Противодействие мошенничеству и киберпреступности

Киберпреступность - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Большинство киберпреступлений совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями.

Типы киберпреступлений

- Мошенничество с электронной почтой и интернет-мошенничество
- Мошенничество с использованием личных данных
- Кража финансовых данных или данных банковских карт
- Кража и продажа корпоративных данных
- Кибершантаж
- Атаки программ-вымогателей
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)

Вирусы-Шифровальщики

Программы-шифровальщики относятся к классу троянцев-вымогателей — это вредоносное ПО, которое вносит несанкционированные изменения в пользовательские данные или блокирует нормальную работу компьютера. Для расшифровки данных и разблокировки компьютера злоумышленники обычно требуют денежного перевода (выкупа).
Как защититься от шифровальщиков?

- Регулярно делать резервные копии данных, чтобы их можно было восстановить в случае инцидента.

- Использовать инструменты для автоматического обнаружения уязвимостей и установки исправлений.

- Своевременно обновлять приложения и операционные системы на всех устройствах.

- Не открывать подозрительные файлы или ссылки в электронных письмах.

- Установить на компьютер антивирус

- Скачивать программы только с сайта разработчика или с проверенных ресурсов.

Вирус-шифровальщик Netwalker

Netwalker — это быстро набирающая масштабы программа-вымогатель, созданная в 2019 году группой киберпреступников, известной как Circus Spider. На первый взгляд Netwalker действует, как и большинство других разновидностей программ-вымогателей: проникает в систему через фишинговые письма, извлекает и шифрует конфиденциальные данные, а затем удерживает их для получения выкупа.

Но Netwalker способен на большее, чем просто удержание захваченных данных. Чтобы продемонстрировать серьезность своих намерений, Circus Spider публикует образец украденных данных в интернете, заявляя, что, если жертва не выполнит их требования вовремя, то в даркнет попадут и остальные данные. Circus Spider выкладывает конфиденциальные данные жертвы в даркнете в защищенной паролем папке и публикует пароль в интернете.

Сферы, атакуемые Netwalker:

- образование
- здравоохранение
- производство;
- управление бизнесом;
- управление потребительским опытом и качеством обслуживания;
- электромобили и решения для накопления электричества;
- образование;

Как работает Netwalker?

- 1: Проникает в систему
- 2: Шифрует данные
- 3: Вымогательство, шантаж, использование данных в личных интересах злоумышленников

Советы по защите от программы-вымогателя Netwalker:

- Выполнять резервное копирование важных данных на локальные хранилища данных;
- Убедиться, что копии критически важных данных хранятся в облаке, на внешнем жестком диске или устройстве хранения;
- Защитить свои резервные копии и убедиться, что данные невозможно изменить или удалить из системы, в которой они хранятся;
- Установить и регулярно обновлять антивирусное программное обеспечение на всех компьютерах;
- Использовать только безопасные сети и избегайте общедоступных сетей Wi-Fi. По возможности используйте VPN;
- Использовать двухфакторную аутентификацию с надежными паролями;
- Регулярно обновлять компьютеры, устройства и приложения.