Patrick Wardle @patrickwardle

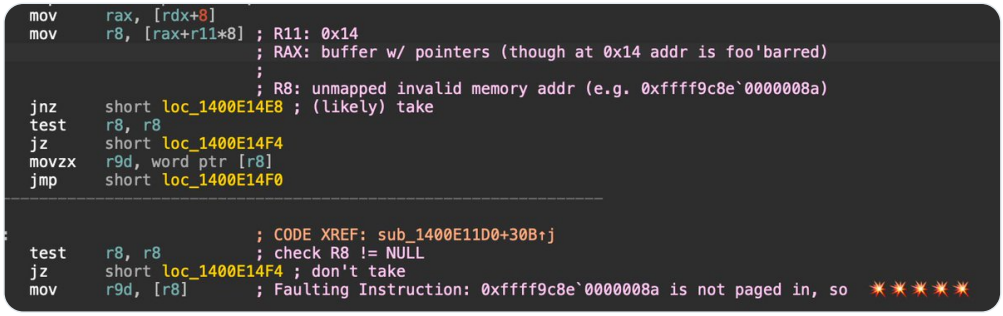
Jul 19, 2024 • 11 tweets • patrickwardle/status/1814343502886477857

I don't do Windows but here are some (initial) details about why the CrowdStrike's CSAgent.sys crashed

Faulting inst: mov r9d, [r8]
R8: unmapped address

...taken from an array of pointers (held in RAX), index RDX (0x14 * 0x8) holds the invalid memory address

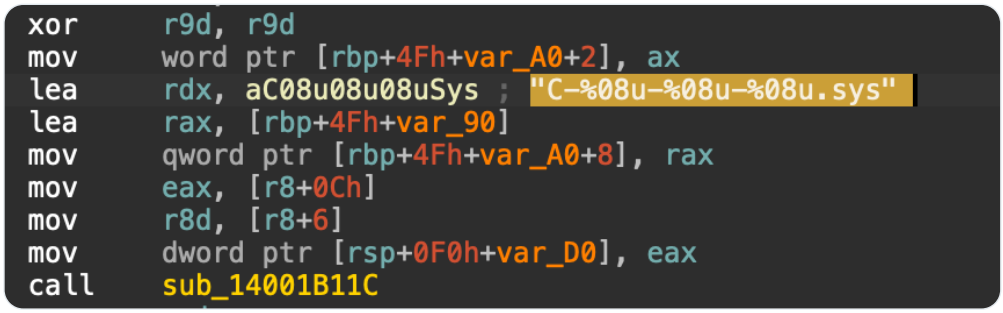
@_JohnHammond



The other "drivers" (e.g. 'C-00000291-...32.sys') appear to be obfuscated data ...and are x-ref'd (perhaps ingested?) by CSAgent.sys

...so maybe invalid (config/signature) data triggered the fault in CSAgent.sys

This would be easier to tell/confirm via debugging 😅



This is all surmised static analysis ...reversing CSAgent.sys (now on VT:)
and data from a single crash dump ...so take with a pinch of 🧂

...and big mahalo to Tom! 🧠🙏
https://www.virustotal.com/gui/file/fc17c021f18ec73d1544ad46dde6a1f1949f126bf3e75f97e241f982e2b07c86

Sharing a .zip with:
▫A few versions of CSAgent.sys (+idb)
▫Various C-....sys files (including the latest that I believe contains the "fix"?)

I don't have any Windows systems/VMs, so hopefully ya'll can keep digging 🥰

#SharingIsCaringhttps://drive.google.com/file/d/1OVIWLDMN9xzYv8L391V1ob2ghp8igoZm/view?usp=share_link

A big outstanding questions to me is; what are the 'C-00000291-...xxx.sys' files?

As deleting them fixes the crash, this seems imply their contents matter (as its CSAgent.sys that has references to them, that is crashing).

But as their contents change between systems... 🤔

"The .sys files causing the issue are channel update files, they cause the top level CS driver to crash as they're invalidly formatted." -Kevin Beaumont

https://cyberplace.social/@GossiTheDog/112812454405913406

Note "channel updates ...bypassed client's staging controls and was rolled out to everyone regardless"

A few IT folks who had set the CS policy to ignore latest version confirmed this was, ya, bypassed, as this was "content" update (vs. a version update)https://www.resetera.com/threads/windows-blue-screen-of-death-bsod-happening-worldwide-right-now-up-caused-by-crowdstrike-falcon-sensor-see-threadmarks.931566/page-17?post=126021399#post-126021399

An update from @CrowdStrike confirms our analysis:

Namely:
▫ The C-...sys files aren't kernel drivers, but rather are "configuration files" dubbed "Channel Files"

▫ C-00000291- "triggered a logic error that resulted in an OS crash" (via CSAgent.sys)

Technical Details on July 19, 2024 Outage | CrowdStrike
Learn more about the July 19, 2024 CrowdStrike outage and the technical details related to it.

https://www.crowdstrike.com/blog/technical-details-on-todays-outage/

@CrowdStrike

Technical Details

On Windows systems, Channel Files reside in the following directory:

`C:\Windows\System32\drivers\CrowdStrike\`

and have a file name that starts with "`C-`". Each channel file is assigned a number as a unique identifier. The impacted Channel File in this event is 291 and will have a filename that starts with "`C-00000291-`" and ends with a `.sys` extension. Although Channel Files end with the SYS extension, they are not kernel drivers.

Channel File 291 controls how Falcon evaluates named pipe[1] execution on Windows systems. Named pipes are used for normal, interprocess or intersystem communication in Windows.

The update that occurred at 04:09 UTC was designed to target newly observed, malicious named pipes being used by common C2 frameworks in cyberattacks. The configuration update triggered a logic error that resulted in an operating system crash.

Channel File 291

CrowdStrike has corrected the logic error by updating the content in Channel File 291. No additional changes to Channel File 291 beyond the updated logic will be deployed. Falcon is still evaluating and protecting against the abuse of named pipes.

This is not related to null bytes contained within Channel File 291 or any other Channel File.

Some surmised a blank (0x0, ...) Channel File was to blame.

@CrowdStrike debunked that stating the issue was "not related to null bytes contained in ...any... Channel File"

Also @MalwareUtkonos notes a check that shows files must start w/ "0xaaaaaaaa":

https://x.com/MalwareUtkonos/status/1814777806145847310

(Others may have mentioned this?) but we find many references "channel files" in @CrowdStrike's patents that provide more insight into their purpose, format, etc.

Search:
"channel file" assignee:(Crowdstrike, Inc.)

For example in US11822515B2 & US11645397B2:

> In some examples, a blocking policy **406** can be can be pushed, or pulled, from a cloud server of the security service **408** to an element of the DC system, which can extract or compile the policy rules and save them to a memory location for later reference. For example, the security service **408** can issue a channel file or other type of file that includes a blocking policy **406** stored in a flat binary format that corresponds to a list of one or more policy rules.

> Global channel files can contain global bounding rules that are to be applied by bounding managers **128** in all security agents **108** on all client devices **104**. Customer channel files can contain customer-specific bounding rules that are to be applied by bounding managers **128** in security agents **108** on client devices **104** associated with a particular customer. For example, a particular customer may want more information about a certain type of event or pattern of events that the

• • •