

Lampion's Portugal-focused phishing campaign delivers multistage malware

A acronis.com/en/tru/posts/lampions-portugal-focused-phishing-campaign-delivers-multistage-malware

Authors: Jozsef Gegeny, Ilia Dafchev, David Catalan Alegre

Summary

[Acronis Threat Research Unit \(TRU\)](#) identified an active Lampion malware campaign targeting Portuguese users through phishing emails masquerading as financial and administrative communications.

First publicly documented in December 2019, [Lampion is a Brazilian banking malware family](#), derived from the ChePro lineage, that has consistently targeted Portugal and other Portuguese-speaking users rather than Brazilian victims.

Initial payloads are delivered through ZIP archives containing heavily obfuscated HTML files designed to evade static detection and analysis. The HTML stage retrieves and executes additional script from attacker-controlled infrastructure, leading to the deployment of a multistage VBS infection chain.

Each stage employs extensive obfuscation techniques, including junk code, encrypted strings and dynamically generated scripts, significantly inflating file sizes while concealing core functionality. The infection chain is deliberately fragmented across multiple independent execution stages, complicating behavioral analysis and reducing the visibility of malicious activity.

Telemetry indicates that the activity is overwhelmingly concentrated in Portugal, reinforcing the assessment that Lampion remains a highly targeted threat focused on Portuguese victims.

Details of the campaign

As part of the Lampion malware campaign we've been tracking in recent weeks, we observed a wave of phishing emails designed to impersonate routine financial or administrative communications. The activity appears to be highly targeted and focuses overwhelmingly on victims in Portugal (94.6% of detections; see Statistics), leveraging Portuguese-language lures and local business impersonation to increase credibility.

Before examining each component in detail, the figure below provides a high-level overview of the infection chain observed in this campaign. The attack progresses through multiple staged components, beginning with a phishing email and culminating in the deployment of the Lampion RAT payload.



Infection chain overview

Below is an example message detected in June 2026, reflecting the most recent iteration of this activity:



Figure 1: Phishing email

This phishing email uses a simple financial pretext to encourage the recipient to open an attachment. It claims to include a “payment receipt,” which is a common social engineering tactic in malware campaigns: Presenting the attachment as an important transactional document to increase the likelihood of execution.

The message is also padded with credibility markers such as a confidentiality notice, an automated mailbox disclaimer and a full business signature with address and social media presence. These elements are typical in Lampion-related phishing lures, where attackers recycle professional-looking templates to blend into legitimate business communication.

The malicious attachment is delivered as a ZIP file named **COMPROVATIVO-JUNHO_OJLWnObxFOyTZkx_01-06-2026_104.zip**. Once extracted, it contains a relatively large web document (~1.3 MB), artificially inflated with nonsensical markup and randomized strings, likely intended to hinder analysis and evade detection.

When opened in a browser, it renders a convincing fake SAPO Transfer page. SAPO is a widely recognized Portuguese internet portal operated by Altice Portugal, offering services such as email, news and online tools, and its branding is abused here to increase trust and encourage user interaction with the malicious content. This abuse of SAPO branding is not new; SAPO impersonation has featured in prior Lampion campaigns.



Figure 2: Fake SAPO file transfer page

In the background, the malicious JavaScript embedded within the rendered page initiates the retrieval of the next-stage payload from an encrypted URL:



Figure 3: Deobfuscated next-stage downloader

Upon decoding, the string

39103C3420686D562A36077B0D2C3A2D2C20281F3A3D3E340D04642A1A145C211A7D615775694A382C23 resolves to: `hxxps://fat-contabislitaca[.]com/js/1898.php`

Once the download is completed successfully, the retrieved JavaScript is dynamically injected into the already loaded document and executed. The script achieves this by creating a new `<script>` element, assigning the downloaded content to its `textContent` property, and appending it to the page's `<head>` section.



Figure 4: Script attach

We assess with moderate confidence that the campaign's infrastructure employs strict geofencing and / or victim-tracking mechanisms, potentially restricting payload delivery. As a result, obtaining the next-stage payload outside of a live infection chain is extremely challenging.

Second stage VBS

The second-stage VBS scripts follow the same naming convention as the ZIP archives and HTML lures used earlier in the infection chain, maintaining the appearance of legitimate financial or administrative documents. Examples observed during this campaign include:

`Comprovativo_Junho_15-06-2026-WjGAxGL.vbs`

`Comprovativo_Maio_18-05-2026-pXiaBxQ.vbs`

Like the preceding stages, these scripts are heavily obfuscated. The sample analyzed for this report was approximately 7MB in size, despite containing only around 22KB of actual code. The remaining content consists primarily of junk variables, unnecessary functions, and encoded strings designed to inflate the file size, hinder static analysis, and evade signature-based detection. After deobfuscation, we determined that this stage performs two primary functions:

Dynamically constructs a downloader script and writes it to the `%TEMP%` directory.

Creates a scheduled task to orchestrate the download and execution of the final VBS stage.



Figure 5: Scheduled task creation



Figure 6: Dynamic script creation

VBS final stage

The final stage represents the most complex component of the infection chain, both in size and functionality. After removing extensive junk code and obfuscation layers, the core logic spans approximately 1,000 lines of code. At a high level, its behavior includes:

- Enforces a single instance via WMI (Win32_Process command lines).

- Wipes every other *.vbs in %TEMP% except self.

- Computes victimId = MD5(user|host|BIOS|MB|GPU) and uses it as the bot-id when talking to C2.

- Checks a marker file under %APPDATA% - if the previously downloaded payload exists, quits; otherwise polls a C2 URL to get a download URL + payload name (response is "url|name").

- Builds a destination path under %APPDATA%\<timestamp>\<timestamp>.dll.

- Schedules persistence/move tasks via the Task Scheduler service.

- Sends a Base64 analytics beacon (host, AV product display name, user, computer name, machine fingerprint) to the C2.

- Downloads the payload in 10MB HTTP Range chunks, stitches them with ADODB.Stream, then schedules a `cmd /c move` task to put it at its final destination and writes a Base64-encoded marker file.

- Schedules a delayed self-restart task (five minutes out).

The primary objective of this stage is the retrieval and deployment of the final DLL payload into the %APPDATA% directory. For example:

C:\Users****\AppData\Roaming\20260304012702\20260304012702.dll



Figure 7: Download of RAT component

The downloaded DLL is executed via rundll32, invoking the exported function **jangadeiro**. The export name is itself a breadcrumb: Jangadeiro is Portuguese for the fisherman who pilots a [jangada](#) raft, a distinctly Brazilian term consistent with the malware's Brazilian origin. Telemetry indicates that the payload is unusually large (~750MB), a size we attribute to extensive junk padding rather than functional complexity — consistent with Lampion's established anti-analysis style and with independent reporting of 700MB+ Lampion loaders, which explains the use of chunked HTTP range-based downloading. The DLL functions as the main RAT component, enabling full remote access and data exfiltration capabilities.

Statistics

The observed activity is overwhelmingly concentrated in Portugal, which accounts for 94.6% of all detections. This strong geographic skew indicates a highly targeted campaign, likely leveraging Portuguese-language lures to maximize credibility and engagement among victims in the region.



Figure 8: Distribution of Lampion's campaign by country

A small minority of activity was observed outside the primary target area, including Spain (4.3%) and the United Kingdom (1.1%). We assess these are likely incidental exposures or spillover outside the intended targeting scope, while the overall distribution strongly reinforces the assessment that the campaign is almost exclusively focused on Portugal.

Conclusion

The latest Lampion campaign demonstrates that the threat actor remains active and continues to refine its delivery techniques while maintaining a clear focus on Portuguese victims. By combining localized phishing lures and a multistage infection chain, the operators increase the likelihood of successful compromise while reducing the visibility of malicious activity.

A notable characteristic of this campaign is the extensive use of obfuscation across every stage of the infection process. From oversized HTML and VBS files padded with junk code to encrypted URLs and dynamically generated scripts, the threat actor employs multiple layers of evasion designed to hinder static analysis and complicate detection. The deliberate separation of execution into multiple independent stages further obscures the relationship between individual events, making the attack chain more difficult to reconstruct and monitor.

MITRE ATT&CK mapping

The observed infection chain maps to the following ATT&CK techniques:

T1566.001 — Phishing: Spear-phishing Attachment (ZIP-attached HTML lure)

T1204.002 — User Execution: Malicious File

T1027 / T1027.001 — Obfuscated Files or Information / Binary Padding (junk-inflated HTML, VBS and the ~750 MB DLL)

T1059.007 — JavaScript (in-page next-stage loader); T1059.005 — Visual Basic (multi-stage VBS)

T1053.005 — Scheduled Task/Job: Scheduled Task (download, move and self-restart tasks)

T1105 — Ingress Tool Transfer (Range-chunked payload download)

T1218.011 — System Binary Proxy Execution: Rundll32 (export jangadeiro)

T1071.001 — Application Layer Protocol: Web Protocols (HTTP C2)

T1518.001 — Security Software Discovery (AV product name in the beacon); T1497 — Virtualization/Sandbox Evasion

Detection and hunting

Defenders can hunt for the following high-signal artifacts from this chain:

rundll32.exe loading a DLL from %APPDATA%\<14-digit timestamp>\<same timestamp>.dll, especially with an export named jangadeiro (or another Portuguese-word export).

Scheduled tasks running cmd /c move into %APPDATA%, and a task scheduling a self-restart ~5 minutes out.

VBScript in %TEMP% that reassembles a file via ADODB.Stream from Range-based HTTP chunks, or that wipes other *.vbs in %TEMP%.

An unusually large (hundreds of MB) DLL written under %APPDATA% in a timestamp-named folder.

Detection by Acronis

This threat is detected and blocked by Acronis [EDR](#) / [XDR](#):



Figure 9: Detection and incident

Indicators of Compromise (IoCs)

Phishing emails (SHA-256):

87efeada5fe39a94cefc6151fd84af223d0e0e2b070daec606274481ed87b87b
ab46f7c4d3f717bb1e61d2f236917976d2a85be6958ae099fee79ea6e9031e37

Zip attachments (SHA-256):

b1c101bd1ba134ffbea61f9fac2b7c8fbd13ca113a37944abdc131ef86da92ac
c6618bb692fb3f5d7959f8db1fedaaac5e8a36fb901397a008aa2b88874448fd

HTML files (SHA-256):

036c8f32012abdc9a389ae9c284da89505e830bca74eb1aa9ea3794b067aab6
d25d32478ae67403484a309591b6409224d26ca3d094c5ccd8428ebef7efcfd1
643c0093baec45952a46b0210f7a6f8fb26883b396b66f1cb609c5b55e6dae1e
050e84d134a32ed7c4885a9d57ce37f8ae5f910960b67e2156941961bd5781ba

Second stage VBS (SHA-256):

7ad89fb0a4a5449a381b8f540238193019673adc7cfb1c008dcd14a745891551
1bd347ce5deee3d783a038e2d2d224bc30cc074e0471a3897c5409ce99816dc9

Final stage VBS (SHA-256):

1541c23f34eb05dfcbede3830741427681d719cee1dfd397a2c04110e0fa81b2
fe769fd85a7440751e1508614c8d9ef0de00bece803329bf3318ff863a146216

Involved domains:

auto-contabilistica.com

autoridade-contabilistica.org

autoridade-financeira.com

fat-contabilistica.com

VBS final stage C2 hosts (defanged): (time-bound; validate before blocking. These IP-based hosts are ephemeral and may be reassigned to unrelated tenants.)

hxxp://18.218.184.201/03_metal7342/trapezio.php

hxxp://18.222.100.142/17_moldura8210/regerem.php

hxxp://18.222.100.142/18_prateleira1967/revigore.php

hxxp://3.135.194.95/09_nsabdo/receado.php

hxxp://3.139.85.102/17_eudhfj/regerem.php

hxxp://3.139.85.102/18_vdsyuh/revigore.php

hxxp://3.139.85.102/20_fjegydk/destravares.php

hxxp://3.141.199.105/13_ytdshe/reimpresso.php

hxxp://3.141.199.105/15_rjhsymc/unificador.php

hxxp://3.141.199.105/16_kdsgyue/raquete.php

hxxp://3.144.37.134/01_sdneow/fruais.php

hxxp://3.144.37.134/02_sjdhie/reestruturado.php

hxxp://3.144.37.134/03_osneops/trapezio.php

hxxp://3.148.240.228/05_dnwodu/equivaler.php

hxxp://3.148.240.228/06_sndiws/galgassems.php

hxxp://3.150.134.118/05_papel6197/equivaler.php

hxxp://3.150.134.118/06_couro8254/galgassems.php

hxxp://52.14.160.173/10_algodao9148/reunia.php