Arth Sunil Maurya

arthmaurya@gmail.com | arth.imbeddex.com | linkedin.com/in/arth-maurya | github.com/arthmaurya

Skills

Programming Languages and scripts: C, C++, x86/x64 Assembly, Python, PHP, Bash Scripting, VBScript, PowerShell scripting.

Low-Level Development & Research: Windows Kernel Manipulation (DKOM, Rootkit techniques), Position Independent Code, Indirect Syscalls, Process Injection (Reflective, APC, Shellcode), API Hooking, Obfuscation, Debugger Evasion, Dynamic API Resolution, Reverse Engineering.

Tools: WinDbg, x64dbg, IDA Pro, Ghidra, Sysinternals Suite, Wireshark, Burp Suite, Git, Visual Studio.

Projects

ETW-Threat Intelligence Bypass | *C++, Windows Kernel DKOM* (Private Repo) | (*Documentation*) *June 2026 - June 2026*

- Reverse engineered **undocumented** ETW-Threat Intelligence kernel functions to identify **EtwProviderEnabled** as a single gating function controlling all ETW-TI telemetry logging across **8+ event types**.
- Developed a data only **DKOM** attack that zeros three boolean flags in kernel memory, eliminating every ETW-Ti event generation with zero code injection; validated against **Elastic EDR v8.11+** and **Windows Defender v4.18.26010.5** on **Windows 11 25H2**.
- Confirmed loss of visibility into **VirtualAllocEx** and **WriteProcessMemory** operations while maintaining system stability. EDR continues logging Dll Loading events and network connections but is **completely blind** to **virtual memory interactions** via ETW-Ti.

VAD-Decoupling Memory Injector | *C, C++, x64 Assembly, Windows Kernel* (*github link*) *May 2025 - June 2026*

- Built a hybrid **user/kernel-mode** reflective DLL injector with a full **manual mapping** backend (custom relocations, import resolver, etc.).
- Demonstrates evasion of disk-based I/O monitoring by streaming raw binaries directly into memory from the C2 server and **injecting** them into **remote processes**.
- Developed **Position Independent Code (PIC)** that dynamically walks the **target** process's **PEB** to **resolve APIs** and executes the mapping logic, eliminating external dependencies.
- Constructs a synthetic **DEVICE_OBJECT** by dynamically resolving unexported globals (e.g., **PsLoadedModuleSpinLock**), validated on bare-metal Windows 11 (**25H2**) with Engine Version: (**1.1.25110.1**) and **PatchGuard** active.
- Surgically modifies the **VAD tree** to decouple **VAD** entries, minimizing forensic artifacts against advanced scanners like **hollows_hunter (v0.4.1.1)**, **PE-sieve (v0.4.1.1)** and **Moneta**.

Polymorphic Syscall Generator | *C++, x64 Assembly, Native API* (*github link*) *April 2025 - May 2025*

- Engineered a syscall engine with randomized **register shuffling** and **assembly obfuscation** strategies, bypassing static analysis of **Windows Defender** (**v4.18+**) and **Avast** (**v25.7.10308**).
- Implements dynamic stub pool generation (**2,000+ unique variants**) to bypass user-mode AV/EDR hooks.
- Leverages techniques like **KnownDlls, Blind Side, Vectored Exception Handling** to retrieve a clean ntdll.dll image.

Hybrid User/Kernel Adversary Emulation Framework | *C/C++, x64 Assembly, Winsock, PHP* (*github link*) *Dec 2024 - Ongoing*

- Architected a **zero-dependency** hybrid implant transitioning to **Ring 0** for privileged control, validated across all **Windows 11** builds up to **25H2** with minimal forensic footprint.
- Developed a **custom C2** server with a **proprietary** protocol over raw TCP sockets, implementing end-to-end **encryption** to evade network signature detection.
- Integrates Polymorphic Engine and Reflective Loader to bypass fully updated Windows **Defender** (**v4.18+**) and sustain **kernel persistence**.

Involvement

Speaker, *44CON*, *London, UK* – (*Link*) *Sep 2026*

- Delivered a technical presentation titled **"Bypassing Windows Kernel Callback Integrity"** to an international security audience.

Experience

VPN and Security Implementation Intern , *UPONLY Technologies* *Jan 2025 - May 2025*

- Engineered a secure remote access infrastructure using **OpenVPN**, enforcing encrypted tunneling for corporate communications.
- Reduced the external attack surface by migrating public-facing API endpoints to a **private VPN** subnet.
- Deployed and **hardened** a local Linux (Ubuntu) hosting environment to support client development workflows.

Security Engineering Intern , *Heptanesia IT Services Pvt. Ltd. Mumbai* *June 2024 - July 2024*

- Designed a robust **security framework** that aligns with **ISO 27001** standards.
- Assisted in the configuration of a **Zero Trust** access model, enforcing strict identity verification and **least-privilege principles** across network.

Certifications

Executive Post Graduate Certification in Cyber Security and Ethical Hacking (*link*) *Jan 2025*
Indian Institute of Technology Roorkee

CEH V12 (Ongoing) *Expected: 2026*
EC-Council

Education

Msc CyberSecurity *Expected 2027*
University Of Southampton