Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

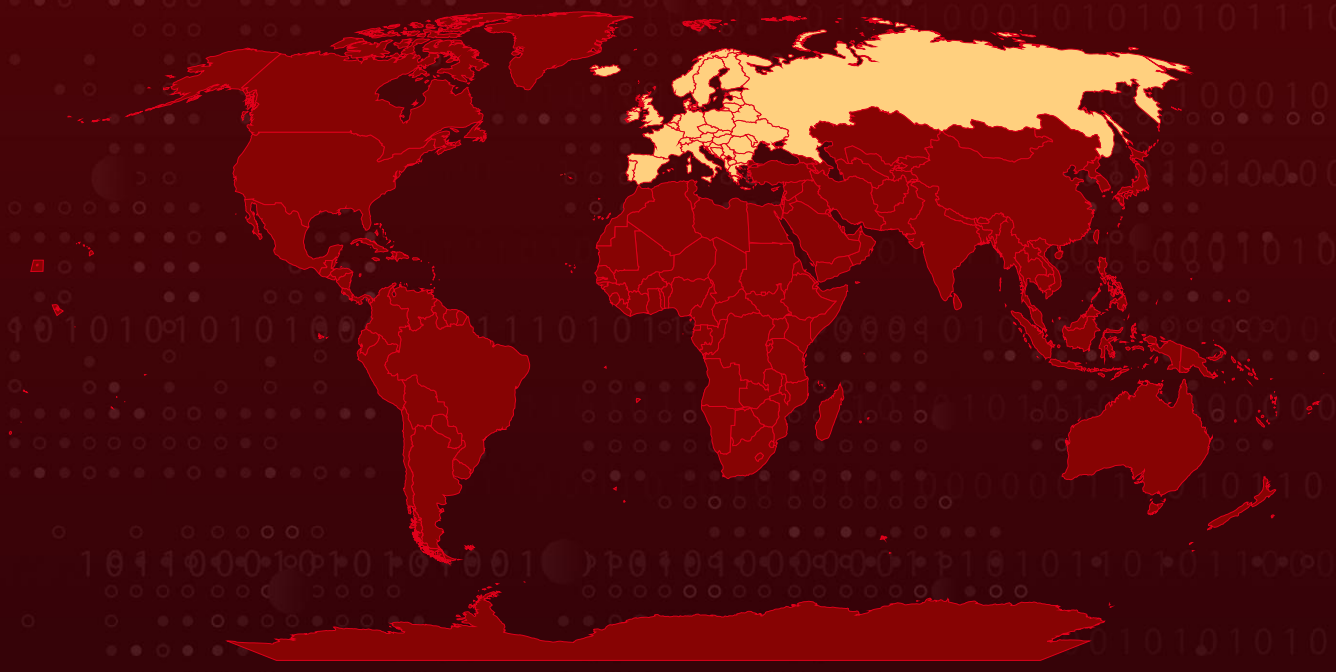
PHALT#BLYX: Fake BSOD Campaign Targets Hospitality

Date of Publication	Admiralty Code	TA Number
January 7, 2026	A1	TA2026006

Summary

First Seen: Late 2025
Targeted Region: Europe
Targeted Platform: Windows
Targeted Industry: Hospitality
Threat Actor: Russian-linked (Unattributed)
Malware: DCRat
Campaign: PHALT#BLYX
Attack: PHALT#BLYX is an active malware campaign targeting the European hospitality sector through phishing emails impersonating Booking.com with fake reservation cancellations. The attack uses ClickFix social engineering and fake Blue Screen of Death tactics to trick victims into manually executing malicious PowerShell commands. The infection chain abuses legitimate Windows tools (MSBuild.exe) to bypass security controls and deploys DCRat, a Russian-linked remote access trojan capable of keylogging, remote control, and process injection. Organizations should monitor for suspicious MSBuild executions, Defender exclusion modifications, and connections to C2 infrastructure on port 3535.

Attack Regions



Attack Details

#1

The PHALT#BLYX campaign is a sophisticated malware infection chain that combines phishing, social engineering, and abuse of trusted Windows tools to evade detection. It primarily targets the hospitality sector in Europe, especially hotel staff handling online reservations. The attack begins with phishing emails impersonating Booking.com, using urgent booking cancellation themes with significant financial charges to pressure recipients into clicking embedded links.

#2

Once the victim clicks the link, they are redirected to a convincing fake Booking.com webpage hosted on a malicious domain. The page first displays a fake browser error stating "Loading is taking too long" with a "Refresh page" button. Clicking this triggers a browser-based full-screen fake Windows Blue Screen of Death (BSOD). This technique, known as ClickFix, manipulates users into pressing Win+R and pasting a command that has already been silently copied to their clipboard.

#3

By following these instructions, the victim manually executes a malicious PowerShell command. This script downloads a malicious MSBuild project file (v.proj) and abuses MSBuild.exe, a legitimate Microsoft build tool, to compile and execute it locally. Before downloading payloads, the malware adds Windows Defender exclusions for the ProgramData directory and critical file extensions (.exe, .ps1, .proj). If running without admin privileges, it employs "UAC Spam“, repeatedly prompting for elevation until the user complies. Persistence is established through an unconventional Internet Shortcut file (DeleteApp.url) in the Startup folder.

#4

The final payload is a customized DCRat variant, a well-known remote access trojan linked to Russian threat actors, evidenced by Russian-language debug strings found in the code. DCRat provides capabilities including remote control, keylogging, and process hollowing into legitimate binaries like aspnet_compiler.exe. The campaign demonstrates technical maturity, highlighting how modern threats increasingly rely on user interaction and trusted system tools rather than traditional exploit-based delivery methods.

Recommendations

User Awareness & Training: Educate employees to recognize phishing emails that use urgency, financial pressure, or impersonate trusted platforms like Booking.com. Train users to identify fake browser-based error screens and BSODs. Reinforce that legitimate system errors never ask users to run commands manually.

Restrict Trusted System Tools: Limit the use of high-risk built-in tools such as msbuild.exe and powershell.exe for non-developer users. Apply application control policies (WDAC/AppLocker) to prevent misuse of trusted binaries. Monitor and alert on unusual or user-initiated executions of these tools.

Enhance Endpoint Monitoring: Enable detailed process creation and command-line logging across endpoints. Turn on PowerShell Script Block Logging to capture malicious scripts. Tune EDR solutions to detect process injection, persistence, and defense evasion behavior.

Strengthen Email & Web Security: Use advanced email filtering to detect brand impersonation and phishing campaigns. Block newly registered and look-alike domains via DNS and web gateways. Continuously test defenses through phishing simulations.

Incident Response Readiness: Create detection rules for abnormal MSBuild and PowerShell execution chains. Prepare response playbooks for RAT infections like DCRat. Ensure rapid isolation and forensic analysis of affected endpoints.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0011 Command and Control
TA0003 Persistence	TA0005 Defense Evasion	TA0004 Privilege Escalation	TA0006 Credential Access
T1566.002 Spearphishing Link	T1566 Phishing	T1059.001 PowerShell	T1059 Command and Scripting Interpreter

T1127 Trusted Developer Utilities Proxy Execution	T1204 User Execution	T1562.001 Disable or Modify Tools	T1562 Impair Defenses
T1127.001 MSBuild	T1204.002 Malicious File	T1055.012 Process Hollowing	T1055 Process Injection
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1095 Non-Application Layer Protocol	T1204.001 Malicious Link
T1548 Abuse Elevation Control Mechanism	T1036.005 Match Legitimate Name or Location	T1036 Masquerading	T1027 Obfuscated Files or Information
T1548.002 Bypass User Account Control	T1027.002 Software Packing	T1140 Deobfuscate/Decode Files or Information	T1056.001 Keylogging
T1056 Input Capture			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	194[.]169[.]163[.]140, 193[.]221[.]200[.]233, 13[.]223[.]25[.]84
Domains	Oncameraworkout[.]com/ksbo, low-house[.]com, asj77[.]com, asj88[.]com, asj99[.]com, wmk77[.]com, 8eh18dhq9wd[.]click
URL	hxxp[:]//2fa-bns[.]com

TYPE	VALUE
File Names	Ps1.ps1, payload_1.ps1, .ps1, v.proj, v.proj.ps1, Stub.exe/Staxs.exe/tydb7.exe, Stub.exe, Stub.exe, Stub.exe, Stub.exe, Stub.exe, Stub.exe, Stub.exe, DeleteApp.url, Wwigu.exe, Wwigu.exe, Lbpyjxefa.dll
SHA256	cd3604fb9fe210261de11921ff1bea0a7bf948ad477d063e17863cede1fadc41, 13b25ae54f3a28f6d01be29bee045e1842b1ebb6fd8d6aca23783791a461d9dd, 9fac0304cfa56ca5232f61034a796d99b921ba8405166743a5d1b447a7389e4f, cd3604fb9fe210261de11921ff1bea0a7bf948ad477d063e17863cede1fadc41, 9fc15d50a3df0ac7fb043e098b890d9201c3bb56a592f168a3a89e7581bc7a7d, bf374d8e2a37ff28b4dc9338b45bbf396b8bf088449d05f00aba3c39c54a3731, 11c1cfce546980287e7d3440033191844b5e5e321052d685f4c9ee49937fa688, 07845fcc83f3b490b9f6b80cb8ebde0be46507395d6cbad8bc57857762f7213a, 08037de4a729634fa818ddf03ddd27c28c89f42158af5ede71cf0ae2d78fa198, 2f3d0c15f1c90c5e004377293eaac02d441eb18b59a944b2f2b6201bb36f0d63, 33f0672159bb8f89a809b1628a6cc7dddae7037a288785cff32d9a7b24e86f4b, 6bd31dfd36ce82e588f37a9ad233c022e0a87b132dc01b93ebbab05b57e5defd, 1f520651958ae1ec9ee788eefe49b9b143630c340dbecd5e9abf56080d2649de,

TYPE	VALUE
SHA256	9c891e9dc6fece95b44bb64123f89ddeab7c5efc95bf071fb44579960 50f10a0, e68a69c93bf149778c4c05a3acb779999bc6d5bcd3d661bfd6656285 f928c18e, 18c75d6f034a1ed389f22883a0007805c7e93af9e43852282aa0c6d5 dafaa970, 91696f9b909c479be23440a9e4072dd8c11716f2ad3241607b542b202ab831ce

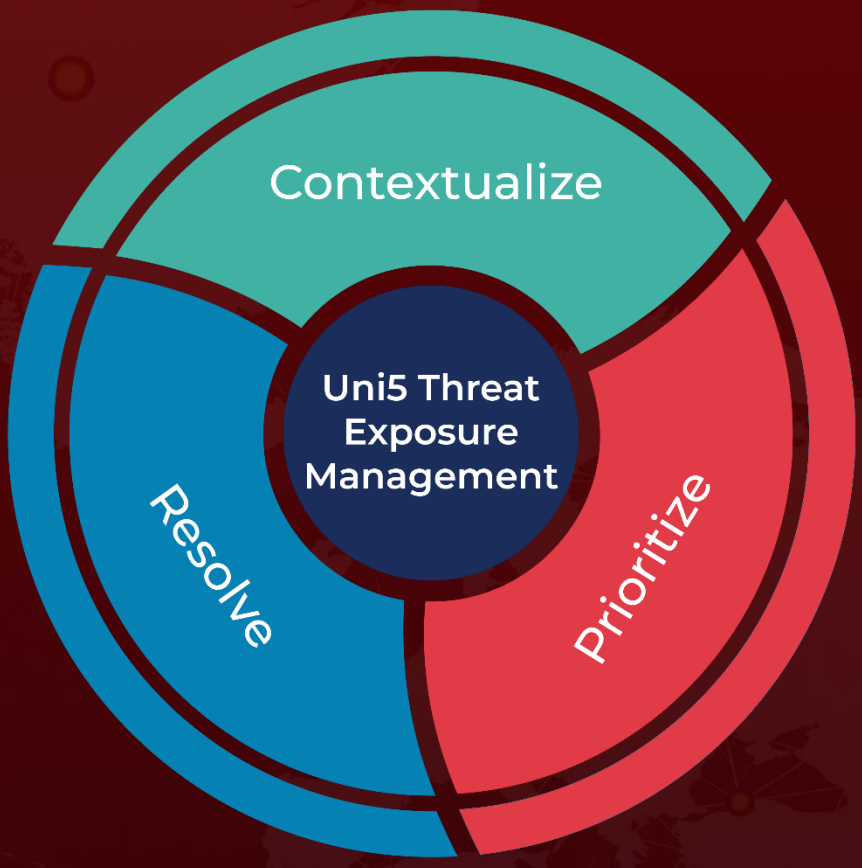
References

https://www.securonix.com/blog/analyzing-phaltblyx-how-fake-bsods-and-trusted-build-tools-are-used-to-construct-a-malware-infection/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 7, 2026 • 7:30 AM

More at www.hivepro.com