www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Нюк-Нюк в эктоплазме дружелюбного Каспера

или как мы угостили Nuclei его же фаст-фудом и приручили KESL

Сергей Гордейчик – генеральный директор СайберОК

В тот летний вечер я всего-то хотел дождаться выхода очередного релиза своего какафон-рок проекта — он традиционно выкатывается в 00:01 по мск, а потом надо раскидать релиз по чатам-каналам и лечь спать.

Но вместо спокойного вечера с сериальчиком мне прилетела задачка от одного крупного госзаказчика: «**Касперский кладёт в карантин IP-адрес фронта, когда ваша СКИПА PentOps его мониторит — что делать?**»

По ходу решения задачи возникло пару полезных артефактов и маскотов, пачка слайдов *«Нюк-нюк в эктоплазме дружелюбного Каспера»* и вот эта статья. Ниже — почти стенограмма, только покомпактнее и без ночных зевков.

Синдром заблокированного фронта или «Что вообще происходит?»

Архитектура у заказчика классическая:
Интернет → Terminat0r-LB → backend, где на каждом узле бекенда крутится **Kaspersky Endpoint Security for Linux (KESL)**, а паранойя включена ровно на максимум: *Network Threat Protection* (NTP) ловит всё, что напоминает атаку, и… банит IP-адрес, откуда прилетели пакеты.

Фронт стоит за балансером, X-Forwarded-For он не смотрит, поэтому **в карантин улетает именно адрес балансера,** а не злобного бота-хакера из пула СКИПА СайберОК. Через час блок снимается, но за это время EASM не ищет баги, SLA горит, DevOpsы плачут, клиенты пишут нехорошее в поддержку.

Можно, конечно отключить сертифицированное средство защиты, но в наше беспокойное время такие идеи на грани предательства.

Попытка воспроизвести (спойлер: не вышло)

Логика подсказывала:
«Повторяем скан ➔ видим блокировку ➔ дальше разберёмся».

Поднял минимальный стенд Nginx, прокинул через балансёр, запустил без пайплайна "все-все-все" шаблоны нуклея, авось что-то стрельнет.

```
nuclei -u http://target.example -t ~/nuclei-templates
```

— и… **тишина**.
KESL NTP молчит, IP-адрес жив. Казалось бы, «задача решена» — но нет, в бою фронтенд всё равно улетает в карантин. Значит, наш макет слишком «чистый», сигнатурам не за что зацепиться. Пришлось копать глубже.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Эхо-сервер: первая, но наивная идея

Как только антивирусу не нравится то, что мы отдаём, давайте отдавать **то, что он хочет**.

Сварганил самый простой «эхо» (псведокод, исходники в гите в конце статьи):

```
from flask import Flask, request
app = Flask(__name__)

@app.route("/", defaults={"path": ""})
@app.route("/<path:path>", methods=["GET", "POST"])
def echo(path):
    return f"{request.method} {request.full_path}", 200
```

Прогнал — снова ноль срабатываний.

Открытие: KESL смотрит не только URI-паттерны, а ещё *ответ* сервера. Мы отдаём безобидный «OK», и антивирус безмятежен.

«Накорми сканер его же шаблоном» — рождение Nuk-Nuke

Каждый шаблон Nuclei (YAML-файл) хранит:

- путь запроса (path или raw)
- и самое главное — **matchers**: набор признаков «успешной атаки»(статус-код, строки, регекспы, заголовки).

```
matchers:
  - type: status
    status:
      - 200
  - type: word
    words:
      - "<title>It works!</title>"
```

И тут щёлкнуло:

Если мы вернём сканеру именно такой статус и текст, шаблон сработает, Nuclei закричит «CRITICAL» — а NTP, увидев точно тот маркер, вешает бан.

Так родился Nuk-Nuke — мини-сервер, который парсит все шаблоны и автоматически подделывает «успешный взлом».

Как устроен «Нюк-Нюк»

1. Генерируем кэш

1. В каталоге ~/nuclei-templates — 10 000+ YAML-ов.
2. Проходим их ProcessPoolExecutor-ом, вытаскиваем (path, status, headers, body).

3. Кладём в один MsgPack. Разок считаем — и стартуем за 0,3 с.

```
python decoy_server.py --rebuild-cache
```

2. Отдаём правильные ответы

```
@app.before_request
def dispatch():
    entry = DECOYS.get(normalise(request.path))
    if entry:
        status, hdrs, body = entry
        return make_response(body, status, hdrs)
```

Пара штрихов:

- Заменяем заголовки, чтобы ответ походил на Apache, а не на Flask dev-server.
- Поддерживаем --prod (Waitress), чтобы не палить баннеры Werkzeug.

Полный код в репозитории.

Демон-тест

1. **Запускаем сервер:**

```
export DECOY_SERVER_HEADER="Apache/2.4.57"
python decoy_server.py --prod --port 8080
```

2. **Стреляем Nuclei:**

```
nuclei -u http://127.0.0.1:880 -t ~/nuclei-templates
```

3. Через пару секунд в kesl-control --get-blocked-hosts — наш IP. Проблема воспроизведена на локалке, можно охотиться на «токсичные» шаблоны.

Фильтруем термо-яд — минус четыре* шаблона

Оказалось, банят ровно четыре древних CVE (Tomcat, Atlassian, Log4Shell). Достаточно запустить бой-скан без них:

```
nuclei -t ~/nuclei-templates \
       -et http/cves/2017/плохой.yaml,http/cves/2021/плохой.yaml \
       -l prod-endpoints.txt
```

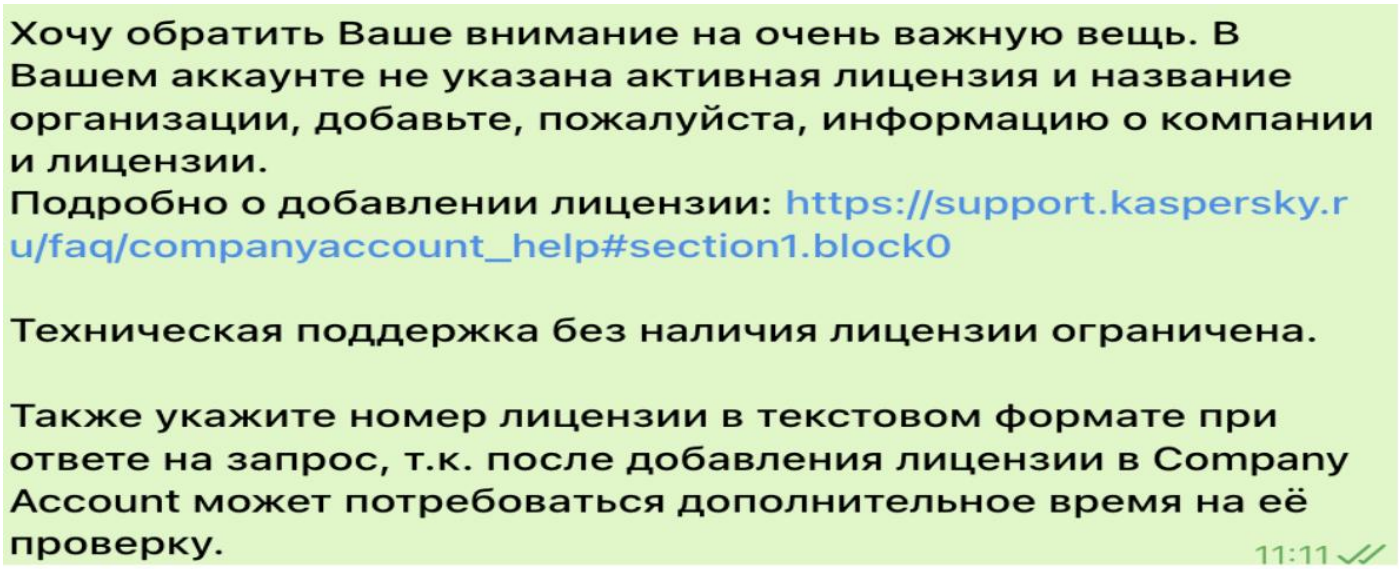
— и KESL больше не реагирует.

*На самом деле все немного сложнее, за эти 4 алерта отвечает пачка шаблонов (особенно за Log4j), но с помощью Nuk-Nuke они очень быстро собираются.

Это ок, но нужно лучше

Ок, мы собрали плохие шаблоны, но что если вылезут другие сигнатуры в будущем? В идеале надо все-таки добавить IP-фронта в исключения. На какой-то момент я сдался и обратился в поддержку.

Их ответ был профессиональным и исчерпывающим.



Эта великая мудрость привела меня к силе и, початив с Гуглом и Гопотой минут десять, я нашел рабочий вариант.

```
# Узнать имя задачи
sudo kesl-control --get-task-list | grep -i network_threat

# Включить исключения и добавить IP
sudo kesl-control --set-settings Network_Threat_Protection \
     UseExcludeIPs=Yes \
     ExcludeIPs.item_0000=10.10.10.10

# Перезапустить задачу
sudo kesl-control --stop-task Network_Threat_Protection
sudo kesl-control --start-task Network_Threat_Protection
```

Что прокачать дальше

Идея	**Зачем**
Tarpit-mode	Спать врагу: после первой «атаки» кладём соединение на паузу 5с
Рандомизация баннеров	Мешаем IIS/Apache/Nginx, чтобы ловились разные сигнатуры

Плагин для Nginx	Отдавать поддельный ответ прямо из error_page 404
Стрим логов в Loki / Slack	Собирать IP-адреса реальных сканеров в SOC

Выводы

- Nuk-Nuke позволяет на тестовом стенде быстро понять, *какие именно* nuclei-шаблоны бьют по антивирусу/IDS.
- После этого достаточно одной короткой строки -et (или исключения в KESL) — и фронтовый IP жив, сканы идут, NTP остаётся включённым.
- Проверить на баги чтобы не взломали через антивзломщик.
- Весь проект — полчаса вайбкодинга.
- Я успел все заделать к выходу какафон-рок релиза, ура!

Иногда, чтобы обмануть защиту, нужно всего-навсего показать ей то, что она ожидает увидеть.

Слайды доклада лежат у нас в телеге, а полный код «Нюк-Нюка» — прямо тут. Забирайте, экспериментируйте и не давайте сканерам скучать!