Hi,贾工：

如刚才沟通，我简要说明一下有关第二份 dump 的分析说明：

1， 从 dump bugcheck 来看，0x139 的问题与当前大规模蓝屏问题的 dump 日志一致，属于内存损坏问题

KERNEL_SECURITY_CHECK_FAILURE (139)
A kernel component has corrupted a critical data structure. The corruption
could potentially allow a malicious user to gain control of this machine.
Arguments:
Arg1: 0000000000000003, A LIST_ENTRY has been corrupted (i.e. double remove).
Arg2: ffffcc00e29d90a0, Address of the trap frame for the exception that caused the bugcheck
Arg3: ffffcc00e29d8ff8, Address of the exception record for the exception that caused the bugcheck
Arg4: 0000000000000000, Reserved

2， 从 call stack 来看，引发此次蓝屏为 McAfee 触发。

STACK_TEXT:
ffffcc00`e29d8d78 fffff807`1d7d76e9 : 00000000`00000139 00000000`00000003 ffffcc00`e29d90a0 ffffcc00`e29d8ff8 : nt!KeBugCheckEx
ffffcc00`e29d8d80 fffff807`1d7d7a90 : ffffcf0e`80402100 fffff807`1d6411dc 00000000`00000000 fffff807`1d929237 : nt!setjmpex+0x7e79
ffffcc00`e29d8ec0 fffff807`1d7d5e8e : ffffcf0e`80402340 ffffcf0e`00000002 00000000`00000000 fffff807`1d83f1ea : nt!setjmpex+0x8220
ffffcc00`e29d90a0 fffff807`1d837b5e : ffffcc00`e29d9240 00000000`00000000 20ca4692`ffffc818 fffff807`358d954e : nt!setjmpex+0x661e
ffffcc00`e29d9230 fffff807`358db6ae : ffffcf0e`8afb8db0 ffffbb81`00000000 ffffcc00`e29d9501 ffffcf0e`8fdbaed0 : nt!memset+0x5f25e
ffffcc00`e29d9280 fffff807`358d9825 : ffffcf0e`94b98a20 ffffcf0e`8afb8db0 ffffcc00`e29d9501 fffff807`358fe423 : mfeavfk+0x1b6ae
ffffcc00`e29d92b0 fffff807`358db0e3 : ffffcf0e`90baecc0 ffffbb81`5233c580 ffffcf0e`90baecc0 ffffcf0e`8fdbaed0 : mfeavfk+0x19825
ffffcc00`e29d92e0 fffff807`358da389 : ffffcf0e`8db57000 ffffcf0e`8afb8db0 ffffcc00`e29d9501 fffff807`1d6b2d07 : mfeavfk+0x1b0e3
ffffcc00`e29d9310 fffff807`358da90d : ffffcf0e`8db57000 ffffcc00`e29d9501 00000000`00000000 fffff807`358d2fb7 : mfeavfk+0x1a389
ffffcc00`e29d9340 fffff807`358db5b3 : ffffcf0e`8db57000 ffffcc00`e29d9501 ffffcc00`e29d9501 fffff807`358cd340 : mfeavfk+0x1a90d
ffffcc00`e29d9370 fffff807`358c7737 : ffffcf0e`8c40e010 ffffcc00`e29d9501 00000000`00000000 fffff807`358c7b1f : mfeavfk+0x1b5b3
ffffcc00`e29d93a0 fffff807`358c8383 : ffffcc00`e29d9501 ffffcf0e`8c40e010 ffffcf0e`9440c040 ffffcf0e`9440c360 : mfeavfk+0x7737
ffffcc00`e29d93d0 fffff807`358c833f : ffffcf0e`8afb8df8 fffff807`1d6b1ca2 ffffcf0e`8c4f9ef0 ffffcf0e`8c40e010 : mfeavfk+0x8383
ffffcc00`e29d9400 fffff807`32f18bc7 : 00000000`00000000 00000000`00000002 ffffbb81`51f84000 fffff807`32fb55a3 : mfeavfk+0x833f

ffffcc00`e29d9430 fffff807`32f1b5ff : ffffcf0e`8c4f9e10 00000000`00000000 ffffcf0e`8c4f9ef0 ffffcf0e`8fdbaed0 : mfehidk+0x8bc7
ffffcc00`e29d9460 fffff807`32f1eafb : ffffcf0e`8afb8db0 ffffcf0e`8afb8db0 ffffcc00`e29d9501 ffffcf0e`5865666d : mfehidk+0xb5ff
ffffcc00`e29d9490 fffff807`32f1eda2 : ffffcf0e`81b51001 ffffcf0e`8afb8db0 ffffcc00`e29d95e0 ffffcf0e`8afb8db0 : mfehidk+0xeafb
ffffcc00`e29d94c0 fffff807`32f1f493 : ffffcf0e`81b51000 ffffcf0e`81b51000 fffff807`1d60e000 ffffcc00`e29d9860 : mfehidk+0xeda2
ffffcc00`e29d9520 fffff807`32faddf3 : 01000000`00000002 ffffcf0e`00000000 ffffcf0e`8fdbae00 00000000`00000000 : mfehidk+0xf493
ffffcc00`e29d95b0 fffff807`1d6ffc29 : ffffcf0e`8c128cf0 00000000`00000000 ffffcf0e`8fdbae00 00000000`00000000 : mfehidk+0x9ddf3
ffffcc00`e29d9630 fffff807`1dc8b564 : 00000000`00000001 ffffcf0e`8c128cf0 ffffcf0e`8fdbae00 00000000`00000000 : nt!IofCallDriver+0x59
ffffcc00`e29d9670 fffff807`1dc94d40 : 00000000`00000001 00000000`00000000 ffffcf0e`80b3e0c0 ffffcf0e`8fdbae00 : nt!NtQueryInformationFile+0xd94
ffffcc00`e29d96f0 fffff807`1d6b5269 : 00000000`00000000 00000000`00000000 00000000`00000001 ffffcf0e`8c128cf0 : nt!MmCopyVirtualMemory+0x1600
ffffcc00`e29d9750 fffff807`1dc60920 : 00000000`ffff8001 ffffcf0e`80b3e0c0 ffffa888`00000000 00000000`00007fff : nt!ObfDereferenceObjectWithTag+0xc9
ffffcc00`e29d9790 fffff807`1dc6519e : ffffcf0e`9440c040 00000000`00000001 00000000`ffffffff 00000000`00000001 : nt!ObOpenObjectByNameEx+0x1020
ffffcc00`e29d98d0 fffff807`1d7d7105 : ffffcf0e`92d63040 ffffbb81`519c0180 ffffcc00`e29d99c0 ffffbb81`00000000 : nt!NtClose+0xde
ffffcc00`e29d9940 fffff807`1d7c9be0 : fffff807`32f620e3 00000000`00000000 ffff8380`01751370 ffffe799`cf423bb2 : nt!setjmpex+0x7895
ffffcc00`e29d9ad8 fffff807`32f620e3 : 00000000`00000000 ffff8380`01751370 ffffe799`cf423bb2 00000000`00000000 : nt!KeSynchronizeExecution+0x2b80
ffffcc00`e29d9ae0 fffff807`1d66f6e5 : ffffcf0e`9440c040 00000000`00000080 fffff807`32f62040 00000000`00000000 : mfehidk+0x520e3
ffffcc00`e29d9b10 fffff807`1d7cd34c : ffffbb81`519de180 ffffcf0e`9440c040 fffff807`1d66f690 ffffcf0e`912b8ac0 : nt!RtlIpv4StringToAddressW+0x4d5
ffffcc00`e29d9b60 00000000`00000000 : ffffcc00`e29da000 ffffcc00`e29d3000 00000000`00000000 00000000`00000000 : nt!KeSynchronizeExecution+0x62ec

lmvm mfeavfk
Browse full module list
start end module name
fffff807`358c0000 fffff807`3591d000 mfeavfk (no symbols)
Loaded symbol image file: mfeavfk.sys
Image path: \SystemRoot\system32\drivers\mfeavfk.sys
Image name: mfeavfk.sys
Browse all global symbols functions data
Timestamp: Fri Aug 16 21:39:41 2019 (5D56B21D)
CheckSum: 0006149C

ImageSize: 0005D000
Translations: 0000.04b0 0000.04e4 0409.04b0 0409.04e4
Information from resource tables:

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：4008180055
电子邮箱 Email: liqi@cmgos.com