Информационная безопасность как основа доверия расчетов

Сычев Артем Михайлович

Советник генерального директора по взаимодействию с госсектором
АО «Позитив Текнолоджиз»

Что было?
Взгляд на 2022 год со стороны PT

В 2022 году сотрудники экспертного центра безопасности Positive Technologies провели более **50 расследований.**

Пик по количеству инцидентов пришелся на **апрель 2022 года.**

Причины инцидентов:

1. рост числа уязвимостей и отсутствие регулярных процедур по патч-менеджменту
2. нехватка кадров более чем у 90% компаний
3. уход иностранных вендоров ИБ

По итогам проведенных нами исследований,

отраслевые интересы группировок, атаковавших российские организации в течение 2022 года

30%

государственные предприятия

16%

IT-компании

10%

Энергетический, промышленный и финансовый сектор

Изменился портрет кибергруппировок, нацеленных на Российскую Федерацию

Злоумышленники использовали вредоносное ПО почти в каждой второй атаке на госучреждения

Наиболее популярными типами вредоносов оказались:

56% Шифровальщики (среди атак с применением ВПО)

29% Вредоносные программы для удаленного управления

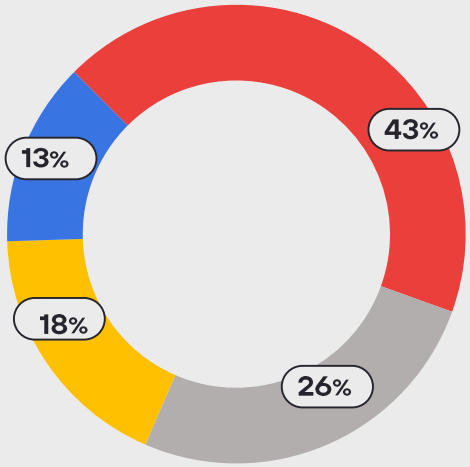
Основным вектором атак осталась **социальная инженерия**, с помощью которой злоумышленники заражали компьютеры сотрудников вредоносным ПО, похищали учетные данные

41% атак был направлен на веб-ресурсы государственных учреждений

5% атак госучреждения становились жертвой компрометации цепочки поставок ПО

Социальная инженерия – инструмент злоумышленника

Для организации таких атак злоумышленники создавали



- фишинговые сайты
- отправляли вредоносные письма по электронной почте
- искали жертв в социальных сетях
- искали жертв в мессенджерах

64% атак злоумышленникам удавалось украсть данные

41% среди украденной информации были учетные данные: **27% персональные и 14% платежные.**

Злоумышленники агрегируют данные, полученные в результат утечки, для составления полного и разнопланового портрета конкретного пользователя для подготовки адресных атак.

С начала года произошли утечки **более 230 млн записей** с личной информацией граждан*

*Данные РКН

Прогнозы на 2023 год?

Особое внимание!

Проводится активный поиск уязвимостей нулевого дня в отечественных операционных системах и офисного программного обеспечения (Astra Linux, ALT Linux, РЕД ОС)

НО:

- Злоумышленники совершенствуют методы обхода многофакторной аутентификации

- Осуществляется переход от хактивизма к целенаправленным атакам для модификации данных в государственных системах и перебоям в предоставлении услуг. Предприятия энергетической отрасли – основная цель для хактивистов

Извечный русский вопрос: что делать?

pt@ptsecurity.com

ptsecurity.com

Спасибо!