СИНЕРГЕТИЧСЕКИЙ ЭФФЕКТ ПРИ КОМБИНИРОВАНИИ РАЗНОРОДНЫХ КИБЕРАТАК

Ковалевич М.А., студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мокеров В.С. – ассистент каф. ЗИ

Аннотация. В работе выполнен теоретический анализ синергетического эффекта при комбинировании разнородных кибератак. Показано, что эффективность композитных атак превышает сумму эффективностей отдельных компонентов, что противоречит традиционным аддитивным моделям. Выявлен эффект композитного перехода – существование пар атак, безопасных по отдельности, но критических в комбинации. Предложена классификация типов синергии по механизму взаимодействия. На основе анализа реальных примеров обоснована необходимость перехода от изолированных средств защиты к кросс-слойной корреляции событий в системах мониторинга безопасности.

Ключевые слова. кибератаки, синергетический эффект, композитные атаки, корреляция событий.

Синергия в кибератаках возникает при объединении различных методов (технических, социальных, психологических), где совокупный эффект превышает сумму действий по отдельности. Ключевые механизмы включают многоступенчатые (APT) атаки, комбинирование фишинга с эксплойтами, использование ботнетов для усиления DDoS, и одновременное воздействие на инфраструктуру и персонал [1].

Ключевым недостатком большинства систем безопасности является отсутствие корреляции разнородных событий. Каждый инцидент анализируется автономно, что исключает возможность обнаружения многоступенчатых атак, проявляющихся только через последовательность событий различных типов.

Синергетический эффект при комбинировании разнородных кибератак возникает вследствие четырех основных механизмов. Первый – ослабление защиты: злоумышленники отключают системы логирования и очищают журналы событий, что снижает эффективность средств обнаружения [2]. Второй – отвлечение внимания: DDoS-атаки служат прикрытием для кражи данных или повышения привилегий, перегружая центры мониторинга безопасности [3]. Третий – сокрытие следов: использование легитимных инструментов ОС (Living Off the Land) и отключение логирования веб-серверов позволяют маскировать вредоносную активность [4]. Четвертый – обход разных слоев защиты: антивирус, файрвол и DLP работают изолированно, а комбинированная атака использует разрывы между ними [5].

Для рассмотрения синергии в кибератаках были выбраны следующие виды кибератак: фишинг, Pass-the-Hash, DDoS, эксфильтрация данных, отключение логирования, эксплуатация уязвимости. В таблице 1 представлена эффективность кибератак по отдельности и в комбинации.

Фишинг представляет собой метод социальной инженерии, при котором злоумышленник создает поддельное электронное письмо, веб-сайт или сообщение, имитирующее легитимную организацию (банк, корпоративный портал, сервис электронной почты). Жертву побуждают перейти по вредоносной ссылке, открыть зараженное вложение или ввести свои учетные данные на поддельной странице. В результате фишинг позволяет злоумышленнику получить доступ к учетным данным жертвы или установить вредоносное программное обеспечение на ее компьютере. Pass-the-Hash (PtH) – это техническая атака, при которой злоумышленник использует хеш пароля пользователя для аутентификации на удаленных системах. В операционных системах Windows хеши паролей хранятся в памяти процесса LSASS или на диске в файле SAM. PtH позволяет атакующему, имеющему хеш, подключаться к другим компьютерам в сети, выдавая себя за легитимного пользователя. Фишинг и PtH образуют последовательную цепочку. Сначала фишинговая атака позволяет получить доступ к рабочей станции и извлечь хеш пароля. Затем, имея хеш, злоумышленник применяет PtH для аутентификации на других компьютерах в сети – серверах, рабочих станциях коллег, контроллерах домена. Каждый новый скомпрометированный компьютер дает новые хеши, что позволяет двигаться дальше.

DDoS-атака (Distributed Denial of Service) – это атака, при которой злоумышленник использует сеть зараженных устройств (ботнет) для отправки огромного количества запросов к целевой системе. Цель – перегрузить вычислительные ресурсы, пропускную способность канала или сетевые сервисы, сделав их недоступными для легитимных пользователей. DDoS-атака генерирует десятки тысяч оповещений в секунду, перегружая центры мониторинга безопасности (SOC). Эксфильтрация данных – это несанкционированное копирование, передача или выгрузка конфиденциальной информации за пределы контролируемой сети. Злоумышленник может использовать легитимные протоколы (HTTP, HTTPS, DNS, FTP), облачные хранилища или скрытые каналы связи. Эксфильтрация требует времени (особенно при больших объемах данных) и создает аномальный

сетевой трафик, который может быть обнаружен DLP-системами, анализаторами трафика или специалистами SOC. DDoS-атака запускается одновременно с эксфильтрацией или незадолго до нее. Массовый поток оповещений от DDoS перегружает SOC – специалисты вынуждены обрабатывать тысячи ложных срабатываний, отвлекаться на восстановление доступности сервисов. На этом фоне эксфильтрация данных остается незамеченной, так как ее трафик теряется в общем шуме. Кроме того, аномалии, связанные с эксфильтрацией, могут быть ошибочно отнесены к последствиям DDoS.

Отключение логирования – это действие, при котором злоумышленник изменяет настройки системы аудита, останавливает службы журналирования, очищает существующие журналы событий или удаляет логи веб-серверов. Цель – уничтожить доказательства своей активности и предотвратить фиксацию последующих действий. Это действие может быть выполнено через скомпрометированную учетную запись, с использованием штатных средств ОС или вредоносного ПО. Эксплуатация уязвимости (exploitation) – это использование программной ошибки, недостатка конфигурации или слабости в реализации для получения несанкционированного доступа, повышения привилегий, выполнения произвольного кода или обхода механизмов безопасности. Эксплуатация может привести к полной компрометации системы. Злоумышленник сначала отключает систему логирования или очищает журналы событий. Это действие может быть выполнено удаленно через скомпрометированную учетную запись. После того как логирование отключено, он эксплуатирует уязвимость – но записать эту эксплуатацию уже некому. Система не фиксирует ошибки, не сохраняет данные о созданных процессах, не регистрирует сетевые подключения.

Таблица 1 – Эффективность реализации кибератак

Вид кибератаки	Оценка эффективности	Ограничения	Эффект
Фишинг	До 5%	Только одна рабочая станция	Дает начальный доступ и хеш пароля
Pass-the-Hash	До 10%	Требует предварительно скомпрометированный хеш	Использует хеш для перемещения по сети
DDoS	До 5%	Не дает доступа к данным	Создает шум и отвлекает SOC
Эксфильтрация	До 15%	Обнаруживается по трафику	Кража данных
Отключение логов	0%	Само по себе безопасно	Не дает права доступа
Эксплуатация уязвимости	До 25%	Оставляет следы в логах	Кибератака со следами

Обобщая рассмотренные примеры, можно выделить четыре основных типа синергии по механизму взаимодействия, результат отображен в таблице 2. К первому типу по механизму взаимодействия относится последовательная синергия, при которой одна атака создает условия, необходимые для проведения другой атаки. Результат первой атаки является предпосылкой для второй: атакующий выстраивает цепочку действий, где каждый шаг расширяет его возможности и приближает к конечной цели. Без первого шага второй невозможен или бессмыслен. Классический пример – комбинация фишинга и Pass-the-Hash. Последовательная синергия характеризуется жесткой зависимостью между атаками и четкой временной последовательностью.

Второй тип – маскировочная синергия, при которой одна атака скрывает следы или отвлекает внимание от другой атаки. Атакующий использует диверсионную атаку как прикрытие для скрытой операции. Примером служит комбинация DDoS-атаки и эксфильтрации данных. Маскировочная синергия не требует жесткой зависимости между атаками – они могут выполняться параллельно, но эффект достигается именно за счет маскировки.

Третий тип – обходная синергия, при которой атаки воздействуют на разные слои защиты, обходя каждый из них по отдельности. Современные системы безопасности изолированы: антивирусные средства проверяют файлы, межсетевые экраны контролируют трафик, DLP-системы анализируют содержимое, а средства защиты от фишинга проверяют ссылки. Каждый из этих инструментов эффективен в своей области, но не способен видеть картину целиком. Обходная синергия использует разрывы между этими слоями: одна атака обходит один слой защиты, а другая атака – другой слой. Классический пример – комбинация отключения логирования и эксплуатации уязвимости.

Четвертый тип – параллельная синергия, при которой несколько атак проводятся одновременно и усиливают друг друга. В отличие от последовательной синергии, здесь нет жесткой зависимости по времени – атаки выполняются параллельно, и их совокупный эффект превышает сумму эффектов каждой по отдельности за счет взаимного усиления. Пример – одновременное проведение атаки на отказ в обслуживании (DDoS) и атаки на подбор паролей (брутфорс). DDoS перегружает систему аутентификации, замедляя ее работу, что затрудняет блокировку брутфорс-атаки по превышению

лимита неудачных попыток. В свою очередь, брутфорс-атака создает дополнительную нагрузку, усугубляя эффект DDoS. Параллельная синергия наиболее опасна в распределенных системах, где ресурсы ограничены и конкурируют между собой.

Таблица 2 – Классификация синергии по механизму взаимодействия

Тип синергии	Механизм
Последовательная	A создает условия для B
Маскировочная	A скрывает следы B
Обходная	Атаки обходят разные слои защиты
Параллельная	Атаки усиливают друг друга одновременно

Для решения проблемы синергии в кибератаках необходим переход от изолированных средств защиты к кросс-слойной корреляции событий. Этот подход предполагает централизованный сбор данных из всех доступных источников: сетевых журналов (файрволы, IDS/IPS, NetFlow), логов конечных точек (Windows Event Log, EDR, системный аудит), событий аутентификации (Active Directory, VPN), оповещений DLP, а также контекстуальной информации об активах, уязвимостях и пользователях. Все эти разнородные данные анализируются совместно в единой системе, что позволяет устанавливать связи между событиями, которые по отдельности выглядят безобидными.

В случае с фишингом и Pass-the-Hash корреляция связывает фишинговое событие (переход по ссылке) с последующей подозрительной аутентификацией с того же хоста, выявляя латеральное перемещение атакующего. При комбинации DDoS и эксфильтрации данных система фиксирует начало DDoS-атаки и автоматически повышает приоритет мониторинга исходящего трафика; обнаружение аномального объема данных в тот же период формирует инцидент «кража под прикрытием DDoS». В случае с отключением логирования и эксплуатацией уязвимости система после фиксации отключения аудита переводит актив в режим повышенного наблюдения за альтернативными источниками (сетевой трафик, запуски процессов); любая аномальная активность после этого интерпретируется как высоковероятная эксплуатация, не оставившая следов в логах. Только такой комплексный подход способен своевременно обнаруживать комбинированные кибератаки, использующие синергетический эффект.

Список использованных источников:

1. Security Vision : [сайт]. – Мск., 2023-2026. – URL: https://www.securityvision.ru/blog/kiberataki-chast-1-tekhnicheskie-instrumenty-i-sposoby-realizatsii/ (дата обращения: 05.04.2026).

2. Fortinet : [сайт]. – Sunnyvale, 2025-2026. – URL: https://www.fortinet.com/blog/threat-research/uncovering-hidden-forensic-evidence-in-windows-mystery-of-autologger (дата обращения: 05.04.2026).

3. Imperva : [сайт]. – San Mateo, 2023-2026. – URL: https://www.imperva.com/blog/why-attackers-target-the-financial-services-industry/ (дата обращения: 05.04.2026).

4. Gurufocus : [сайт]. – Austin, 2024-2026. – URL: https://www.gurufocus.com/news/2422355/honeywell-report-reveals-silent-residency-is-driving-escalating-cyber-threat-for-industrial-and-critical-infrastructure-facilities (дата обращения: 05.04.2026).

5. ITworld: [сайт]. – Мск., 2026-2026. – URL: https://www.it-world.ru/news-company/5tj379eqtns484o0kwskko0cococwwg.html (дата обращения: 05.04.2026).