and the structural family hunt.
2. **Alert** users/helpdesk to a "Solstice Google Photos update" lure theme; treat unexpected admin-elevation prompts from such a file as malicious.
3. **Update IR playbooks** for LB 5.0: assume no static config; add contained detonation + process-memory forensics.
4. **Re-validate** any LockBit detection content keyed on 3.0 artefacts — ineffective here.

---

## 9. Indicators of Compromise

| Type | Value |
|---|---|
| SHA-256 | `6d0166d181db1f6c381c3ff5fff4fe4106fbc17bc29316e3cf3f65136ee4803c` |
| MD5 | `bb7c2ca539a63f5828f053cc6ddb6680` |
| Size | 728,968 bytes |
| PE | x86-64, ImageBase `0x140000000`, EP `0x140013250`, spoofed TS 2010-09-27 |
| Masquerade | CompanyName `Corteva`; Product/FileDescription `Solstice Google Photos`; OriginalFilename `Solstice Google Photos.exe`; Comments "Solstice Google Photos Update"; LegalTrademarks "Corteva TM"; FileVersion `1,45,1078,558`; manifest `requireAdministrator` |
| Structural | empty IAT; `.rdata` ≈ 541 KB at ent ≈ 8.00; `.data` virtual `0x50CEC0` over raw `0x400` |
| Code-level (loader) | string decryptor `sub_1400027A0` (28 IDs / 78 sites) |
| Host (payload behaviour) | RunPE hollowing (target string `\defrag.\svchost`); drops note **`ReadMeForDecrypt.txt`**; ETW patch + event-log clear; **VSS shadow delete via COM** (`vssapi.dll` + `ole32.dll`); internal ARP/port-scan; SCM enum + bulk process kill |
| Payload crypto | X25519 + ChaCha20-20 + Keccak-f1600/SHAKE256 |
| Embedded config | exclusions (`$Recycle.Bin`, `Hyper-V`, `System Volume Information`,...), exts `exe/lnk/dll/cpl/sys`, **targets** **`vhdx`** / **`avhdx`**, drives A–Z + `ADMIN$`, modes `all/local/net`, note `ReadMeForDecrypt.txt` |
| Detection | YARA `lockbit5_sample3.yar` (4 rules, validated loader/payload, 0 FP on S1) |
| Onion — DLS/leak | `lockbitapt67g6rwzjbcxnww5efpg4qok6vpfeth7wx3okj52ks4wtad.onion` |
| Onion — chat | `lockbitsuppyx2jegaoyiw44ica5vdho63m5ijjlmfb7omq3tfr3qhyd.onion` |
| Onion — affiliate | `lockbitfbinpwhbyomxkiqtwhwiyetrbkb4hnqmshaonqxmsrqwg7yad.onion` |
| Version tag | `ChuongDong v1.06 \| x64` |
| Note | `ReadMeForDecrypt.txt` (full text `artifacts/RANSOM_NOTE.txt`) |
| Network (onions) | from detonated note (runtime-assembled); also pivot on internal port-scan/ARP spread |