E11. Archive lineage and configuration rotation

Ilja Krasnjanski
24 October 2026 · Edited evidence report
Historical evidence through 24 July 2026; later engineering checks identified separately.

This report synthesizes the cited case records. Exhibits distinguish retained artifact excerpts from secondary analytical records and claims whose original inputs are unavailable. Excerpts may be redacted or reformatted; extraction methods and limitations are stated locally. Fingerprints identify inputs, not the truth of their claims. Bracketed S labels identify the analysis records listed at the end.

Historical material

The ECHOES delivery-history record describes four archive revisions in a repository created in March 2026. The preserved lure structure includes the same decoy images and an encoding scheme, with changes to retrieval configuration and later staging behavior. No archive was launched to prepare this report. [S1]

Revision sequence

- 5 March 2026, 06:17 UTC, commit `03f1795d`: the earliest recorded retrieval configuration and task tag DDD.
- 17 March, 05:14 UTC, commit `ded13153`: a different account/repository destination, retaining DDD and changing scheduled-task timing.
- 25 March, 03:54 UTC, commit `b209f365`: another repository destination, task tag WORD and an added VBS persistence layer.
- 25 March, 13:29 UTC, commit `4b6ea6b2`: a further destination change and a new access token; the staging is otherwise unchanged from `b209f365`.

Commit identifiers and dates are reported by the historical note; the retained archives support the content comparison, but the original remote history is not retained. The history supports continuity of the staging kit with changing retrieval locations. The later persistence addition also means the revisions should not be described as differing only in configuration. Embedded access tokens and archive-password values are not reproduced. [S1]

Missing final stage

The referenced final PowerShell payloads were unavailable through the unauthenticated retrieval routes examined. Recovered operator credentials were not used to obtain them. The archive lineage can therefore establish staging and configuration relationships, but cannot supply capabilities for the missing final payload. It should not be assumed to be the same payload as the VSIX or ClickFix branches.

Account-status limitations

The record discusses an account returning 404 while its name remained unavailable for registration. That pattern supported a suspension hypothesis, with acknowledged alternatives. It is not a provider confirmation and does not establish the current account state. Nearby numeric account identifiers were also examined without a discriminating sibling-account pattern. Registration adjacency alone is not evidence of coordinated account creation.

Assessment

The strongest evidence is the preserved revision sequence and repeated staging structure. Claims about who controlled an account, why it became unavailable, or what the unrecovered payload would do require additional evidence. E14 separately covers the poster's recorded provenance metadata.

Exhibits

The retained ECHOES material comprises three historical archives, their LNK members and the analyst-decoded stage-two scripts (each file named after a commit prefix), plus the current archive and its decoded stage two. The mapping of the current archive to commit `4b6ea6b2`, and all commit dates and times, come from the analysis note; no clone or commit JSON of the delivery repository is retained (see the final list). Archive members were listed, never extracted or opened. The archive password is redacted from every command.

Exhibit E11-1. Same three decoy images in all four archives; only the LNK changes

Artifact: Historical archive rar-03f1795d · 2292670 bytes · SHA-256
`4ff03731d2061ad2f50da9f63dc1481374908d5bc837c86d0c7574d23b23a37b`
Artifact: Historical archive rar-ded13153 · 2292622 bytes · SHA-256
`2bd4cfd495fdcad6d7b2adaedc31614ca2984ea1246aed7608c339eaa82eb978`
Artifact: Historical archive rar-b209f365 · 2294542 bytes · SHA-256
`11bf34ccce585fe051abaa8d01ba1b29e2d44727c070b56ab0dd84a9dc9f91b2`
Artifact: Current archive ECHOES_OF_THE_UNBORN_SUN.rar · 2294526 bytes · SHA-256
`7db6789c09e29305c728bf3d7b94c5ef1c3e13eef1b321ee52d3ae3997731f56`
Location: RAR5 file headers (member names and stored CRC32), header-encrypted archives
Extraction: `for f in rar-03f1795d.rar rar-ded13153.rar rar-b209f365.rar ECHOES_OF_THE_UNBORN_SUN.rar; do echo "== $f"; lsar -p [REDACTED: archive password] -L "$f" | grep -E "^ Name:|RAR5CRC32:" | paste - - | awk '{print $2, $3, $4, $5, $6, $7, $8}' | sed 's/ */ /g'; done`
Supports: "The preserved lure structure includes the same decoy images"

```
== rar-03f1795d.rar
Lyra.png RAR5CRC32: 0x9b8aceaf
Solace.png RAR5CRC32: 0xcfeb813a
ECHOES OF THE UNBORN SUN.pdf.lnk RAR5CRC32: 0xcd5d161c
Kael.png RAR5CRC32: 0x9edff8e3
== rar-ded13153.rar
Lyra.png RAR5CRC32: 0x9b8aceaf
Solace.png RAR5CRC32: 0xcfeb813a
ECHOES OF THE UNBORN SUN.pdf.lnk RAR5CRC32: 0xb3515c98
Kael.png RAR5CRC32: 0x9edff8e3
== rar-b209f365.rar
Solace.png RAR5CRC32: 0xcfeb813a
Kael.png RAR5CRC32: 0x9edff8e3
ECHOES OF THE UNBORN SUN.pdf.lnk RAR5CRC32: 0x844da265
Lyra.png RAR5CRC32: 0x9b8aceaf
== ECHOES_OF_THE_UNBORN_SUN.rar
Lyra.png RAR5CRC32: 0x9b8aceaf
Solace.png RAR5CRC32: 0xcfeb813a
ECHOES OF THE UNBORN SUN.pdf.lnk RAR5CRC32: 0x5a66790f
Kael.png RAR5CRC32: 0x9edff8e3
```

Trailing spaces on the PNG lines are removed. The three PNG CRCs (and their sizes, 816478, 862883 and 605016 bytes in `lsar -l`) are identical in every revision; only the LNK CRC differs.

Exhibit E11-2. One stage-one decoding key in all four LNK launchers

Artifact: LNK from rar-03f1795d · 420736 bytes · SHA-256
`9c7b507eba958ecee653ff42f13cf4e084f49cd38985d3abfd77ab2bfa40b4e2`
Artifact: LNK from rar-ded13153 · 420512 bytes · SHA-256
`bbbeadae38bf1406f331c9e42ab49cbdd22f503cd9caecb6b390964bafa1b56f`
Artifact: LNK from rar-b209f365 · 429662 bytes · SHA-256
`b80028534a414f199992a49610f8d5ffa94f8098d5a820653f68b8a9eb51e3ca`
Artifact: LNK from the current archive · 429728 bytes · SHA-256
`a44068e9758262a65861b91f2b00d0a3eca019d3b35543dd60c1c7f2e0ba1952`
Location: fourth UTF-16LE string (the command-line argument), key-assignment segment
Extraction: `for f in lnk-03f1795d.lnk lnk-ded13153.lnk lnk-b209f365.lnk "ECHOES OF THE UNBORN SUN.pdf.lnk"; do strings -el "$f" | sed -n 4p | grep -o '\$Apkengsidefg = [^;]*;' | sha256sum; done`
Supports: "an encoding scheme" shared across revisions (continuity of the staging kit)

```
b2f7dbb83b3189754c7b57fa8bd6d3f105c24088e1b08c0deb154ef7dc33d303  -
b2f7dbb83b3189754c7b57fa8bd6d3f105c24088e1b08c0deb154ef7dc33d303  -
b2f7dbb83b3189754c7b57fa8bd6d3f105c24088e1b08c0deb154ef7dc33d303  -
b2f7dbb83b3189754c7b57fa8bd6d3f105c24088e1b08c0deb154ef7dc33d303  -
```

The key literal itself is not shown; the identical hash of the assignment segment `$Apkengsidefg = \"[REDACTED: stage-1 decoding key]\";` demonstrates that all four launchers carry the same key while the encoded payload numbers that precede it differ.

Exhibit E11-3. Task tag and VBS layer, revision by revision

Artifact: Decoded stage two, 03f1795d · 1629 bytes · SHA-256
`5e405ef279e7d33d375a7427361bce07936dd2258f02f3991441fb3e1c1cf2a2`
Artifact: Decoded stage two, ded13153 · 1603 bytes · SHA-256
`83c0b5f3db2e4ced741ee641a7a775fd949e769ed51ee8584229a862d268939e`
Artifact: Decoded stage two, b209f365 · 2943 bytes · SHA-256
`f5c729ce6f06d4c6f6d98cc1e23547c25f1b6207fdc347ed6cdbb60dad1203ae`
Artifact: Decoded stage two, current archive · 2961 bytes · SHA-256
`70ee2f3ec1370960b225fd86cbe92a9477a788fc276567af2bd8c50e6744ae71`
Location: whole files (single-line scripts)
Extraction: `grep -o 'Task-[A-Z]*-' stage2-03f1795d.decoded.ps1 stage2-ded13153.decoded.ps1 stage2-b209f365.decoded.ps1; grep -c 'whale.vbs' stage2-03f1795d.decoded.ps1 stage2-ded13153.decoded.ps1 stage2-b209f365.decoded.ps1; grep -o 'Task-[A-Z]*-' firefox_stage2.decoded.ps1; grep -c 'whale.vbs' firefox_stage2.decoded.ps1`
Supports: task tag DDD in the first two revisions, WORD later; the VBS persistence addition

```
stage2-03f1795d.decoded.ps1:Task-DDD-
stage2-ded13153.decoded.ps1:Task-DDD-
stage2-b209f365.decoded.ps1:Task-WORD-
stage2-03f1795d.decoded.ps1:0
stage2-ded13153.decoded.ps1:0
stage2-b209f365.decoded.ps1:1
Task-WORD-
1
```

The last two lines are the current archive's stage two (`firefox_stage2.decoded.ps1`). The VBS reference is already present in b209f365, not only in the final revision (see Exhibits E11-3 and E11-6).

Exhibit E11-4. 03f1795d to ded13153: credential, destination and timing only

Artifact: Decoded stage two, 03f1795d · 1629 bytes · SHA-256
`5e405ef279e7d33d375a7427361bce07936dd2258f02f3991441fb3e1c1cf2a2`
Artifact: Decoded stage two, ded13153 · 1603 bytes · SHA-256
`83c0b5f3db2e4ced741ee641a7a775fd949e769ed51ee8584229a862d268939e`
Location: statements 2, 3 and 23 after splitting on `;`
Extraction: `diff <(tr ';' '\n' < stage2-03f1795d.decoded.ps1) <(tr ';' '\n' < stage2-ded13153.decoded.ps1)`
Supports: "17 March … a different account/repository destination, retaining DDD"

```
2,3c2,3
< $tkf="[REDACTED: GitHub personal access token]"
< $bstr="h"+"tt"+"p"+"s"+…[REDACTED: obfuscated raw-content URL, account A / repository 1]…
---
> $tkf="[REDACTED: GitHub personal access token]"
> $bstr="h"+"t"+"tp"+"s"+…[REDACTED: obfuscated raw-content URL, account B / repository 2]…
23c23
<  $trigger = New-ScheduledTaskTrigger -Once -At (Get-Date).AddMinutes(30) -RepetitionInterval\
 (New-TimeSpan -Minutes 2100)
---
>  $trigger = New-ScheduledTaskTrigger -Once -At (Get-Date).AddMinutes(20) -RepetitionInterval\
 (New-TimeSpan -Minutes 1440)
```

Tokens and the split-string URLs (which spell the account and repository names) are redacted; the account names are not reproduced. Trigger lines hard-wrapped. Every other statement is identical.

Exhibit E11-5. b209f365 to the current archive: credential and destination only

Artifact: Decoded stage two, b209f365 · 2943 bytes · SHA-256
`f5c729ce6f06d4c6f6d98cc1e23547c25f1b6207fdc347ed6cdbb60dad1203ae`
Artifact: Decoded stage two, current archive · 2961 bytes · SHA-256
`70ee2f3ec1370960b225fd86cbe92a9477a788fc276567af2bd8c50e6744ae71`
Location: statements 7–8 after splitting on `;`
Extraction: `diff <(tr ';' '\n' < stage2-b209f365.decoded.ps1) <(tr ';' '\n' < firefox_stage2.decoded.ps1)`
Supports: (contradicts) "13:29 UTC, commit 4b6ea6b2: a further destination change and an additional VBS persistence layer"

```
7,8c7,8
< $tkf="[REDACTED: GitHub personal access token]"
< $bstr="h"+"t"+"t"+"p"+"s"+…[REDACTED: obfuscated raw-content URL, account B / repository 3]…
---
> $tkf="[REDACTED: GitHub personal access token]"
> $bstr="h"+"t"+"tp"+"s:"+…[REDACTED: obfuscated raw-content URL, account A / repository 3]…
```

This is the entire diff: the final revision changes only the token and the destination. The elevation check, hidden relaunch and `whale.vbs` layer were all introduced at b209f365.

Exhibit E11-6. The VBS persistence layer as written by b209f365

Artifact: Decoded stage two, b209f365 · 2943 bytes · SHA-256
`f5c729ce6f06d4c6f6d98cc1e23547c25f1b6207fdc347ed6cdbb60dad1203ae`
Location: statements 16–19 and 29–33 after splitting on `;`
Extraction: `tr ';' '\n' < stage2-b209f365.decoded.ps1 | sed -n '16,19p;29,33p'`
Supports: the "additional VBS persistence layer" and the WORD task tag

```
$ppp = Join-Path ($env:AppData) "wale.ps1"
 $Sch = Join-Path $env:AppData "whale.vbs"
 $whaleContent = "Dim asdfasdfasdf`nSet asdfasdfasdf = CreateObject(…[elided: VBS launcher body that\
 starts hidden PowerShell on wale.ps1]…"
 Set-Content -Path $Sch -Value $whaleContent -Encoding ASCII
 $action = New-ScheduledTaskAction -Execute 'wscript.exe' -Argument "`"$Sch`""
 $trigger = New-ScheduledTaskTrigger -Once -At (Get-Date).AddMinutes(5) -RepetitionInterval\
 (New-TimeSpan -Minutes 60)
 $triggerBoot = New-ScheduledTaskTrigger -AtStartup
 $settings = New-ScheduledTaskSettingsSet -Hidden
 Register-ScheduledTask -TaskName "OneDrive Reporting Task-WORD-1-4-21-53529385-53453634-5354364\
59-55601" -Action $action -Trigger $trigger,$triggerBoot -Settings $settings
```

The VBS body is elided so that the excerpt is not a working launcher; long lines are hard-wrapped. The earlier revisions instead schedule `PowerShell.exe` directly, with no boot trigger.

Claims without a retained primary artifact

- The delivery repository's creation in March 2026, and the four commit dates and times (5 March 06:17, 17 March 05:14, 25 March 03:54 and 13:29 UTC): no clone, bundle or commit JSON of the delivery repository is retained. The commit prefixes survive only in the file names, and the current archive's attribution to `4b6ea6b2` rests on the analysis note.
- Unavailability of the final PowerShell payloads (`bpvme.ps1`, `coks.ps1`) via unauthenticated routes, and the decision not to use recovered tokens: recorded only in the note.
- Account status (404 while the name stayed unavailable for registration), the suspension hypothesis and the adjacent-ID check: these were HTTP observations; no responses were saved.
- The decoded stage-two files are analyst derivations of the LNK command lines; the decoding was not re-run for this exhibit set (the shared key in E11-2 and the LNK size increase at b209f365, 420 KB to 429 KB, are consistent with them).

Exhibit inputs

Retained inputs identified by size and SHA-256. These include artifacts and analytical records; each exhibit identifies its evidence type and extraction limitations. The files themselves are not distributed.

Historical ECHOES archive, commit prefix 03f1795d · 2,292,670 bytes

`SHA-256 4ff03731d2061ad2f50da9f63dc1481374908d5bc837c86d0c7574d23b23a37b`

Historical ECHOES archive, commit prefix ded13153 · 2,292,622 bytes

`SHA-256 2bd4cfd495fdcad6d7b2adaedc31614ca2984ea1246aed7608c339eaa82eb978`

Historical ECHOES archive, commit prefix b209f365 · 2,294,542 bytes

`SHA-256 11bf34ccce585fe051abaa8d01ba1b29e2d44727c070b56ab0dd84a9dc9f91b2`

Current ECHOES archive (attributed to 4b6ea6b2) · 2,294,526 bytes

`SHA-256 7db6789c09e29305c728bf3d7b94c5ef1c3e13eef1b321ee52d3ae3997731f56`

LNK launcher from 03f1795d · 420,736 bytes

`SHA-256 9c7b507eba958ecee653ff42f13cf4e084f49cd38985d3abfd77ab2bfa40b4e2`

LNK launcher from ded13153 · 420,512 bytes

`SHA-256 bbbeadae38bf1406f331c9e42ab49cbdd22f503cd9caecb6b390964bafa1b56f`

LNK launcher from b209f365 · 429,662 bytes

`SHA-256 b80028534a414f199992a49610f8d5ffa94f8098d5a820653f68b8a9eb51e3ca`

LNK launcher from current archive · 429,728 bytes

`SHA-256 a44068e9758262a65861b91f2b00d0a3eca019d3b35543dd60c1c7f2e0ba1952`

Decoded stage two, 03f1795d · 1,629 bytes

`SHA-256 5e405ef279e7d33d375a7427361bce07936dd2258f02f3991441fb3e1c1cf2a2`

Decoded stage two, ded13153 · 1,603 bytes

`SHA-256 83c0b5f3db2e4ced741ee641a7a775fd949e769ed51ee8584229a862d268939e`

Decoded stage two, b209f365 · 2,943 bytes

`SHA-256 f5c729ce6f06d4c6f6d98cc1e23547c25f1b6207fdc347ed6cdbb60dad1203ae`

Decoded stage two, current archive · 2,961 bytes

`SHA-256 70ee2f3ec1370960b225fd86cbe92a9477a788fc276567af2bd8c50e6744ae71`

Source records and fingerprints

SHA-256 identifies the reviewed source bytes, not acquisition time or every artifact described. Restricted originals are not reproduced.

[S1] ECHOES archive and configuration history · 5,681 bytes

`SHA-256 fc18853ef5c344179c451ea26eac12266e7f643b7525d2e812978c1ecdcde60f`