

Threat Talks

Nothing to Block, Nothing to Patch



Ransomware that hides in a blockchain. Fraud that runs on a phone call.

Two threats from August 2026, and neither hands you the usual target. One keeps its command and control where no registrar, host or court can touch it. The other needs no exploit, no CVE and no patch. Just a phone call.

Deadlock ransomware stores its proxy address and its leak blog in smart contracts on the Polygon blockchain. The ransom note is an HTML app that reads them for free: no wallet, no fee, no trace.

WindRelay turns a victim's own Android phone into a card reader and streams the live card payment to a fraudster at a real terminal, while a fake bank employee keeps the victim talking.

The lesson for both: when there is nothing to block and nothing to patch, decide what is allowed. Default-deny egress, least privilege and verified identity still work.

In this Threat Talks infographic we discuss:

- DeadLock: ransomware with a blockchain for a backbone
- WindRelay - SpyNote: the phone call that runs the fraud



\$0

to read DeadLock's next hop from the blockchain: **no wallet, no fee, no trace of the read.**



13 min

one phone call, **two payout channels**: a loan in the victim's name and card-present fraud with their PIN.



80+

victims claimed on DeadLock's leak site. **Attacker claims: ZeroFox gives roughly even odds many are genuine.**



+188%

NFC relay attacks on Android blocked, January to April 2026: **35,600 attempts, year on year.**

NOTHING TO BLOCK

DeadLock

The ransom note asks the blockchain where to go next.



DeadLock is Windows ransomware, first seen in July 2025, that keeps its extortion infrastructure in two smart contracts on the Polygon blockchain: one holds the current proxy address, the other the leak blog. The technique, EtherHiding, dates from 2023; DeadLock brings it to ransomware. Its leak site only surged in June 2026, and the same encryptor is used by more than one crew. But "nothing to block" is half true. The blockchain hides the pointer, not the proxy, storage and RPC endpoints behind it. Those remain points where the operation can be disrupted.

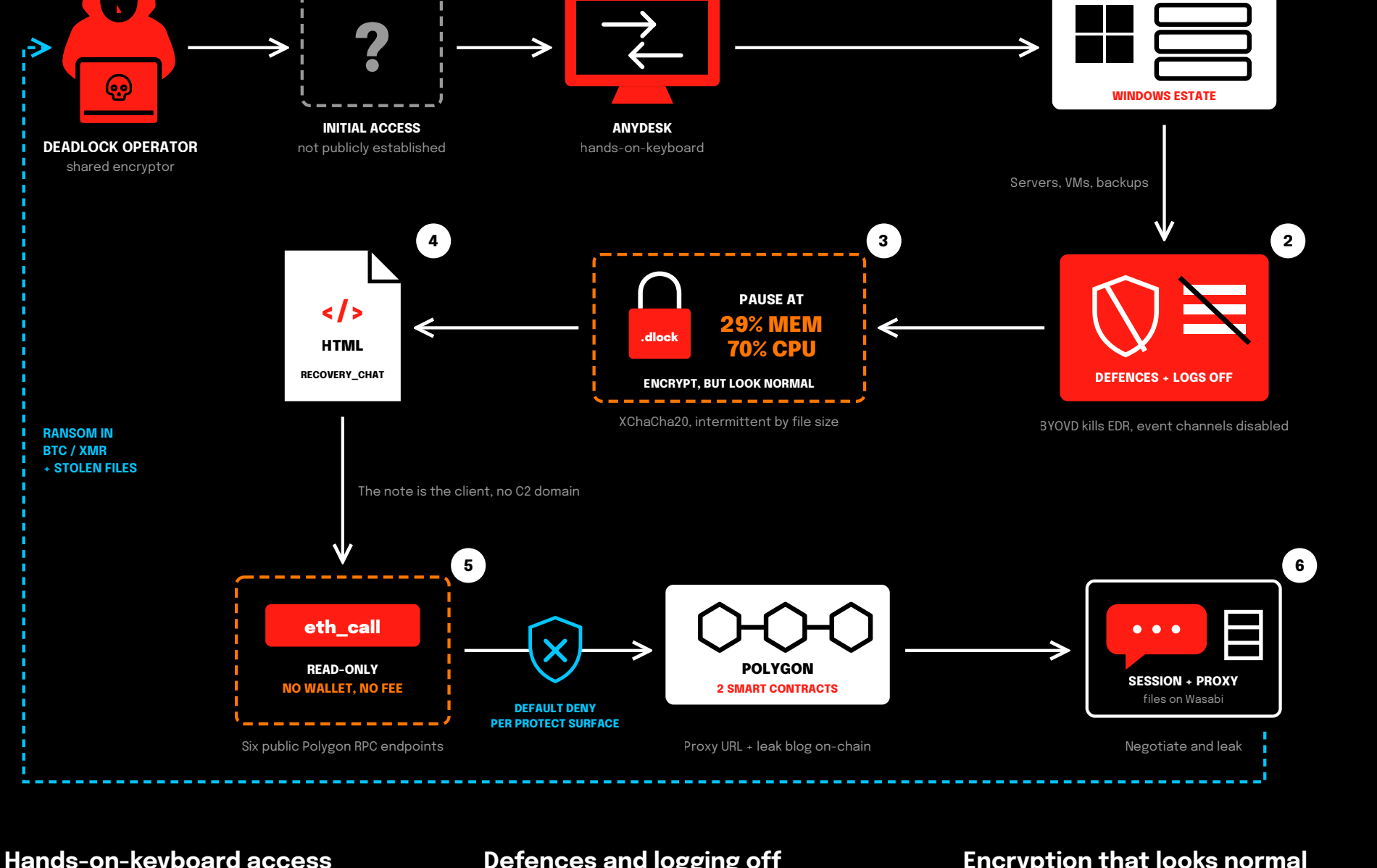
Technique family EtherHiding (blockchain dead drop resolver)
mSOC confidence score Confirmed
Threat category Cyber Attacks, Ransomware, Data Theft / Extortion
Severity High

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
------------------	-----------------	---------	------------	-------------

T1102.001 - Web Service: Dead Drop Resolver (- T1665 - Hide Infrastructure)	Store the current proxy address in a Polygon smart contract and let the ransom-note page read it back with a read-only eth_call, so no C2 domain is baked into any artefact	Looks like an HTTPS POST to a legitimate blockchain API; reads are free and leave no trace; six interchangeable RPC endpoints; a contract cannot be taken down	Medium	Windows estates in IT, mining, transport, manufacturing, hospitality and consumer goods; over half of claimed victims in Europe
---	---	--	--------	---

ATT&CK Mitigation	Attack Vector	Detection	Threat Level	Threat Actor Type
-------------------	---------------	-----------	--------------	-------------------

M1021 - Restrict Web-Based Content	A process or victim-facing page fetching its next hop from a public blockchain RPC endpoint instead of a hard-coded domain	JSON-RPC eth_call to a known RPC provider, especially from a non-browser process; sudden shifts in a Protect Surface's outbound destinations; RECOVERY_CHAT.html on desktops	High	Financially motivated ransomware operators, no known state nexus; encryptor shared with other crews, including a Lynx and INC affiliate
------------------------------------	--	--	------	---



Hands-on-keyboard access

- The way in is unknown. The documented chain starts with an operator already inside, driving Windows through AnyDesk.
- Allowlist remote management tools. Segmentation decides how far one session can reach.

Defences and logging off

- Defender, backups and shadow copies go first. A vulnerable driver kills EDR, then every event log channel is switched off.
- Enable tamper protection and blocklist vulnerable drivers. Stream telemetry off-host so a silenced host still reports.

Encryption that looks normal

- Files are encrypted to .dlock, large ones only partly. The encryptor pauses above 29% memory or 70% CPU, so nothing hangs.
- Don't wait for resource spikes. Use ransomware ASR rules and keep immutable, separated backups.

The ransom note is the app

- An HTML file on the desktop is the full negotiation client. There is no C2 domain inside to extract.
- Hunt for unexpected HTML files on desktops and drive roots after suspicious file activity.

Ask the blockchain

- The note reads the current proxy address from a Polygon smart contract. No wallet, no fee, no domain to sinkhole.
- Make blockchain RPC an egress category. With default-deny per Protect Surface, a file server calling Polygon was never allowed.

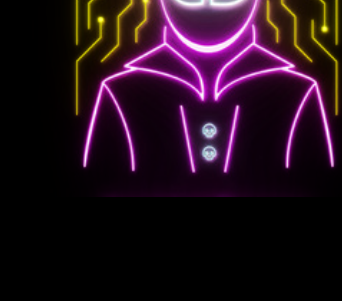
Negotiate and leak

- Chat runs through Session over that proxy. The leak blog sits in a second contract, stolen files on Wasabi.
- The proxy is a plain IP and can be blocked. Agree the extortion playbook in advance.

NOTHING TO PATCH

WindRelay + SpyNote

Not card cloning. A live relay, kept alive by a phone call.



WindRelay is Android malware, first documented by Group-IB on 12 August 2026, that turns a victim's phone into a rogue contactless card reader and streams the live card exchange to a fraudster at a real payment terminal. In one 13 minute call, a fake bank employee had the victim sideload a SpyNote RAT named after themselves, installed WindRelay silently, took out a loan in the victim's name and captured card and PIN. No CVE, no exploit. EMV did not break: contactless simply has no mandatory check that the card is near the terminal.

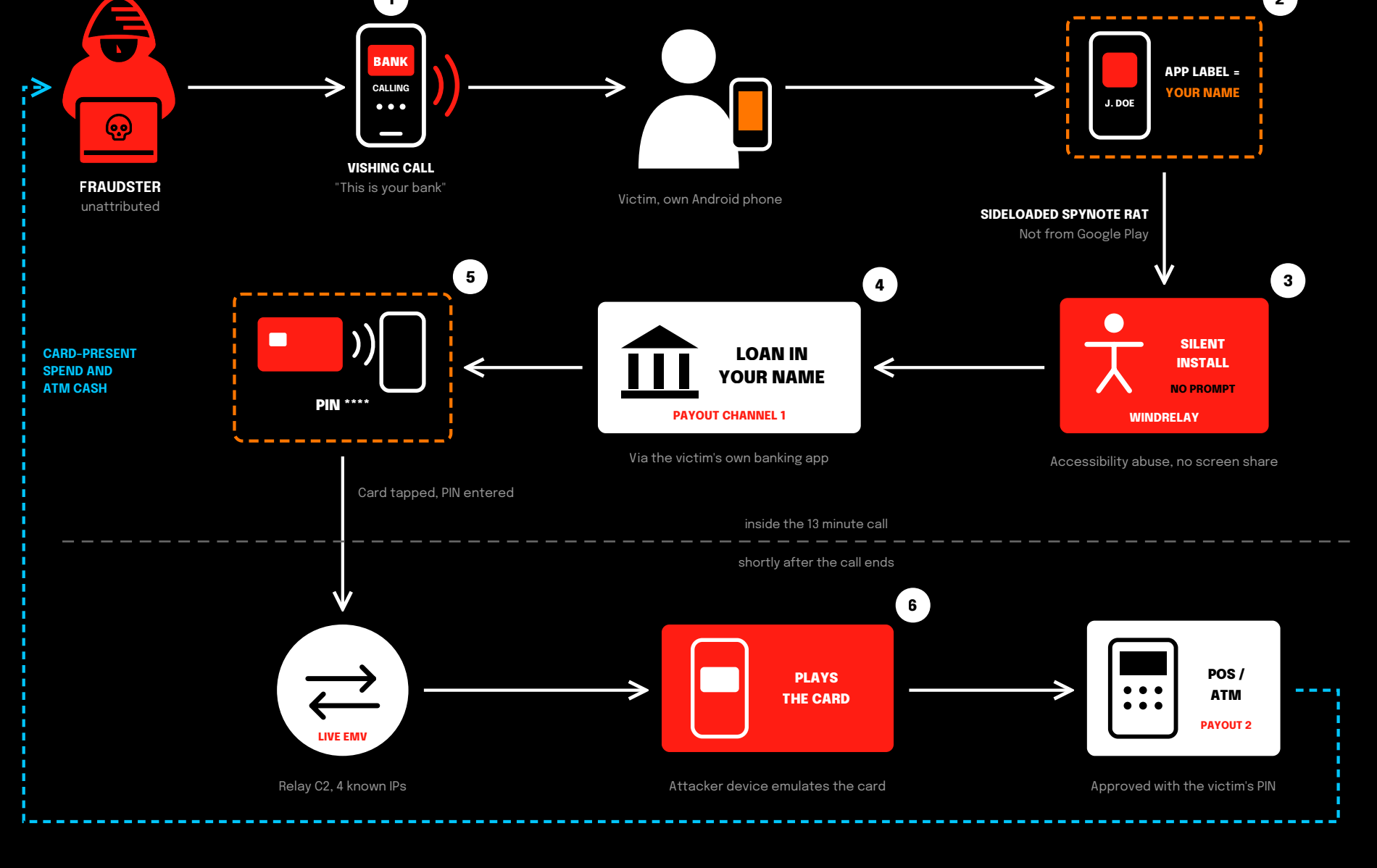
First documented 12 August 2026 (Group-IB); attribution not established
mSOC confidence score Confirmed
Threat category Social Engineering, Mobile Banking and Payment Fraud
Severity High

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
------------------	-----------------	---------	------------	-------------

T1660 - Phishing (vishing)	Call the victim as a bank employee reporting a card problem, talk them through sideloading a personalised APK, then keep the call live to synchronise the card tap and PIN entry	No CVE, no exploit, no Google Play; the APK carries the victim's own name; the second install needs no approval and raises no screen-sharing prompt	Low	Retail banking customers on their own Android phones; samples mimic banks in Czechia, Slovakia and Slovenia
----------------------------	--	---	-----	---

ATT&CK Mitigation	Attack Vector	Detection	Threat Level	Threat Actor Type
-------------------	---------------	-----------	--------------	-------------------

M1011 - User Guidance	An inbound call that asks the customer to install an app, then tap their card to the phone and enter their PIN	Sideloading install during an active call; a silent second install. Accessibility or device-admin grant right after a call starts; loan plus card-present spend in a short window	High	Unattributed, financially motivated mobile fraud crew; no actor or Fraud-as-a-Service vendor published
-----------------------	--	---	------	--



The call

- A fake bank employee calls about a card problem and keeps the victim talking. The relay only works during the call.
- Verify the caller, not the call. No bank asks you to install an app or tap your card on your phone.

Sideloading RAT

- Guided on the call, the victim sideloads SpyNote. The app label is the victim's own name, killing the one cue users check.
- Block unknown sources on installed devices. For banks, a sideloaded install during an active call is a signal on its own.

The silent second install

- Using SpyNote's Accessibility access, the fraudster installs WindRelay himself. No approval, no screen-sharing prompt, so screen-share detection never fires.
- Treat an Accessibility grant as admin rights. Alert on Accessibility grants right after a call starts.

Payout one: the loan

- With remote access live, the fraudster takes out a loan in the victim's name through their own banking app.
- Require step-up or out-of-band confirmation for loans requested during an active call or after a new app install.

The tap

- The victim taps the card on the phone and enters the PIN. WindRelay streams the live exchange out. Nothing is cloned.
- Put the card away or switch NFC off: the relay dies. Prefer wallet cards, which verify every payment.

Payout two: the cash-out

- The attacker's phone plays the card at a real terminal or ATM. Approved with the victim's PIN, it looks like a normal chip payment.
- Correlate a loan and a card-present payment for the same customer in a short window. Detect the sequence, not the hash.

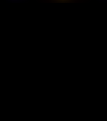
Taxonomy

ATT&CK Technique Which technique of the MITRE ATT&CK framework does the threat correspond to.	Evasion Tactics used by the attacker to avoid detection or bypass security.	Target Type The category of organization that may potentially be targeted.
ATT&CK Mitigation Which mitigation of the MITRE ATT&CK framework can be applied.	Detection Mechanism to identify malicious activities or system anomalies.	Threat Actor Type What type of threat actor may be involved.
Attack Strategy Plan devised by the attacker to exploit specific system vulnerabilities.	Complexity How easy it is to exploit the vulnerability or carry out the attack.	
Attack Vector What is the primary method of attack.	Threat Level How severe the threat is.	

How we score what you're reading:

Not all threat intelligence is equal. Every source we use is rated 0 (untrustworthy) to 5 (verified). Every news item is rated A (reliable) to E (unreliable). Together they classify a threat as Confirmed, Verified, or Credible; the same framework our Global SOC uses to separate signal from noise for customers worldwide.

Want this rigor applied to threats targeting your organization? Our Security Special Service Team will walk you through how it works > team@threat-talks.com



threat-talks.com

on2IT
ZERO TRUST INNOVATORS

amsix