

# Forum:[Hack Forums](#)

Thread: [2026 EXPLOIT - Windows SCRIPT - Office MACRO - JAR Launcher \(for java rat\)](#)

**bay.albatros** - December 31, 2025, 7:12 am

? WSC - Silent Payload Delivery System ?

? FUD - Fully Undetectable Three powerfull tools in one platform:

- WSC - Windows Script Creator
- MOM - Microsoft Office Macro Generator
- JLC - Java Launcher Creator

? Key Features:

? Silent EXE Download & Execute

Download and run EXE files in background without user visibility. No prompts, no traces.

? JAR Silent Execution (best settings for JAVA RAT - Always FUD)

Auto-download portable Java runtime and execute JAR files completely hidden. No Java installation required on target.

? Weaponized Office Macros

Generate obfuscated VBA macros for Word & Excel with auto-execution capabilities.

? Advanced Obfuscation

Multi-layer code obfuscation with variable randomization and string encryption.

? Persistence & Startup

Built-in registry persistence and startup folder methods for maintaining access.

? Stealth Mode

Hidden window execution, AMSI bypass, and anti-debugging techniques included.

? Why Choose?

- Bypass Windows Defender, Eset, Avast, AVG, Kaspersky & more

- Multiple output formats: BAT, VBS, JS, HTA, PS1, DOCM, XLSM
- Portable Java bundling - works without Java on target
- Decoy document display while payload executes
- Self-deleting scripts after execution
- Credit based system - pay for what you use
- Regular updates to maintain FUD status

? Payment: Crypto accepted

? Access: Instant after payment

## [VIDEO](#)

**SpiderSpicy** - January 19, 2026, 2:58 pm

I have installed JDK and JRE.

**xer0x1** - February 3, 2026, 2:45 pm

Need Ur telegram

Need Ur telegram

**bay.albatros** - February 4, 2026, 3:46 am

(Feb 3, 2026 03:45 PM)xer0x1 Wrote: [\[CITE\]](#) Need Ur telegram

Need Ur telegram -----

Hi....

TG

@quimatrow

You can write to me here.

**MeW11** - February 4, 2026, 7:35 am

what is the cve?

**bay.albatros** - February 4, 2026, 8:22 am

(Feb 4, 2026 08:35 AM)MeW11 Wrote: [\[CITE\]](#) what is the cve?

We utilize a private, highly obfuscated macro-based execution technique.

Unlike public CVEs that are quickly patched by Microsoft, our method relies on custom-coded logic and polymorphic VBA engines.

This ensures that your delivery remains stable across various Office environments without being dependent on a specific software vulnerability.

However, our new project, [xll.app](#), takes stealth to the next level.....

While macros are still effective, XLL files are the future of office-based execution.

Here is why xll.app is superior:

Native Execution: XLL files are essentially DLLs that Excel treats as trusted add-ins. They run as

native code, bypassing the security limitations often found in the VBA engine.

No "Enable Macro" Friction: XLLs don't trigger the same heavy "Warning" banners that modern Excel versions show for traditional macros. This significantly increases your conversion/execution rates.

Memory-Only Loading: [xll.app](#) is designed to execute your payload directly in memory. Since it leverages a legitimate Excel feature (xlAutoOpen), it provides a silent and much more stealthy bypass compared to any Doc or XLS macro.

AND - Doc/XLS is our reliable classic, but [xll.app](#) is our high-performance, native-binary powerhouse.

**SIM-5735617** - February 8, 2026, 1:38 am

Please Explain More About Pricing And How Deal Happend!

**bay.albatros** - February 8, 2026, 6:33 am

(Feb 8, 2026 02:38 AM)SIM-5735617 Wrote: [\[CITE\]](#) Please Explain More About Pricing And How Deal Happend!

-----