DOI 10.36622/VSTU.2021.24.1.004
УДК 004.056.53

МОДЕЛИРОВАНИЕ, АНАЛИЗ И ПРОТИВОДЕЙСТВИЕ СЦЕНАРИЯМ КОМПЬЮТЕРНЫХ АТАК, РЕАЛИЗУЕМЫХ ГРУППИРОВКОЙ APT3 В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А.Л. Сердечный, А.В. Айдаркин, М.А. Тарелкин, А.Е. Дешина

В работе представлены результаты моделирования способов реализации долговременных целенаправленных атак на корпоративные распределённые компьютерные системы со стороны одной из опасных киберпреступных группировкок – Advanced Persistent Threat 3 (APT3). Осуществлено моделирование способов, реализуемых APT3. Построение моделей осуществлялось с использованием аппарата сетей Петри на основании сведений о технических приёмах, содержащихся в базе данных MITRE ATT&CK. Разработанные модели взаимосвязаны по условиям и последствиям реализации основных технических приёмов, актуальных для корпоративных распределённых компьютерных сетей. Реализованный подход также позволяет моделировать меры защиты, регламентируемые нормативными и методическим документами, что даст возможность принятия обоснованных решений при построении системы защиты с учётом специфики защищаемого объекта.

Ключевые слова: киберпреступные группировки, APT-атаки, сети Петри, ATT&CK, APT 3, распределенные компьютерные системы.

Введение

Исследование деятельности APT-группировок в контексте моделирования способов реализации компьютерных атак является актуальным. Актуальность обусловлена высокой квалификацией нарушителя, что подразумевает возможность создания принципиально нового или модификацию существующего способа компьютерной атаки.

В условиях пандемии COVID-19 и карантина, введенного во многих странах, нарушители стали искать способы нажиться на страхе перед вирусом. Известные APT-группы стали использовать эту тему для рассылки фишинговых писем [2].

Согласно исследованию Positive Technologies, не все компании всерьез воспринимают APT-атаки как отдельную угрозу. Две трети представителей финансовой отрасли (63%) на практике сталкивались с последствиями кибератак, и 34% признали, что организация понесла прямые финансовые потери. При всем этом только 39% участников отмечают, что защита от APT-атак — приоритетное направление развития ИБ в компании [3].

Учитывая опасность угроз, вызванных деятельностью APT-группировок, важным является осуществление обоснованного выбора мер и средств защиты от них на основании количественных оценок сценариев, реализуемых типовыми и наиболее опасными APT-группировками, среди которых рассматриваемая в настоящей работе киберпреступная группировка APT3.

Реализация данного подхода предполагает наличие достаточно полных баз данных, в которых были бы объединены сведения о способах реализации компьютерных атак. В настоящий момент такая база формируется силами основных исследователей и разработчиков средств защиты от APT-атак (такими как The MITRE Corporation, Лаборатория Касперского, McAfee, Microsoft и др.) в рамках проекта MITRE ATT&CK [4].

База данных ATT&CK содержит описания сотен технических приёмов, используемых нарушителями в ходе проведения компьютерных атак. Однако в данной базе не представлены сведения о причинно-следственных связях между такими техническими приёмами.

Несмотря на наличие дополнительных информационных ресурсов, в которых имеются сведения о причинно-следственных связях между техническими приёмами, используемыми киберпреступной группировкой APT3 имеются (например, проект ATT&CK EVALUATIONS [5]), представленная в них описания не обладают достаточной формализацией, а сами причинно-следственные связи зачастую определяются лишь на основании порядка следования действий нарушителя в ходе реализации атаки без учёта логической связи с предыдущими действиями.

Для реализации представленного подхода в первую очередь требуется формирование модели причинно-следственных связей между способами реализации компьютерных атак. В рамках настоящей работы осуществляется моделирование атаки группировки APT3.

Существующие модели этой атаки отражают только общую картину, в них не производится оценка и управление рисками.

Данные модели обладают следующими положительными свойствами:

- прозрачность - подробность оценки, включая протокол тестирования и охват тестов, доступность.

- подробная оценка обнаружения - вместо того, чтобы предоставлять простые двоичные результаты обнаружения, MITRE предоставил детальную оценку, основанную на методах и способах обнаружения.

- методы множественных атак - оценка охватывала широкий спектр методов, которые задокументированы в структуре MITRE ATT&CK и могут применяться во время реальных сложных атак, в отличие от сосредоточения внимания на конкретных методах, таких как компоненты вредоносного ПО.

Однако данные модели показывают только определенные фазы атаки, нет четких границ перехода от одной фазы к другой и нет возможности количественно оценить риски. Поэтому представляется необходимым формирование новой модели:

- модель в виде связанных между собой элементов, которая эффективнее чем многочисленные отдельные техники и тактики;

- применение ранжирования и взвешивания методов атаки, что позволит останавливать наиболее важные и эффективные действия по взлому;

- модель, которая позволит произвести оценку и регулирование рисков.

В ходе анализа существующих подходов было установлено, что не существует методики для снижения рисков нарушения информационной безопасности от APT-атак. Все текущие методики рассматривают APT-атаки совместно с другими угрозами, никак не выделяя их, поэтому необходимо создать методическое обеспечение, которое будет ориентировано на снижение рисков нарушения информационной безопасности распределенной компьютерной системы организаций кредитно-финансовой сферы при реализации на неё кибератак группировки APT3 с учётом особенностей APT-атак такого типа.

Технология моделирования

Для построения модели использовалась исходные данные, полученные экспертным сообществом в рамках реализации проекта ATT&CK EVALUATIONS [5, 6]. Информационный ресурс [5] и руководство по проведению экспериментальных исследований [6] содержат информацию о технических приёмах (техниках), использовавшихся киберпреступной группировкой APT3.

Данная группировка полагается на сбор учетных данных, ввод команд на клавиатуре и использование программ, которым уже доверяет операционная система. Стоит отметить, что данная группа не использует сложные методы написания сценариев, эксплойты, руткиты или буткиты.

Для оценки деятельности APT3 было протестировано 56 техник Enterprise ATT&CK по 10 тактикам ATT & CK. Данные техники можно разделить на шаги. Каждый шаг соответствовал намеченной цели нарушителя во время операции.

Атаку можно разделить на фазы и шаги:

- фаза №1 «Первоначальная компрометация РКС» (рис. 1):
  - а)шаг №1 «Проникновение в РКС»;
  - б) шаг №2 «Обход защиты»;
  - в)шаг №3 «Обнаружение»;
- фаза №2 «Распространение в РКС» (рис. 2):
  - а) шаг №4 «Обнаружение»;
  - б) шаг №5 «Повышение привилегий / Обход средств защиты»;
  - в) шаг №6 «Доступ к учётным данным»;
  - г) шаг №7 – «Закрепление в РКС».
  - д) шаг №8 «Распространение в РКС».
- фаза №3 «Вывод данных из РКС (эксфильтрация)» (рис. 3):
  - а) шаг №9 – «Сбор данных»;
  - б) шаг №10 – «Сжатие данных»;
  - в) шаг №11 – «Эксфильтрация».

Технология моделирования сценария, реализуемого группировкой APT3, заключалась в выполнении для каждого этапа и шага атаки следующих действий:

– из описанных в базе данных MITRE ATT&CK [4] приемов были выбраны технические приёмы, используемые группировкой APT3 в ходе реализации сценария атаки [5, 6];

– проведён анализ описания каждого выбранного технического приёма с целью определения следующих сведений:

а) условий реализации технического приёма;
б) действий, которые оказывает прием на атакуемую систему;
в) последствий успешной реализации технического приема.

– для каждого технического приёма определялась его взаимосвязь с другими приёмами на основании полученных сведений об условиях и последствиях;

– осуществлялось построение модели с использованием аппарата сетей Петри.

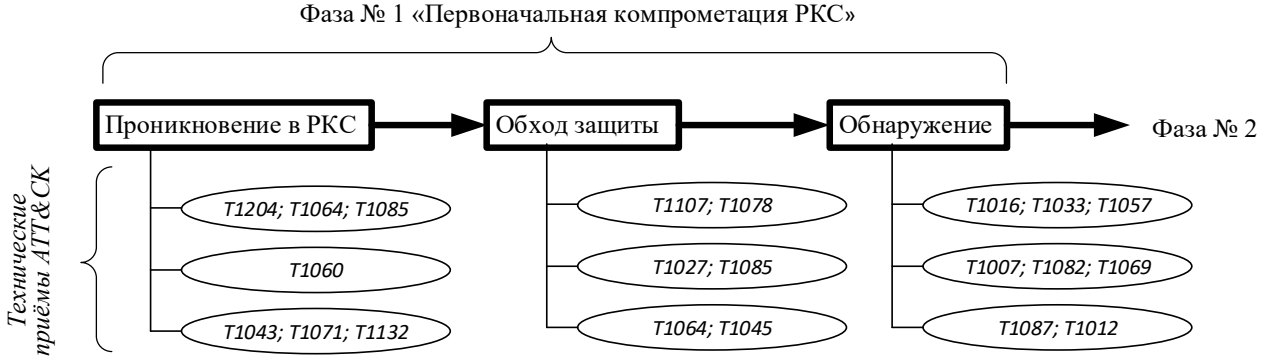

Рис. 1. Схема реализации фазы № 1 «Первоначальная компрометация информационной системы», осуществляемой киберпреступной группировкой APT3

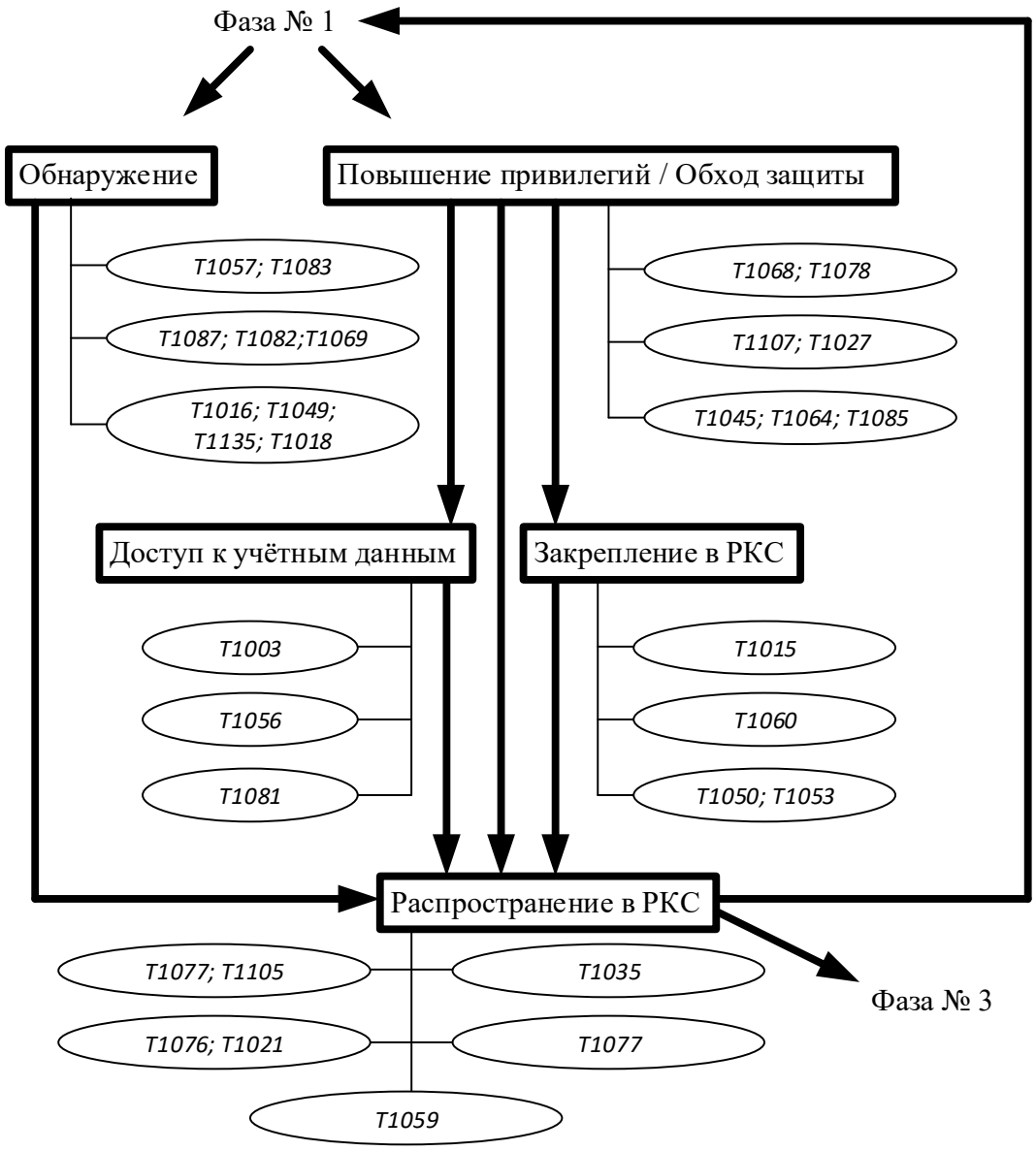

Рис. 2. Схема реализации фазы № 2 «Распространение в РКС», осуществляемой киберпреступной группировкой APT3

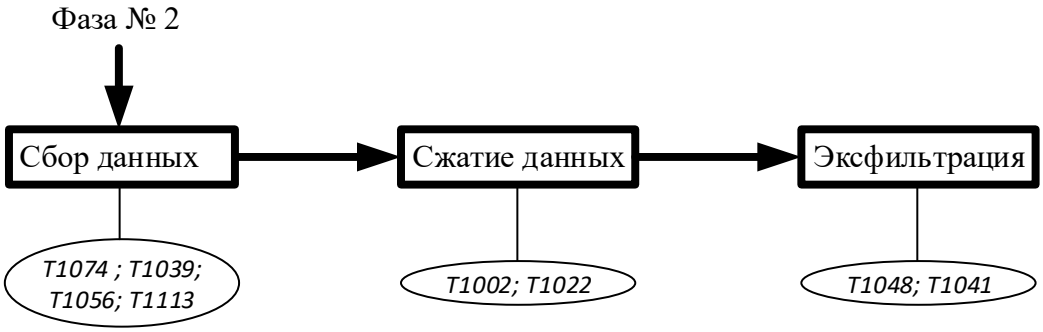

Рис. 3. Схема реализации фазы № 3 «Вывод данных из РКС (эксфильтрация)», осуществляемой киберпреступной группировкой APT3

Построение модели сценариев атак группировки APT3

В рамках реализации первой фазы злоумышленники из APT3 проникают в систему и устанавливают соединение с управляющим севером (далее – C2). Действия злоумышленника в рамках первой фазы моделируются следующей сетью Петри:

$$C^1=(P^1, T^1, I^1, O^1), \quad (1)$$

где P^1 – множество позицией, моделирующих условия/последствия для действий, выполняемых злоумышленником в ходе первой фазы;

T^1 – множество переходов, моделирующих действия, выполняемые злоумышленником в ходе первой фазы;

I^1 и O^1 – входные и выходные функции для участка сети Петри, моделирующего действия злоумышленника в ходе первой фазы.

$$P^1= \{P0, P1, P2, P3, P4, P5, P6\}, \quad (2)$$

где P0 – Злоумышленник готов к проведению атаки на РКС;

P1 – Возможность исполнения вредоносного кода на компьютере;

P2 – Имеется возможность выполнения файлов элементов панели управления;

P3 – Вредоносный код остался в системе и работает после перезагрузки системы;

P4 – Установлено соединения через C2 канал;

P5 – Собрана информация о системе:

1) Работающая версия Windows;

2) Информация о текущем пользователе, домене, группах принадлежности пользователя, привилегиях безопасности;

3) Список текущих запущенных процессов и служб в системе;

4) Отображение списка учетных записей локального администратор;

5) Текущее значение реестра для служб терминалов.

P6 – Злоумышленник скрыл факт своего проникновения в РКС.

$$T=\{T1,T2,T3,T4,T5,T6,T7,T8,T9,T10, T11,T12,T13,T14,T15,T16,T17,T18\}, \quad (3)$$

где T1 – Техника T1204 / T1218.011 (Исполнение пользователем / User Execution);

T2 – Техника T1085 (Rundll32);

T3 – Техника T1064 (Скриптинг / Scripting);

T4 – Техника T1060 / T1547.001 (Выполнение автозапуска загрузки или входа в систему);

T5 – Техника T1043 (Non-Standard Port / Использование нестандартного порта);

T6 – Техника T1071 (Стандартный протокол прикладного уровня);

T7 – Техника T1132 (Кодирование данных / Application Layer Protocol);

T8 – Техника T1016 (Обнаружение конфигурации сети системы / System Network Configuration Discovery);

T9 – Техника T1033 (Обнаружение владельца системы/пользователя / System Owner/User Discovery);

T10 – Техника T1057 (Обнаружение процесса / Process Discovery);

T11 – Техника T1007 (Обнаружение системных служб / System Service Discovery);

T12 – Техника T1082 (Обнаружение системной информации / System Information Discovery);

T13 – Техника T1069 (Обнаружение групп разрешений / Permission Groups Discovery);

T14 – Техника T1087 (Обнаружение учетной записи / Account Discovery);

T15 – Техника T1012 (Реестр запросов / Query Registry);

T16 – Техника T1107 (Удаление файлов / File Deletion);

T17 – Техника T1027 (Обфускация файлов Obfuscated Files);

T18 – Техника T1045 (Упаковка программного обеспечения / Software Packing).

Входные и выходные функции представлены в табл. 1, а соответствующий фрагмент сети Петри показан на рис. 4.

Таблица 1

Входные и выходные функции для участка сети Петри фазы №1

$t \subset T^1$	Входные функции, $I^1(t)$	Выходные функции, $O^1(t)$
{T1}	{P0}	{P1}
{T2, T3 }	{P1}	{P2}
{T4}	{P2}	{P3}
{T5, T6, T7}	{P3}	{P4}
{T8 – T15}	{P4, P6, P16}	{P5}
{T16, T17, T18}	{P1}	{P6}

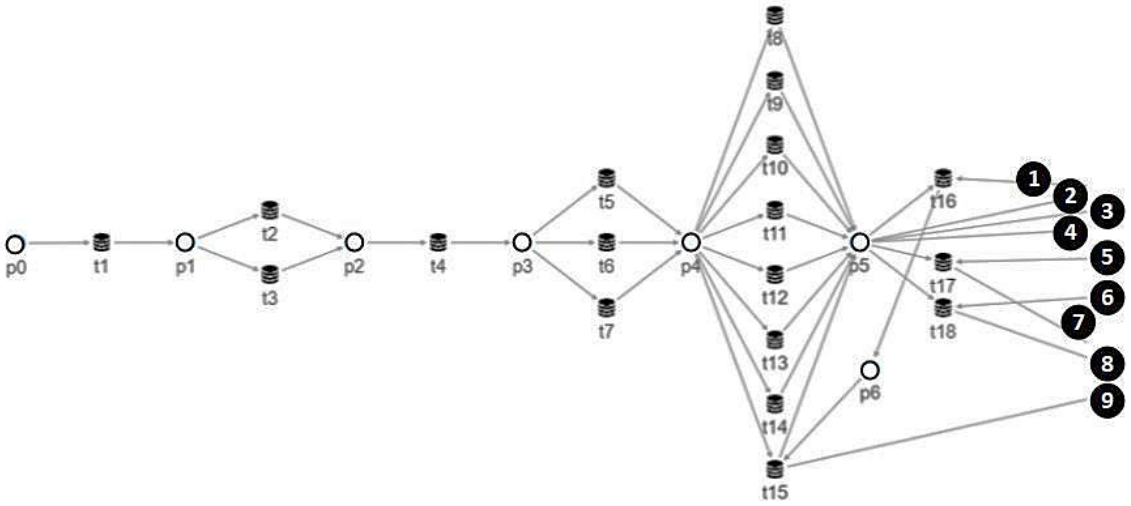

Рис. 4. Участок сети Петри, моделирующий действия злоумышленника в ходе фазы №1 «Первоначальная компрометация РКС»

Целью фазы № 2 «Распространения в РКС» является идентификация и переход к представляющим интерес объектам атакуемой системы с целью обнаружения учетных данных и документов, содержащих конфиденциальные сведения. На данном этапе атаки нарушители из APT3 закрепились в системе и собрали нужные для себя итоговые данные.

Аналогично (1) действия злоумышленника в рамках второй фазы моделируются сетью Петри:

$$C^2=(P^2, T^2, I^2, O^2), \quad (4)$$

$$P^2=\{P6, P7, P8, P9, P10, P11, P12, P13, P14, P15, P16\}, \quad (5)$$

где P6 – Получена возможность обхода контроля учетных записей;

P7 – Повышены локальные привилегии;

P8 – Получена информация о системе:

1) Таблица ARP;

2) Отображение текущих сетевых подключений TCP / IP;

3) Отображение сервера входа в активный каталог рабочей станции.

P9 – Сброшены учетные данные пользователей;

P10 – Получена информация о системе:

1) Дамп хэшей из файла SAM Hive;

2) Токен доступа для подключения к другим службам и компьютерам;

P11 – Создана учетная запись и добавлена в группу администраторов;

P12 – Возможность выполнять действия от имени пользователя;

P13 – Установлен постоянный доступ к системе;

P14 – Получены данные о тексте, набранном пользователем;

P15 – Получен снимок экрана пользователя;

P16 – Собраны данные находящиеся в системе.

$$T^2 = \{T16, T17, T18, T19, T20, T21, T22, T23, T24, T25, T26, T27, T28, T29, T30, T31, T32, T33, T34, T35\}, \quad (6)$$

где T16 – Обход контроля учетных записей пользователей (T1088);

T17 – Обнаружение процесса (T1057);

T18 – Ввод процесса (T1055) Встроенная возможность внедрения процесса, выполняемая для внедрения обратного вызова в cmd.exe;

T19 – Обнаружение удаленной системы T1018;

T20 – обнаружение конфигурации сети системы (T1016);

T21 – обнаружение сетевых подключений системы (T1049);

T22 – Манипулирование токенами доступа (T1134) Встроенная возможность дублирования токена обхода UAC, выполненная для изменения токена текущего процесса [7];

T23 – Сброс учетных данных (T1003);

T24 – Манипулирование токенами доступа (T1134);

T25 – Создание учетной записи (T1136);

T26 – Удаленное копирование файла (T1105);

T27 – Запланированное задание (T1053);

T28 – Ввод процесса (T1055);

T29 – Графический интерфейс пользователя (T1061);

T30 – Открытие счета (T1087);

T31 – Обнаружение файлов и каталогов (T1083);

T32 – Снимок экрана (T1113);

T33 – Входной захват(T1056);

T34 – Обнаружение окна приложения (T1010);

T35– Ввод процесса (T1055).

Входные и выходные функции для фазы № 2 представлены в табл. 2, а соответствующий фрагмент сети Петри – на рис. 5.

Таблица 2

Входные и выходные функции участка сети Петри – Фаза №2

$t \subset T^2$	Входные функции, $I^2(t)$	Выходные функции, $O^2(t)$
{T16}	{P5}	{P6}
{T17, T18}	{P5}	{P7}
{T19, T20, T21}	{P5, P8}	{P8}
{T22}	{P7, P10}	{P9}
{T23}	{P7}	{P10}
{T24}	{P7}	{P11}
{T25, T26}	{P7}	{P13}
{T27}	{P9}	{P10}
{T28}	{P11}	{P12}
{T29}	{P12}	{P13}
{T30}	{P10, P16, P8, P13}	{P16}
{T31}	{P10, P8, P13}	{P16}
{T32}	{P10, P8, P13}	{P14}
{T33}	{P10, P8, P13}	{P15}
{T34}	{P14}	{P16}
{T35}	{P5}	{P16}

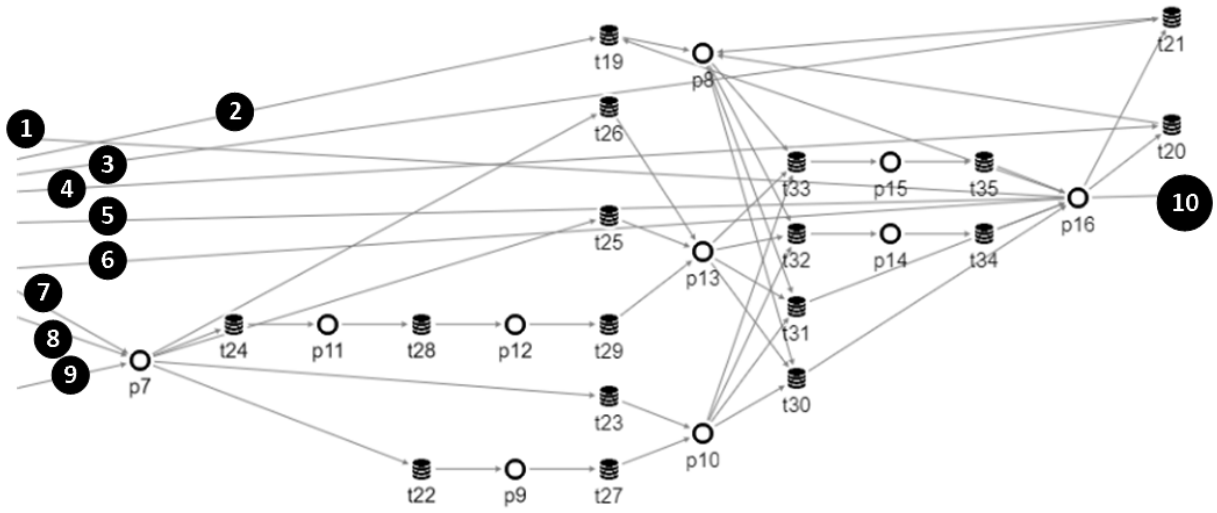

Рис. 5. Участок сети Петри, моделирующий действия злоумышленника в ходе фазы №2 «Распространение в РКС»

В ходе реализации фазы №3 злоумышленник совершает следующие действия:

- обнаружение документов на компьютере жертвы (T1005 - Данные из локальной системы) [8];
- использование архиватора WinRAR для сжатия и шифрования обнаруженных документов (T1002 - Data Compressed) [9];
- размещение сжатой и зашифрованной информации в удалённых файлах с целью маскировки найденной информации до того, как она будет передана на командный сервер C2 [10];
- передача найденной информации на командный сервер C2 через сетевую службу, прослушивающую порт 443, (T1043 - Commonly Used Port) [11].

Участок сети Петри для данного шага изображен на рис. 6.

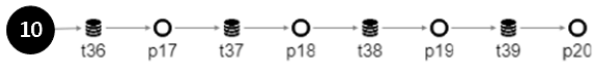

Рис. 6. Участок сети Петри, моделирующий действия злоумышленника в ходе фазы №3 «Вывод данных из РКС (эксфильтрация)»

Аналогично (1) и (4) действия злоумышленника в рамках третей фазы моделируются сетью Петри:

$$C^3=(P^3, T^3, I^3, O^3), \quad (7)$$

$$P^3=\{P17, P18, P19, P20\}, \quad (8)$$

где P17 – Найдены интересующие файлы;

P18 – Данные сжаты/зашифрованы;

P19 – Данные размещены в центральном каталоге или хранилище;

P20 – Данные отправлены нарушителю.

$$T=\{T\_36,T\_37,T\_38,T\_39,T\_40\}, \quad (9)$$

где T36 – Данные из локальной системы (T1005);

T37 – Архивировать собранные данные (T1002);

T38 – Поэтапные данные (T1074);

T39 – Нестандартный порт (T1043).

Соответствующие входные и выходные функции представлены в табл. 3.

Таблица 3

Входные и выходные функции участка сети Петри – Фаза №3

$t \subset T^3$	Входные функции, $I^3(t)$	Выходные функции, $O^3(t)$
{T36}	{P16}	{P17}
{T37}	{P17}	{P18}
{T38}	{P18}	{P19}
{T39}	{P19}	{P20}

Разработка мер защиты информации для смоделированного сценария компьютерной атаки группировкой APT3

Моделирование мер защиты залучается в дополнении разработанной модели сценария реализации компьютерной атаки группировкой APT3 позициями и переходами, наличие которых снижает скорость достижения нарушителем состояний, приводящих к ущербу для РКС, или делают невозможным выполнение каких-либо траекторий атаки.

Так, например, для фазы № 1 администратор безопасности РКС может запретить нарушителям запустить Rundll32.exe при помощи таких инструментов, как Attack Surface Reduction (ASR) в EMET и Advanced Theart Protection (средство защиты операционной системыWindows).

Другой мерой противодействия нарушителю на фазе № 1 может быть направлен на предотвращение возможности закрепления нарушителя в системе путём добавления в реестре Windows параметров автозапуска или ссылок в директорию «Автозагрузка». Такая программа будет запускаться от имени и с правами текущего пользователя. Нарушители также могут маскировать ключи запуска в реестре, чтобы они выглядели как настоящие и безопасные программы [13]. Для защиты от данного способа рекомендуется проводить мониторинг изменений папки «Автозагрузка» и веток реестра, хранящих ключи запуска.

Пример участка сети Петри с рассмотренными мерами защиты представлен на рис. 6.

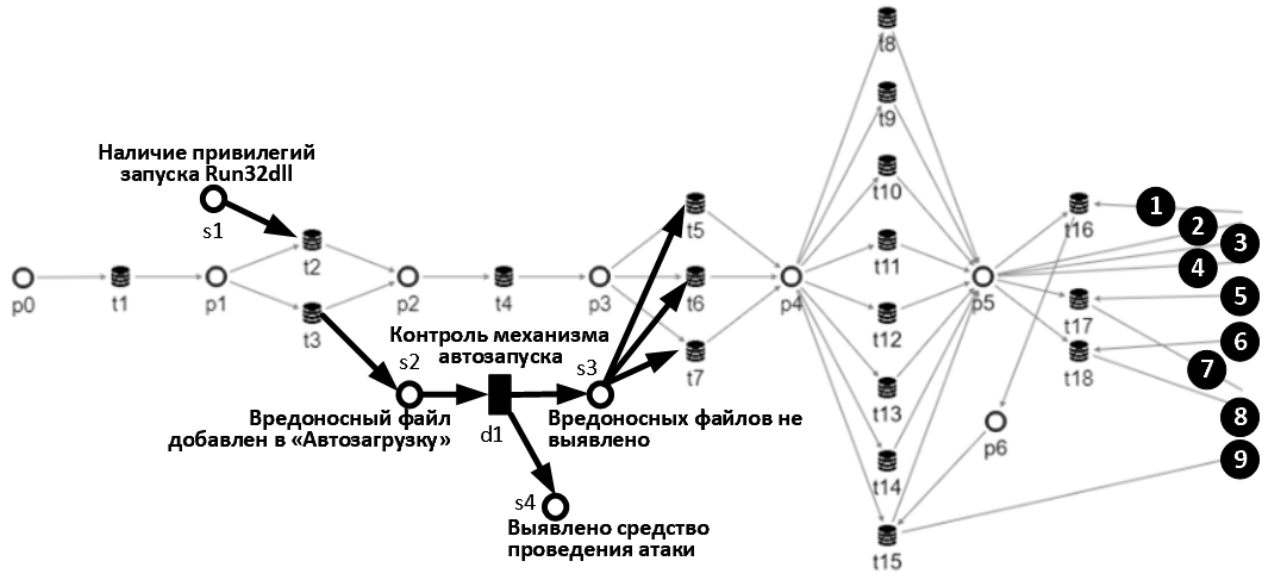

Рис. 7. Участок сети Петри, моделирующий меры противодействия успешной реализации сценария атаки группировкой APT3 в фазе № 1

Для указанного на рис. 6 фрагмента модели меры защиты представлены следующим фрагментом сети Петри:

$$C^{m1}=(S^1, D^1, I^{m1}, O^{m1}), \quad (10)$$

$$S^1=\{S1, S2, S3, S4\}, \quad (11)$$

где S1 – Наличие привилегий запуска Run32dll;

S2 – Вредоносный файл добавлен в «Атозагрузку»;

S3 – Вредоносных файлов не выявлено в ходе контроля механизма автозапуска;

S4 – Выявлено средство проведения атаки.

$$D^1=\{D1\}, \quad (12)$$

где D1 – Контроль механизма автозагрузки.

Входные и выходные функции для мер защиты представленного на рис. 6 фрагмента сети приведены в табл. 4.

Таблица 4

Входные и выходные функции участка сети Петри для рассмотренных мер защиты

$t \subset T^1 \cup D^1$	Входные функции, $I^{m1}(t)$	Выходные функции, $O^{m1}(t)$
{T2}	{S1}	{ }
{T3}	{ }	{S2}
{D1}	{S2}	{S3, S4}
{T5, T6, T7}	{S1}	{ }

Так, в результате запрета на запуск Run32dll, который моделируется позицией S1, возможность срабатывания перехода T2 исключается до тех пор, пока нарушителем не будут получены соответствующие привилегии. Наличие же механизма автозапуска может привести к выявлению средства проведения атаки нарушителя, что делает невозможным выполнения его дальнейших действий.

Также возможно оказать противодействие нарушителю и на других этапах.

Нарушители могут пытаться получить перечень учетных записей локальной системы или домена. Они используют различные техники для получения учетных данных пользователей.

Необходимо предотвратить возможность перечисления учетных записей администраторов при повышении уровня прав через UAC, поскольку это приведёт к раскрытию имен учетных записей администраторов. Соответствующий раздел реестра можно отключить с помощью GPO [14].

Так как атака группировки APT3 развивается по спирали, то есть после окончания фазы №2, она возвращается в конец фазы №1, то очень важным является постоянный глубокий анализ сетевого трафика.

Такой подход позволит обнаружить нарушителя в инфраструктуре даже по прошествии нескольких месяцев после проникновения.

Как правило если атака достигла фазы № 3, то её цели практически достигнуты и противодействие следовало оказывать на более ранних этапах. В качестве возможных мер противодействия на данном этапе является использование DLP-систем с целью организации сигнатурного анализа трафика на предмет выявления известных средств организации канала управления и эксфильтрации или наличие конфиденциальной информации в выходном потоке данных.

Проводить анализ трафика на предмет необычных потоков данных (например, клиент отправляет значительно больше данных, чем получает с сервера). Не соответствие используемого номера порта и номера порта, установленного в сетевом протоколе по умолчанию, может также указывать на вредоносную активность [15].

Анализ трафика является основным методом для защиты от группировки APT3. Чем надежнее защищена сеть, тем больше техник будут вынуждены применять злоумышленники, оставляя за собой следы в сетевом трафике и системных журналах.

Заключение

В ходе работы был осуществлён анализ действий киберпреступной группировки APT3 и выполнено моделирование реализованного ею сценария атаки. Сформированная модель была получена с использованием аппарата сетей Петри в которой показаны причинно-следственные связи между различными способами, используемыми нарушителями в ходе атаки.

Для разработанной модели были предложены меры защиты от подобных сценариев атак. Полученная модель может быть использована в будущем для количественной оценки риска распределенных компьютерных систем при условии её преобразования в сеть Петри-Маркова путём предложения методик расчёт вероятностно-временных характеристик для участков модели. Такая сеть позволит определить вероятность достижения состояний, приводящих к ущербу для.

Реализованный подход позволяет осуществить моделирование мер защиты, регламентируемых нормативными и методическим документами, что даст возможность принятия количественно обоснованных решений при построении системы защиты с учётом специфики защищаемого объекта.

При этом необходимо отметить, что модель сети Петри, учитывающая большинство основных способов реализации компьютерных атак и мер защиты от них с продемонстрированным уровнем детализации потребует порядка тысячи позиций и переходов, что создаёт определённые сложности для поддержки таких моделей. Преодоление данного ограничения возможно за счёт реализации экспертной системы на базе картографических методов работы с графовыми моделями, примеры использования которых были показаны в [16, 17, 18].

Список литературы

1. Fireeye Mandiant Services / Special report M-Trends. – 2020. – pp 29 – 38.

2. Обзор активности APT-групп в 2020 году. Аналитика и отчёты о киберугрозах «Касперского». URL|: https://securelist.ru/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99480 (дата обращения 15.01.2021).

3. APT-атаки на кредитно-финансовую сферу в России: обзор тактик и техник. Positive Technologies – официальный сайт компании. URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-finance-2019 (дата обращения 15.01.2021).

4. База данных способов реализации компьютерных атак MITRE ATT&CK. The MITRE Corporation URL: https://attack.mitre.org/ (дата обращения 15.01.2021).

5. Результаты моделирования действий киберпреступной группировки APT3 в рамках проекта ATT&CK EVALUATIONS. The MITRE Corporation. URL: https://attackevals.mitre-engenuity.org/enterprise/evaluations.html?round=APT3 (дата обращения 15.01.2021).

6. Руководство проведения экспериментальных исследований в рамках моделирования действий киберпреступной группировки APT3 в рамках проекта ATT&CK EVALUATIONS. The MITRE Corporation. URL: https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf (дата обращения 15.01.2021).

7. Access Token Manipulation, Technique. URL:https://attack.mitre.org/techniques/T1134/ (дата обращения 15.01.2021).

8. Data from Local System, Technique. URL:https://attack.mitre.org/techniques/T1005/ (дата обращения 15.01.2021).

9. Archive Collected Data, Technique. URL:https://attack.mitre.org/techniques/T1002/ (дата обращения 15.01.2021).

10. File and Directory Discovery, Technique. URL: https://attack.mitre.org/techniques/T1083/ (дата обращения 15.01.2021).

11. Non-Standard Port, Technique. URL: https://attack.mitre.org/techniques/T1571/ (дата обращения 15.01.2021).

12. Data Staged, Technique. URL: https://attack.mitre.org/techniques/T1074/ (дата обращения 15.01.2021).

13. Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 7. URL: https://habr.com/ru/post/425177/ (дата обращения 15.01.2021).

14. Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 5. URL: https://habr.com/ru/post/432624/ (дата обращения 15.01.2021).

15. Defeating Windows User Account Control by abusing built-in Windows AutoElevate backdoor. URL: https://github.com/hfiref0x/UACME (дата обращения 15.01.2021).

16. Serdechnyi A.L. Mapping retrieval method for academic publications in the field of aerospace technology safety / Serdechnyi A.L., Goncharov A.A., Ostapenko A.G., Bataronov I.L. //В сборнике: IOP Conference Series: Materials Science and Engineering. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. 2020. С. 52028.

17. Калашников А.О. Картографический подход в библиометрическом исследовании отечественных научных школ, сложившихся в области защиты информации и обеспечения информационной безопасности / Калашников А.О., Сердечный А.Л., Остапенко А.Г. // Информация и безопасность. 2019. Т. 22. № 4. С. 455-484.

18. Сердечный А.Л. Картографический подход к описанию киберпространства в контексте обеспечения безопасности информации и информационной безопасности / Сердечный А.Л., Остапенко А.Г. // Информация и безопасность. 2019. Т. 22. № 3. С. 387-398.

Государственный научно-исследовательский испытательный институт
проблем технической защиты информации ФСТЭК России
State science research experimental institute of technical information protection problem
of Federal service of technical an export control

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 20.01.2021

Информация об авторах

Сердечный Алексей Леонидович – канд. техн. наук, начальник лаборатории, Государственный научно-исследовательский испытательный институт, e-mail: alex-voronezh@mail.ru

Айдаркин Александр Владимирович – студент, Воронежский государственный технический университет, e-mail: aidarkinsasha@mail.ru

Тарелкин Михаил Андреевич – научный сотрудник, Государственный научно-исследовательский испытательный институт, e-mail: mihail.tarelkin.93@mail.ru

Дешина Анна Евгеньевна– канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: 2199199@mail.ru

MODELING, ANALYSIS AND COUNTERING SCENARIOS OF PREPARING COMPUTER ATTACKS REALIZED BY THE GROUP APT3 IN DISTRIBUTED COMPUTER SYSTEMS

A.L. Serdechnyy, A.V. Aydarkin, M.A. Tarelkin, A.E. Deshina

The paper presents the results of modeling methods for implementing APT-attacks on corporate distributed computer systems by one of the most dangerous cybercrime groups – Advanced Persistent Threat 3 (APT3). The methods implemented by APT3 are modeled. The models were constructed using the Petri nets apparatus based on the information about technical techniques contained in the MITRE ATT&CK database. The developed models are interrelated in terms of the conditions and consequences of the implementation of the main technical techniques relevant for corporate distributed computer networks. The implemented approach also allows to model the protection measures from regulatory and methodological documents, which will make it possible to make informed decisions when building a protection system, taking into account the specifics of the protected object.

Keywords: cybercrime groups, APT attacks, Petri nets, ATT&CK, APT 3, distributed computer systems.

Submitted 20.01.2021

Information about the authors

Alexey L. Serdechnyy – Cand. Sc. (Technical), Chief of Laboratory, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: alex-voronezh@mail.ru

Aleksander V. Aydarkin – Student, Voronezh State Technical University, email: aidarkinsasha@mail.ru

Mihail A. Tarelkin – Scientific researcher, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: mihail.tarelkin.93@mail.ru

Anna E. Deshina– Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: 2199199@mail.ru