

Forum: [Hack Forums](#)

Thread: [Offering free crypts temporarily.](#)

XDDDev - July 23, 2025, 3:58 pm

Because my crypter is now undetected runtime on all but eset and crowdstrike ill give out some free crypts

comment below if you want one and ill msg you my details.

also big tip! read this:

<https://hackforums.net/showthread.php?pid=62787733>

- Native PE Files: x32 and x64 Windows executables
- .NET Assemblies: Managed code applications
- Shellcode: Raw binary payloads
- DLL Files: Dynamic link libraries

- XOR Encryption: Fast, lightweight encryption with 16-byte keys
- Chunked Processing: Large payloads (>1MB) split into 64KB chunks to prevent memory issues
- Dynamic Key Generation: Unique encryption keys per build
- Header Separation: Payload data stored in separate header files

EDR Evasion Techniques:

AMSI (Antimalware Scan Interface) Bypass
ETW (Event Tracing for Windows) Bypass
NTDLL Unhooking

Intelligent payload execution:

PE File Detection

- Validates MZ (DOS) header signature
- Verifies PE header structure
- Determines architecture (x32/x64)

.NET Assembly Detection

- Checks COM descriptor directory
- Identifies managed code assemblies
- Uses CLR execution method

1. .NET Assemblies: Temporary file + CreateProcess
2. Native PE: RunPE (Process Hollowing) technique
3. Shellcode: Direct memory execution with VirtualAlloc

RunPE Advantages:

- No temporary files created on disk
- Direct memory injection into legitimate process
- Bypasses file-based detection
- Maintains process legitimacy
- Harder to detect than file-based execution

SIM-5635902 - *July 24, 2025, 1:14 pm*

I'll Give it a Try Thanks

XDDev - *July 25, 2025, 2:43 pm*

Closed, retards keep sending to virustotal