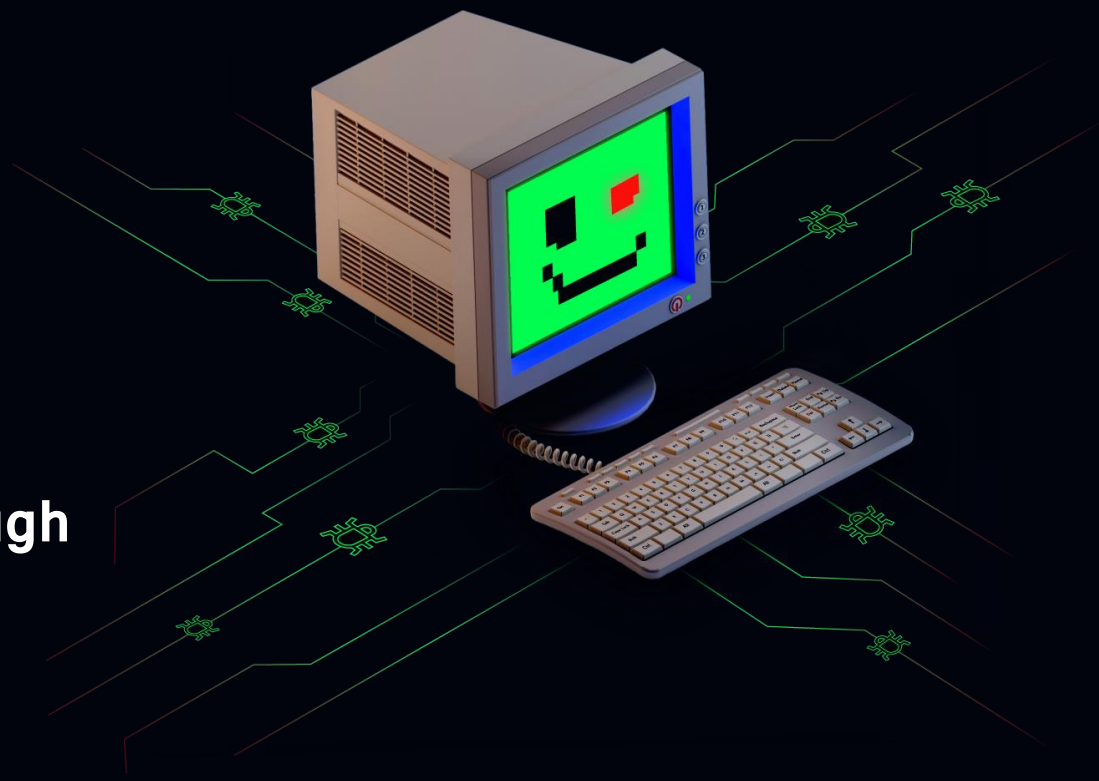
THE H@CK SUMMIT

previously WHAT THE H@CK



C:\>

KDP and the Secure Pool

When protected memory isn't protected enough

Yarden Shafir

Software Engineer, Crowdstrike

www.thehacksummit.com | 5/12/2020 | online / Warsaw

ORGANIZERS: Academic Partners FUNDACJA | CBC

About me

- Circus artist and aerial instructor
- Software engineer @Crowdstrike
- Windows Internals instructor @Winsider
- Former pastry chef
- Taught mom how to unmute zoom
- Almost succeeded at training a cat
- Usually found upside down

Ring Levels and Protection

- Kernel-Mode code runs in ring 0 and User-mode code in ring 3
- Kernel code is protected from user-mode
  - Unless there is a vulnerability
- But ring 0 runs a lot of code…
  - Windows components
  - Hardware drivers (video cards, network cards…)
  - AV drivers
  - Virtualization tools (vmware, virtualbox)
  - Games, analysis tools, and more…

VTL1 vs. VTL0

- Possible with Hyper-V
- VTL1 isolates code from VTL0
  - Has ring 3 and ring 0 code running in it
  - VTL0 can’t access VTL1 at all without a vulnerability
- VTL1 only allows very few things to run in it
  - All are Windows components
- Can 3rd party drivers use VTL1 to protect themselves from other ring 0 code?

Dynamic KDP - Secure Pool

- Allocated in VTL1 and managed by the secure kernel
  - Has a read-only mapping in VTL0
- Normal kernel drivers can allocate memory in it to keep sensitive data
- Secure Pool is protected from VTL0 code and can only be modified by the secure kernel
- Helps drivers protect dynamic memory against data corruption attacks
  - And even make sensitive data a bit harder to find (but only a bit…)

Using the Secure Pool

- Create a handle with ExCreatePool
- Allocate a block with ExAllocatePool3
  - ExtendedParameters.Type == PoolExtendedParameterSecurePool
- Caller specifies handle, buffer, cookie and flags
  - SECURE_POOL_FLAGS_FREEABLE
  - SECURE_POOL_FLAGS_MODIFIABLE
  - Allocation can only be freed or modified if matching flag is requested
- Receives back an address in the normal kernel's mapping of the secure pool (read only)

Modifying and Freeing

- Only possible if matching flag was set when allocating
  - SecureKernel will bugcheck otherwise
- ExSecurePoolUpdate and ExFreePool2 will validate allocation flags and supplied tag and cookie
- If modifying, driver needs to supply a buffer with new data to write into the block

Static KDP

- Allows a driver to protect a whole data section
- Makes the section read-only for VTL0
  - Enforced by VBS
  - Data in the section cannot be modified without a VTL0->VTL1 exploit
- Impossible to protect only part of a section
- Used through MmProtectDriverSection
  - Driver has to specify MM_PROTECT_DRIVER_SECTION_ALLOW_UNLOAD to be able to unload safely

Who Wants to Use KDP?

- Security Products
- DRM / Anti-cheat
- Windows Components
  - SGRM and CI already use static KDP

THE H@CK SUMMIT

previously WHAT THE H@CK

Thank you for your attention!

Leave your questions in the comment section below and remember to join Q&A session on the 5th of December.

www.thehacksummit.com | 5/12/2020 | online

ORGANIZERS: Academic Partners FUNDACJA | CBC