

Forum:[Hack Forums](#)

Thread: [Beaconism](#) | [EDR/XDR EVASION](#) | [.DLL Sideloadng Implant](#) |

Beaconism - August 15, 2025, 4:23 pm

Beaconism DLL Sideloadng

No Cert - No Problem

The Beaconism DLL Sideloadng Solution delivers advanced persistence and payload execution through Windows DLL sideloading vulnerabilities. Built on our proven Beaconism implant framework, it offers robust evasion of EDR, antivirus, and behavioral analytics at a competitive price. Ideal for red teaming and penetration testing, it ensures covert operation by exploiting legitimate system processes.

Technical Features DLL Sideloadng: Exploits Windows DLL search order to load a malicious DLL via a trusted executable, evading signature and heuristic detection.

Evasion Framework: Features obfuscation, anti-analysis, and dynamic code adaptation to bypass EDR hooks and memory scanning. Proprietary Persistence: Kernel-aware, registry-based startup mechanism for resilient, undetectable persistence.

Compatibility: Supports Windows 10 and 11 (x64), with minimal resource usage for seamless execution.

Components java-rmi.exe (Primary Stub; periodically updated):

Role: Loads the malicious DLL using Windows DLL search order, masquerading as a Java RMI application.

Behavior: Brief console window appears due to Java-based architecture; does not impact stealth.

Obfuscation: Code-level obfuscation and polymorphism to evade static analysis and sandboxes.

Beaconism DLL:

Payload: Executes in-memory payloads with minimal disk footprint.

Evasion: Anti-debugging, anti-VM, and encrypted communications.

Dependency-Free: Operates independently once loaded.

For detailed evasion techniques, refer to Beaconism | State Of Art modular loader

Deployment Guidelines

1. Standard Deployment: Distribute the folder containing java-rmi.exe and the DLL to ensure proper sideloading via the local directory search path.

2. Custom Initial Access: Use .lnk, .hta, or .pdf vectors for delivery. Do not add custom persistence—our kernel-hardened mechanism is pre-configured and conflicts with external implementations.

3. Execution Requirements: Compatible with Windows 10/11 (x64). Files must remain in the same directory.

Technical Warnings File Integrity: Do not rename java-rmi.exe or the DLL to maintain the sideloading chain.

Directory Co-Location: Files must stay in the same directory to avoid loading legitimate libraries.

Detection Mitigation: Suppress console window visibility via scripting if needed. Avoid sandboxed environments with aggressive logging.

Testing: Validate in a controlled environment to confirm evasion and payload execution.

* Updates: Regular patches for java-rmi.exe and DLL to counter new Windows updates and EDR signatures.

Pricing and Availability

Competitively priced for advanced operators, with bulk discounts for enterprise campaigns. Contact

us for a quote or custom payload integration via support channels.

Price: 400\$ per crypt.

Contact:

Telegram @BEACONISM_SUPPORT

Sticky Bot - August 15, 2025, 4:53 pm

Hi, I'm Sticky Bot. The owner of this thread has purchased a Paid Sticky. Hack Forums does not get involved in deals or deal disputes. We do not vouch for the product or the service offered by members. Please note that all deals are at your own risk. The sticky will expire on Aug 22, 2025. If you or a loved one are interested in buying a sticky please visit this page: [Buy Sticky](#). For more information about Paid Stickies you can read our [Help Doc](#).

SlimeSkeet - August 17, 2025, 8:15 am

Lol it shows a console screen, and wtf is kernel aware registry persistence the oldest trick in the book but now it's suddenly 'kernel aware' whatever that means

LOVESOSA098997 - August 19, 2025, 8:15 am

thanks for sharing

Beaconism - August 25, 2025, 10:05 am

(Aug 17, 2025 08:15 AM)SlimeSkeet Wrote: [\[CITE\]](#) Lol it shows a console screen, and wtf is kernel aware registry persistence the oldest trick in the book but now it's suddenly 'kernel aware' whatever that means

IT does not show a console screen.

if you want full documentation you can ask for it.

YAK_CODER - August 29, 2025, 11:07 am

(Aug 15, 2025 04:23 PM)Beaconism Wrote: [\[CITE\]](#) Price: 400\$ per crypt. ARE YOU JUST JOKING

Beaconism - August 30, 2025, 3:15 pm

(Aug 29, 2025 11:07 AM)YAK_CODER Wrote: [\[CITE\]](#) ARE YOU JUST JOKING

No.

Normal price for .dll sideloading.

Check prices on exploit xss and you will know.

Hackers - October 29, 2025, 5:12 pm

(Aug 17, 2025 08:15 AM)SlimeSkeet Wrote: [\[CITE\]](#) Lol it shows a console screen

(Aug 25, 2025 10:05 AM)Beaconism Wrote: [\[CITE\]](#) IT does not show a console screen.

Your thread says this:

(Aug 15, 2025 04:23 PM)Beaconism Wrote: [\[CITE\]](#) Behavior: Brief console window appears due to Java-based architecture; does not impact stealth.

Does it show a console screen / window / pop up while it loads?

[Cap](#) this thread should be in marketplace
wrong forum

Beaconism - November 2, 2025, 5:02 am

(Oct 29, 2025 05:12 PM)nodes Wrote: [\[CITE\]](#) Your thread says this:

Does it show a console screen / window / pop up while it loads?

[Cap](#) this thread should be in marketplace
wrong forum

As it said in the thread, it can be removed and it's now fully removed in the new versions :)

Hackers - November 2, 2025, 5:21 am

(Nov 2, 2025 06:02 AM)Beaconism Wrote: [\[CITE\]](#) As it said in the thread, it can be removed and it's
now fully removed in the new versions :)
thanks for the update!

JonteAka - November 19, 2025, 12:13 pm

Your telegram @BEACONISM_SUPPORT not active user

Beaconism - December 8, 2025, 2:57 pm

(Nov 19, 2025 01:13 PM)JonteAka Wrote: [\[CITE\]](#) Your telegram @BEACONISM_SUPPORT not
active user

New telegram @Beaconismsup