

Кибербезопасность цифрового пространства



Кибератаки на страну

КИБЕРАТАКИ НА КОМПАНИИ И ГОССЕКТОР



Госкомпании



РОИВы



Промышленность



Первые лица
компаний



ФОИВы и системы
госуправления

Новые векторы атак:

- Атаки через ИТ-поставщиков
- Атаки на разработчиков ПО
- Атаки через каркасные ИТ-системы

Цели атак:

- Контроль над ИТ-инфраструктурой
- Конфиденциальная информация
- Парализация работы и вымогательство

Текущая статистика

- В 90% Компаний отсутствует автоматический или ручной процесс установки обновлений
- 60 % имеют в своей инфраструктуре признаки ВПО WannaCry, WannaMine
- Более 5 дней время от появления нового ресурса в домене gov.ru до первой целевой атаки на него
- Более 24 часов проходит с момента опубликования уязвимости до появления эксплойта

WannaCry вредоносная программа, сетевой червь и программа-вымогатель денежных средств, поражающая компьютеры под управлением операционной системы Microsoft Windows. После заражения компьютера программный код червя шифрует почти все хранящиеся на компьютере файлы и предлагает заплатить денежный выкуп в криптовалюте за их расшифровку. В случае неуплаты выкупа в течение 7 дней с момента заражения возможность расшифровки файлов теряется навсегда

Основные киберцели

- ФОИВы
- Федеральные и региональные Госуслуги
- Системообразующие компании
- Объекты критической информационной инфраструктуры

Три плоскости атак

1. Информационные атаки, направленные на дестабилизация ситуации
 2. Массовые атаки на web, направленные на вывод из строя госсервисов
 3. Целевые атаки на объекты жизнеобеспечения
-

Возможные негативные события

Потеря аккаунтов и доступов

- Похищение доступов к служебным системам
- Похищение аккаунтов к соцсетям и почтам
- Похищение биржевых и банковских аккаунтов

Потеря денег

- Похищение денег со счетов и карт
- Похищение криптовалютных кошельков
- Похищение балмов, кристаллов, танков, игрового прогресса

Шантаж и вымогательство

- Похищение персональных данных и архивов (переписки, фотографий)
 - Вы – объект вымогательства
 - Вы – объект информационной атаки
-

Взлом корпоративного ИТ через руководителей

Последствия

- Утечки служебной информации
 - Доступ в информационные системы с уровнем «топ-менеджер»
 - Подписание корпоративными ЭЦП
 - Бескрайние возможности социальной инженерии
-

Как узнать, что я заражен?

1. Сообщения антивирусов
 2. Правила переадресация почты, которые вы не ставили
 3. Запросы подтверждения входов со странных адресов или устройств
 4. «Промаргивания» окон особенно в корпоративных системах
 5. Сообщения всему вашему контакт-листу от вашего имени
-

ПЯТЬ ШАГОВ К БЕЗОПАСНОСТИ

ШАГ 1

Пароли, пароли и еще раз пароли

Четыре простых правила:

1. Каждому аккаунту - свой пароль
2. Сложный пароль
3. Пароль часто меняемый
4. Изменяемый с надежного устройства

!!! А еще нужно везде включить двухфакторную аутентификацию

12345

Jxtyrn skj;ysq gfhjkm!!!

ПЯТЬ ШАГОВ К БЕЗОПАСНОСТИ

ШАГ 2

Обновления

НЕ ОБНОВЛЯТЬ

ПЯТЬ ШАГОВ К БЕЗОПАСНОСТИ

ШАГ 3

Чистое устройство

Чистое устройство

Задачи:

- Корпоративные/служебные экаунты
- Мобильные банки
- Официальные экаунты социальных сетей
- «Чистый» почтовый ящик
- Мессенджеры

Задачи:

- Серфинг по интернету
- Игры
- Интернет-магазины

«Грязное» устройство

- Почтовый ящик для рассылок
- Фильмы/Музыка
- Торренты Дети

ПЯТЬ ШАГОВ К БЕЗОПАСНОСТИ

ШАГ 4

переписка



Удалите почтовые архивы в личных ящиках, которые лежали «на всякий случай»

Включите второй фактор аутентификации

ПЯТЬ ШАГОВ К БЕЗОПАСНОСТИ

ШАГ 5

1. Не ходите на сомнительные сайты
2. Не открывайте любопытные письма и не нажимайте в них на ссылки
3. Не устанавливайте непонятные программы, тем более не через appstore, google play или официальные сайты
4. Забудьте про публичные wi-fi и автоподключения
5. Чужие флэшки и флэшки с конференций - угроза!

И не забудьте, что принцип «один раз не считается» в кибербезопасности не работает!!! ©

Рекомендации

1. Максимально закрыть выход в Интернет
 2. Полностью закрыть доступ в ЛВС через Интернет
 3. Тотальная проверка писем до их открытия
 4. Установка паролей (сложных, часто)
 5. Обязательная проверка USB и иных накопителей
-