Защита от некоторых классов вредоносного программного обеспечения в ОС семейства Linux

И.Б. Бережной, Н.Д. Соловьев

НИИ прикладных проблем математики и информатики
Белорусский государственный университет

06.10.2026

Записка программы-вымогателя

Программы-вымогатели

Ransomware = ransom + software — тип вредоносного программного обеспечения для вымогательства путем зашифровывания данных, ценных для пользователя компьютерной системы, и последующего требования выкупа за их восстановление.

Концепция была представлена в 1996 году на конференции IEEE Security & Privacy conference.

БЕЛАРУСКІ ДЗЯРЖАЎНЫ УНІВЕРСІТЭТ

Программы-вымогатели в 2026 году

БЕЛАРУСКІ ДЗЯРЖАЎНЫ УНІВЕРСІТЭТ

Программы-вайперы

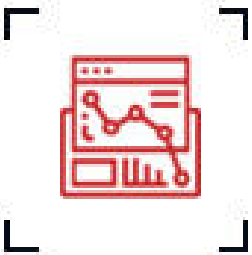
От английского To wipe = стирать.

Вайперы — тип вредоносного программного обеспечения, главная цель которого — полностью или частично уничтожить данные на компьютере жертвы путем безвозвратного зашифровывания данных.

Методы детектирования системами EDR и MDR

На основе сигнатур:

- наличие в оперативной памяти образцов вредоносного кода,
- доступ к подозрительным URL.



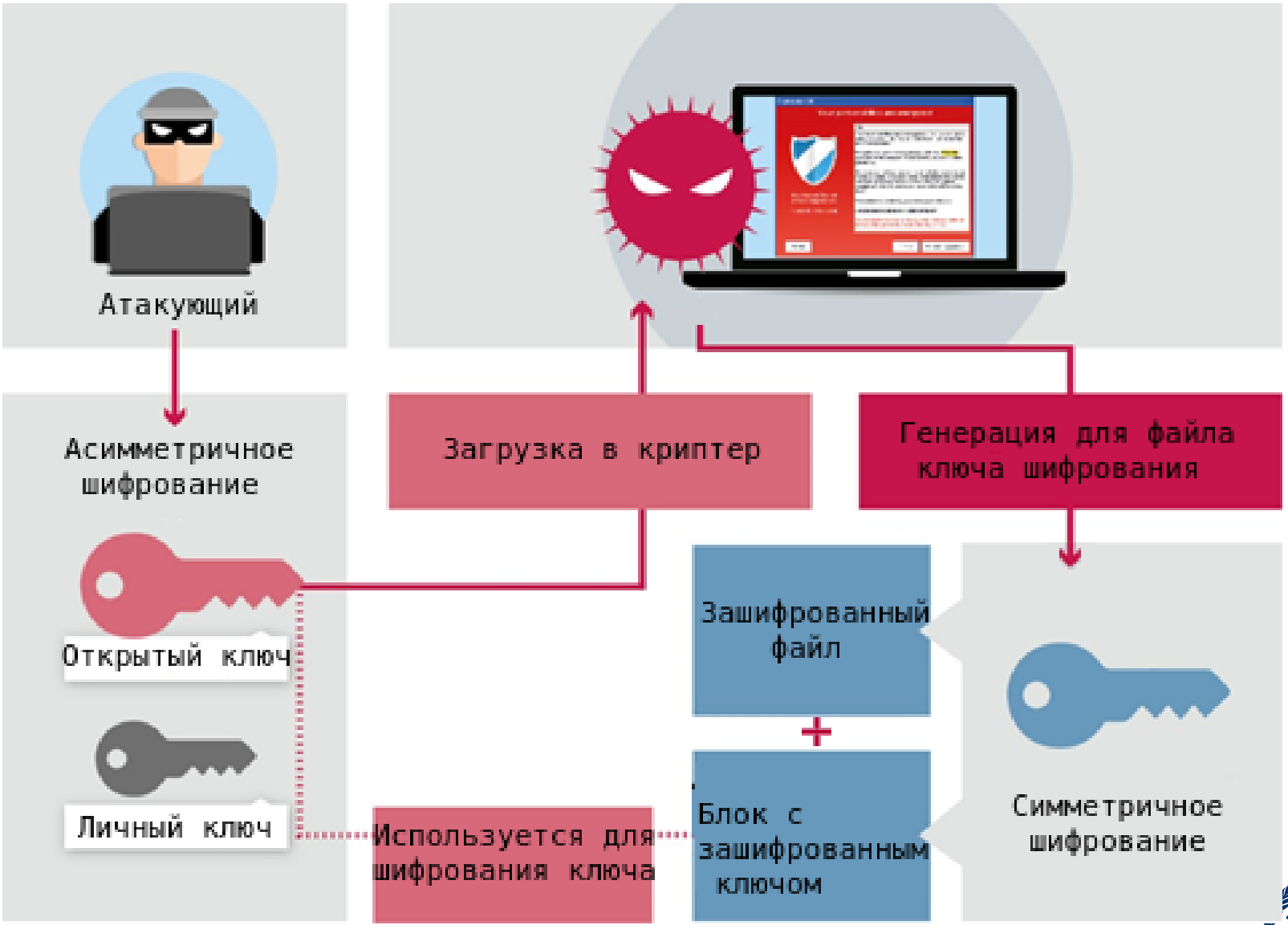
Анализ сетевого трафика:

- доступ к подозрительным узлам,
- работа с сетевыми устройствами.

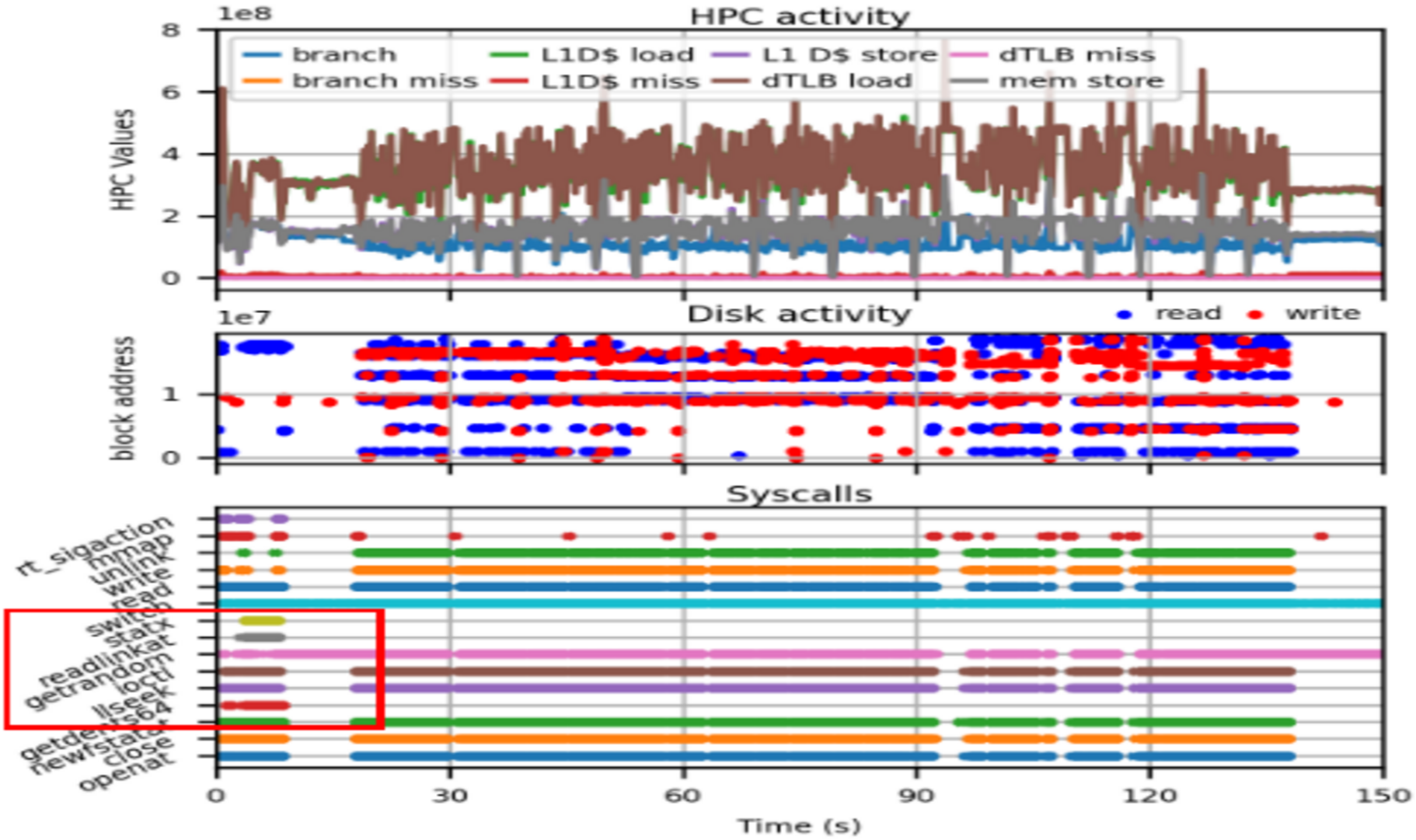
Анализ базовых взаимодействий с ОС:

- активная работа с реестром,
- получение дампов памяти LSASS,
- запуск подозрительных сервисов и программ,
- добавление пользователей и повышение их привилегий.

Общая схема криптографического ядра ransomware



Потребление случайности в программе-вымогателе



Уязвимость криптографического ядра ransomware

Основное тонкое место описанной схемы ядра ransomware — получение данных от генератора псевдослучайных чисел (ГПСЧ).

ГПСЧ может быть реализован:

- полностью самостоятельно с использованием доступных ВПО источников энтропии,
- с использованием штатных ГПСЧ операционной системы.

Самостоятельная реализация ГПСЧ

```
void generate_random(char *buffer, int size)
{
    uint64_t t = get_current_time_nanosecond();
    char seed[32];
 //in the real code, it uses C++ code to convert i
    snprintf(seed, sizeof(seed), "%lld", t);
    struct yarrow256_ctx ctx;
    yarrow256_init(&ctx, 0, NULL);
    yarrow256_seed(&ctx, strlen(seed), seed);
    yarrow256_random(&ctx, size, buffer);
}
```

Decrypting Encrypted files from Akira Ransomware (Linux/ESXI variant 2024) using a bunch of GPUs

admin

March 13, 2025

hacks, reverse-engineering, security

define, Final

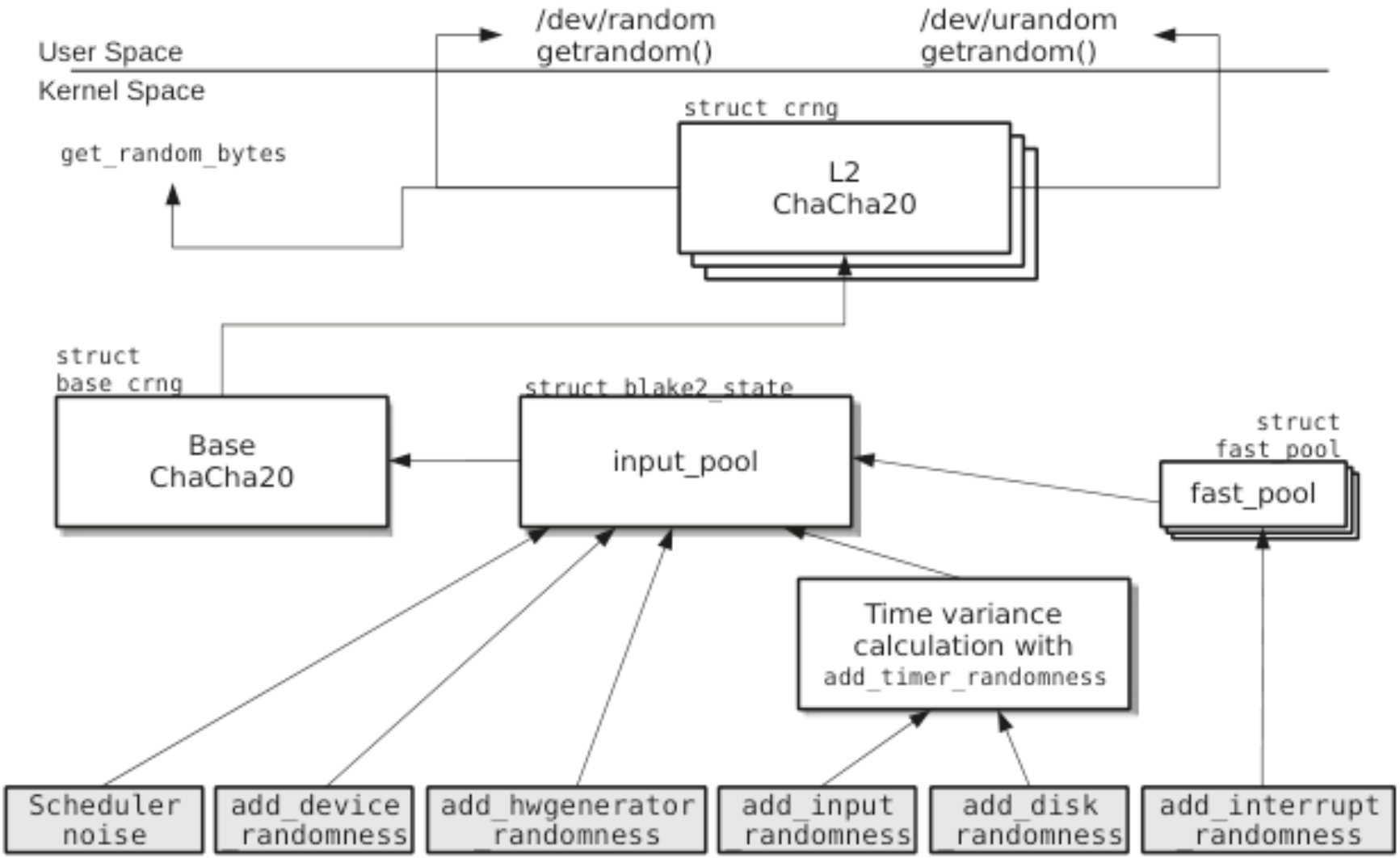
I recently helped a company recover their data from the Akira ransomware without paying the ransom. I'm sharing how I did it, along with the full source code.

The code is here: https://github.com/yohanes/akira-bruteforce

To clarify, multiple ransomware variants have been named Akira over the years, and several versions are currently circulating. The variant I encountered has been active from late 2023 to the present (the company was breached this year).

БЕЛАРУСКІ ДЗЯРЖАЎНЫ УНІВЕРСІТЭТ

Архитектура ГПСЧ с версии 5.18.1 ядра Linux



Источники случайности для User Space

Interface	Pool	Blocking behavior	Behavior when pool is not yet ready
/dev/random	Blocking pool	If entropy too low, blocks until there is enough entropy again	Blocks until enough entropy gathered
/dev/urandom	CSPRNG output	Never blocks	Returns output from uninitialized CSPRNG (may be low entropy and unsuitable for cryptography)
getrandom()	Same as */dev/urandom*	Does not block once pool is ready	Blocks until pool ready
getrandom() **GRND_RANDOM**	Same as */dev/random*	If entropy too low, blocks until there is enough entropy again	Blocks until pool ready
getrandom() **GRND_NONBLOCK**	Same as */dev/urandom*	Does not block once pool is ready	**EAGAIN**
getrandom() **GRND_RANDOM** + **GRND_NONBLOCK**	Same as */dev/random*	**EAGAIN** if not enough entropy available	**EAGAIN**

БЕЛАРУСКІ ДЗЯРЖАЎНЫ УНІВЕРСІТЭТ

Фреймворк динамической трассировки Ftrace

В ОС семейства Linux начиная с версии ядра 2.7.27, представленной в 2008 году, встроен фреймворк динамической трассировки Ftrace (от англ. Function Trace) для детальной фиксации низкоуровневых событий, происходящих внутри ядра операционной системы.

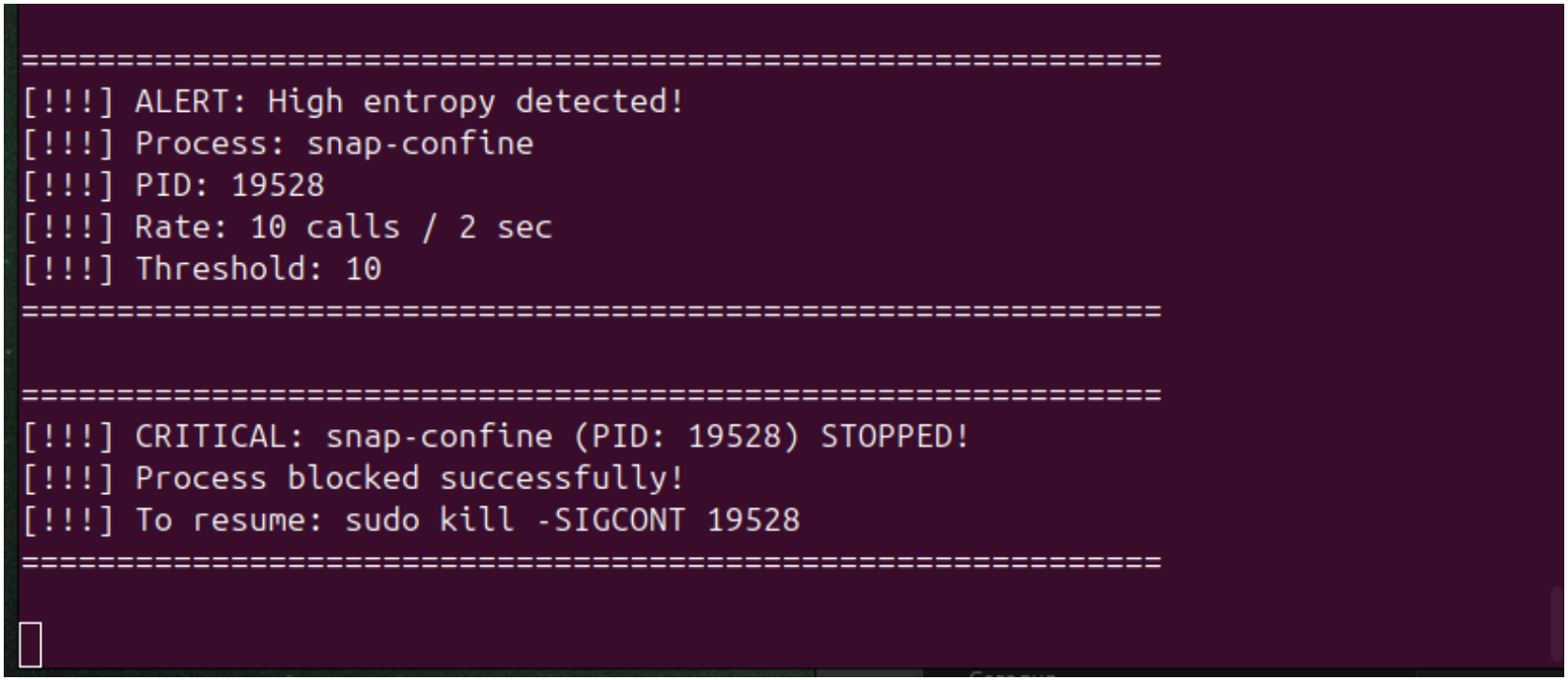
```
# tracer: function
#
# entries-in-buffer/entries-written: 140080/250280   #P:4
#
#                              _-----=> irqs-off
#                             / _----=> need-resched
#                            | / _---=> hardirq/softirq
#                            || / _--=> preempt-depth
#                            ||| /     delay
#           TASK-PID   CPU#  ||||    TIMESTAMP  FUNCTION
#              | |       |   ||||       |         |
           bash-1977  [000] .... 17284.993652: sys_close <-system_call_fastpath
           bash-1977  [000] .... 17284.993653: __close_fd <-sys_close
           bash-1977  [000] .... 17284.993653: _raw_spin_lock <-__close_fd
           sshd-1974  [003] .... 17284.993653: __srcu_read_unlock <-fsnotify
           bash-1977  [000] .... 17284.993654: add_preempt_count <-_raw_spin_lock
           bash-1977  [000] ...1 17284.993655: _raw_spin_unlock <-__close_fd
           bash-1977  [000] ...1 17284.993656: sub_preempt_count <-_raw_spin_unlock
           bash-1977  [000] .... 17284.993657: filp_close <-__close_fd
           bash-1977  [000] .... 17284.993657: dnotify_flush <-filp_close
           sshd-1974  [003] .... 17284.993658: sys_select <-system_call_fastpath
           ....
```

БЕЛАРУСКІ ДЗЯРЖАЎНЫ УНІВЕРСІТЭТ

Метод защиты от ransomware и вайперов

1. настраивается мониторинг через Ftrace вызовов функций ядра, связанных с запросами к ГПСЧ (__sys_getrandom);
2. при каждом вызове целевой функции в кольцевом буфере ядра, доступном из User Space через файл /sys/kernel/debug/tracing/trace_pipe, формируется запись;
3. скрипт из User Space осуществляет непрерывное чтение из буфера записей, агрегацию событий по идентификатору процесса (PID) и расчёт частоты вызовов в скользящем окне заданной длины;
4. при превышении порогового значения частоты вызовов некоторым процессом ему отправляется системный сигнал SIGSTOP, переводя его в состояние приостановки.

Экспериментальное программное обеспечение



ПО показало высокую скорость детектирования (меньше 2,7 секунд с начала работы процесса ВПО при размере скользящего окна в 2 секунды) и малую ресурсоемкость (нагрузка на CPU меньше 5%), при этом точность детектирования в ходе модельных экспериментов превосходит 0,98.

БЕЛАРУСКІ ДЗЯРЖАЎНЫ УНІВЕРСІТЭТ

Достоинства и недостатки предложенного метода

К достоинствам предлагаемого метода можно отнести:

- пригодность для борьбы с ВПО различных семейств и классов,
- низкое количество ошибок первого рода у детектора ransomware в силу относительно малой потребности в ГПСЧ для обычных пользовательских процессов,
- возможность остановки процесса ВПО до начала этапа шифрования файлов.

К недостаткам метода можно отнести:

- необходимость отслеживания всех возможных интерфейсов ГПСЧ,
- необходимость настройки предварительного белого списка в случае работы некоторых пользовательских процессов,
- невозможность детектирования ВПО, имеющего собственную реализацию ГПСЧ.

Спасибо за внимание!