Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

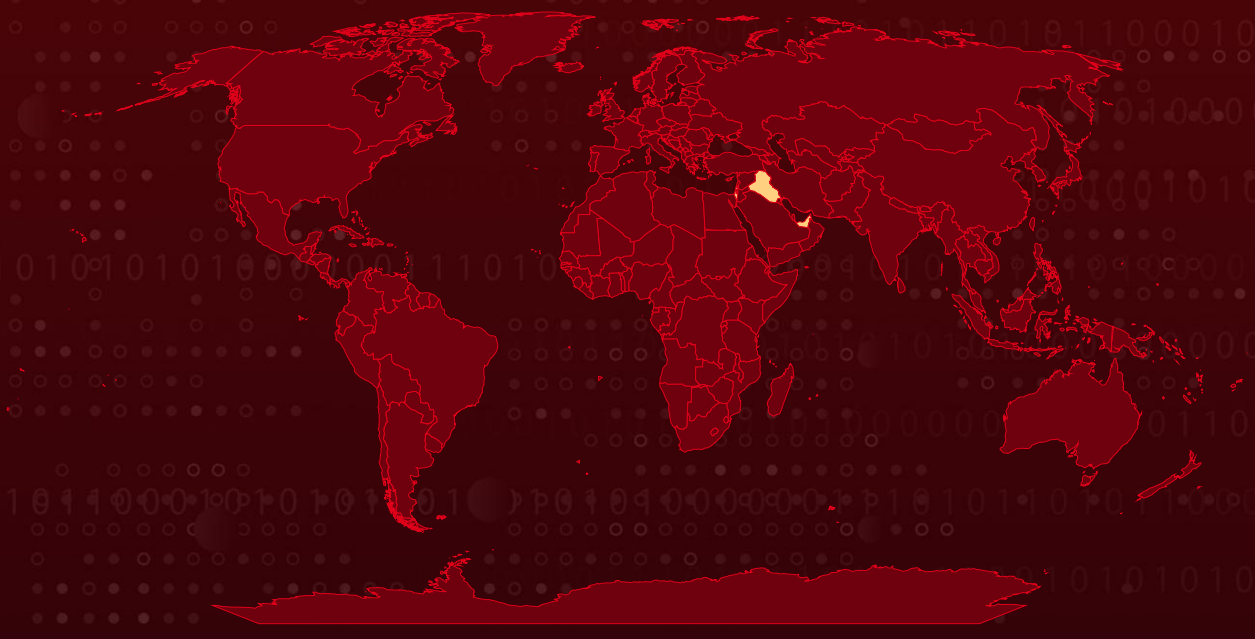
Blinder Tunnel: Iran-Nexus Actor Hides Backdoor in Fake Coding Test

Date of Publication	Admiralty Code	TA Number
October 09, 2026	A1	TA2026293

Summary

First Seen: November 2025
Targeted Regions: Iraq, Israel, United Arab Emirates
Targeted Platform: Windows
Targeted Product: Microsoft Visual Studio
Targeted Industries: Critical Infrastructure, Telecommunications, Aviation
Threat Cluster: CL-STA-1178
Campaign: Blinder Tunnel
Malware: ShelbyLoader, ShelbyC2, PsProxy, Blackwood
Attack: CL-STA-1178, an Iran-nexus threat cluster, is impersonating the Dubai Airports IT department to send a targeted engineer a trojanized Visual Studio coding test that silently launches ShelbyLoader V2 the moment the project is opened. The malware hides its command traffic inside GitHub repositories and issue comments, loads the ShelbyC2 V2 backdoor alongside an in-memory PowerShell engine, and deploys the Blackwood Chisel loader to tunnel covertly into victim networks.

Attack Regions



Attack Details

#1 An Iran-nexus cluster tracked as CL-STA-1178, known for pursuing telecommunications and aviation targets across Iraq, Israel and the UAE, runs the Blinder Tunnel campaign against Iraqi critical infrastructure. After staging infrastructure from November 2025, the operators went live in March 2026, posing as the Dubai Airports IT department to offer an engineer in Iraq a development job. The victim was first told to install a harmless decoy careers portal, then received DubaiAirport_Carrers_IT_Test.zip, a Visual Studio coding test with a personalized readme and a deliberate bug.

#2 The trap springs once the project opens. Its FlightManager.csproj file overrides the GetFrameworkPaths target that Visual Studio runs during its silent background build, so MSBuild copies hidden binaries into %LOCALAPPDATA%\Microsoft\RuntimeBrokers and launches a signed Microsoft hosting process renamed RuntimeBroker.exe. A tampered configuration file then hijacks the .NET AppDomainManager, disables Event Tracing for Windows, and sideloads the malicious RuntimeBroker.dll, known as ShelbyLoader V2.

#3 ShelbyLoader V2 screens for sandboxes, adds a MicrosoftRuntime Run key for persistence, and beacons every 63 seconds to an attacker-owned GitHub repository with a hard-coded token, uploading a host fingerprint and pulling Base64 commands. If the token is revoked, it recovers fresh C2 details from encrypted text hidden in GitHub issue comments. It then decrypts ShelbyC2 V2 in memory, which passes PowerShell scripts to PsProxy.dll to run inside a hidden runspace without starting PowerShell.exe.

#4 In May 2026, the actor added Blackwood, pulled from a second GitHub repository and sideloaded through the same configuration trick. It decrypts an embedded Chisel tunneling tool and opens a reverse SOCKS proxy to an attacker relay, giving operators a covert bridge for pivoting into the internal network.

#5 A Blackwood tunnel server also hosted Google-themed lookalike domains used in May and June 2026 to harvest credentials from an Israeli entity through conflict-themed lures. Iranian-hosted infrastructure, Iranian music-site metadata and a recurring Peaky Blinders theme tie the activity together, showing how one job offer can become a stealthy foothold.

Recommendations

Verify Job Offers and Isolate Coding Tests: Confirm recruiter identity through the company's official careers channel before engaging. Open any unsolicited project files or "assessments" only in an isolated virtual machine, never on corporate workstations.

Lock Down IDE Project Trust: Turn on the IDE's trust settings so downloaded projects need approval before they open. Alert when MSBuild or Visual Studio creates folders under %LOCALAPPDATA% or launches executables from there.

Detect .NET Configuration Tampering: Flag .exe.config files that contain appDomainManagerType or etwEnable="false", especially next to binaries outside Program Files. Also watch for System.Management.Automation.dll being loaded by processes other than PowerShell.

Hunt Sideloading and Persistence: Treat any RuntimeBroker.exe outside System32 as suspicious, along with any signed vshost binary loading unsigned DLLs from user directories. Review the MicrosoftRuntime value under the HKCU Run key.

Monitor GitHub API and Tunneling Traffic: Baseline which hosts and processes are expected to call api.github.com. Flag regular, beacon-like polling of repository contents or issue searches from non-developer processes, and block or alert on reverse SOCKS tunnels over HTTP.

Enforce Phishing-Resistant MFA and Block IOCs: Deploy passkeys or FIDO2-based MFA to blunt credential harvesting through fake Google Drive and login pages. Block the listed IPs and typosquatted domains at the DNS, proxy and email layers.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1589: Gather Victim Identity Information	
	T1598: Phishing for Information	T1598.003: Spearphishing Link
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.006: Web Services
		T1583.003: Virtual Private Server
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.002: Tool
	T1608: Stage Capabilities	T1608.001: Upload Malware
Initial Access	T1566: Phishing	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1127: Trusted Developer Utilities Proxy Execution	T1127.001: MSBuild
	T1574: Hijack Execution Flow	T1574.014: AppDomainManager
		T1574.001: DLL
	T1562: Impair Defenses	T1562.006: Indicator Blocking
	T1036: Masquerading	T1036.003: Rename Legitimate Utilities

Tactic	Technique	Sub-technique
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
		T1027.009: Embedded Payloads
	T1140: Deobfuscate/Decode Files or Information	
	T1620: Reflective Code Loading	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
	T1012: Query Registry	
Command and Control	T1102: Web Service	T1102.002: Bidirectional Communication
		T1102.001: Dead Drop Resolver
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1105: Ingress Tool Transfer	
	T1572: Protocol Tunneling	
	T1090: Proxy	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	6e7d9b33f1e72ea1ede71373a604ecdb060dab7d42055179c1eede9ecd1fd239, f5b12772db6817f7a765a6fe7565fd3d4f87edc28e42fe3ec0244a372a410fc9, 53f35e49eb9b271fd8cbcd3daacb525328dbf159a03dbd1c7adebe0363daa402, 3fd810a3aa0039993393741b32287c367a9a5037a41e826906440887cdd3ed13, 76273382e4252c1f60a2251141e108942494409c7593583207358917 62c0682e, d3561bd4aad003dc3e08157b0891860bb496b80cd6e44901692e08ab1d4e8260, f5ba1645694c62f527ed6ceda8c68a5c3dd92b4032439167e8e937e72803b4bd, 7cc571aca6d8715d9aaad3d83e1bcd30467565d583db1dfe73697c5d00a1f875
IPv4	91[.]107[.]156[.]29, 87[.]248[.]129[.]239, 65[.]109[.]214[.]145, 38[.]180[.]136[.]127
IPv4:Port	65[.]109[.]214[.]145[:]8080
Domains	cloud[.]g-drive[.]cam, googeldrive[.]cam, drivegoogel[.]cam, googelmeet[.]online, meetonline[.]cam, asdfafadafg[.]online
URLs	hxxps[:]//cloud[.]g-drive[.]cam/signin/v2/identifier?from=landing, hxxps[:]//github[.]com/peakyblinders-tm, hxxps[:]//github[.]com/GreenBeret0

TYPE	VALUE
Filename	DubaiAirport_Carrers_IT_Test.zip, FlightManager.csproj, RuntimeBroker.dll, RuntimeBroker.exe.config, RuntimeBrokerApi.dll, PsProxy.dll, Blackwood.dll, Blackwood.dll.conf, vshost32.exe.config, Client.zip, WarUnPublishedDocuments.zip
File Path	%LOCALAPPDATA%\Microsoft\RuntimeBrokers\RuntimeBroker.exe
Registry Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\MicrosoftRuntime

References

https://unit42.paloaltonetworks.com/blinder-tunnel-targets-critical-infrastructure/

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 Demo of **HivePro**.

REPORT GENERATED ON

October 09, 2026 • 07:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com