Understanding the Virtual Address Descriptor (VAD) in Windows Memory Management

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-11-17

Introduction to the Virtual Address Descriptor

The Virtual Address Descriptor, commonly known as the "VAD", is a fundamental component in the memory management system of the Windows operating system. Primarily it is responsible for managing and tracking the memory allocations within a process's virtual address space. You can read more about virtual address spaces in Windows in a previous article.

Location and Structure of VAD

VADs reside within the private memory space of each process and are managed by the Windows kernel as part of the process's Virtual Memory Control Block (VMCB). The structure of a VAD is a binary tree, with each node representing a block of virtual memory. These nodes contain crucial information about the memory block, including its starting address, size, and state.

Role of VAD in Memory Management

VADs meticulously track all allocated memory regions in a process’s address space. This includes detailed information about loaded Dynamic Link Libraries (DLLs), such as their memory range, access permissions, and the type of memory (private or mapped). For instance, when a DLL is loaded into a process, a VAD node is created to record its memory region, access permissions, and the file it's mapped to.

Memory Protection and Permissions

The memory protection level of each memory block, such as read, write, or execute permissions, is also stored in VADs. These permissions are crucial for maintaining system stability and security; incorrect permissions can lead to vulnerabilities, such as buffer overflows or unauthorised code execution. VAD records the permissions at the time of memory allocation, and although they can be changed, modifications by user-mode processes are typically restricted and monitored to prevent security breaches.

Cooperation with the Memory Manager

The Windows Memory Manager interacts closely with VADs for efficient memory allocation and deallocation. When a process requests memory, the Memory Manager consults the VAD structure to find a suitable memory region. This cooperation ensures that memory is allocated in an optimized and conflict-free manner. The Memory Manager,

therefore, relies on the information in the VAD to understand the current layout of a process's memory.

Interaction with Page Tables

VADs and page tables are intrinsically linked. While VADs manage higher-level allocation of memory blocks, page tables handle the actual mapping of virtual addresses to physical addresses. The data in page tables, stored in system memory, contains detailed mappings for each page, including its physical address and current status (such as whether it's in memory or paged out). VADs use this information to keep track of the allocation and state of each memory block.

VAD and Security

Security in Windows heavily relies on the integrity and accuracy of VAD structures. By analyzing VADs, security professionals can detect anomalies like unauthorised code injections. Tools like WinDbg or Volatility facilitate the analysis of VAD structures, providing insights into the state and usage of each memory section.

VAD in Process Execution

During process execution, the VAD tree is traversed to allocate memory effectively and efficiently. This process ensures a well-organised and optimised use of the virtual address space.

Technical Inspection of VADs

Tools such as WinDbg can be used to inspect VADs in Windows. Commands in WinDbg like **!vad** can dump the VAD tree of a specified process, revealing details about each memory region, including size, location, and permissions.

Also, in WinDbg, you can use the command **!process 0 0 process_name.exe** to get the address of the process and then **!vad address** to inspect the VAD of that process.

Advanced Uses of VAD

In advanced memory forensics, VADs are scrutinized to understand a process's behaviour, particularly in cases of malware analysis or debugging complex software issues. This involves looking into each node of the VAD tree to decipher the layout and use of the process's memory.

Summary

The Virtual Address Descriptor is a cornerstone in Windows memory management, ensuring efficient, secure, and optimised use of a process's virtual address space. Its detailed structure and interaction with various system components make it a crucial area for professionals working with Windows internals, security, and system optimisation. Understanding VADs is key to gaining a deeper insight into Windows memory management and is indispensable for advanced system analysis and troubleshooting.

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858