Hide Your Valuables!

Mitigating Physical Credential Dumping Attacks

Gabriel Landau
Mark Mager

January 21, 2023

Welcome

Gabriel Landau | Principal Engineer

Gabriel Landau is a principal at Elastic Security with a passion for Windows Internals. His public research includes Kernel Mode Threats and Practical Defenses (BH USA), Process Ghosting, AV sandboxing attacks, PPLGuard, and CI Spotter. His non-public work includes endpoint protections, penetration testing, exploit mitigation, product & DRM evaluation, and malware reversing. Though he mostly wears blue these days, his heart will always be red.

elastic

Welcome

Mark Mager | Endpoint Protections Lead

Mark Mager leads Elastic's Endpoint Protections Team and has served in prominent technical leadership roles in the research and development of advanced computer network operations tools and provided reverse engineering subject matter expertise to government and commercial clients in the Washington, D.C. area.

elastic

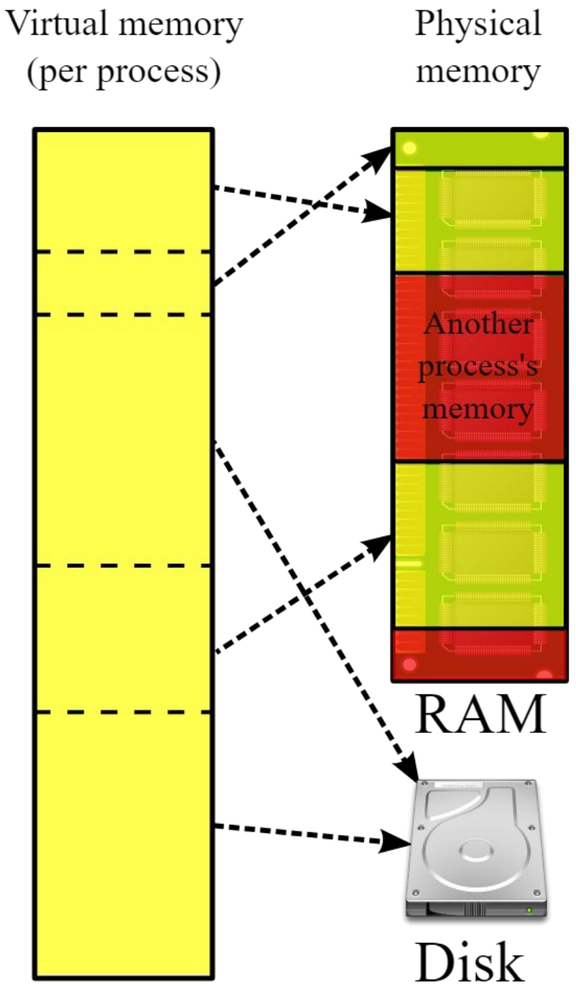
Outline

- Physical and Virtual Memory
- Credential Storage
- Credential Dumping Attacks
- Mitigations

elastic

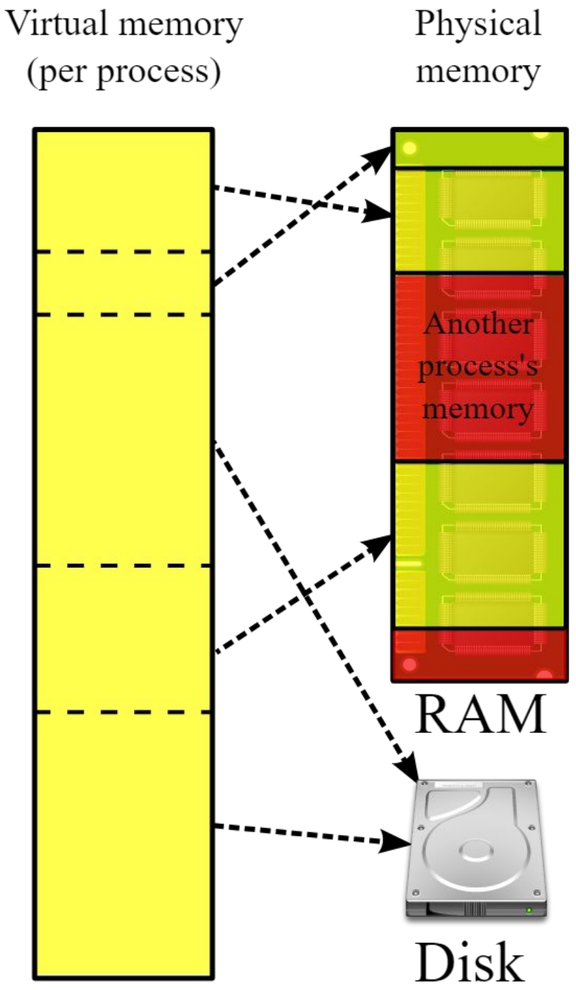
Physical Memory

- Corresponds to RAM
  - “Memory *is* RAM!” - Maurice Moss
- Accessible in x86 Real Mode
- On Windows, owned by the Memory Manager



Virtual Memory

- OS + CPU create illusion of private contiguous address space using page tables
  - Page tables “instanced” per process
- Divided into pages (typically 4KB or 2MB)
- Address space is sparse with most addresses invalid
- Pages can be backed by RAM, files, or the pagefile
- Paging enables Memory Manager to provide seamless access to virtual memory not resident in physical memory
- Kernel provides access to other processes’ address spaces
  - NtReadVirtualMemory / ReadProcessMemory



elastic

Virtual Memory

Address	Type	Size	Committed	Private	Total WS	Private WS	Shareable WS	Shared WS	Locked WS	Blocks	Protection	Details
00000200A8A00000	Heap (Private Data)	2,048 K	1,224 K	1,224 K	1,224 K	1,224 K				34	Read/Write	Heap ID: 1 [COMPATABILITY]
00000200A8C00000	Heap (Private Data)	2,048 K	1,572 K	1,572 K	1,572 K	1,572 K				13	Read/Write	Heap ID: 1 [COMPATABILITY]
00000200A8E00000	Shareable	4 K	4 K		4 K		4 K	4 K		1	Read	
00000200A8E01000	Unusable	60 K										
00000200A8E10000	Shareable	2,048 K	8 K		8 K		8 K	8 K		2	Read	
00000200A9010000	Shareable	32 K	16 K		16 K		16 K	16 K		2	Read	
00000200A9018000	Unusable	32 K										
00000200A9020000	Shareable	1,540 K	1,540 K		1,540 K		1,540 K	20 K		1	Read	
00000200A91A1000	Unusable	60 K										
00000200A91B0000	Shareable	772 K	16 K		16 K		16 K	8 K		2	Read	
00000200A9271000	Unusable	60 K										
00000200A9280000	Private Data	4 K	4 K	4 K	4 K	4 K				1	Read/Write	
00000200A9281000	Unusable	60 K										
00000200A9290000	Shareable	4 K	4 K		4 K		4 K	4 K		1	Read	
00000200A9291000	Unusable	60 K										
00000200A92A0000	Mapped File	28 K	28 K		28 K		28 K	28 K		1	Read	C:\Windows\Registration\R0000(
00000200A92A7000	Unusable	36 K										
00000200A92B0000	Private Data	64 K	4 K	4 K	4 K	4 K				2	Read/Write	
00000200A92C0000	Private Data	288 K	288 K	288 K	288 K		288 K	288 K		1	Copy on write	
00000200A9308000	Unusable	32 K										
00000200A9310000	Free	960 K										
00000200A9400000	Heap (Private Data)	2,048 K	168 K	168 K	168 K	168 K				2	Read/Write	Heap ID: 1 [COMPATABILITY]
00000200A9600000	Free	133,094,159,616 K										
00007DF4C8340000	Shareable	1,024 K	20 K		20 K		20 K	20 K		2	Read	
00007DF4C8440000	Private Data	4,194,432 K	8 K	8 K	8 K	8 K				5	Read/Write	
00007DF5C8460000	Private Data	32,772 K	8 K	8 K	8 K	8 K				4	Read/Write	
00007DF5CA461000	Unusable	60 K										
00007DF5CA470000	Shareable	4 K	4 K		4 K		4 K	4 K		1	Read	
00007DF5CA471000	Unusable	60 K										
00007DF5CA480000	Shareable	2,147,483,648 K	20,832 K		816 K	8 K	808 K	500 K		64	Read	
00007FF5CA480000	Free	5,600,320 K										
00007FF720190000	Image (ASLR)	72 K	72 K	4 K	72 K	12 K	60 K			5	Execute/Read	C:\Windows\System32\lsass.exe
00007FF7201A2000	Unusable	56 K										
00007FF7201B0000	Free	5,706,432 K										
00007FF87C660000	Image (ASLR)	388 K	388 K	8 K	388 K	16 K	372 K			5	Execute/Read	C:\Windows\System32\vaultsvc.(

elastic

Outline

Physical and Virtual Memory

Credential Storage

Credential Dumping Attacks

Mitigations

elastic

Local Security Authority Subsystem (LSASS)

Windows process hosting critical services and functions

- CNG Key Isolation
  - Stores private cryptographic keys
- Security Accounts Manager
  - Manages SAM database which contains usernames and passwords
- Credential Manager
  - Stores credentials
- Authentication Packages
  - Kerberos tickets
  - NTLM hashes
  - Cleartext passwords*

* Deprecated but still configurable

elastic

Local Security Authority Subsystem (LSASS)

Keys to the Kingdom

- Privilege Escalation
  - User → Domain Admin
- Persistence
  - Maintain foothold, perform reconnaissance
- Lateral Movement
  - Spread across network

Outline

Physical and Virtual Memory

Credential Storage

Credential Dumping Attacks

Mitigations

elastic

Credential Dumping - Virtual Memory Attacks

Dump Virtual Memory with OS Features

- ProcDump
  - Read process virtual memory then save to DMP file
  - Can fork target (PssCaptureSnapshot) then dump child
  - Uses NtReadVirtualMemory to access virtual memory
- Mimikatz
  - Supports direct access via NtReadVirtualMemory
  - Can process memory dumps
  - Variants include pypykatz

Credential Dumping - Virtual Memory Mitigations

Protected Process Light (PPL/RunAsPPL)

- Built-in Windows capability designed for securing critical processes
- Limits handle rights via OpenProcess and similar functions
- Block PROCESS_VM_READ → NtReadVirtualMemory
- Blocks PROCESS_CREATE_PROCESS → forking
- Blocks write operations → code injection & control flow hijacking
- Require Microsoft signatures → various DLL injection techniques

Credential Dumping - Virtual Memory Attacks (cont.)

Bring Your Own Vulnerable Driver (BYOVD)

- Bring a signed legitimate driver with a vulnerability
- Load driver into the kernel and exploit it to “puppet” it
  - Driver is used to provide camouflage / legitimacy to your attack
- Disable or bypass PPL protection
  - Nerf LSASS EPROCESS.Protection
  - Elevate attacker’s EPROCESS.Protection
  - Read virtual memory from kernel
  - Duplicate handle from kernel
  - Elevate low-privilege handle
  - Inject code from kernel
  - Read physical memory from kernel
- Mitigated via Vulnerable Driver Blocklist (Win10 / Win11)

Credential Dumping - Physical Memory Attacks

Accessing Physical Memory

- C:\Windows\MEMORY.DMP
  - Windows feature to debug bugchecks (BSODs)
  - Can dump all of physical memory, not just kernel memory
  - Search old dumps, or BSOD to create a new dump
- \Device\PhysicalMemory
  - Inaccessible from user mode since XP
  - Accessible via forensic tools WinPmem, DumpIt
  - Drivers not included in Microsoft's blocklist
- Virtual Machine Memory Files (.VMEM)
  - Physical memory of virtual machine is kept in a flat file
  - Convert to Microsoft DMP with Vmss2core
- Hibernation File (C:\hiberfil.sys)
  - Convert to Microsoft DMP with Hibr2Dmp

elastic

Credential Dumping - Physical Memory Attacks

Processing Physical Memory Dumps

- Mimilib
  - Mimikatz DLL that can run as a WinDbg extension
  - Load MEMORY.DMP into WinDbg, then extract credentials with Mimilib
- physmem2profit
  - Server loads WinPmem, exposed via network
  - Client connects to server for access to physical memory
  - Client uses rekall forensic framework to reconstruct LSASS virtual address space
  - Creates user-mode minidump. Process with mimikatz/pypykatz
- Rekall & Volatility mimikatz plugins

Outline

Physical and Virtual Memory

Credential Storage

Credential Dumping Attacks

Mitigations

elastic

Working Set

Address	Type	Size	Committed	Private	Total WS	Private WS	Shareable WS	Shared WS	Locked WS	Blocks	Protection	Details
00000200A8A00000	Heap (Private Data)	2,048 K	1,224 K	1,224 K	1,224 K	1,224 K				34	Read/Write	Heap ID: 1 [COMPATABILITY]
00000200A8C00000	Heap (Private Data)	2,048 K	1,572 K	1,572 K	1,572 K	1,572 K				13	Read/Write	Heap ID: 1 [COMPATABILITY]
00000200A8E00000	Shareable	4 K	4 K		4 K		4 K	4 K		1	Read	
00000200A8E01000	Unusable	60 K										
00000200A8E10000	Shareable	2,048 K	8 K		8 K		8 K	8 K		2	Read	
00000200A9010000	Shareable	32 K	16 K		16 K		16 K	16 K		2	Read	
00000200A9018000	Unusable	32 K										
00000200A9020000	Shareable	1,540 K	1,540 K		1,540 K		1,540 K	20 K		1	Read	
00000200A91A1000	Unusable	60 K										
00000200A91B0000	Shareable	772 K	16 K		16 K		16 K	8 K		2	Read	
00000200A9271000	Unusable	60 K										
00000200A9280000	Private Data	4 K	4 K	4 K	4 K	4 K				1	Read/Write	
00000200A9281000	Unusable	60 K										
00000200A9290000	Shareable	4 K	4 K		4 K		4 K	4 K		1	Read	
00000200A9291000	Unusable	60 K										
00000200A92A0000	Mapped File	28 K	28 K		28 K		28 K	28 K		1	Read	C:\Windows\Registration\R0000(
00000200A92A7000	Unusable	36 K										
00000200A92B0000	Private Data	64 K	4 K	4 K	4 K	4 K				2	Read/Write	
00000200A92C0000	Private Data	288 K	288 K	288 K	288 K		288 K	288 K		1	Copy on write	
00000200A9308000	Unusable	32 K										
00000200A9310000	Free	960 K										
00000200A9400000	Heap (Private Data)	2,048 K	168 K	168 K	168 K	168 K				2	Read/Write	Heap ID: 1 [COMPATABILITY]
00000200A9600000	Free	133,094,159,616 K										
00007DF4C8340000	Shareable	1,024 K	20 K		20 K		20 K	20 K		2	Read	
00007DF4C8440000	Private Data	4,194,432 K	8 K	8 K	8 K	8 K				5	Read/Write	
00007DF5C8460000	Private Data	32,772 K	8 K	8 K	8 K	8 K				4	Read/Write	
00007DF5CA461000	Unusable	60 K										
00007DF5CA470000	Shareable	4 K	4 K		4 K		4 K	4 K		1	Read	
00007DF5CA471000	Unusable	60 K										
00007DF5CA480000	Shareable	2,147,483,648 K	20,832 K		816 K	8 K	808 K	500 K		64	Read	
00007FF5CA480000	Free	5,600,320 K										
00007FF720190000	Image (ASLR)	72 K	72 K	4 K	72 K	12 K	60 K			5	Execute/Read	C:\Windows\System32\lsass.exe
00007FF7201A2000	Unusable	56 K										
00007FF7201B0000	Free	5,706,432 K										
00007FF87C660000	Image (ASLR)	388 K	388 K	8 K	388 K	16 K	372 K			5	Execute/Read	C:\Windows\System32\vaultsvc.(

Working Set (Emptied)

Address	Type	Size	Committed	Private	Total WS	Private WS	Shareable WS	Shared WS	Locked WS	Blocks	Protection	Details
00000200A8A00000	Heap (Private Data)	2,048 K	1,232 K	1,232 K	16 K	16 K				34	Read/Write	Heap ID: 1 [COMPATABILITY]
00000200A8C00000	Heap (Private Data)	2,048 K	1,576 K	1,576 K	96 K	96 K				11	Read/Write	Heap ID: 1 [COMPATABILITY]
00000200A8E00000	Shareable	4 K	4 K							1	Read	
00000200A8E01000	Unusable	60 K										
00000200A8E10000	Shareable	2,048 K	8 K							2	Read	
00000200A9010000	Shareable	32 K	16 K							2	Read	
00000200A9018000	Unusable	32 K										
00000200A9020000	Shareable	1,540 K	1,540 K							1	Read	
00000200A91A1000	Unusable	60 K										
00000200A91B0000	Shareable	772 K	16 K							2	Read	
00000200A9271000	Unusable	60 K										
00000200A9280000	Private Data	4 K	4 K	4 K						1	Read/Write	
00000200A9281000	Unusable	60 K										
00000200A9290000	Shareable	4 K	4 K							1	Read	
00000200A9291000	Unusable	60 K										
00000200A92A0000	Mapped File	28 K	28 K							1	Read	C:\Windows\Registration\R0000(
00000200A92A7000	Unusable	36 K										
00000200A92B0000	Private Data	64 K	4 K	4 K						2	Read/Write	
00000200A92C0000	Private Data	288 K	288 K	288 K						1	Copy on write	
00000200A9308000	Unusable	32 K										
00000200A9310000	Free	960 K										
00000200A9400000	Heap (Private Data)	2,048 K	168 K	168 K	8 K	8 K				2	Read/Write	Heap ID: 1 [COMPATABILITY]
00000200A9600000	Free	133,094,159,616 K										
00007DF4C8340000	Shareable	1,024 K	20 K							2	Read	
00007DF4C8440000	Private Data	4,194,432 K	8 K	8 K						5	Read/Write	
00007DF5C8460000	Private Data	32,772 K	8 K	8 K	8 K	8 K				4	Read/Write	
00007DF5CA461000	Unusable	60 K										
00007DF5CA470000	Shareable	4 K	4 K							1	Read	
00007DF5CA471000	Unusable	60 K										
00007DF5CA480000	Shareable	2,147,483,648 K	20,832 K		12 K		12 K	12 K		64	Read	
00007FF5CA480000	Free	5,600,320 K										
00007FF720190000	Image (ASLR)	72 K	72 K	4 K	12 K	4 K	8 K			5	Execute/Read	C:\Windows\System32\lsass.exe
00007FF7201A2000	Unusable	56 K										
00007FF7201B0000	Free	5,706,432 K										
00007FF87C660000	Image (ASLR)	388 K	388 K	8 K	12 K		12 K			5	Execute/Read	C:\Windows\System32\vaultsvc.(

elastic

Working Set (contd)

Removing pages from physical memory

- Empty Working Set
  - EmptyWorkingSet()
  - Unmodified pages moved to Standby List
  - Modified pages moved to Modified List
- Flush Standby and Modified lists
  - NtSetSystemInformation(SystemMemoryListInformation)
  - Unmodified pages discarded and zeroed
  - Modified pages flushed to backing stores (files, pagefile)

Silhouette

Keep secrets out of physical memory

- Proof of Concept
- Kernel Driver
  - Compatible with RunAsPPL
- Filesystem Minifilter
  - Detect and respond to paging I/O

Demo - Physical Memory Protection

What about the Pagefile?

Rekall can “page in” missing data during analysis*

- Requires a timely copy of the pagefile
- Windows locks the pagefile to prevent access
- Bypass: Raw disk access
  - Silhouette: Block raw reads to pagefile (FO_VOLUME_OPEN)
    - Protects both pagefile and hibernation file
  - Alternative mitigation: Enable NTFS Pagefile Encryption
- Bypass: Volume Shadow Copy (VSS)
  - Silhouette: Block access to files with the pagefile’s NTFS file ID, which is identical in shadow copies

* http://blog.rekall-forensic.com/2014/10/windows-virtual-address-translation-and.html

Demo - Pagefile Protection

elastic

Silhouette - Attacks

Full memory dumps are slow, but fast attacks should be spammable

- RPC Spamming
  - Silhouette ensures pages are only resident briefly
  - Residence window is much shorter than a full memory dump duration
  - Retrying targeted WinPmem physical reads until the pages are resident
  - Defense: Block drivers such as WinPmem and DumpIt
  - Variant: WerFaultSecure
    - WerFaultSecure can run as PPL
    - Able to touch LSASS's memory, triggering page faults
    - Defense: Block PROCESS_VM_READ to LSASS with object manager callback

Silhouette - Attacks

Disable/resize the pagefile

- Change registry value then reboot - nowhere to hide!
- Defense: Monitor registry changes with EDR
- Defense: Lock registry value from the kernel
- Defense: At startup, restore known-good value then reboot

Silhouette - Future Work

- Apply principles offensively - hide your implant
  - Defeat physical memory forensics with two APIs
    - EmptyWorkingSet()
    - NtSetSystemInformation(SystemMemoryListInformation)
- Extend VSS protection to other files:
  - SAM hive
  - Ntds.dit

- Wishlist:
  - Flush standby/modified pages for a specific process
  - “UEFI Lock” for more/arbitrary security-sensitive configuration options

Silhouette - Summary

Keep secrets out of physical memory

- Lack of resident pages breaks all tested attacks
  - Physmem2Profit + mimikatz
  - DumpIt + mimilib
  - Vmss2core + mimilib (tested but not shown)
- Hardening to mitigate pagefile acquisition*
  - Raw disk access (Invoke-NinjaCopy)
  - Volume Shadow Copy (hobocopy)
- Negligible performance overhead in basic performance testing
  - Overhead will vary by workload and hardware
- Open source: https://github.com/elastic/Silhouette

Conclusions & Recommendations

Conclusions

- Paging is taken for granted. It happens more often than you think*

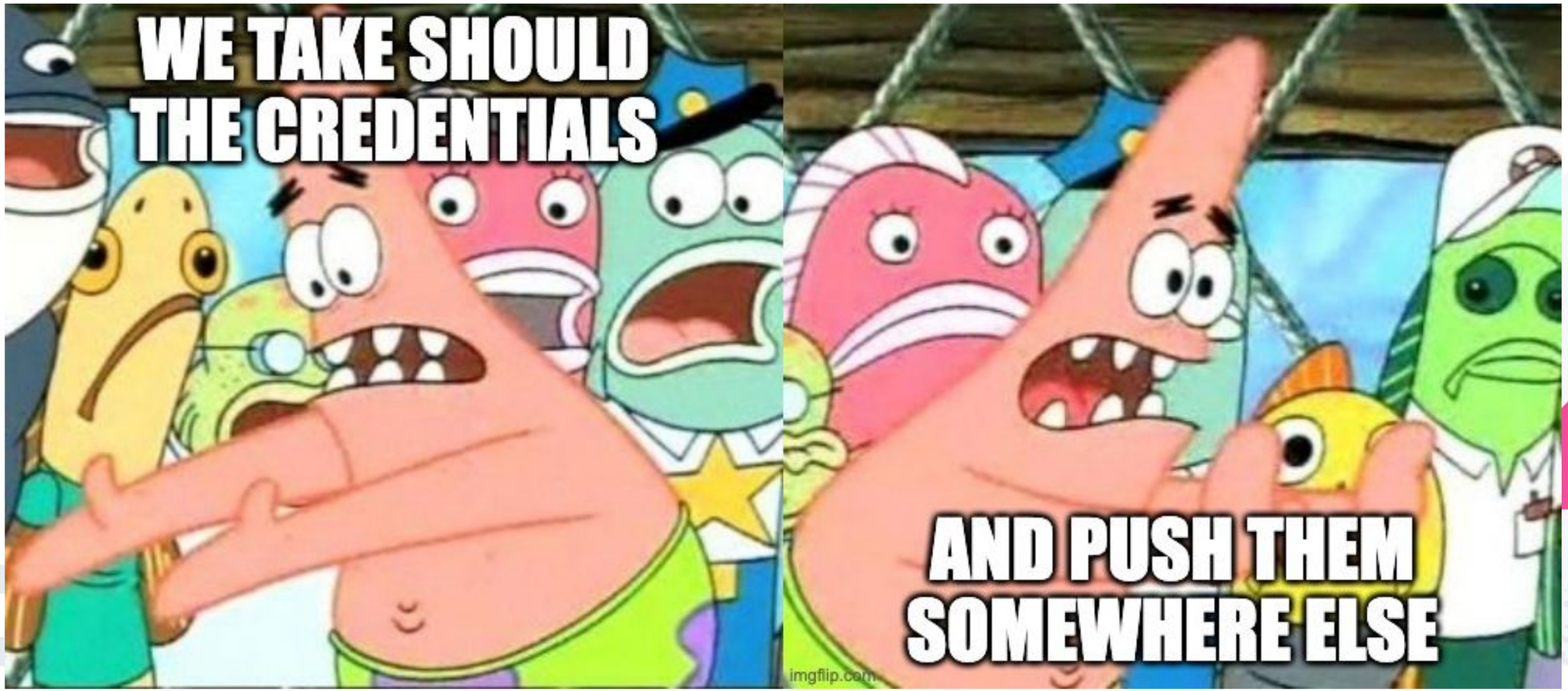
Recommendations

- Enable RunAsPPL with UEFI lock to block a variety of attacks
- Enable Credential Guard if possible
- Deploy WDAC vulnerable driver blocklisting
  - Use Microsoft blocklist as a baseline
  - Include forensic drivers such as WinPmem and DumpIt
- Disable hibernation where it’s not needed

* This is especially apparent when debugging pageable code/data from MEMORY.DMP and coding >= DISPATCH_LEVEL

elastic

Questions?



elastic