Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

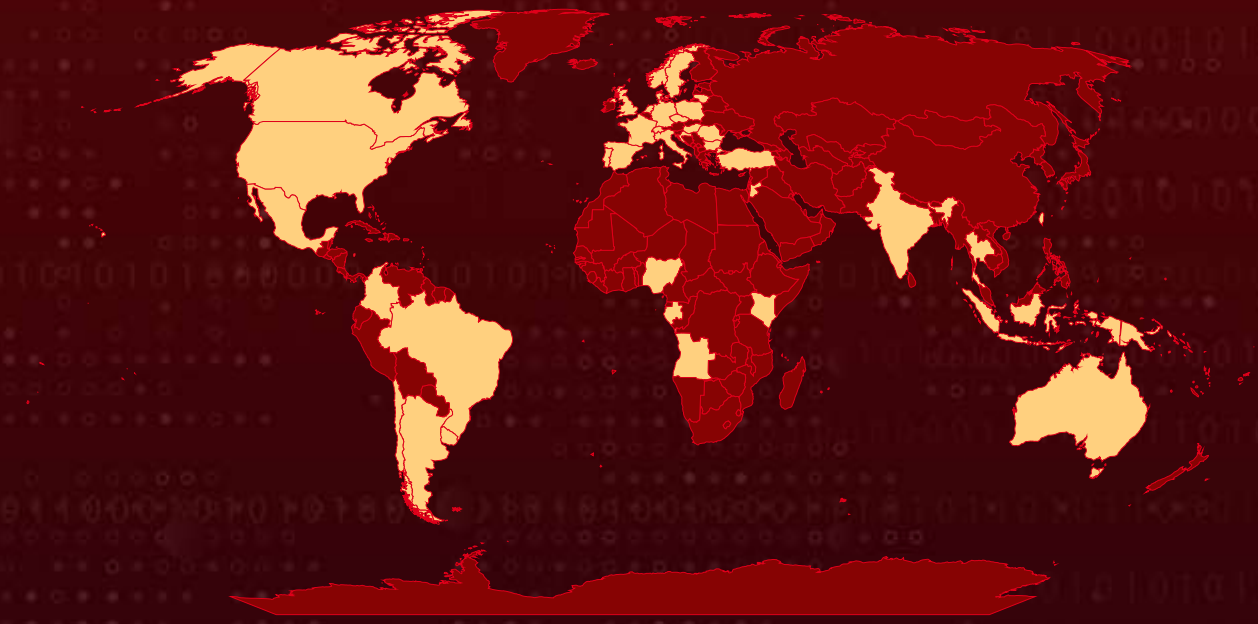
# DeadLock Ransomware Anchors Extortion to the Polygon Blockchain


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| August 14, 2026 | A1 | TA2026232 |

# Summary

**First Seen:** July 2025
**Targeted Regions:** North America, Europe, Asia, South America, Africa, Oceania
**Targeted Platform:** Microsoft Windows
**Targeted Products:** Baidu Antivirus (BdApiUtil.sys kernel driver, abused via BYOVD)
**Targeted Industries:** Professional Services, Manufacturing, Information Technology and IT Consulting, Engineering Services, Transportation, Logistics, Energy, Utilities, Oil and Gas, Healthcare, Pharmaceuticals, Financial Services, Accounting, Government, Municipal, Hospitality, Leisure, Retail, E-Commerce, Mining, Consumer Goods, Chemicals, Education, Research, Legal, Waste and Environmental Services, Agriculture and Food Production
**Malware:** DeadLock ransomware
**Attack:** DeadLock is a financially motivated, human-operated ransomware operation active since mid-2025 that combines double extortion with a decentralized back end. They load a legitimate Baidu antivirus driver with a known flaw (CVE-2024-51324) and use it to kill EDR from the kernel, turning a security product into the weapon that blinds the rest.

## Attack Regions





Targeted  Non-Targeted

## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2024-51324 | Baidu Antivirus Improper Privilege Management Arbitrary Process Termination Vulnerability | Baidu Antivirus | ⊗ | ⊗ | ⊗ |

# Attack Details

**#1**

DeadLock is a financially motivated, human-operated ransomware operation active since July 2025 that combines double extortion with a decentralised back end. Access comes from stolen credentials rather than exploitation of an internet-facing system, using domain and local accounts alongside external remote services. Once inside, operators enable RDP, open inbound TCP 3389 on the Windows firewall, and install AnyDesk for durable remote access.

**#2**

In one intrusion, they held access for five days before deploying the ransomware, adding a fresh AnyDesk instance the day before encryption through a silent install that started the client with Windows, set an unattended-access password, and disabled updates so a version change could not sever the connection. AnyDesk is their main remote access tool and the only non-native service their PowerShell script spares.

**#3**

They then dismantle defences. A legitimate but vulnerable Baidu Antivirus driver, BdApiUtil.sys, is loaded to terminate EDR processes from the kernel via CVE-2024-51324, while a PowerShell script bypasses UAC, disables Defender, stops every service outside a whitelist, and deletes all volume shadow copies. The encryptor then clears and disables every Windows event log channel, empties the recycle bin on all drives, appends a victim ID and the .dlock extension to each encrypted file, and replaces the desktop wallpaper.

**#4**

Its distinguishing feature is the recovery infrastructure. An HTML page dropped alongside the ransom note reads its proxy address and leak-blog content from Polygon smart contracts, relays end-to-end encrypted negotiation traffic through the Session messenger network, and provides an in-browser file explorer for stolen data hosted on Wasabi object storage. Because the proxy address is stored on-chain, operators can repoint their negotiation infrastructure with a single transaction, without altering the malware or registering new DNS records.

# Recommendations

**Block the vulnerable Baidu driver by hash:** Add 'BdApiUtil.sys' to the Microsoft vulnerable driver blocklist and to any equivalent driver allowlisting control, and alert on the file appearing under a renamed guise. In the observed intrusion, the driver was staged as 'DriverGay.sys' in a user's Videos folder, so match on hash and on the device name '\\.\BdApiUtil' rather than on filename alone.

**Enable Microsoft vulnerable driver blocklist and HVCI:** Turn on the Windows driver blocklist and, where hardware permits, Hypervisor-Protected Code Integrity so unsigned and known-abusable kernel drivers cannot load. This is the single control that most reliably breaks the BYOVD step in this attack chain regardless of which vulnerable driver the actor rotates to next.

**Hunt for the DeadLock file artefacts now:** Sweep endpoints and file shares for the '.dlock' extension, 'HOW_RECOVER.<ID>.txt', 'RECOVERY_CHAT.<ID>.html', and '<ID>.ico' and '<ID>.bmp' files written to 'C:\ProgramData'. The HTML note is dropped to every drive root and every Desktop folder, which makes it a high-yield hunt target, and note that the text note is only written on the second directory-processing pass, so its absence does not rule out an infection.

**Hunt for shadow copy destruction and service mass-disabling:** Alert on 'vssadmin', WMI or PowerShell deletion of volume shadow copies, and on bulk 'sc config' operations setting service start types to disabled. A script that stops every service outside a whitelist is a strong pre-encryption indicator and often the last point at which the chain can be interrupted.

**Monitor for public blockchain RPC traffic from endpoints:** Outbound connections from a workstation or server to public Polygon RPC endpoints are anomalous in most enterprises and here indicate the recovery-chat page is resolving its proxy address. Treat DNS queries and HTTP requests to blockchain RPC providers from non-development hosts as an investigative lead, and do not blocklist those endpoints wholesale, since they are legitimate shared infrastructure.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1078: Valid Accounts | T1078.002: Domain Accounts |
| | | T1078.003: Local Accounts |
| | T1133: External Remote Services | |
| Execution | T1059: Command and Scripting Interpreter | T1059.001: PowerShell |
| | | T1059.003: Windows Command Shell |
| | T1106: Native API | |
| | T1569: System Services | T1569.002: Service Execution |
| Persistence | T1219: Remote Access Tools | T1219.002: Remote Desktop Software |
| | T1543: Create or Modify System Process | T1543.003: Windows Service |
| Privilege Escalation | T1548: Abuse Elevation Control Mechanism | T1548.002: Bypass User Account Control |
| | T1134: Access Token Manipulation | |
| | T1068: Exploitation for Privilege Escalation | |
| Defense Evasion | T1211: Exploitation for Defense Evasion | |
| | T1562: Impair Defenses | T1562.001: Disable or Modify Tools |
| | | T1562.002: Disable Windows Event Logging |
| | | T1562.004: Disable or Modify System Firewall |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Defense Evasion | T1070: Indicator Removal | T1070.001: Clear Windows Event Logs |
| | | T1070.004: File Deletion |
| | T1112: Modify Registry | |
| | T1055: Process Injection | |
| | T1497: Virtualization/Sandbox Evasion | T1497.003: Time Based Evasion |
| | T1480: Execution Guardrails | |
| | T1036: Masquerading | T1036.005: Match Legitimate Resource Name or Location |
| | T1006: Direct Volume Access | |
| Credential Access | T1003: OS Credential Dumping | T1003.001: LSASS Memory |
| | | T1003.005: Cached Domain Credentials |
| Discovery | T1018: Remote System Discovery | |
| | T1069: Permission Groups Discovery | T1069.002: Domain Groups |
| | T1033: System Owner/User Discovery | |
| | T1046: Network Service Discovery | |
| | T1057: Process Discovery | |
| | T1083: File and Directory Discovery | |
| | T1614: System Location Discovery | T1614.001: System Language Discovery |
| | T1135: Network Share Discovery | |
| Lateral Movement | T1021: Remote Services | T1021.001: Remote Desktop Protocol |
| | | T1021.002: SMB/Windows Admin Shares |
| | T1218: System Binary Proxy Execution | T1218.014: MMC |
| Collection | T1039: Data from Network Shared Drive | |
| Command and Control | T1102: Web Service | T1102.002: Bidirectional Communication |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Command and Control | T1071: Application Layer Protocol | T1071.001: Web Protocols |
| | T1573: Encrypted Channel | T1573.002: Asymmetric Cryptography |
| | T1090: Proxy | T1090.002: External Proxy |
| Exfiltration | T1567: Exfiltration Over Web Service | |
| Impact | T1486: Data Encrypted for Impact | |
| | T1489: Service Stop | |
| | T1490: Inhibit System Recovery | |
| | T1491: Defacement | T1491.001: Internal Defacement |
| | T1657: Financial Theft | |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | a1fdf65020ce4a0f0940c793c6425baf8a0b994ec48b9baaf72788661a9d29f4, 2d89fb7455ff3ebf6b965d8b1113857607f7fbda4c752ccb591dbc1dc14ba0da, 47ec51b5f0ede1e70bd66f3f0152f9eb536d534565dbb7fcc3a05f542dbe4428, be1037fac396cf54fb9e25c48e5b0039b3911bb8426cbf52c9433ba06c0685ce, 3cd5703d285ed2753434f14f8da933010ecfdc1e5009d0e438188aaf85501612, 3c1b9df801b9abbb3684670822f367b5b8cda566b749f457821b6481606995b3, c9cc95ff8f2998229394dfd31c2bd6b723e826a3ca5e008d2b5be19ba419ae2c, 2b214bddaab130c274de6204af6dba5aeec7433da99aa950022fa306421a6d32, 50a32403f8d323129ac25761b62e085f24e2a998e5c151084d5819271c9e7d28, e3edfeb4f36c4e79bcd2849b27001bf0f0072cb212d26ffb7a19a4469f711c6a, 4f61f20fa1edfd0ce1de2ca8110c725c9d9c16a9680748c12042a3302054fc72, 5a1f1b6c81b6686b6810012a3413c73625736c8bda193ac1f785aac17bc8a347, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | eeef8e787e1aa0e59e519fe36a9376a20b942d9eb72a4ec0bcc3742752581000, b44a512e36ba155019dee5aa5b291cd32e15eb0dfa1a8c1de56c4ec84fff1694, 3a6880053382cd25f16a8d76c440905beb553c6c3d998eba3f02d064751c4d04, 4e7b5ce8aa9d4095a2c0184e20b4175fc91e82b4ce3199b7b3bcf3b2f89a5298, 6e024b4e1c4d9e2873de93461cf8b5172c03cba530a89ec65b88710a45c260bb, 9d6ac8103e546ba984e10bf3e6ecdd0b88f18e5a84d64ac6782fae8bc6743f00, 9e69862c4a5b34c12c10fbf2d345e7fd654c71adcb5f9b6524d7a54209fce343, c64a4a3b67438337f31bbd0425e1e016c8ba72b3db38cb69fe24d7b4b4b6c66b, e10da901a4359348b2bdfb468f35800c7fee888dad8dd6b41f8da805ebf4d2a7, 32198295d2a2700b9895fff999c2b233f9befb0bc175815ec4b71ee926b6edfc |
| SHA1 | e5ba4affd0f49a9e451aa913115cf16b481fe1dc, 45f7f7e87d18fbe71745a0cc170ae08571c2ba0d, 2204d64b82765db4598714fe8bc6e71a24958a7f, 235d6bdf25437b0b004152a263cb483aac08fd10 |
| MD5 | 505d23c7a66a02239056ac3cfed24132, 9a4dcce25a87819585aa0a1dd16186c8, 4374eb7807fbcb767ae3a6202b4dd8f8, c8e16b76ae25d2f27e581a9bef134ea8 |
| IPv4 | 138[.]226[.]236[.]51, 94[.]74[.]164[.]207 |
| Domains | deadlock[.]liveblog365[.]com, dlock[.]liveblog365[.]com, deadlockblog[.]great-site[.]net, deadlockblog[.]medianewsonline[.]com |
| TOR Address | deadblogdbdu5wprek7wa2o4ce7rnt6u6ntqeud3hzjjcveosgpsqqqd[.]onion |
| URLs | hxxps[:]//deadlock[.]liveblog365[.]com/, hxxp[:]//138[.]226[.]236[.]51/prrq[.]php, hxxp[:]//94[.]74[.]164[.]207/prrq[.]php, hxxps[:]//94[.]74[.]164[.]207/prrq[.]php, hxxps[:]//biggoalsports[.]co[.]za/minif[.]php, hxxps[:]//nmsneustadtl[.]ac[.]at/xml[.]php, |

| TYPE | VALUE |
|---|---|
| URLs | hxxps[:]//envisionreg[.]com/wp-activate[.]php,<br>hxxp[:]//sitecom[.]com,<br>hxxps[:]//hamzit[.]tra,<br>hxxp[:]//guel[.]cm |
| Filename | svhost.exe,<br>stop.ps1,<br>EDRGay.exe,<br>DriverGay.sys,<br>BdApiUtil.sys,<br>HOW_RECOVER.<UID>.txt,<br>RECOVERY_CHAT.<UID>.html,<br>READ ME.<hex_identifier>.txt,<br>run.txt |
| File Path | C:\ProgramData\<UID>.ico,<br>C:\ProgramData\<UID>.bmp,<br>C:\Documents and Settings\All Users\Application Data\<UID>.bmp,<br>C:\Program Files (x86)\AnyDesk\AnyDesk.exe |
| Registry Key | HKLM\SOFTWARE\Classes\.dlock\DefaultIcon,<br>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Wallpaper,<br>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels,<br>HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server |
| Session ID | 05084f9b14b02f4ffa97795a60ab1fafaf5128e3259c75459aaaeaebc80c14da78,<br>05b0c8da191a5b3c41105fa034a31784c6d595c49655f232e10e06277ee145c07c,<br>057726c909af65969646b040bbbfa5c4df67f5166a33cbac6cd9e1302b0b3ca148 |
| Tox ID | 50DADDED26D859469371938B793456D8210A5AE02DD3C42979F5E52411BCB648F1CA68A5EDE5 |
| Polygon Contract Address | 0x8EF7c3e531d871D3B9D559722DE77EB1dEc19dAe,<br>0x757984507c82c8dA1d3969c535dB5706eEE6426C,<br>0xAc9f868E285C8141617a97b85b667f229147815c |
| Polygon Wallet Address | 0x8f2fef1339E0d90362F3cEAd9C27B661d964a022 |
| Cryptographic Key | 03bf50bbf97c4e951e66ff12b689a37a3ce675b4921e254eae76da77573843e4a9 |
| File Extension | .dlock |

# Recent Breaches

https://ltg.com.ph
https://www.ahenklab.com.tr
https://diater.com/en
https://pasello.com
https://takisbiotech.com
https://www.hasltda.com
https://tesco-engineers.com
https://www.highclasscarlimo.com
https://www.westafricanresources.com
https://www.caspianone.com
https://sbmp.ch
https://www.hidromek.com
https://www.kemek.eu
https://kenha.co.ke
https://www.bioresearch.pl
https://relesa.com.ar
https://gruporelesa.com
https://carrier.se
https://enedopower.com
https://powernet.fi
https://inissionpower.com
https://toscanacentro.cna.it
https://vinilon.com
https://aldacogrupoavance.es
https://weinberg.hu
https://mortongroveparks.com
https://www.lasevillanita-online.com
https://cpasch.com
https://www.wibeats.it
https://grupovanguardia.com
https://www.whm.de
https://www.doctususa.com
https://acu.com.uy
https://ciati.com.ar
https://quetzalquimica.com
https://abhayprabhavana.org
https://gmm.com.tr
https://www.3gisolutions.com
https://grupolider-ao.com
https://grupoactual.pt
https://www.barcargolift.pl
https://baer-cargolift.pl
https://expresokna.pl
https://www.tptoys.com

https://www.ifceuropa.com
https://esnova.com
https://www.noegasystems.com/en
https://iask.hu/en
https://finamgabon.com
https://www.afw.sg
https://www.nipponexpressitalia.com
https://www.nuovatraconf.it
https://www.francovago-transitarios.pt
https://bers.bg
https://www.muzeumvalassko.cz
https://www.bredaenergia.it
https://autopark.com.br
https://ville-ouangani.yt
https://www.seciltr.com
https://www.cad93.it
https://www.fidelitypensionmanagers.com
https://nobani.com
https://www.chenghengpaper.com
https://donjon.com.sg
https://tele-finity.com
https://www.hornavanhotell.se
https://summa4.es
https://www.fortune-chemical.com
https://rtpbz.ro

## References


https://www.microsoft.com/en-us/security/blog/2026/08/10/deadlock-ransomware-breaking-down-a-rust-based-encryptor-with-decentralized-recovery-infrastructure/

https://socprime.com/active-threats/deadlock-ransomware-analysis/

https://www.group-ib.com/blog/deadlock-ransomware-polygon-smart-contracts/

https://blog.talosintelligence.com/byovd-loader-deadlock-ransomware/

https://github.com/magicsword-io/LOLDrivers/issues/204

# 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

**August 14, 2026 • 01:00 AM**



More at www.hivepro.com