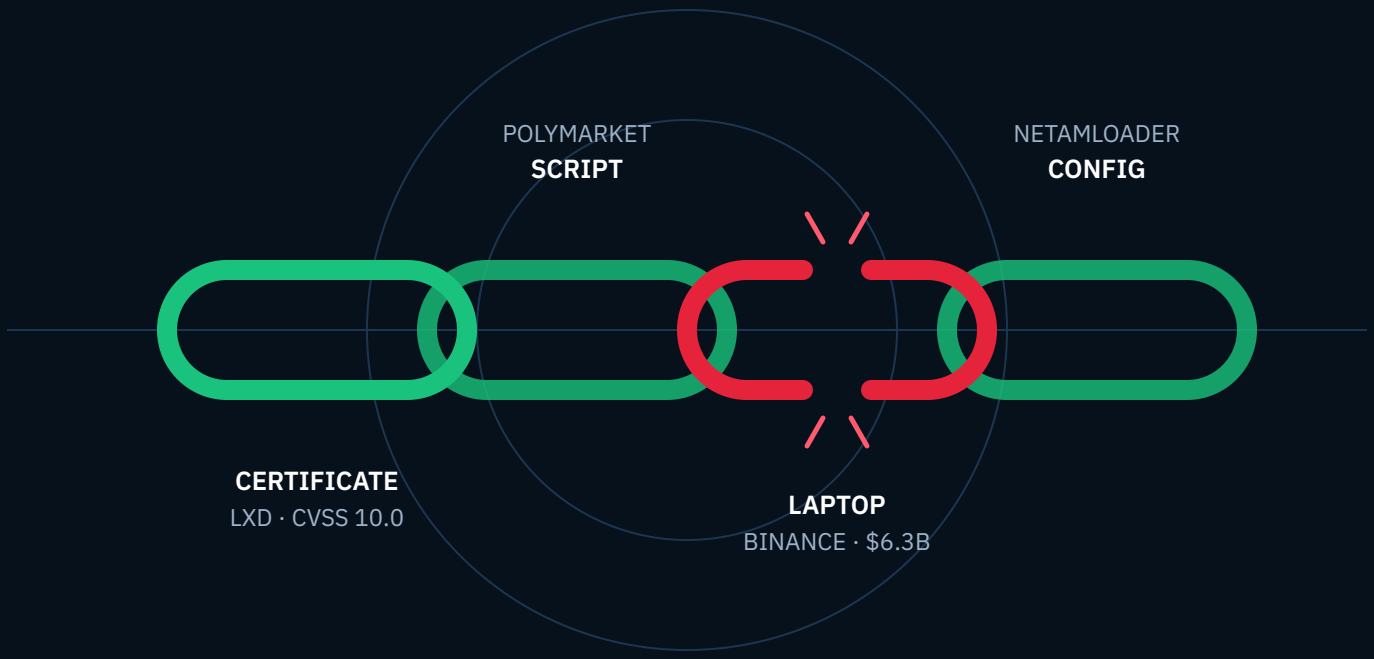
MAG212 CYBER

DAILY INTELLIGENCE

NOVEMBER 1, 2026

EDITION A · BROKEN TRUST



BROKEN TRUST.

A certificate that proved nothing, a speed script that sold your positions, a laptop worth $6.3 billion and a signed binary that loaded a stranger's code.

P.03
LXD: the chain nobody checked

P.04
Inside the Polymarket drainer, minute by minute

P.06
Binance: keys safe, money gone

P.07
NetamLoader in the update folder

00 / BRIEFING

Four trust boundaries, four failures

Each of today's incidents abused something that was supposed to be trusted: a public certificate, a vendor script, an engineer's laptop, a signed Microsoft binary. None needed a zero-day in the crypto, the browser or the OS.

LXD / MICROCLOUD
10.0
CVSS 4.0, network, no privileges

POLYMARKET
726
wallets refunded, about $2.7M stolen

BINANCE
$6.3B
largest crypto theft on record

NETAMLOADER
20–40
minutes of silence before first C2 call

INCIDENT	WHAT WAS TRUSTED	WHAT ACTUALLY HAPPENED	STATUS
LXD · MicroCloud	Any certificate in the client's chain	Only the leaf proves a private key; the rest is attacker-supplied	PATCHED 29 OCT
Polymarket	A page-speed script from a vendor CDN	Replaced file used the page's own trading client and signer	EXPLOITED
Binance	A DevOps engineer's endpoint and service identity	Unauthorized withdrawals submitted; no key leak reported	EXPLOITED
NetamLoader	Microsoft-signed .NET assemblies in an update CAB	A .config file told them to load attacker code	TARGETED

THE PATTERN

In every case the defenders' control worked as designed: TLS encrypted, the CSP allowed only listed hosts, keys stayed in custody, binaries were validly signed. What failed was the assumption about what that control proved. Identity, intent and integrity each need their own check.

Read with Edition B for today's exploited-CVE deadlines: PHP2Shell, Ivanti, the poisoned Claude Code extension, GitLab and PAN-OS.

MAG212 ACTION ORDER

1. **LXD and MicroCloud.** Refresh to 6.10.1 · 5.21.9 · 5.0.11 · 4.0.15; MicroCloud 2.1.5 · 3.4.1. Public PoC code appeared 31 Oct.
2. **Third-party scripts.** Pull RUM and analytics tags from any page that can sign, trade or pay.
3. **Block the FBI's 628 addresses** if you run a wallet, exchange or payment service.
4. **Hunt .config files** with appDomainManager entries outside known applications.

01 / CLOUD INFRASTRUCTURE

LXD: the certificate chain nobody checked

CVE-2026-112816 · CWE-295 · CVSS 4.0 10.0 · LXD, MicroCloud and Incus · disclosed 28 Oct

CLIENT SENDS THIS CHAIN

[0] LEAF
Attacker's own cert. TLS proves they hold its key.

[1] "INTERMEDIATE"
Victim admin's public cert. Proves nothing.

VULNERABLE SERVER

Compares **every** peer certificate with the trust store. Entry [1] matches, so the session runs as the victim admin.

→ full cluster + VM control

FIXED SERVER

Checks only the **leaf**, the one certificate whose key the handshake proved. Leaf is not trusted.

→ 403, connection refused

REPORTED FACTS

The Incus project found the bug and referred it to Canonical, which confirmed LXD was affected. Fixes shipped 29 Oct with no LXD workaround. Affected: 4.0.14, 5.0.10, 5.21.8 and 6.9. Public PoC code appeared 31 Oct. [S1][S2][S3]

WHO IS EXPOSED

Standalone LXD isn't on the network by default. MicroCloud is: capture a member's public certificate as it joins, then log in as that member. [S1][S3]

FIXED RELEASES · SNAP

6.10.1	5.21.9	5.0.11	4.0.15
MicroCloud	2.1.5	3.4.1	

lxc config trust list illustrative

NAME	TYPE	FINGERPR.
admin-laptop	client	3f9a1c…
ci-runner-old	client	8be2d0…
node-02	server	c41e7a…

Each entry is a borrowable identity. Prune unused ones.

LINUX / BASH · EXPOSURE, INVENTORY, PATCH

```
# 1. API on the network? (empty = no)
$ lxc config get core.https_address
# 2. Installed revision, every member
$ snap list lxd microcloud
# 3. Whose identity can be borrowed?
$ lxc config trust list
# 4. Patch, then re-check the revision
$ sudo snap refresh lxd microcloud
# 5. Watch API activity during review
$ lxc monitor --type=lifecycle --pretty
```

MAG212 ANALYSIS

Mutual TLS has two jobs: prove a key and map it to an identity. This bug kept the first and broke the second. Firewalling port 8443 is a good second barrier, but it does not fix the bug.

WHAT IS NOT ESTABLISHED

No confirmed in-the-wild abuse. This is not a general Ubuntu login flaw. Review recent instance and trust-store changes before you call it closed.

02 / WEB SUPPLY CHAIN

Inside the Polymarket drainer, minute by minute

A DebugBear page-speed script became a wallet drainer on 29 Oct · about $2.7M refunded to 726 wallets

TIMELINE · 29 OCT · UTC

16:54	Vendor origin errors out; another server answers
17:10	First POL reaches the attacker
17:26	First position tokens move
17:59	Polymarket ships "remove debugbear rum script"
18:28	28.6M POL split to three wallets in 10 min
19:00	Trading fully restored, refunds promised

Ohey reconstruction from chain data and archives. [S4]

HOW 15,187 BYTES EMPTIED A WALLET

1. **Find a live session.** Reads Polymarket's localStorage for login params, the deposit wallet and trading API keys.
2. **Borrow the page's signer.** No keys of its own: it walks React fiber trees to find the page's order client.
3. **Move everything.** Swaps cash to POL and signs EIP-712 batches through Polymarket's relayer. Email-login positions are dumped with fill-and-kill orders at 97%, 50%, then the minimum tick.
4. **Report home.** Posts portfolio data, sweep results, IP and country to four paths on data.debugbear[.]com, a host the CSP already allowed.

28.64M
POL received by the attacker

33
deposit wallets lost positions

49 min
first theft to script removal

15 KB
drainer vs 60 KB clean file

DEVTOOLS › NETWORK · polymarket.com · what a victim's browser did — illustrative, from S4 IOCs

METHOD	URL	STATUS	SIZE
GET	cdn.debugbear[.]com/C7xcKKrjUnXK.js	200	15,187 B
POST	data.debugbear[.]com/metrics/init	200	—
POST	Polymarket relayer · EIP-712 batch	200	—
POST	data.debugbear[.]com/submit · /update · /handle	200	—

REPORTED FACTS

DebugBear says its DNS records were compromised through its domain registrar. Each customer loads its own script copy; Polymarket's was the one swapped. Polymarket is refunding about $2.7M to 726 wallets. [S5][S6]

WHAT IS NOT ESTABLISHED

No post-mortem yet from either company. Counts differ by method, so don't add the trace totals to the refund figure. Private keys were not shown to leak.

DEFENSIVE ENGINEERING / 02 / BROWSER INTEGRITY

Defend the page that signs

A script on your page runs with your page's authority. A CSP allowlists hosts, not the bytes they serve.

29 OCT · ONE ORIGIN, ONE TRUST LEVEL

polymarket.com page

- Order client + signer
- API creds in localStorage
- Vendor RUM script (swapped)

The vendor script could read everything the app could, and call the same signer.

MAG212 PROPOSAL · SPLIT THE AUTHORITY

signing origin
- First-party code only
- Self-hosted, SRI-pinned

sandboxed frame
- Analytics, RUM
- No access to signer

Creds out of page storage; every signature confirmed.

HTML + HEADER · PIN WHAT YOU LOAD

```
<!-- self-host a reviewed copy -->
<script src="/vendor/rum-2026-10.js"
  integrity="sha384-<digest>"
  crossorigin="anonymous"></script>

# response header on signing pages
Content-Security-Policy:
  script-src 'self';
  connect-src 'self' https://api.example;
  frame-src https://telemetry.example;
```

BASH · AUDIT AND MONITOR

```
# every third-party script in a build
$ grep -RhoE 'src="https?://[^"]+\.js' dist/
\
    | sort -u
# SRI digest for a reviewed file
$ openssl dgst -sha384 -binary rum.js \
    | openssl base64 -A
# alert when a vendor file changes
$ curl -s "$VENDOR_URL" | sha256sum \
    | diff - rum.sha256 || alert
```

MAG212 proposals: test in staging first. SRI only works with fixed bytes, so dynamic vendor scripts need self-hosting or a frame. [S13]

INDICATORS · DEFANGED · FROM OHEY [S4]

Drainer URL	hxxps://cdn.debugbear[.]com/C7xcKKrjUnXK.js
Exfil endpoints	data.debugbear[.]com/metrics/init · /submit · /update · /handle
Drainer SHA-256	0755e767504d8103f6c27b9e765a1026507a17c04513242adb503df7777879e5
Clean SHA-256	0525f046c83daa429e0f676d36650d51d9e283ba5cacfa56097c80bad586128b

IF YOU RUN DEBUGBEAR RUM

Remove the embed as the vendor asked, then search proxy and DNS logs for both hosts.

IF YOU BUILD WEB3 FRONTENDS

No third-party code on signing pages. Keep trading creds out of localStorage.

IF YOU TRADED THAT HOUR

Revoke trading API keys, review approvals, and move funds to a fresh wallet.

03 / PRIVILEGED ACCESS

Binance: the keys were safe. The money left anyway.

About $6.3B on 29 Oct · FBI names North Korea's TraderTraitor · phased withdrawals from 1 Nov [S15]

BINANCE'S PRELIMINARY PATH · 30 OCT

01 ENDPOINT
DevOps engineer's laptop compromised

→

02 WORKLOAD
Access to a service container

→

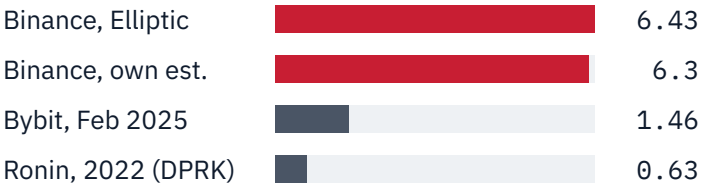
03 REQUEST
Unauthorized withdrawals submitted

→

04 SIGNED
Signer approved; no key leak found

Binance later reported "additional points of breach"; co-CEO Richard Teng said it was not one engineer's permissions or a one-click action. [S9][S8]

LARGEST CRYPTO THEFTS · USD BILLIONS



REPORTED FACTS

The FBI attributed the theft to TraderTraitor on 31 Oct and published 628 addresses: 608 Ethereum, 19 Bitcoin and one Solana. It asked services to block transfers. TRM Labs and Chainalysis reached the same view, and Chainalysis saw funds mixing with September's Bitget loot. Around $3B was frozen on-chain early on. [S7][S9][S16]

KUBERNETES · WHO CAN REACH THE SIGNER?

```
# what the withdrawal service may do
$ kubectl auth can-i --list \
  --as=system:serviceaccount:pay:withdrawer
# exec sessions in the audit log
$ jq -c 'select(.objectRef.subresource
  =="exec") | [.user.username,
  .objectRef.name, .stageTimestamp]' \
  audit.log
```

SCREENING · FBI ADDRESS LIST

```
# normalise the FBI list (one per line)
$ tr 'A-F' 'a-f' < fbi_tt.txt \
    | sort -u > deny.txt
# any hits in 7 days of transfers?
$ cut -d, -f4 transfers.csv \
    | tr 'A-F' 'a-f' | sort -u \
    | comm -12 - deny.txt
```

Generic MAG212 checks for comparable services; namespace, file and column names are placeholders.

MAG212 ANALYSIS

Key custody stops theft of the key, not misuse of the signer. Put an independent approval step between "a service asked" and "the wallet signed": destination allowlists, value and velocity limits, and a quorum outside the cluster for anything large.

WHAT IS NOT ESTABLISHED

How the laptop was compromised, what the other breach points were, and which control failed. Attribution is the FBI's assessment, not a court finding.

04 / ENDPOINT RESEARCH

NetamLoader: signed code, hostile config

Kaspersky GReAT, 29 Oct · a government-only Windows 10 build in Asia · one victim · unattributed

INFECTION CHAIN · SECURELIST [S10]

01 CAB in `SoftwareDistribution\Download`, mostly genuine files

02 Patch My PC runner starts; its .config sets a Microsoft-signed AppDomainManager

03 That class reads `fabric.config`, which loads `Resources.resx`, the only malicious file

04 BinaryFormatter + TypeConfuseDelegate run `XamlReader.Parse()` on XAML-1

05 AES key = SHA-256 of its own command line: wrong arguments, nothing decrypts

06 AMSI patched, ETW off, traces wiped; hops into `dllhost.exe`

07 Waits 20–40 min, polls `openaigpt4v[.]com`, runs its XAML

C2 TIMING

First contact	**20–40 min**
Poll after reply	**5–6 min**
Back-off, no reply	**22–28 h**
Watchdog exit	**~28 h**

TRAFFIC

AES-128-CBC with HMAC-SHA256. Any TLS certificate accepted. Data in query parameters b and c on `/model_v4/<guid>`. C2 sits behind Cloudflare.

THE HIJACK · .exe.config (STRUCTURE)

```
<configuration>
 <runtime>
  <appDomainManagerAssembly value=
   "Microsoft.HostIntegration.Connectors"/>
  <appDomainManagerType value=
   "Microsoft.ApplicationServer.Caching
    .DataCacheFactoryConfiguration"/>
  <NGenAssemblyUsageLog enabled="0"/>
 </runtime>
</configuration>
```

THE AMSI PATCH · x64 BYTES

```
; written over Console.Clear()
41 C7 00 01 00 00 00  mov dword [r8], 1
33 C0                 xor eax, eax
C3                    ret
; AMSI Scan (vtable +0x18) now jumps
; here: every scan returns CLEAN
```

Config rebuilt from names Kaspersky published; disassembly is MAG212's reading of the bytes. [S10]

MAG212 ANALYSIS

Every executable passes a signature check; the attack lives in the config and data beside them. Allowlisting signed binaries without controlling their .config files leaves this path open.

WHAT IS NOT ESTABLISHED

How the CAB arrived, which country was hit, or who did it. Patch My PC is not reported as compromised.

DEFENSIVE ENGINEERING / 04 / ENDPOINT DEFENSE

Hunt NetamLoader across the fleet

It deletes its own files and logs, so hunt the traces it can't remove: registry, network, process lineage.

POWERSHELL · ONE HOST, READ-ONLY

```
# 1. config/resx in the update cache
PS> gci C:\Windows\SoftwareDistribution\
  Download -Recurse -Include *.config,
  *.resx -EA 0 | select FullName,
  LastWriteTime
# 2. the surrogate key it creates
PS> Test-Path 'HKLM:\SOFTWARE\Classes\
  AppID\{ff259bcd-2f0a-44de-b34a-
  0092fec1d8a2}'
# 3. prefetch, if not wiped
PS> gci C:\Windows\Prefetch\PATCHMYPC-
  SCRIPTRUNNER.EXE-*.pf -EA 0
# 4. C2 name in the DNS cache
PS> Get-DnsClientCache | ? Entry
  -like '*openaigpt4v*'
```

DEFENDER XDR · KQL · WHOLE FLEET

```
// runner launched from the update cache
DeviceProcessEvents
| where FileName =~
    "PatchMyPC-ScriptRunner.exe"
| where FolderPath has
    @"\SoftwareDistribution\Download"
| project Timestamp, DeviceName,
    ProcessCommandLine

// C2 by name, never by shared IP
DeviceNetworkEvents
| where RemoteUrl has "openaigpt4v.com"
| summarize count() by DeviceName
```

MAG212 proposals built from Securelist indicators. 104.18.14[.]219 is a shared Cloudflare address: alert on it, don't block it. [S10] [S14]

EVENT VIEWER › SYSMON · WHAT A HIT LOOKS LIKE illustrative

ID	EVENT	DETAIL
11	FileCreate	…\Download\Install\fabric.config
1	ProcessCreate	PatchMyPC-ScriptRunner.exe -updatepackage -applicationid=…
13	RegistryValueSet	HKLM\…\AppID\{ff259bcd-…}\DllSurrogate = ""
7	ImageLoad	dllhost.exe ← System.Xaml.dll, clr.dll
22	DnsQuery	dllhost.exe → openaigpt4v[.]com (20–40 min later)

FILE INDICATORS · MD5 · SECURELIST [S10]

CAB archive	F2458ED133F8D0CA19E22C10F577E98E
Resources.resx	E1DC6F1ED193594F2284BE22AE08DFA4
ScriptRunner.exe.config	514AC0D73B8A1B73488EF5E2E55A75C3
fabric.config	67E3617F8709D34F806F8E02BADBA8A5
.NET 1 Loader	AB81564BCB8CA7E710C66832DE747556
.NET 2 Plugin	CFB8B281BDF5D9390E64B10C312FB2C1

HARDEN

WDAC / AppLocker: treat .exe.config beside signed binaries as code, not data.

Alert on appDomainManagerType in any .config you didn't ship (ATT&CK T1574.014). [S12]

Forward Sysmon off-host: the loader wipes Prefetch and CLR usage logs.

SOURCES & METHOD

Where every number comes from

S1 Canonical · LXD and MicroCloud advisory, 28 Oct · discourse.ubuntu.com

S2 CVE record · CVE-2026-112816, upd. 31 Oct · opencve.io

S3 The Hacker News · LXD and MicroCloud flaw, 1 Nov · thehackernews.com

S4 Ohey · Polymarket drainer analysis and IOCs, 29 Oct · ohey.ca

S5 Hudson Rock · Wallet-draining third-party script, 29 Oct · infostealers.com

S6 The Hacker News · Polymarket refunds, 1 Nov · thehackernews.com

S7 Hackread · FBI publishes 628 addresses, 1 Nov · hackread.com

S8 Elliptic · Largest theft in history, upd. 31 Oct · elliptic.co

S9 CNBC · $6.3B Binance hack, 30 Oct · cnbc.com

S10 Kaspersky GReAT · NetamLoader report, 29 Oct · securelist.com

S11 GBHackers · NetamLoader summary · gbhackers.com

S12 MITRE ATT&CK · T1574.014 AppDomainManager · attack.mitre.org

S13 MDN · Subresource Integrity · developer.mozilla.org

S14 Microsoft · DeviceProcessEvents schema · learn.microsoft.com

S15 Tech Insider · Binance phased withdrawals, 1 Nov · tech-insider.org

S16 Forbes · Binance hack began with one laptop, 30 Oct · forbes.com

REPORTING METHOD

Facts come from vendor advisories, the CVE record, agency statements and named research teams, checked on 1 November 2026. Secondary reporting fills gaps where primary pages were not reachable. Analysis is labelled MAG212. Commands and queries are proposed read-only checks, not tests run on affected systems.

LIMITATIONS

Loss figures are estimates and differ by method. Attribution is an agency assessment, not a court finding. Diagrams show trust boundaries, not victim networks; console panels are illustrative. Indicators are defanged; verify with the original report before blocking.

ALSO TODAY · EDITION B · DEADLINE DAY

PHP2Shell under active exploitation, Ivanti's three-bug chain to root, the trojanized Claude Code extension on Cursor's marketplace, GitLab's two CVSS 10 regex flaws and the PAN-OS route to the hypervisor. At cyber.mag212.com.

MAG212 CYBER
UNDERSTAND THE THREAT. BUILD THE DEFENSE.
Subscribe free
cyber.mag212.com/subscribe-free/