KPMG Cyber Threat Intelligence Platform

Blinder Tunnel - Delivering Backdoor via Trojanized VS Projects

TLP : Clear

KPMG. Make the Difference.



Blinder Tunnel, first observed in November 2025, is a targeted operation conducted by an Iranian state-aligned threat actor, CL-STA-1178. The operation involves weaponizing native Windows developer files to establish covert access. Across Iraq, Israel, and the United Arab Emirates, it mainly targets organizations within the telecommunications and aviation sectors.

Initial access is gained through recruitment-themed social engineering lures impersonating the Dubai Airports IT department. A trojanized Microsoft Visual Studio coding challenge containing a malicious .csproj file is delivered, enabling the execution of malicious code when the project is loaded, before the developer attempts to compile the code. To evade detection, AppDomainManager hijacking is used to execute ShelbyLoader V2 within a trusted process and disable Event Tracing for Windows (ETW). DLL sideloading is then performed using a renamed, legitimate Microsoft-signed binary, RuntimeBroker.exe, to load the malicious RuntimeBroker.dll payload. Malware deployment is carried out using ShelbyLoader V2 as the primary loader and ShelbyC2 V2 as the primary backdoor, while Blackwood is used as a tunneling tool. To execute PowerShell commands, PsProxy.dll runs commands in memory without launching PowerShell.exe. For command and control (C2), GitHub APIs are misused to fetch decryption keys, payloads, and retrieve commands, while GitHub Issues serve as a fallback C2 mechanism. Network tunneling is enabled by Blackwood, which loads the open-source Chisel utility to establish encrypted TCP tunnels over HTTP with SOCKS5 proxy support, enabling access to compromised internal networks.

Blinder Tunnel's abuse of developer build processes highlights the need to secure developer environments, monitor binaries that load non-standard DLLs outside system directories, and inspect anomalous GitHub API traffic.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Restrict execution of untrusted binaries that load non-standard DLLs outside system directories.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context.

The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Srinivas Potharaju
Partner & HoF
Cyber Security & Tech Mgmt
T: +91 98459 19740
E: srinivasbp@kpmg.com

Sony Anthony
Partner & SSL-HoD
Cyber Defense and IR
T: +91 98455 65222
E: santhony@kpmg.com

Rishabh Dangwal
Partner
Cyber Defense and IR
T: +91 99994 30277
E: rishabhd@kpmg.com

Abhishek Dashora
Director
Cyber Defense and IR
T: +91 88671 86493
E: abhishekdashora@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Blinder Tunnel - Delivering Backdoor via Trojanized VS Projects

TLP : Clear

KPMG. Make the Difference.



Indicators of Compromise: IP Addresses	
91.107.156[.]29	65.109.214[.]145
194.62.249[.]19	87.248.129[.]239
38.180.136[.]127	194.62.249[.]114

Indicators of Compromise: Domains	
meetonline[.]cam	cloud.g-drive[.]cam
drivegoogel[.]cam	googelmeet[.]online
googeldrive[.]cam	asdfafadafg[.]online

Indicators of Compromise: Hashes
9876c685f8bcf351fc06db4b98ee192e
974eb3d5bd550feaea763f6d7f3f2b97
7244a27029d2fb104a598b40e9f284d9
2ab34636eeab843b4bcbb6e44f033eab
b53f5d8baf6840fa3a5ea8e56d208ddf
8a062a2d0741b57fab9635920b17275b
38aa0f535e2c6273ccf4de19a7a0f044
f2f8db8dc4c4f9573e5aa265235c9d49
3d809693b3d63f33126e9eb630fef8ff
5a796cdce448eddbf1aec1c7c186dacf
84cb7188c9f8d70ecdf122a604dfaaf581848bb8
2ec1ca6d4a98da6a76f8f1c703431890518dc01b
aa7f18c1552042d4d0854de69d5c69ee47a21ba2
9842b996277682a136562aa27e08919eac542c15
701f2a5c8d8bdc28e51e11a12955197fbd652698
90f733c6aa7eaa37dbd654ef1f4cedfbb711dc03

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Blinder Tunnel - Delivering Backdoor via Trojanized VS Projects

TLP : Clear

KPMG. Make the Difference.



Indicators of Compromise: Hashes
8c839823f58e8965c770c900be2b2cf14e054871
7fa5ce4031e57e608b4a2f92cacdaf9183dfe76a
f320cd3c6de7efb61b59669ce70c81fc8a94758a
18586ca8e3e3c4633ed3fccd909a0be87ba0a573
052702d652286482863a70eaa37e4fc894f40c8b08dccf245ced46916e7f419f
06d68dcb8088546cb40fb3d7e87d6a593cbdf4cc1e43017604faf786ad6dbd41
3fd810a3aa0039993393741b32287c367a9a5037a41e826906440887cdd3ed13
53f35e49eb9b271fd8cbcd3daacb525328dbf159a03dbd1c7adebe0363daa402
6e7d9b33f1e72ea1ede71373a604ecdb060dab7d42055179c1eede9ecd1fd239
76273382e4252c1f60a2251141e108942494409c759358320735891762c0682e
7cc571aca6d8715d9aaad3d83e1bcd30467565d583db1dfe73697c5d00a1f875
d3561bd4aad003dc3e08157b0891860bb496b80cd6e44901692e08ab1d4e8260
f5b12772db6817f7a765a6fe7565fd3d4f87edc28e42fe3ec0244a372a410fc9
f5ba1645694c62f527ed6ceda8c68a5c3dd92b4032439167e8e937e72803b4bd

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.