x86matthew

Twitter: @x86matthew E-Mail: x86matthew@gmail.com

03/02/2024

WoWMIPS - MIPS Emulator for Windows, Part 6: Testing

Writing a Windows NT MIPS emulator for x86 - part 6

03/02/2024

WoWMIPS - MIPS Emulator for Windows, Part 5: Additional details

Writing a Windows NT MIPS emulator for x86 - part 5

03/02/2024

WoWMIPS - MIPS Emulator for Windows, Part 4: Windows API calls

Writing a Windows NT MIPS emulator for x86 - part 4

03/02/2024

WoWMIPS - MIPS Emulator for Windows, Part 3: Emulating the MIPS R4000 CPU

Writing a Windows NT MIPS emulator for x86 - part 3

03/02/2024

WoWMIPS - MIPS Emulator for Windows, Part 2: Mapping the executable image

Writing a Windows NT MIPS emulator for x86 - part 2

03/02/2024

WoWMIPS - MIPS Emulator for Windows, Part 1: Introduction

Writing a Windows NT MIPS emulator for x86 - part 1

11/11/2023

Flare-On 2023 Challenge 7 (flake) - Solving a compiled Python challenge using native tools

Flare-On 2023 write-up

11/01/2023

SelfDebug - A useless anti-debug trick by forcing a process to debug itself

Forcing a process into a state which prevents a real debugger from attaching

10/12/2022

StealthHook - A method for hooking a function without modifying memory protection

Discovering and overwriting nested global pointers to hook functions without suspicion

20/10/2022

SharedMemUtils - A simple tool to automatically find vulnerabilities in shared memory objects

A tool to simplify a common weakness in services that can often lead to successful exploitation

20/09/2022

Exploiting a Seagate service to create a SYSTEM shell (CVE-2022-40286)

A brief overview of a simple vulnerability that I recently discovered

09/09/2022

WriteProcessMemoryAPC - Write memory to a remote process using APC calls

Another alternative to WriteProcessMemory, this time by scheduling APC calls to call RtlFillMemory

02/04/2022

AudioTransmit - Transmitting data between computers using audio

A simple proof-of-concept to transfer data between computers using software-generated audio tones

01/03/2022

NTSockets - Downloading a file via HTTP using the NtCreateFile and NtDeviceIoControlFile syscalls

Reverse-engineering communications with the afd.sys driver to create a basic Winsock wrapper

25/02/2022

LogNT32 - Part 2 - Return-address hijacking implemented to improve efficiency

Improvements added to the original LogNT32 code

23/02/2022

LogNT32 - Trace all ntdll function calls without a pre-defined list of headers

Log all user-mode ntdll syscalls (32-bit only)

10/02/2022

WindowsNoExec - Abusing existing instructions to executing arbitrary code without allocating executable memory

Using a custom exception handler to single-step over existing instructions to execute a custom payload

04/02/2022

CreateSvcRpc - A custom RPC client to execute programs as the SYSTEM user

> Reverse-engineering the RPC protocol to create Windows services using native NT APIs