УДК 004.056

***МУЦЕНЕК ВИТУС ЕВГЕНЬЕВИЧ***

# ЭКСПЕРТНАЯ ОЦЕНКА ВРЕМЕННЫХ ПАРАМЕТРОВ АТАКИ

**АННОТАЦИЯ**

Дана характеристика комплексных атак на защищаемые информационные системы, рассмотрена современная интерпретация этапов их осуществления. Описаны источники доказательств в цифровой форме, позволяющие определить время подготовки, проникновения и воздействия. Предложены варианты применения экспертных методов для анализа атак относительно их временных параметров.

**Ключевые слова:** инцидент информационной безопасности; доказательство в цифровой форме; экспертная оценка; криминалистическая версия.

***MUTSENEK V. E.***

# EXPERT ASSESSMENT OF ATTACK TIMINGS

**ABSTRACT**

The characteristics of complex attacks on protected information systems are given, a modern interpretation of the stages of their implementation is considered. Sources of digital evidence that allow determining of preparation, penetration and impact timings are described. A variety of assessment methods, for analyzing attacks in relation to their timings, are suggested.

**Keywords:** information security incident; digital evidence; expert assessment; forensic version.

Термин «атака», применительно к действиям злоумышленника при попытке преодоления системы защиты информационной системы, используется уже довольно долго. Практически значимые исследования, описывающие методы обнаружения атак, основанные на актуальных данных, проводятся на протяжении уже двадцати лет (например [1, 2]). Точность формулировки термина[1] не вызывает сомнений, однако за период активного развития информационных технологий практикующие специалисты неоднократно приходили к выводу о необходимости рассмотрения атаки не как единичного тактического действия, а как комплексного и многоэтапного процесса. Рассмотрение атаки как комплекса действий позволяет говорить о фрагментарности временных параметров, описывающих атаку, таких как время проникновения. Учитывая, что время проникновения, время обнаружения и реагирования составляют набор параметров, позволяющий определить эффективность пресечения атаки, переосмысление временных характеристик позволит составить представление о реальных возможностях по противодействию злоумышленникам в киберпространстве.

Достаточно подробное описание распределённой комплексной атаки приведено в работе Ю.А. Матвиенко [3]. Обобщая опыт предыдущих исследований, автор разбивает комплексную атаку на пять этапов: подготовка, вторжение, атакующее воздействие, развитие и завершение атаки. В случае, если цель атаки достижима без закрепления злоумышленника в системе, этот жизненный цикл можно сократить до четырёх этапов, однако это не избавляет расследователя инцидентов безопасности от необходимости нахождения причинно-следственных связей между этапами.

Атаку, описанную Ю.А. Матвиенко, можно отнести к классу таргетированных (целевых). Особенностями таких атак специалисты называют четкое целеполагание, скрытность и протяженность во времени. Одиночные атаки являются «молниеносными» и направлены на большое количество слабозащищенных систем, достигая целей за счёт массовости, тогда же как от начала целевой атаки до получения результатов могут пройти месяцы или годы [4, с.3]. Многоэтапность атаки и её протяженность затрудняют анализ: действия злоумышленника на отдельных этапах могут выглядеть как не связанные события, кроме этого при условии успешной подготовки, этап воздействия может быть начат безусловно[2] по отношению к атакуемой системе.

1 «А.12 атака: Попытка преодоления системы защиты информационной системы». (ГОСТ Р 53114-2008, переиздание 2018 г., Приложение А)

2 Вне зависимости от состояния системы и в произвольный момент времени.

Комплексность атаки предполагает некоторый параллелизм действий злоумышленника, выражающийся в воздействии на разные элементы одной системы или на элементы не связанных друг с другом систем (например, попытки саботажа системы охранного телевидения с целью сокрытия факта физического доступа к защищаемой ЭВМ). При таргетированной атаке это может привести к сокрытию реальных целей злоумышленников. Особенности, характерные для этого класса атак, достижимы при строгой регламентации деятельности и высоком уровне подготовки злоумышленников. Вероятными нарушителями, обладающими ресурсами для проведения подобных атак, могут являться участники организованных преступных групп и сотрудники спецслужб иностранных государств.

Показательна в этом отношении деятельность преступной группы Cobalt: для достижения конечной цели (атаки на платёжные системы) группа использовала скомпрометированные вычислительные ресурсы третьих лиц [5]. Если рассматривать время получения доступа к контроллеру домена как время осуществления подготовки атаки, этот параметр может принимать значения от 10 минут до недели. Ещё некоторое время злоумышленникам требовалось для изучения структуры сети и подготовки атаки на конкретный банкомат (этап вторжения). Упоминается ограничитель, встроенный во вредоносную программу, использовавшуюся при совершении преступлений: проверка месяца, в котором должна осуществляться атака [6]. Таким образом, временное окно для выполнения и завершения атаки составляет до 30 дней с момента компрометации компьютерной системы.

Проиллюстрируем жизненный цикл гипотетической атаки с точки зрения злоумышленника. Все этапы могут включать действия по преодолению системы защиты информации. Так, например, на этапе подготовки могут быть предприняты попытки сканирования защищаемых компьютерных сетей, для чего может понадобиться преодоление межсетевого экранирования. На этапах проникновения и воздействия предпринимаются попытки преодоления системы разграничения доступа. На этапе завершения атаки предпринимаются попытки преодоления подсистемы регистрации событий безопасности. Возможны и сценарии нарушения защищенности, в которых злоумышленник использует пассивные методы перехвата информации, не оставляющие следов: например, перехватывая аутентификационную информацию через утечки по техническим каналам, и затем используя её для выдачи себя за легального пользователя. В этом случае набор доказательств должен быть дополнен сведениями, источники которых не входят в атакованную систему. Предлагается также обрабатывать единичные инциденты информационной безопасности на предприятиях, относящихся к объектам критической информационной инфраструктуры, как элементы комплексной атаки, пока не доказано обратное.

Так или иначе, для доступа к объекту в компьютерной системе с целью нарушения конфиденциальности, целостности или доступности злоумышленнику придётся выполнить последовательность действий, даже если эти действия будут разделены значительными перерывами в активности. Для каждого этапа однотипных целевых атак представляется возможным также определить набор событий-признаков.

Основным источником доказательств в цифровой форме при анализе атаки является подсистема регистрации и учета. Основными параметрами, непосредственно хранящими сведения о времени, в ней являются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- дата и время выдачи документа (обращения к подсистеме вывода);
- дата и время попытки доступа к защищаемому файлу или объекту;
- дата и время запуска;
- дата и время изменения полномочий и статуса.

В то же время, устройство подсистемы подразумевает хранение сведений о времени наступления всех регистрируемых событий. Журналы подсистем регистрации и учета разных средств защиты информации могут иметь несовместимые форматы [7].

Системы защиты могут заимствовать сведения о событиях безопасности из журналов операционной системы, например как это реализовано в СЗИ серии «Аура» [8]. При использовании подгрузки событий из источника flock в подсистему

регистрации событий безопасности СЗИ «Аура» существует вероятность переполнения журнала событиями (например, при чтении файла генерируются события, связанные как с доступом к файлу, так и с обнаружением этого файла на жёстком диске). Для успешного обнаружения таргетированной атаки в данном случае потребуется увеличение максимально допустимого размера журнала или отказ от политики перезаписи журнала по достижении им максимально возможного размера. Также для поиска целевых атак актуальной становится проблема автоматизации выявления событий-признаков атаки во множестве зарегистрированных событий.

Существуют и другие доказательства в цифровой форме, позволяющие делать выводы о времени каких-либо этапов атаки. Так например в меморандуме[3], посвященном анализу доклада комиссии Мюллера, отмечается особенность передачи данных через компьютерную сеть в сравнении с копированием данных на съёмный носитель. При копировании на носитель, отформатированный в файловой системе на основе таблиц размещения файлов (FAT), даты последней модификации округляются в сторону ближайшего четного числа. Скомпрометированная переписка Национального комитета Демократической партии США, выложенная WikiLeaks, в метаданных содержит только четные отметки времени, что косвенно свидетельствует в пользу того, что файлы не были получены по сети (как было бы в случае взлома в результате сетевой атаки). Отметки времени, содержащиеся в метаданных, позволили также установить предположительное значение скорости передачи данных, с которой создавались копии файлов. Это значение многократно превышает скорость передачи данных по сети «Интернет», но соответствует скоростям обмена информации с отчуждаемыми носителями [9].

Рассмотрим варианты применения экспертных методов в определении временных параметров гипотетической атаки.

Причинно-следственную связь событий в атаке можно представить в виде ориентированного графа. Вершины графа будут составлять события с отметками времени, веса рёбер графа могут обозначить длительность временного интервала между зарегистрированными событиями. Злоумышленник может провести параллельную отвлекающую атаку, а задачей эксперта по оценке времени исполнения этапов атаки станет составление причинно-следственной цепочки атаки и поиск наиболее вероятной альтернативы в попытке определить истинные цели злоумышленника.

Для определения событий, имеющих отношение к комплексной атаке, можно воспользоваться методом ранговой корреляции. В качестве ранжируемых факторов целесообразно использовать события-признаки, отобранные из журнала подсистемы регистрации в пределах некоторого диапазона отметок времени. Если необходимо выявить несколько альтернативных сценариев, имеет смысл предоставить экспертам для оценивания выборки, сделанные на временных интервалах разного масштаба. Слишком короткие интервалы негативно скажутся на репрезентативности выборки, верхние пределы целесообразно выбирать, исходя из опыта обнаружения протяженных по времени атак. Полученные перечни событий в порядке увеличения отметок времени следует проанализировать на предмет возникновения скрытых каналов передачи информации (например, нарушений корректности субъектов, ассоциированных с объектами воздействия, в отношении которых зарегистрированы события безопасности; это требует создания субъектно-ориентированной модели защищаемой системы).

Исследователи А.В. Федорченко и И.В. Котенко в качестве способа ранжирования событий безопасности указывают определение силы связей между типами событий и между отдельными событиями. В качестве возможных видов связей в графе, моделирующем атаку, они называют:

1. удельные веса прямой, косвенной однотипной и косвенной разнотипной связей между типами событий, задающиеся количеством равнозначных, неравнозначных однотипных и неравнозначных разнотипных свойств соответственно;
2. относительные веса связей между экземплярами событий, определяющиеся отношением количества совпадающих значений свойств к соответствующим удельным весам [10].

3 Меморандум ассоциации «Ветераны-профессионалы разведки за рассудительность» (Veteran Intelligence Professionals for Sanity) Генеральному прокурору США от 13.03.2019

Разумно будет предположить наличие некоторого минимально возможного частотного порога, и если количество выявленных событий, относящихся к завершённой целевой атаке, составит значение существенно меньшее, чем пороговое, значит рассмотренные временные окна не охватывают все этапы атаки. Рассматривая события не в связи с целой атакой, а с ей этапами, представляется возможным определить текущее состояние атаки. Понижение частотности событий (вплоть до исчезновения) на начальном (подготовка) и среднем этапе (проникновение и закрепление в системе) могут свидетельствовать о том, что злоумышленник принял меры к сокрытию своего присутствия или атака осуществлялась не только в рамках защищаемой системы. Отсутствие событий средних и завершающих этапов атаки свидетельствует о приостановке атаки (без возможности сделать выводы о причинах, будь то отказ от замысла, смена тактики или приостановка с целью сокрытия активности).

Из множества возможных сценариев выбор наиболее вероятной альтернативы можно осуществить с помощью метода анализа иерархий.

Исследование М.А. Нехаева [11] наглядно иллюстрирует применимость метода анализа иерархий не только для определения предпочтительных альтернатив, но и для оценки значимости факторов в цепочке событий. В работе предложено применить метод анализа иерархий дважды: сначала для определения приоритетных аспектов функционирования системы по отношении к общей цели, затем для определения приоритетных событийных кластеров.

События, характеризующие целевую атаку, можно кластеризовать в зависимости от подсистемы защищаемой информационной системы, в которой они возникают. В ходе анализа реальной системы, таким образом, можно будет определить приоритетное направление поиска доказательств в цифровой форме. События за временное окно приоритетной альтернативы, относящиеся к приоритетному кластеру, будут нуждаться в детальном изучении. В случае отсутствия выявленных событий приоритетного событийного кластера за временное окно приоритетной альтернативы, следует рассмотреть варианты переопределения временных окон и поиска следов действий злоумышленника по сокрытию своего присутствия в системе.

Грубая оценка времени, затраченного злоумышленником на выполнение каждого этапа целевой атаки, таким образом, будет определяться разностью отметок времени событий, соотнесённых с этапами атаки. Более точное определение временных параметров возможно только при наличии как можно более полного набора данных, включающего сведения из источников за рамками защищаемой информационной системы. Методы ранговой корреляции и анализа иерархий одинаково применимы в процессе анализа атаки, однако требуют тщательной подготовки исходных данных и наличия хотя бы типовых сценариев нарушения защищенности для рассматриваемой информационной системы.

**Список литературы**

1. *Лукацкий А.В.* «Обнаружение атак». – СПб.: «БХВ-Петербург», 2001.

2. *Лукацкий А.В.* Ностальгия по обнаружению атак или куда продвинулась российская наука ИБ за 15 лет [Электронный ресурс]. – Режим доступа: https://lukatsky.blogspot.com/ Бизнес без опасности. [Электронный ресурс]. – Режим доступа: https://lukatsky.blogspot.com/2015/04/15.html (дата обращения 13.04.2018).

3. *Матвиенко Ю.А.* Комплексная информационная атака типа «киберстачка» на промышленную систему: анатомия явления и подходы к защите // Информационные войны. – 2012. – № 1(21). – С.85-94.

4. Технология динамического обнаружения. White paper [Электронный ресурс]. – Режим доступа: https://www.cezurity.com/++theme++common/assets/docs/cezurity_cota_white_paper.pdf (дата обращения: 14.04.2018)

5. Cobalt: эволюция и совместные операции [Электронный ресурс]. – Режим доступа: https://www.group-ib.ru/resources/threat-research/cobalt-evolution.html (дата обращения 10.06.2018).

6. По следу Cobalt: тактика логической атаки на банкоматы в расследовании Group-IB [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/group-ib/blog/323996/ (дата обращения 12.04.2018)

7. *Верхорубов А. И., Жуков В. Г.* О проблеме анализа интегрированных результатов работы средств защиты информации в автоматизированных системах // Актуальные проблемы авиации и космонавтики. – 2012. – № 8. – С.367-368.

8. Система защиты информации от несанкционированного доступа «Аура 1.2.6». Руководство системного программиста [Электронный ресурс] Режим доступа: http://cobra.ru/prod/aura1_26 (дата обращения 01.06.2018)

9. Ветераны-профессионалы разведки за рассудительность: лишенные криминалистического подтверждения находки Мюллера (на англ. языке) / VIPS: Mueller's Forensics-Free Findings // Consortium News [Электронный ресурс]. – Режим доступа: https://consortiumnews.com/2019/03/13/vips-muellers-forensics-free-findings/ (Дата обращения: 20.03.2019)

10. *Федорченко А. В., Котенко И. В.* Корреляция информации в SIEM-системах на основе графа связей типов событий // Информационно-управляющие системы. – 2018. – № 1. – С. 58-67.

11. *Нехаев М.А.* Применение метода анализа иерархий в экспертной оценке значимости факторов в цепочке событий функционирования сортировочной станции // Вестник транспорта. – 2012. – № 4. – С. 31-40.

*Статья поступила в редакцию 18 апреля 2019 г.*
*Принята к публикации 27 июня 2019 г.*