Построение государственного центра мониторинга и популярные векторы кибератак в 2023 году

Начальник отдела по защите информации министерства цифрового развития и связи Приморского края

Бондаренко Максим Евгеньевич

Развитие системы защиты информации

ГОД	СОВЕРШЕНСТВОВАНИЕ ТЕХНОЛОГИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ
2012	Создание единого защищенного информационного пространства
2013	Программно-аппаратный комплекс контентной фильтрации
2014	Модернизация локальной вычислительной сети, средства МЭ и АВЗ
2015	СОВ и средство защиты среды виртуализации
2016	Средства анализа защищенности, СЗИ от НСД, программный комплекс контроля состава технических средств

АКТУАЛЬНАЯ УГРОЗА

Подмена доменных имен, внедрение вредоносных скриптов и участков кода в веб-сайты

Спам рассылки,
эпидемии «шифровальщиков»

Развитие системы защиты информации

ГОД	СОВЕРШЕНСТВОВАНИЕ ТЕХНОЛОГИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ
2017	Улучшение средства АВЗ до расширенной версии и его централизованное управление
2018	Система мониторинга и анализа защищенности
2019	Система управления событиями информационной безопасности, программный комплекс зеркалирования сетевого трафика
2020	Пилотные запуски систем мониторинга и анализа защищенности инфраструктуры
2021	Создание собственного центра мониторинга и реагирования на компьютерные инциденты

АКТУАЛЬНАЯ УГРОЗА

Уязвимости программного обеспечения, вредоносное программное обеспечение для удаленного администрирования, «вымогатели», «майнеры», многокомпонентные сетевые атаки

Работа регионального Штаба

> 2 МЛН. КИБЕРАТАК

ОТРАЖЕНО НА ПУБЛИЧНЫХ РЕСУРСАХ ПРАВИТЕЛЬСТВА ПРИМОРСКОГО КРАЯ

3 УРОКА

ПО «КИБЕРГИГИЕНЕ» В ШКОЛАХ С ТРАНСЛЯЦИЕЙ В СЕТИ ИНТЕРНЕТ

213 УВЕДОМЛЕНИЙ

НАПРАВЛЕНО О НАЛИЧИИ ПРИЗНАКОВ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ

> 40 МЛН. АДРЕСОВ

ЗАБЛОКИРОВАНО В РАМКАХ МЕРОПРИЯТИЙ ПО РЕАГИРОВАНИЮ

> 700 ТЫС. ПИСЕМ

СОДЕРЖАЛИ ВРЕДОНОСНЫЕ ССЫЛКИ ЛИБО ВЛОЖЕНИЯ

92 УЯЗВИМОСТИ

ИНФОРМАЦИЯ О КОТОРЫХ РАСПРОСТРАНЕНА СРЕДИ УЧАСТНИКОВ

Управление знаниями об актуальных угрозах

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

РЕГИОНАЛЬНЫЙ ШТАБ ПО БОРЬБЕ С КИБЕРУГРОЗАМИ

КОММЕРЧЕСКИЕ ЦЕНТРЫ МОНИТОРИНГА, РАСПОЛОЖЕННЫЕ В ПРИМОРСКОМ КРАЕ

ПОПУЛЯРНЫЕ ВЕКТОРЫ КИБЕРАТАК

В 2023 ГОДУ

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

DDOS-АТАКИ

Эксплуатация уязвимостей

Уязвимые службы на периметре информационной инфраструктуры (в том числе служб удаленного администрирования, доступных из сети «Интернет», ошибки настройки)

Уязвимости прикладного программного обеспечения веб-ресурсов

Уязвимости сервисов электронной почты

Инвентаризация внешнего сетевого пространства и контроль транслируемых сетевых адресов

Своевременное обновление программного обеспечение

Организация сетевого доступа методами «белого» списка

Мониторинг событий информационной безопасности и угроз

Блокирование популярных хостеров и VPN-провайдеров

DDOS-атаки

Осуществление DDOS-атаки с использованием протокола HTTP на прикладном уровне (L7)
Атака заключалась в специально сформированных клиентских HTTP-запросах с различными методами (GET, PUT, TRACE, OPTIONS и др.), предназначенными для обхода установленных ограничений методов доступа к серверному программному обеспечению, занесенных в «черные» списки на средствах межсетевого экранирования

Настройка блокирования на средствах межсетевого экранирования неизвестных HTTP-запросов («UNKNOWN») по умолчанию

Мониторинг событий информационной безопасности на публично доступных информационных ресурсах для выявления аномальной активности обращений к ним

Своевременное блокирование скомпрометированных сетевых адресов на используемых средствах межсетевого экранирования

Безопасные настройки веб-сервисов (использование CSP)

СПАСИБО ЗА ВНИМАНИЕ

Начальник отдела по защите информации министерства цифрового развития и связи Приморского края

Бондаренко Максим Евгеньевич