ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ: ОСОБЕННОСТИ И МЕТОДЫ ЗАЩИТЫ

Шарый Д.Н. Чопик К.В.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Ионин В.С. – канд.техн.наук, доцент

В статье рассматриваются понятия «целенаправленная атака», стадии целевой атаки, цели и особенности таких атак, обосновывается необходимость комплексной стратегии противодействия целевым атакам.

В последнее время растет число компаний, подвергающихся таргетированным (целенаправленным, целевым) атакам. Целенаправленная атака – это непрерывный процесс несанкционированной активности в инфраструктуре атакуемой системы, управляемый киберпреступником в режиме реального времени. Процесс всегда строится под конкретную коммерческую или государственную организацию, обычно управляется организованной группой профессионалов. Как правило, такие атаки хорошо спланированы и включают несколько этапов. Чаще всего, результатом атак является закрепление в инфраструктуре организации, при этом злоумышленник может оставаться незамеченным в течение месяцев или даже лет.

Следует отметить следующие особенности целевых атак, которые отличают их от обычных:

– адресность;
– скрытность;
– продолжительность;
– использование разнородных инструментов и методов;
– разработка вредоносного ПО для конкретной атаки;
– наличие центра управления атакой.

Основными целями таргетированных атак являются:

– телеком: атака на корпоративных клиентов, контроль билинга, манипуляция почтовым сервером в целях социальной инженерии, манипуляция с раскрученными веб-ресурсами в целях фишинга;
– государственный сектор: шпионаж, манипуляция информацией, нарушение доступности online-сервисов, хищение персональных данных;
– финансы: хищение денежных средств, персональных данных;
– медицина: хищение информации пациентов, атака на телеуправляемое медицинское оборудование;
– бизнес: манипуляция бизнес-процессами, ослабление в конкурентной борьбе, шантаж, вымогательство, хищение данных.

Целевая атака в своем жизненном цикле имеет четыре фазы [1], представленные на рисунке 1.

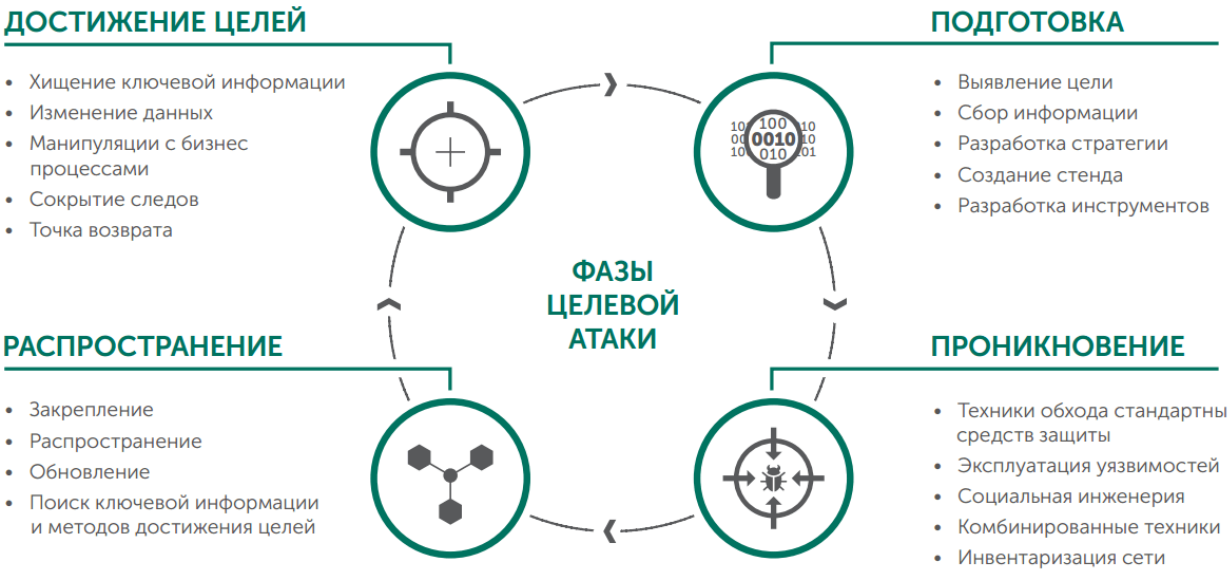

Рисунок 1 – Фазы целевой атаки

На каждом этапе выполняются мероприятия по сокрытию следов целенаправленной атаки. На последнем этапе киберпреступник может создать «точку возврата», то есть оставить средство внутри инфраструктуры, позволяющее, при необходимости, вернуться обратно.

Злоумышленники используют комбинированный подход, а также комбинирование инструментов для целевых атак. При атаках учитываются все потенциальные слабые места, которые становятся известными при использовании сразу нескольких механизмов разведки (атаки разных уровней). После сбора информации создается стенд, который повторяет инфраструктуру организации. На этом же стенде проходит отработка различных техник скрытого внедрения и обхода стандартных средств защиты информации. В других случаях киберпреступники могут создавать новое вредоносное ПО или использовать уже существующие инструменты, которые решают различные задачи целевой атаки.

Из-за особенностей целенаправленных атак, таких как изучение средств защиты организации, разработка вредоносного ПО, скрытности, и из-за существующих ограничений стандартных средств защиты необходим комплексный подход [2].

Комплексный подход позволит совместить большое количество функций для сбора и анализа информации и предотвращении атак. Комплексная стратегия включает в себя четыре компонента системы защиты, представленных на рисунке 2.

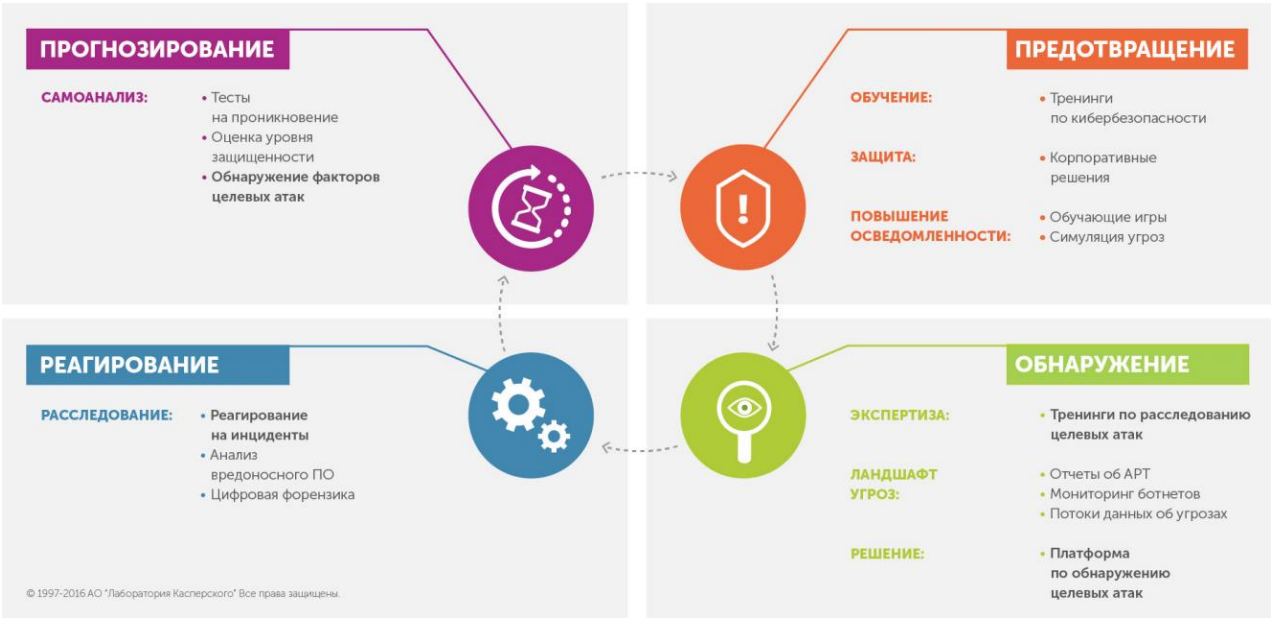

Рисунок 2 – Комплексная стратегия защиты

Целью предотвращения является препятствование началу и развитию атак. Далее ставится цель обнаружение атаки: определение признаков и связь всех деталей в общую картину. При обнаружении атаки устанавливаются последствия и формируются мероприятия по устранению. Важным подходом является прогнозирование, целью которой является оценка уровня защищенности, анализ собственных уязвимостей [3].

В современном мире киберпреступники могут не только обходить средства защиты информации, но и влиять на пользователей и системы, что сильно усложняет выявление целевых атак стандартными средствами защиты. Поэтому необходимо использовать различные алгоритмы и комплексные стратегии, которые позволят собирать информацию о событиях в режиме 24/7, быстро находить следы таких атак, сообщать об инцидентах информационной безопасности, документировать выявленные инциденты, получать статистику угроз через разные виды инфраструктур.

Список использованных источников:

1. Технологии Kaspersky daily [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru. – Дата доступа: 23.03.2020.

2. Tadviser. Государство. Бизнес. ИТ [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru. – Дата доступа: 23.03.2020.

3. Целенаправленные атаки – обнаружение и защита / Н.В. Петров // Издание «Информационная безопасность». – 2014. – № 2. – С. 8-12.