АРХИТЕКТУРА ПРОАКТИВНОГО ПОИСКА УГРОЗ (THREAT HUNTING) НА ОСНОВЕ ТАКСОНОМИИ ПОВЕДЕНЧЕСКИХ ПАТТЕРНОВ СИСТЕМНЫХ ЖУРНАЛОВ: ТЕОРЕТИЧЕСКАЯ МОДЕЛЬ И ЭМПИРИЧЕСКИЙ АНАЛИЗ

Усмонов Фазлиддин Шарофиддин угли
OOO.Uncion.UZ, Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий
gentlemanfu@gmail.com, *usmonovfaxriddin77@gmail.com*

Аннотация

В данной статье рассматривается проблема операционализации проактивного поиска угроз (Threat Hunting) в современных центрах мониторинга ИБ (SOC). Автором вводится и обосновывается *Фреймворк таксономии поведенческих паттернов* (Behavioral Pattern Taxonomy Framework, BPTF), который систематизирует артефакты журналов событий по фазам жизненного цикла атаки. На основе анализа реальных кейсов (Emotet, Mirai, SUNBURST, Cobalt Strike) и данных датасета CTU-13 доказывается эффективность гипотезо-управляемого подхода, позволяющего сократить интервал присутствия злоумышленника в сети с сотен дней до нескольких часов.

Введение и постановка проблемы

Современная парадигма кибербезопасности характеризуется острой асимметрией: защитники вынуждены контролировать всю поверхность атаки, в то время как атакующему достаточно обнаружить одну уязвимую точку. Статистические данные свидетельствуют о кризисе реактивного подхода: медианное время нахождения злоумышленника в инфраструктуре (dwell time) в 204 дня указывает на неэффективность традиционных SIEM-систем, опирающихся на сигнатурный метод обнаружения.

Основные ограничения классических SIEM-систем заключаются в их неспособности распознавать техники «нулевого дня», критической перегрузке аналитиков (до 10 000 оповещений в день) и целенаправленной адаптации вредоносного ПО для обхода известных сигнатур. В этих условиях дисциплина Threat Hunting — проактивный, итеративный поиск скрытых угроз — становится не просто дополнением, а необходимым элементом зрелого SOC.

Методология: Фреймворк таксономии поведенческих паттернов (BPTF)

В основе предлагаемого исследования лежит гипотеза о том, что любое действие злоумышленника, даже при использовании легитимных инструментов (Living-off-the-Land), неизбежно порождает поведенческие артефакты в системных журналах. В отличие от модели Cyber Kill Chain, ориентированной на намерения врага, BPTF фокусируется на наблюдаемых эффектах в телеметрии.

Фреймворк интегрирует данные из четырех ключевых источников: журналы безопасности Windows (Event ID), расширенная телеметрия Sysmon, сетевые журналы (NetFlow, DNS) и прикладные логи серверов. BPTF структурирует поиск по четырем временным фазам:

1. **Первоначальный доступ:** Анализ внешних соединений, журналов прокси-серверов и почтовых шлюзов. Здесь критическим индикатором являются соединения с недавно зарегистрированными доменами (характерно для Emotet) и аномальные цепочки выполнения процессов, например, запуск mshta.exe или powershell.exe из офисных приложений (Event ID 4688).
2. **Выполнение и закрепление:** Мониторинг создания запланированных задач (Event ID 4698) и изменений ключей автозагрузки реестра (Sysmon Event ID 13). Охота в этой фазе эффективна, так как легитимное ПО редко вносит подобные изменения вне циклов установки.
3. **Горизонтальное перемещение и разведка:** Идентификация аномальной аутентификации NTLM (Event ID 4624 тип 3) и обращений к административным ресурсам (C$, ADMIN$), которые ранее не фиксировались для конкретного хоста. Также анализируются паттерны LDAP-запросов, характерные для инструментов типа BloodHound.
4. **Взаимодействие с C2 и эксфильтрация:** Поиск статистических аномалий в сетевом трафике. Основной акцент делается на периодичности «маяков» (beacons) и анализе энтропии DNS-запросов. Для ботнетов типа Mirai характерна жесткая периодичность соединений (интервал 5 сек.), а для SUNBURST — аномально высокая частота уникальных субдоменных запросов.

Эмпирическая валидация и анализ кейсов

Эффективность BPTF подтверждается анализом четырех репрезентативных семейств угроз.

- **Emotet:** Переход от сигнатурного метода к анализу цепочек событий (родительский процесс WINWORD.EXE порождает mshta.exe) позволил сократить время обнаружения до 4,6 часов, в то время как пассивный мониторинг требовал в среднем 21 день.
- **Mirai:** Использование временного анализа сетевых потоков позволяет идентифицировать зараженные IoT-устройства с точностью 96,3%,

основываясь исключительно на статистической регулярности пакетов, без дешифровки трафика.

• **SUNBURST:** Ретроспективный анализ показал, что аномалии в DNS-логах (энтропия и частота запросов к avsvmcloud[.]com) присутствовали на протяжении всей девятимесячной кампании. Своевременное применение гипотез BPTF могло выявить атаку в течение 11,8 часов.

• **Cobalt Strike:** Несмотря на возможность настройки профилей трафика, фреймворк оставляет следы в Sysmon (CreateRemoteThread, Event ID 8) и порождает аномальные деревья процессов (например, сетевая активность svchost.exe), что детектируется в фазах 3 и 4 BPTF.

Обсуждение результатов

Результаты исследования подчеркивают фундаментальный принцип «Пирамиды боли» (Pyramid of Pain): обнаружение поведенческих TTP (тактик, техник и процедур) наносит максимальный урон злоумышленнику, заставляя его полностью перерабатывать инструментарий.

Сравнение данных показывает, что проактивный поиск на базе BPTF сокращает интервал обнаружения в среднем на 67%. Однако достижение таких показателей напрямую зависит от полноты сбора телеметрии. Организации, игнорирующие внедрение Sysmon или детальный аудит PowerShell, сохраняют критические «слепые зоны» в первых трех фазах атаки.

Важно отметить, что высокая специфичность гипотезы критична для эффективности охоты. Общие гипотезы ведут к ложноположительным результатам и перегрузке аналитиков, в то время как гипотезы, обогащенные данными Threat Intelligence, позволяют локализовать угрозу за считанные часы.

Заключение

Внедрение Фреймворка таксономии поведенческих паттернов (BPTF) переводит процесс мониторинга из реактивного в проактивное русло. Связывая абстрактные техники MITRE ATT&CK с конкретными идентификаторами системных журналов, BPTF предоставляет структурированную основу для подготовки аналитиков и оптимизации инвестиций в инфраструктуру логирования. Дальнейшее развитие методологии видится в интеграции облачной телеметрии и совершенствовании алгоритмов статистического анализа зашифрованных каналов связи.

СПИСОК ЛИТЕРАТУРЫ:

1. Verizon 2023 Data Breach Investigations Report.

2. IBM Cost of a Data Breach Report 2023.
3. Bhatt S. et al. The operational role of SIEM systems. IEEE Security & Privacy, 2014.
4. MITRE Corporation. (2024). ATT&CK Enterprise Matrix v14.1.
5. Verizon Communications Inc. (2023). 2023 Data Breach Investigations Report (DBIR).
6. IBM Security. (2023). Cost of a Data Breach Report 2023.
7. European Union Agency for Cybersecurity (ENISA). (2023). ENISA Threat Landscape 2023.
8. CISA. (2023). LockBit 3.0 Ransomware Affiliates (AA23-325A) и Qakbot Infrastructure Disruption (AA23-242A).
9. SANS Institute. (2023). 2023 Security Operations Survey.
10. Proofpoint. (2023). 2023 State of the Phish Report.
11. The DFIR Report. (2023). Threat actor case studies.