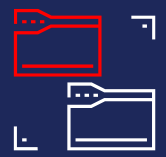
Актуальные угрозы безопасности информации в современных условиях

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Атаки и угрозы в начале 2022 года

1. Массированные DDOS атаки, в т.ч. на инфраструктурные элементы рунета
2. Отключения провайдеров от крупных магистральных каналов
3. Атаки на СМИ для создания инфоповодов
4. Массовые отзывы сертификатов
5. Прекращение функционирования СЗИ зарубежных производителей
6. Появление вредоносного кода в обновлениях ПО

Информационные атаки в начале 2022 года



Утечки, собранные
из старых данных

Утечки с завышенной
ценностью (почти публичная
информация)

Утечки из других компаний,
выдаваемые за КИИ
или системообразующие
предприятия

Данные, собранные
из открытых источников

Основные изменения в настоящее время

1. Более высокий уровень координации атакующих
2. Смена направленности с создания инфоповодов на нанесение реального урона
3. Большее количество утечек, меньшее количество фейков
4. DDOS-атаки как маскировка выгрузки данных
5. Многочисленные атаки через цепочку поставщиков
6. Увеличение времени присутствия в атакованной инфраструктуре

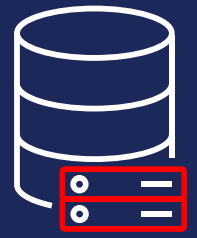
ТОП-3 векторов проникновения

1. Подрядчики и системы, имеющие сопряжение с целевой инфраструктурой
2. Эксплуатация уязвимостей на периметре
3. Фишинг

Наибольшая зона риска

Промышленность

Органы государственной власти и муниципального управления



ИТ-компании и разработчики ПО как цепочка поставки

Атаки через подрядчиков. Что нужно предпринять

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

Спасибо за внимание!

incident@cert.gov.ru

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ