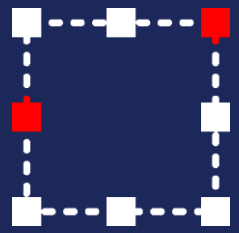
Актуальные угрозы безопасности информации в современных условиях

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

ТОП векторов проникновения

Подрядчики и системы, имеющие сопряжение с целевой инфраструктурой

01



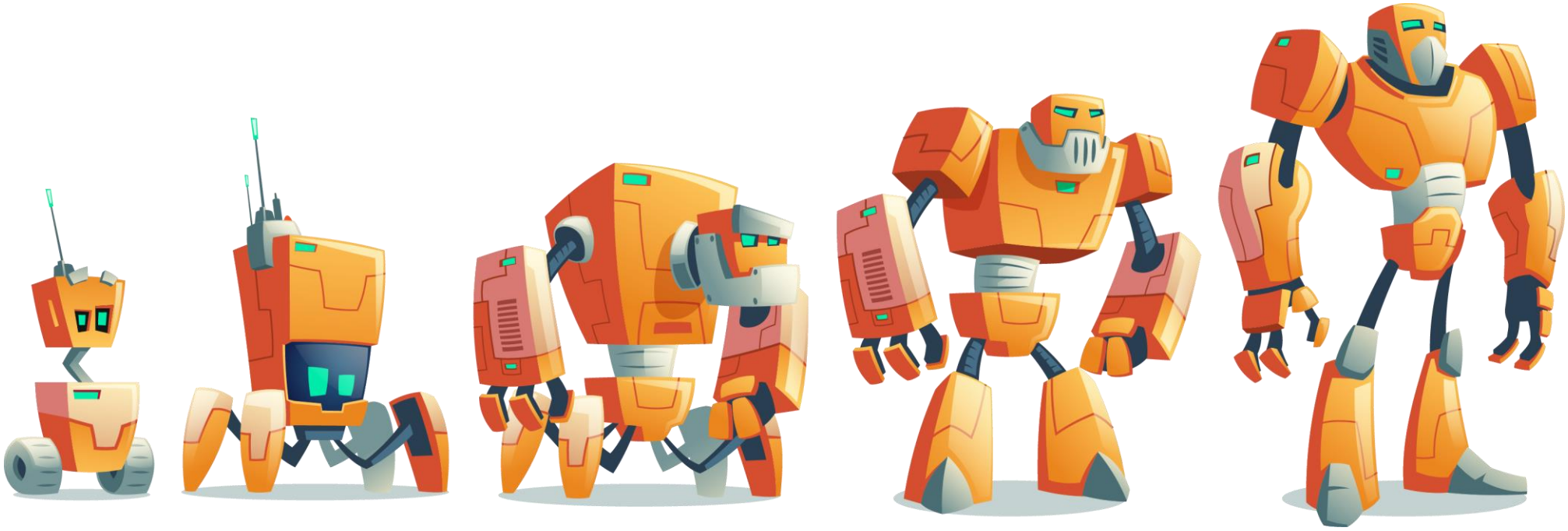
Эксплуатация уязвимостей на периметре

02

Фишинг

03

Эволюция атак



Основные атаки 2022 года

DDOS-атаки 01

Отключения провайдеров от крупных магистральных каналов 02

Атаки на СМИ для создания инфоповодов 03

Массовые отзывы сертификатов 04

Прекращение функционирования СЗИ зарубежных производителей 05

Появление вредоносного кода в обновлениях ПО 06

Конвейер

Берите и используйте для своих задач

Информация о новой уязвимости

Результаты сканирования

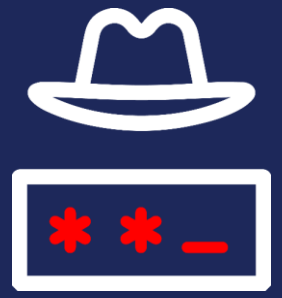
Перечень взломанных ресурсов

Результаты взлома

Мы взяли нужное, остальное здесь

Использование полученных ранее данных для организации новых атак

Поиск уязвимых ресурсов



Первичный доступ к инфраструктуре

Кража и публикация данных

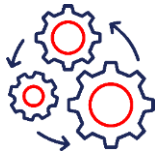
Данные, полученные в результате предыдущих атак, находящиеся в открытом доступе

Интерес злоумышленников к любым данным

Традиционные цели:

Служебная

Коммерческая



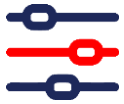
Техническая

Другие данные:

Персональные данные

Сведения об учетных записях

Почтовые сообщения



Конфигурационные данные

Журналы регистрации событий

Компании, управляющие ИТ-инфраструктурой заказчика, становятся причиной инцидентов

x1 = x10

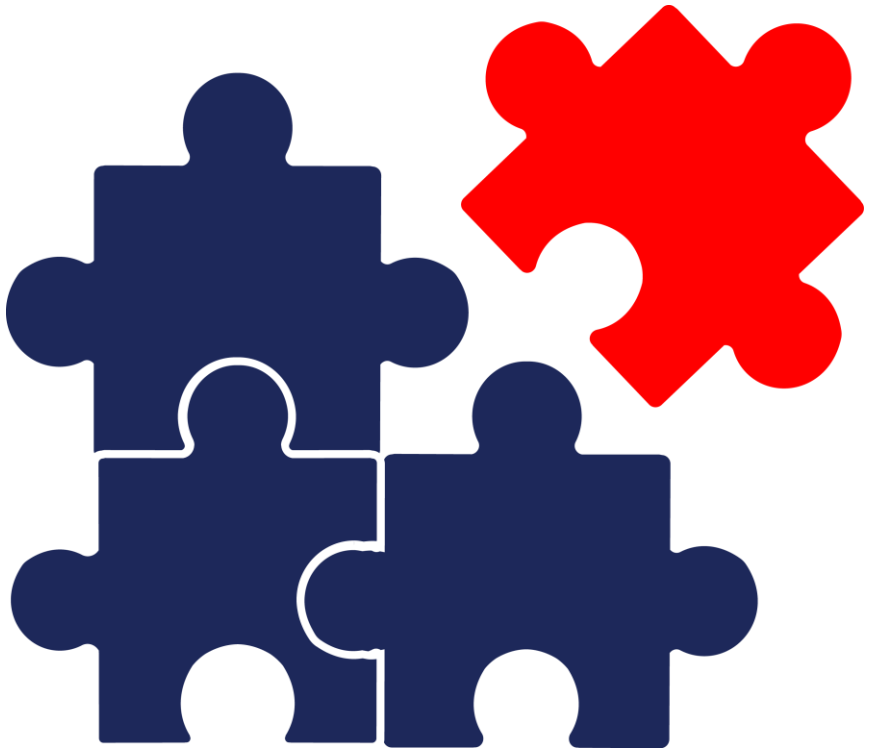
инцидент у интегратора

заказчиков под угрозой

Сокрытые инциденты, ставят под угрозу общую безопасность

НКЦКИ будет предупреждать участников ГосСОПКА об инцидентах в компаниях-подрядчиках

Нужны требования по безопасности к интеграторам



Пока требований нет, компании сами должны предпринимать меры предосторожности

Рекомендации по минимизации угрозы

1. Минимизировать каналы удаленного управления и вообще доступ сторонних специалистов из внешних систем

2. Контролировать действия внешних пользователей, особенно администраторов

3. Отслеживать информацию об инцидентах, например, утечках в подрядных организациях

4. Иметь план действий на случай появления признаков компрометации инфраструктуры подрядчика.

5. Выдвигать требования по обеспечению безопасности инфраструктур подрядчиков

Основные тренды

Меньше пиара, больше разрушений

01

Использование результатов предыдущих компьютерных атак для организации новых

02

DDoS-атаки маскируют выгрузку данных

03

Интеграторы становятся причиной инцидента в обслуживаемых компаниях

04

Компании замалчивают произошедшие инциденты

05

Спасибо за внимание!

incident@cert.gov.ru

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ