БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Практика построения системы защиты от целевых атак

Скородумов Анатолий Валентинович

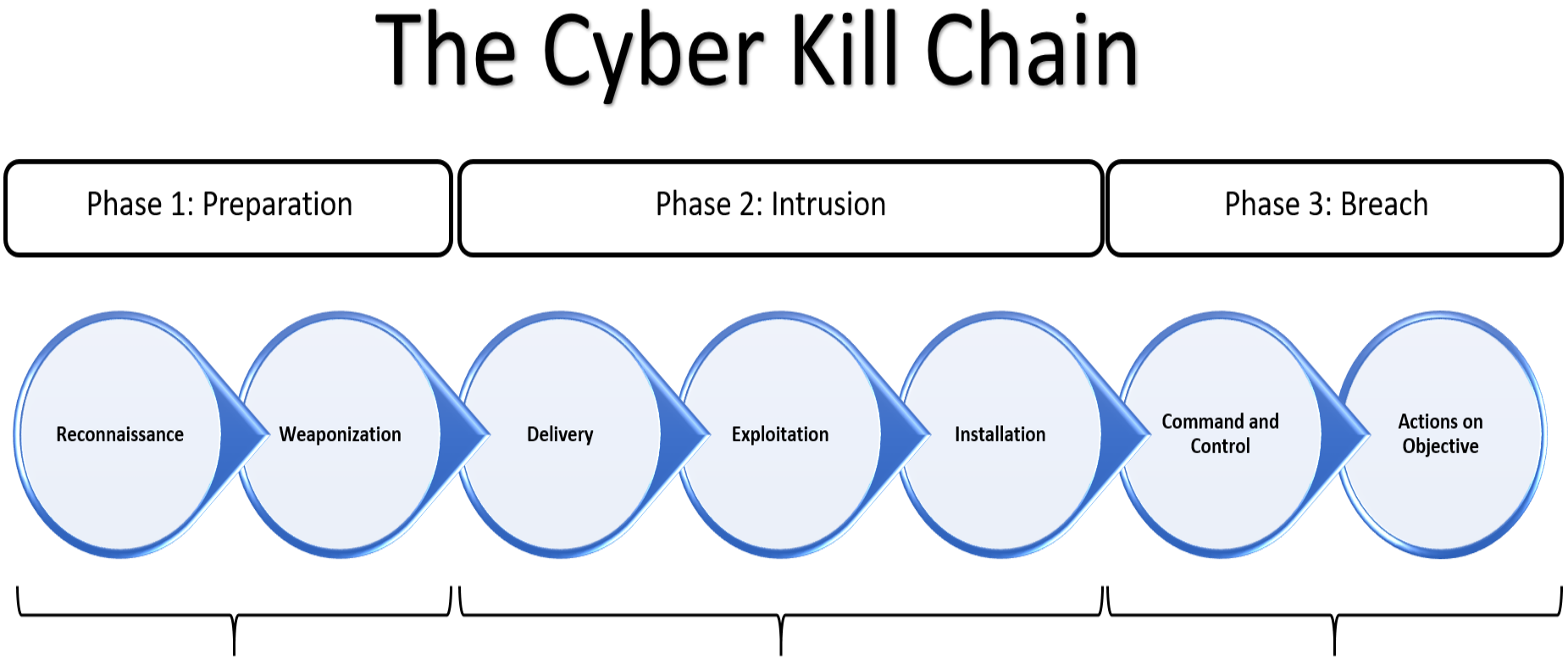
Архитектор информационной безопасности

Целевая атака

- Атаки против конкретной компании, организации, ведомства
- Атака имеет совершенно конкретную цель
- Атаки носят длительный характер, как в части подготовки, так и в реализации
- Вредоносное ПО разрабатывается или адаптируется под конкретную атаку
- Атака имеет, как правило, очень серьезные последствия для организации

Зачастую в целевых атаках используются те же механизмы взлома и проникновения, что и при обычных массовых атаках. Системы защиты от APT-атак эффективны против обычных массовых кибератак

Kill Chain целевой кибератаки



Современные системы защиты могут достаточно эффективно работать на всех этапах проведения целевой атаки

Противодействие на этапе подготовки атаки

- Межсетевые экраны (NGFW, WAF)
- Системы обнаружения, предотвращения атак (IDS/IPS)
- Сканеры безопасности - регулярные проверки в рамках процесса управления уязвимостями
- Сбор и корреляция событий ИБ (SIEM)
- Анализ Darknet

Основная задача – максимально затруднить злоумышленникам выявление уязвимостей, через которые можно атаковать организацию.

Противодействие на этапе проникновения

- «Песочница» для почтового трафика
- «Песочница» для Web-трафика и файловой передачи данных
- Система антивирусной защиты
- EDR (endpoint detection & response) на рабочих станциях
- Сбор и корреляция событий ИБ (SIEM)

Важно тесное взаимодействие всех компонентов системы защиты от APT-атак между собой.
Важно выстраивание взаимодействия с контрагентами, поставщиками и иными третьими сторонами

Выявление на этапе закрепления в сети

- EDR на серверах и рабочих станциях
- Системы выявления аномалий на уровне вычислительной сети
- Контроль взаимодействия с управляющими серверами
- Сегментация сети и отслеживание взаимодействия между различными сегментами
- Системы класса Deception или Honeypot
- Управления привилегированными учетными записями (PAM)
- Сбор и корреляция событий ИБ (SIEM)

Отсутствие свободного доступа в интернет с рабочих станций работников существенно усложняет процесс закрепления злоумышленника в сети

Повышение осведомленности работников в вопросах ИБ

- Выявление фишинга
- Реагирование на подозрительные активности (звонки, контакты в соц. сетях, физический контакт незнакомых лиц, нахождение «утерянные» флешек и т.д.)
- Культура публикаций информации в социальных сетях
- Правила работы на «удаленке»
- Классические требования ИБ при работе на офисном компьютере

Это относительно эффективно при обычных массовых атаках, но малоэффективно при целевых атаках

Реагирование на завершающих стадиях атаки

- Защита основных «целей» в вашей организации с использованием сегментации, МСЭ, систем IDS/IPS, строгой двухфакторной аутентификации, ограничений по доступу только с конкретных защищенных рабочих станций и т.д.
- Максимальный аудит всех подозрительных действий и событий
- Четкие инструкции по действиям при инцидентах ИБ
- Внешние сервисы-«песочницы»

При выявлении атаки на завершающих стадиях есть риски того, что атаку не удастся предотвратить. Процесс удаления вредоносного ПО и восстановления работоспособности ИТ-систем может занять существенное время.

Проведение расследования

- Выявления точки (источника) заражения
- Определение всего скоупа зараженных хостов
- Определение методов и путей проникновения и распространения вредоносного ПО
- Проведение форенсики
- Определение целей кибератаки
- Сбор юридически значимых доказательств проведения кибератаки против организации и нанесения ей ущерба

При серьезных кибератаках со значительным ущербом для организации проведение расследования целесообразно предоставить внешней квалифицированной компании, которая не только организует и проведет расследование инцидента, но и подготовит пакет документов для подачи в правоохранительные органы

SOC как ключевой элемент выявления и реагирования на целевую атаку

- Мониторинг событий ИБ
- Обработка событий ИБ, их классификация и выявления инцидентов ИБ
- Анализ инцидентов ИБ и сбор дополнительных данных
- Реагирование на инциденты ИБ
- Расследование инцидентов ИБ
- Управление источниками событий ИБ
- Сбор и обработка информации о новых угрозах (Threat Intelligence)
- Взаимодействие со смежными подразделениями
- Настройка правил сбора и корреляции событий ИБ
- Управление уязвимостями
- Ведение базы знаний SOC
- Формирование регулярной отчетности

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Скородумов Анатолий Валентинович

E-Mail: Skorodumov@bspb.ru

Телефон (812) 329-50-64

Благодарю за внимание!