CHECK POINT

EXPOSURE MANAGEMENT

THREAT INTELLIGENCE REPORT

HYFLOCK

From Underground Recruitment to Public Extortion

October 19, 2026

Ransomware operation profile · Malware and cryptographic analysis · Indicators and MITRE ATT&CK mapping

Confidential | Check Point Copyright © All Rights Reserved 2026

Table of Contents

Executive Summary 3

01 HYFLOCK Background and Chronology 4

1.1 Recruitment proposition 5

1.2 Public victim activity 5

02 Operating Model, Branding and Victim Communications 6

2.1 Earlier affiliate platform 6

2.2 Victim-facing workflow 6

2.3 Branding continuity 7

03 Ransomware Architecture and Execution Chains 8

3.1 April and July: the earlier Rust/Nishi generation 9

3.2 October execution chain 9

04 Capability and Evidence Matrix 10

05 Cryptographic and File-Processing Assessment 12

5.1 Key generation and protection 12

5.2 Encrypted-file structure 12

5.3 April and July cryptographic continuity 14

06 April/July-to-October Evolution 14

07 MITRE ATT&CK Mapping 16

A Sample and Indicator Appendix 18

Contact Us 19

Confidential | Check Point Copyright © All Rights Reserved 2026

OVERVIEW

Executive Summary

6+ mo	**8**	**4**	**73**
from first underground promotion to first public victim claims	victim claims published in a single batch on October 13	ransomware generations analyzed: April, July, earlier October and October 17	CRC-valid members recovered from seven encrypted Office files without a key

KEY JUDGMENT

HYFLOCK is an evolving ransomware operation that combines a developed technical foundation with uneven implementation quality. Initially promoted as an affiliate-oriented Ransomware-as-a-Service platform, the group later changed its stated positioning, describing HYFLOCK as "not traditional RaaS" and portraying participants as part of a more integrated internal organization. **We treat this as a change in public messaging, not as proof that the earlier affiliate model or externally recruited participation ceased.**

Through our investigation, we've seen HYFLOCK progress through four visible phases: underground promotion beginning in late March 2026, structured recruitment during May and June, and public extortion activity beginning with eight victim claims on October 13. This indicates a period of development and recruitment before public victim publication, but does not establish when individual intrusions began.

The samples we analyzed show a developed Rust/Nishi ransomware core as early as April, with the July generation remaining closely related. October introduces the first substantial change in orchestration and deployment. The earlier October chain uses a Go carrier with a revised Rust payload, while the October 17 build returns to a standalone Rust form that stages a copy of itself for background execution. **October therefore represents the first substantial technical evolution we observed, but not a single fixed packaging model.**

Across the October builds, we confirmed encryption, ransom-note deployment, scheduled-task use, network-share activity, and recovery-inhibition attempts. The October 17 sample provides stronger runtime confirmation of several of these behaviors, including successful scheduled-task registration and extensive file and administrative-share processing. GPO, WinRM, and WMI/DCOM deployment remain implemented capabilities, but the sample did not demonstrate successful domain-wide propagation. Newer operator statements provide context for the background-execution design, although claims such as RDP-session resilience, BYOVD-based security-tool killing and multiple-instance reliability remain unverified or only partially corroborated.

Our analysis also identified uneven cryptographic and file-processing behavior. The earlier October build contains a defect that may cause permanent data loss even when the correct key is available. In the October 17 build, larger collected files had only their first 4,096 bytes encrypted, allowing us to recover 73 CRC-valid members from seven encrypted Office files without a key. **This demonstrates partial data recovery, not complete decryption; no plaintext AES key, RSA private key, or general keyless decryptor was recovered.**

OPERATION

Promotion preceded public victim claims by more than six months.

EARLY LOCKER

The April sample shows that HYFLOCK had a developed Windows locker shortly after its first promotion.

Confidential | Check Point Copyright © All Rights Reserved 2026

EVOLUTION

April and July are closely related. **October is the first substantial technical jump we observed, but the October builds use different outer forms.** The earlier build uses a Go carrier and Rust child, while the October 17 build runs as a standalone Rust encryptor and stages a copy of itself for background execution.

LIMITATION

Advanced functions remain partly configuration-gated, unobserved, or based only on operator claims.

SECTION 1

HYFLOCK Background and Chronology

HYFLOCK presents itself as an affiliate-oriented ransomware platform rather than a closed intrusion crew. Its early messaging centered on encryptor speed, broad platform coverage, automated revenue sharing, and an integrated service model for affiliates. Operator statements are treated as claims unless supported by malware or runtime evidence.

March 29 — **Initial promotion**
A Rust-based RaaS is advertised with cross-platform and performance claims.

April 12–14 — **Launch messaging, Platform and first sample**
The actor states that the service has officially started work and publishes a Tox contact. Earliest HYFLOCK Windows Ransomware sample found.

May 14–29 — **Structured recruitment**
Posts describe affiliate economics, an integrated panel, negotiation support, access procurement, red-team assistance, and technical capabilities.

June 13–23 — **Expansion claims**
The actor promotes an AI-driven C2 concept, claims access, and recruits penetration testers.

July 15 — **Closely related generation**
A functional Rust loader carrying a Rust/Nishi ransomware child, configuration, and an RSA public key is seen.

October 7 — **Locker-upgrade announcement**
The group announces several locker upgrades, including background scheduled encryption and expanded GPO triggering, some of which we identified in the October sample.

October 11 — **HYFLOCK 2.0 release**
HYFLOCK announces version 2.0 and shifts its messaging from a traditional affiliate-oriented RaaS toward a more integrated operating model.

October 13 — **Public extortion**
First recorded batch of eight publicly claimed victims.

October 17 — **Updated ransomware build**
A standalone Rust build provides stronger runtime evidence of encryption, scheduled-task registration, and administrative-share processing.

Confidential | Check Point Copyright © All Rights Reserved 2026

1.1 Recruitment proposition

The May campaign describes an all-in-one affiliate environment with team management, shared negotiation rooms, automated revenue distribution, and an internal marketplace. The advertised platform share begins at 20% and falls to 15% for later operations. The operators also claim to offer data analysis, penetration-testing support, DDoS services, and communications assistance.

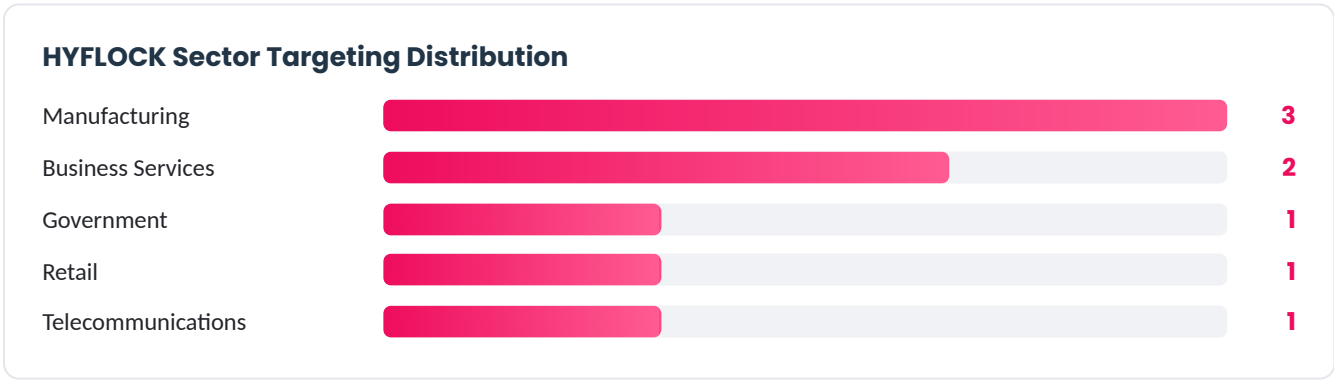
In newer statements, HYFLOCK changed its stated positioning. After months of explicitly advertising a RaaS platform, affiliate economics and external recruitment, the operators said that HYFLOCK was "not traditional RaaS" and presented participants as members of a tightly integrated internal organization rather than conventional affiliates. The same messaging nevertheless continued to welcome operators who lacked their own initial access. **We therefore assess this as a change in public framing toward a more closely managed and collaborative operating model**, not as proof that affiliate participation or the previously advertised revenue-sharing structure ended.

The group also claims to have developed a custom tool capable of generating more than 100 initial-access opportunities per day and offers support to participants who lack their own access. **This remains an operator-service claim rather than a malware finding**: the samples we analyzed do not contain an initial-access capability or establish the claimed volume, quality or origin of those opportunities.

Targeting rules exclude Armenia, Belarus, China, Russia and North Korea while explicitly permitting attacks against government, healthcare, education, law enforcement and critical infrastructure. These rules indicate the operation's stated policy; they do not independently establish actual victim selection or operator location.

1.2 Public victim activity

Our monitoring recorded eight HYFLOCK victim claims on October 13 across multiple countries and sectors. Their near-simultaneous publication pattern indicates a coordinated launch of the public-extortion phase, but the listings remain actor claims unless corroborated through victim disclosure, incident response, or technical artifacts.



Publicly claimed HYFLOCK victims by sector, October 13 batch (n=8).

Confidential | Check Point Copyright © All Rights Reserved 2026

SECTION 2

Operating Model, Branding and Victim Communications

HYFLOCK's public positioning combines ransomware tooling with services intended to lower the operational burden on affiliates. The advertised model includes access procurement, technical assistance, shared negotiations and automated settlements. This positioning aligns with a RaaS offering, although the maturity and availability of each service have not been independently established.

2.1 Earlier affiliate platform

External reports of the HYFLOCK affiliate platform in April described direct access to an authenticated management panel and version 1.0.0 user manuals. The reported interface included automated builders for Windows, Linux/NAS and ESXi, as well as configurable options for GPO spreading, network-only encryption and shadow-copy deletion. The same reporting described an 80/20 affiliate-platform split, a model in which affiliates did not receive the decryptor, and an integrated marketplace for exploit code, leaked databases and privilege-escalation tools.

That reporting also noted Chinese comments in CSS resources and Russian and English-language interfaces. We treat these details as observations of the earlier platform rather than evidence of developer nationality, operator location, or capabilities independently confirmed in every HYFLOCK payload.

A SLIMMER PUBLIC-FACING OPERATION

The earlier affiliate-platform onion is no longer available. The current data-leak site does not show or mention the marketplace, builder resources, or internal panel elements visible in the April screenshots. The public-facing operation therefore appears to have slimmed down or become more focused since HYFLOCK began publishing victims. **Their absence from the current site does not prove that the underlying services were discontinued or removed from private affiliate access.**

2.2 Victim-facing workflow

The October ransom note is a polished HTML artifact styled as an "enterprise encryption" notice. The recovered note includes a populated victim identifier, a Session contact, the Tox identifier reused from earlier recruitment, an email fallback and an onion address described as a customer panel. It directs the victim to make contact within 48 hours and claims a response window of 2-24 hours.

Confidential | Check Point Copyright © All Rights Reserved 2026

```
HYFLOCK :: SECURITY NOTICE
HYFLOCK
Security Division :: Enterprise Encryption System
► SYSTEM ENCRYPTION PROTOCOL :: v2.7.1
► STATUS :: ALL FILES SECURED
► NODE :: [redacted]
⚠ CRITICAL SECURITY NOTICE
IMMEDIATE ACTION REQUIRED
DO NOT attempt to decrypt files yourself
DO NOT modify or delete encrypted files
DO NOT use third-party decryption tools
DO NOT reboot or shut down your system
Contact us within 48 hours to avoid data loss
Your files have been secured with military-grade AES-128-CTR encryption. They are NOT deleted, only inaccessible without the unique decryption key.
◈ DECRYPTION CREDENTIALS
◈ YOUR VICTIM IDENTIFIER
[redacted]
[ COPY TO CLIPBOARD ]
SESSION MESSENGER (CHAT ONLY – NOT A LOGIN ID)
0545[redacted]
TOR SITE (DARKNET PANEL)
4wo3[redacted].onion
TOX CONTACT (ALTERNATIVE)
37BC[redacted]
EMAIL (BACKUP CHANNEL)
hyflock[redacted]
⏱
Response time: 2-24 hours. Save your Victim ID - it is required for decryption.
⚠
CONTACTING US IS MANDATORY.
Your files will NOT recover on their own – without contacting us the data stays inaccessible forever. Reach us through ANY channel above within 48 hours. When you write, ALWAYS include your Victim ID
and your own most important contact
(e-mail / Session ID / phone) so we can reach you back.
📖 INSTALLATION GUIDE
1
INSTALL TOR BROWSER
Tor Browser is required for secure communication with our team.
Windows / macOS / Linux:
Download: https://www.torproject.org/download/
INSTALLATION STEPS:
1. Click the download link above
2. Download the appropriate version for your OS
3. Run the installer and follow prompts
4. Launch Tor Browser
```

Figure 1: *HYFLOCK October ransom note, styled as an "enterprise encryption" notice.*

The group has also recently claimed that dedicated personnel contact victims through WhatsApp, email, and other channels. We did not corroborate this proactive-outreach service in the samples we analyzed. The recovered ransom note confirms email as one victim-initiated contact option, alongside Session, Tox, and a customer-panel onion, but it contains no WhatsApp identifier and does not demonstrate operator-initiated outreach.

The October 17 ransom note directs victims to a different onion address described as a decryption and payment panel. **This indicates variation in the victim-facing infrastructure embedded across the October samples, but does not establish whether the earlier panel was replaced, remained available in parallel or served a different operational role.**

> **INFRASTRUCTURE STATUS**
>
> The October samples contain different victim-panel onion addresses. The earlier address was inaccessible during our analysis, while the October 17 ransom note directs victims to a new address described as a decryption and payment panel. We did not independently verify the availability of the newer service. **These sample-derived victim portals are distinct from HYFLOCK's public DLS/blog and from the historical affiliate-platform infrastructure.**

The executable was not observed automatically connecting to the note's Session, Tox, email, or onion channels. Legitimate software-download and font references included in the HTML are supporting instructions and should not be treated as attacker infrastructure on their own.

2.3 Branding continuity

- HYFLOCK branding and the displayed protocol version remain consistent across the July and October note material.
- The same Tox identifier appears in recruitment posts and both malware generations.
- The internal "Nishi" naming, three-layer pipeline terminology, and file-association identity provide additional technical continuity.
- Continuity supports common tooling lineage; it does not by itself identify individual operators or prove that a given sample was deployed against a named victim.

Confidential | Check Point Copyright © All Rights Reserved 2026

SECTION 3

Ransomware Architecture and Execution Chains

Our strongest comparison remains between the ransomware cores. **April and July share the same Rust/Nishi foundation, while the October builds preserve that lineage but introduce revised staging, network orchestration, and background execution.** Packaging varies within October: the earlier chain uses a Go carrier with an embedded Rust payload, whereas the October 17 build is a standalone native Rust encryptor that stages a byte-identical copy of itself.

	LOADER / STAGING	RANSOMWARE CORE	OBSERVED IN OUR ANALYSIS	IMPLEMENTED / GATED
APRIL	`Standalone Rust/Nishi executable`	Rust/Nishi core Read → Encrypt → Write/Rename	Early initialization only; runtime coverage did not reach encryption	Encryption; SMB/UNC; VSS; Defender interference; cloud handling; GPO/SYSVOL; cleanup
JULY	`Rust loader` → `EXEPACK1` → `zstd/ZIP` → `unpacked_<PID>.exe`	Rust/Nishi child Configuration + RSA public key	Payload extraction and launch; configuration loading; security-impairment commands	Encryption pipeline; shares; recovery inhibition; cloud handling; GPO/task deployment; self-delete
EARLIER OCTOBER	`Go carrier` → `.hyflock-<PID>.exe` → `EdgeUpdate_<suffix>\eu.exe --daemon`	Revised Rust/Nishi child; integrated local and LAN orchestration	Task-creation attempts; note deployment; .locked activity; TCP/445 and share activity	GPO disabled; LDAP/RPC/WinRM, cloud handling, wallpaper and security impairment not fully demonstrated
OCTOBER 17	`Standalone Rust encryptor` → `byte-identical EdgeUpdate_<suffix>\eu.exe` → `scheduled task`	Native Rust/Nishi encryptor with embedded configuration and RSA key	Successful task registration; 500 .locked_<identifier> renames; 17 validated encrypted files; recovery-sabotage attempts; administrative-share processing	Successful task registration; 500 .locked_<identifier> renames; 17 validated encrypted files; recovery-sabotage attempts; administrative-share processing

Figure 2: *HYFLOCK execution-chain evolution. April and July form the earlier Rust/Nishi generation; the two October builds share revised orchestration but use different outer packaging. Runtime-observed effects are separated from implemented or configuration-gated capabilities.*

Confidential | Check Point Copyright © All Rights Reserved 2026

3.1 April and July: the earlier Rust/Nishi generation

The April sample is a standalone, unsigned Rust/Nishi ransomware executable rather than a loader. Its code already supports configurable multithreaded encryption, local and network targets, cloud-synchronized folders, recovery inhibition, security interference, ransom-note deployment, cleanup, and optional GPO-based distribution. **Runtime coverage was limited to early initialization, so we classify most of these behaviors as implemented rather than successfully observed.**

The July generation retains the same ransomware design but adds a separate Rust parent loader. During our analysis, we recovered its EXEPACK1 container, authenticated and decrypted the packaging layer, decompressed the zstd data, and extracted a ZIP containing nishi.exe, config.toml, and public.pem. The loader stages the child as unpacked_<PID>.exe, writes the configuration, and launches the ransomware.

The July child remains closely aligned with April in language, Nishi identity, processing pipeline, .locked extension, ransom-note design, AES/RSA approach, share processing, recovery inhibition, security interference, cloud handling, GPO templates, and cleanup. **The most meaningful April-to-July change is therefore packaging and configuration delivery, not a new ransomware architecture.**

3.2 October execution chain

The earlier October chain begins with an unsigned Go carrier containing a Rust ransomware PE and a 16-byte HYFLCK03 footer. The carrier writes the recovered payload as a temporary .hyflock-<PID>.exe and launches it. The Rust child then stages itself under ProgramData\EdgeUpdate_<suffix> as eu.exe, writes eu.cfg, and attempts a one-shot scheduled-task relaunch using eu.exe --daemon.

The October 17 build removes the separate Go carrier and executes as a standalone native Rust encryptor. It stages a byte-identical copy of itself as ProgramData\EdgeUpdate_<suffix>\eu.exe, writes eu.cfg, and successfully registers a scheduled task for background execution. **The runtime evidence confirms task registration, but not subsequent task-triggered execution, retained SYSTEM context, or reliable survival of an RDP-session termination.**

> **EARLIER OCTOBER ARTIFACT CAVEAT**
>
> A separately analyzed October child retained the loader's 16-byte footer. Because configuration is located relative to end-of-file, the retained footer shifts the lookup and changes execution behavior. **The footer-retaining file is an extraction artifact**, not evidence of a separate ransomware generation.

Confidential | Check Point Copyright © All Rights Reserved 2026

SECTION 4

Capability and Evidence Matrix

Evidence labels are applied per capability: **Confirmed** means directly observed or established at implementation level; **Implemented** means code is present but runtime success is not shown; **Intended** means configuration or control structure indicates expected use; **Unresolved** means the available evidence does not support a firm conclusion.

CONFIRMED | CONFIRMED, QUALIFIED | PARTIALLY CORROBORATED | IMPLEMENTED | UNRESOLVED

CAPABILITY	APRIL / JULY	OCTOBER BUILDS	STATUS
File encryption and ransomware renaming	April implementation confirmed but runtime incomplete; July pipeline and configuration confirmed.	Earlier October artifacts confirmed encryption. The October 17 run produced 500 successful .locked_<identifier> renames and 17 validated encrypted files.	CONFIRMED
Three-stage processing pipeline	Present in April and July Rust/Nishi cores.	Function-level read/encrypt/write implementation recovered.	CONFIRMED
Symmetric and asymmetric cryptography	AES counter-mode and RSA key-backup paths; July carries a 4,096-bit RSA public key.	Both October builds use AES counter-mode and RSA-protected key material. The October 17 build uses a recovered 4,096-bit RSA public key and stores wrapped-key data in each validated trailer.	CONFIRMED
SMB / UNC targeting	Share discovery, mapping and coordination logic present; runtime coverage limited.	The October 17 run performed TCP/445 probing and extensive UNC and administrative-share processing. Some paths may represent the sandbox host's own shares; compromise of another system was not established.	CONFIRMED — SCOPE QUALIFIED
Recovery inhibition	VSS, File History and System Restore operations implemented; a subset launched in July.	The October 17 run attempted recovery-sabotage operations through Command Shell, PowerShell, WMIC and VSSADMIN. Individual command outcomes varied and complete recovery-object deletion was not proven.	CONFIRMED ATTEMPTS
Security-tool impairment	Broad Defender/service/registry command sequence; a subset launched in July.	Configured setting exists; effective schema handling remains unclear.	UNRESOLVED
Cloud-aware processing	Pause, locate, process, clean-cache and resume logic already present.	Implemented in both October builds. Enabled in the earlier configuration but explicitly disabled in the October 17 configuration.	IMPLEMENTED / CONFIGURATION-GATED
GPO / domain deployment	GPO, SYSVOL, startup-task and WMI-related machinery present; success not observed.	LDAP, SYSVOL, RPC task, WinRM and WMI/DCOM paths are implemented. The October 17 configuration sets enable_gpo_spread=false, and eu.cfg includes --no-gpo; no domain-wide propagation was observed.	IMPLEMENTED, NOT OBSERVED
Process termination	Process enumeration, retry and termination paths present.	Process termination implementation recovered.	IMPLEMENTED

Confidential | Check Point Copyright © All Rights Reserved 2026

CAPABILITY	APRIL / JULY	OCTOBER BUILDS	STATUS
Wallpaper and file association	File association and presentation assets present; April note filename differs.	Enabled with embedded assets and registry logic.	IMPLEMENTED
Self-deletion	Cleanup templates present; July loader and child cleanup paths observed.	Cleanup generator and deletion activity evidenced.	CONFIRMED
Data exfiltration	No dedicated workflow established.	No dedicated workflow established.	UNRESOLVED
AI-driven C2	Operator claim only; no supporting component identified.	No supporting component identified.	UNRESOLVED
Detached background encryption / RDP-session resilience	No equivalent detached daemon path established.	Both October builds implement EdgeUpdate_<suffix>\eu.exe, eu.cfg and task-based daemon staging. The October 17 task was successfully registered, but subsequent task execution and RDP-session resilience were not demonstrated.	PARTIALLY CORROBORATED
SYSTEM-context daemon launch	SYSTEM-oriented paths existed in domain-deployment functionality.	The October 17 sample first requested /ru SYSTEM and then registered using the default context. The final retained principal and task execution were not established.	PARTIALLY CORROBORATED
Multiple concurrent instances and interrupted-run recovery	Not established.	Advertised on October 11; no multi-instance or interruption/decryption round trip performed.	UNRESOLVED — CLAIM ONLY
GPO immediate triggering	GPO/SYSVOL and WMI-related deployment paths present.	RPC scheduled-task, WinRM and WMI/DCOM trigger paths are statically supported in the October 17 build, but GPO execution was disabled and remote triggering was not observed.	IMPLEMENTED, NOT OBSERVED
BYOVD-based security-tool killing	No recovered driver chain established.	Operators claim updated BYOVD-killer drivers; no driver artifact or vulnerable-driver execution recovered.	UNRESOLVED — CLAIM ONLY
Virtualization / xpc-ng support	Not established.	Advertised on October 7; no xpc-ng-specific implementation or runtime validation identified.	UNRESOLVED — CLAIM ONLY
Prefix encryption and partial content recovery	Effective encrypted-file extent was not established from the available runtime artifacts.	In the October 17 run, larger collected files had only their first 4,096 bytes encrypted. Seventy-three CRC-valid members were recovered from seven encrypted Office files without a key.	CONFIRMED FOR OCTOBER 17 BUILD

Confidential | Check Point Copyright © All Rights Reserved 2026

SECTION 5

Cryptographic and File-Processing Assessment

5.1 Key generation and protection

Across the generations we analyzed, HYFLOCK uses 16-byte symmetric keys and implements AES counter-mode file processing with RSA protection of recovery material. The July package and both October builds contain 4,096-bit RSA public keys with exponent 65537. In the October 17 build, all 17 collected encrypted files contained the same 512-byte wrapped-key block and distinct per-file IVs, consistent with a shared run-level pipeline key and separately initialized counter streams.

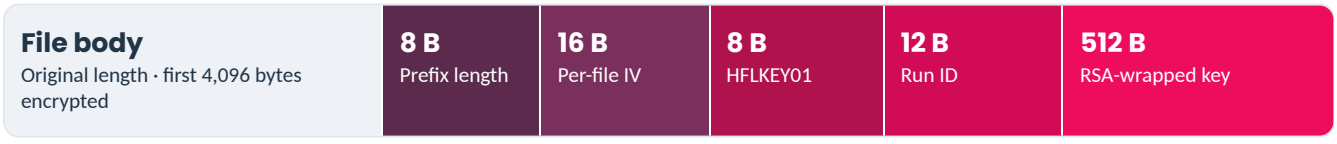
The ransomware attempts to store protected key material in system_config.dat. Its failure paths allow processing to continue when RSA wrapping or backup storage fails. We assess this fail-open design as a recovery risk: **files may be encrypted even when durable operator-side recovery material was not created.**

The October 17 build also contains diagnostic paths capable of printing the plaintext symmetric key. **This creates a conditional recovery opportunity only if output or relevant memory from the original affected execution survives.** We did not recover such material from the analyzed artifacts, and a new execution would generate different key material rather than recreate the earlier key.

5.2 Encrypted-file structure

Our analysis now shows two different levels of encrypted-file evidence across the October builds. In the earlier October artifacts, we identified a processed body followed by a 24-byte length-and-nonce record. The October 17 sample provides a more complete, build-specific on-disk format validated across 17 collected files.

Each October 17 output retains the original-length body and appends a 556-byte trailer containing an eight-byte encrypted-prefix length, a 16-byte per-file IV, the HFLKEY01 marker, a 12-character run identifier and a 512-byte RSA-wrapped symmetric key. All 17 trailers validated. Fourteen larger files recorded a 4,096-byte encrypted prefix, while three smaller files were encrypted across their complete original lengths. **Configuration values such as full_mode=true and encrypt_ratio=100 therefore did not correspond to encryption of every byte in the larger collected files.**



Confidential | Check Point Copyright © All Rights Reserved 2026

recovery_trailer.rs

```rust
// Analyst reconstruction of the October 17 sample observed in 17 collected files.
// Not original source. Helper names are illustrative.

fn encode_recovery_trailer(
    encrypted_prefix_length: u64,
    iv: &[u8; 16],
    run_id: &[u8; 12],
    wrapped_key: &[u8; 512],
) -> Bytes {
    concatenate([
        little_endian_u64(encrypted_prefix_length),   // 8 bytes
        iv,                                           // 16 bytes
        b"HFLKEY01",                                  // 8 bytes
        run_id,                                       // 12 bytes
        wrapped_key,                                  // 512 bytes
    ])   // Total: 556 bytes, appended after modified file content.
}
```

Figure 3: *Analyst reconstruction of the October 17 HYFLOCK recovery-trailer structure. The reconstruction is based on the validated encrypted-file format and is not original HYFLOCK source code.*

Prefix-only encryption left usable content beyond the encrypted region. During our recovery analysis, 73 CRC-valid members were recovered from seven encrypted Office files without obtaining a key. This included Office package content such as worksheet and shared-string data. **This is partial content recovery, not decryption or reconstruction of complete original files.** The overwritten prefixes remain unavailable without the matching key or an exact trusted copy.

The October 17 build retains the nonstandard AES-NI key schedule identified in the earlier October analysis. Conventional AES-CTR tooling cannot be assumed to reproduce this accelerated implementation, and the defect does not currently provide a practical unknown-key attack.

BUILD-SPECIFIC RECOVERY CHARACTERISTICS

The earlier October build contains a paired-block tail omission that may permanently discard bytes even if the correct key is later obtained. The October 17 artifacts instead demonstrate prefix-only encryption, leaving substantial plaintext content beyond the encrypted prefix and enabling partial recovery from some affected files. These findings complement rather than replace one another: they apply to different analyzed builds and should not be generalized across every HYFLOCK sample.

RECOVERY ASSESSMENT

Partial content recovery is demonstrated for selected October 17 Office files, and plaintext-key diagnostics may offer a conditional opportunity if output from the original execution survives. **No complete victim file was decrypted, no plaintext AES key or RSA private key was recovered, and no general evidence-backed keyless decryptor is available.**

Current recovery assessment: **no evidence-backed keyless decryptor is available.** The identified defects weaken confidence in correct restoration but do not presently provide a general decryption method.

Confidential | Check Point Copyright © All Rights Reserved 2026

5.3 April and July cryptographic continuity

The April and July samples use the same general AES/RSA design and nearly identical processing architecture. July provides stronger configuration evidence because its loader archive contains both the TOML configuration and matching public.pem. The April sample is standalone and lacks a recovered operational RSA key, making its effective configuration and recovery behavior less certain. We therefore treat July as the better-documented instance of the early generation, not as a separate cryptographic design.

SECTION 6

April/July-to-October Evolution

The ransomware core remains stable from April through July. October introduces the first substantial change in staging, background execution, and network orchestration, but the two October builds show that HYFLOCK does not rely on a single delivery format. **October therefore appears to represent continued iteration around a shared Rust/Nishi ransomware core rather than migration to one fixed new architecture.**

AREA	APRIL / JULY	OCTOBER	ASSESSMENT
Ransomware form	April is standalone Rust/Nishi; July packages a closely related child behind a Rust loader.	Earlier October uses a Go carrier and revised Rust child. October 17 is a standalone native Rust encryptor that self-stages.	October represents a major orchestration change, but packaging remains flexible.
Packaging	April has no wrapper. July uses EXEPACK1, authenticated transformation, zstd and ZIP.	Earlier October carries a recoverable Rust PE behind a Go bootstrap. October 17 has no separate carrier or inner executable.	HYFLOCK moved between standalone and wrapped forms without replacing the Rust/Nishi core.
Configuration	April lacks a recovered operational configuration; July carries config.toml and public.pem.	Both October builds integrate configuration with the Rust payload. October 17 stores plaintext JSON and a 4,096-bit RSA public key in an appended container.	Configuration is more integrated, although enabled behavior still varies by build.
Background execution	April runs as the original executable; July launches an extracted child.	Both October builds stage eu.exe and use eu.cfg. October 17 stages a byte-identical copy and successfully registers a task.	The daemon design is better corroborated, but task-triggered execution and RDP resilience remain unresolved.
Network scheduling	Share mapping and UNC processing already present; top-level execution appears more sequential.	LAN/share work is integrated alongside local traversal.	Orchestration improvement; performance remains unmeasured.
Share coordination	Earlier owner/timestamp marker design.	Revised .hyflock_claim handling and mapped-drive deduplication.	An existing capability was revised rather than newly introduced.
Domain deployment	GPO, SYSVOL, scheduled-task and WMI-related paths.	Native LDAP, RPC/remote-task and WinRM fallback paths; operators additionally advertise WMI immediate triggering.	Expanded RPC/WinRM implementation is supported, but GPO was disabled in the recovered configuration and successful deployment was not observed. The October WMI-trigger claim remains uncorroborated.

Confidential | Check Point Copyright © All Rights Reserved 2026

AREA	APRIL / JULY	OCTOBER	ASSESSMENT
Victim communication	April and July are primarily Tox-focused.	Both October notes add Session and email. The October 17 note introduces a different sample-derived decryption/payment-panel onion.	October broadens the contact workflow and shows replaceable victim-panel infrastructure.
File-processing outcome	Effective runtime extent remains incompletely documented.	Earlier October artifacts exposed implementation defects. October 17 larger files were prefix-encrypted, with 73 Office ZIP members partially recoverable without a key.	Recovery characteristics vary by build and must be validated from affected artifacts.
Engineering quality	Developed core with limited runtime coverage; July adds explicit packaging and key/config delivery.	October adds stronger orchestration and deployment scaffolding, while retaining crypto irregularities and producing configuration-versus-runtime inconsistencies.	Greater operational breadth does not establish stronger cryptographic correctness or end-to-end reliability.
Concurrency and recovery reliability	Worker concurrency and share coordination already present.	Operators claim multiple-instance support and successful decryption after starting or pausing.	No multi-instance, interruption/resume or complete decryption test was performed; the claim remains unresolved.

BOTTOM LINE

October is best assessed as a HYFLOCK 2.0 orchestration and deployment refactor around a shared ransomware core. The earlier build packages the revised core behind a Go carrier, while the October 17 build deploys it directly as a standalone Rust executable with self-staging for background execution. **The newer sample strengthens evidence for encryption, scheduled-task registration and administrative-share processing, but claims of reliable RDP-session survival, effective BYOVD killing, correct multi-instance recovery and successful domain propagation remain unverified.**

Confidential | Check Point Copyright © All Rights Reserved 2026

SECTION 7

MITRE ATT&CK Mapping

Our mapping is selective and based primarily on behavior we observed or capabilities directly supported by the analyzed samples. **Inclusion does not mean that a technique completed successfully in every run, and operator claims alone are not used to justify additional mappings.**

TECHNIQUE	NAME	EVIDENCE QUALIFICATION
T1486	Data Encrypted for Impact	The October 17 run produced 500 successful ransomware-extension renames and 17 validated encrypted artifacts. Larger collected files were prefix-encrypted rather than fully encrypted byte-for-byte.
T1053.005	Scheduled Task/Job	The October 17 sample successfully registered a one-shot daemon task. Subsequent task execution, durable persistence, retained SYSTEM context and RDP-session resilience were not demonstrated.
T1135	Network Share Discovery	net view, share enumeration and administrative-share discovery were observed in the October 17 run.
T1046	Network Service Discovery	The October 17 sample performed broad TCP/445 probing across the sandbox LAN.
T1021.002	SMB/Windows Admin Shares	Extensive UNC and administrative-share processing was observed. Some paths may represent the sandbox host's own shares; compromise of another host was not established.
T1490	Inhibit System Recovery	Recovery-sabotage commands were launched through Command Shell, PowerShell, WMIC and VSSADMIN. Outcomes varied, and complete deletion of recovery objects was not proven.
T1036.005	Match Legitimate Resource Name or Location	EdgeUpdate-themed ProgramData staging.
T1070.004	File Deletion	Temporary-file cleanup and self-deletion.
T1027.009	Embedded Payloads	Applies to the earlier October Go carrier and its appended Rust executable; it does not apply to the standalone October 17 build.
T1083	File and Directory Discovery	Local, mounted-volume, sync-folder and share traversal.
T1484.001	Group Policy Modification	GPO and SYSVOL deployment is implemented, but disabled in the October 17 configuration and bypassed through --no-gpo; successful policy modification was not observed.
T1021.006	Windows Remote Management	WinRM is implemented as a remote-deployment fallback; successful use was not observed.
T1562.001	Impair Defenses	Security-tool impairment code and launched commands; complete effectiveness not established.
T1112	Modify Registry	File association, wallpaper, FileHistory and security-policy paths.
T1047	Windows Management Instrumentation	PowerShell CIM/WMI was used in attempted shadow-copy deletion. Separate WMI/DCOM remote-deployment functionality remains statically implemented but was not observed executing.

Confidential | Check Point Copyright © All Rights Reserved 2026

Recent operator statements provide additional context for the intended operational purpose of several observed capabilities, but we do not use those claims alone to justify additional ATT&CK mappings without corresponding evidence in the samples or runtime data.

NOT MAPPED AS ESTABLISHED BEHAVIOR

Initial-access exploitation, credential theft, dedicated data exfiltration, executable Tor command-and-control, raw-disk encryption or process injection. Available sandbox labels and generic strings are insufficient for those conclusions.

Confidential | Check Point Copyright © All Rights Reserved 2026

APPENDIX

Sample and Indicator Appendix

Indicators below are intended for correlation. Generic filenames, extensions, and registry paths should not be treated as malicious in isolation.

ARTIFACT	SHA-256 / VALUE	CONTEXT
July parent loader	`80c474154b1df816cf513ae978936875b6dd77f47ef6bce78dda83ab1b89525b`	Rust loader
July ransomware child	`ac233f0bfefb8b39ea84c61b0bec54037285caf5fe439f2c5160842fa4eea815`	Rust/Nishi encryptor
October Go carrier	`b15482d0846ef997f9c049e77d85efeba4ab9b33550b4384052efeb1a3dcc8cc`	Carrier with embedded Rust PE
October exact child	`a120f0c0defe4b6943e09f06272a86ae75d1a4524fa9bf21da25c8c0d747ef5a`	Operational Rust payload
Footer-retaining artifact	`414fc72899a49c8e86590e3391bc07234bc0ea4aba1b0d72712d4d85d616daea`	Analysis artifact; config behavior differs
Ransom notice	`bb6fc3a93a723aba41bffc901617eab7f9e94fd5877a1e811c1b49948fb1a569`	Recovered October note
October 17 standalone encryptor	`b1f0a2fff8baab47463fa04b1ee279ef86265db24a58f7fc1b56c5576ec801db`	Native Rust/Nishi encryptor; staged eu.exe is byte-identical
October 17 ransom notice	`c4e603d94f0472894730d003f0de2169bb4fc2ba436cac919b44d3031201a7e4`	How to Restore My Files.txt
Loader marker	`HYFLCK03`	October carrier footer
Configuration marker	`HYFLOCK_NIS_CFG`	Rust payload configuration slot
Runtime artifacts	`.hyflock-<PID>.exe; EdgeUpdate_<suffix>\eu.exe; eu.cfg; .hyflock_claim; .encrypting_flag; encryption_progress.log`	Correlate with process, task, file and share activity; individual names and suffixes vary
Impact artifacts	`.locked; .locked_<identifier>; How to Restore My Files.html; How to Restore My Files.txt; system_config.dat; system_config_<identifier>.dat; testdecryptkry_<identifier>.dat`	Encryption, victim notice and wrapped-key material; identifier-suffixed forms are run-specific
Registry identity	`hyflockerEncFile`	Encrypted-file association
Recovery-format marker	`HFLKEY01`	October 17 encrypted-file trailer marker
Run-specific encrypted extension	`.locked_7541d2e1b535`	Specific to the analyzed execution; use .locked_<12-character identifier> for broader correlation
Run-specific key backup	`testdecryptkry_7541d2e1b535.dat`	Contains RSA-wrapped key material and the run identifier, not a plaintext decryption key

Confidential | Check Point Copyright © All Rights Reserved 2026

Contact Us

ISRAEL

Tel: +972-73-226-4555

5 Shlomo Kaplan Street
6789159

USA

Tel: 1-800-429-4391

100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318

78 Shenton Way, #09-01 Tower 1
Singapore 079120

PHILIPPINES

Tel: +63-2-8465-9200

Unit 2005, 20th Floor, Zuellig Building, Makati Avenue,
corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44-20-7628-4211

85 London Wall, 4th Floor
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340

Toranomon Kotohira Tower 25F, 1-2-8, Toranomon
Minato-ku, Tokyo 105-0001

ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.

With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: **checkpoint.com/exposure-management**

CHECK POINT
EXPOSURE MANAGEMENT

Confidential | Check Point Copyright © All Rights Reserved 2026